


BİLGİ VE VERİ GÜVENLİĞİ İLE GÜÇLENDİRİLEN SİVİL TOPLUM ÇALIŞMALARI

SİVİL TOPLUMDA DİJİTAL GÜVENLİĞİ GÜÇLENDİRMEYE YÖNELİK PRATİK DİJİTAL DÖNÜŞÜM KILAVUZU VE MÜFREDAT

SİVİL TOPLUMDA DİJİTAL GÜVENLİĞİ GÜÇLENDİRMEYE YÖNELİK PRATİK DİJİTAL DÖNÜŞÜM KILAVUZU VE MÜFREDAT

Ankara, 2026

Bu çalışma, Erasmus+ Programı kapsamında Türkiye Ulusal Ajansı ve Avrupa Komisyonu tarafından desteklenen “BİLGİ VE VERİ GÜVENLİĞİ İLE GÜÇLENDİRİLEN SİVİL TOPLUM ÇALIŞMALARI” (2023-1-TR01-KA220-YOU-000161230) adlı proje kapsamında gerçekleştirilmiştir.

Bu proje Erasmus+ kapsamında Avrupa Komisyonu tarafından desteklenmektedir. Burada yer alan içerik yazarın görüşlerini yansıtmaktadır ve bu görüşlerden Avrupa Komisyonu ve Türkiye Ulusal Ajansı sorumlu tutulamaz.


2026

Akademik Danışman: Erman Akıllı

Kapak Tasarımı ve Düzeni:

Editörler: Sibel Koru

Zeyneb Güşta Arık

Metin Düzeltmeleri: Cenay Babaoğlu

Tarih: Ankara, 2026

Günümüzün hiperbağlantılı dünyasında, sivil toplum kuruluşları (STK'lar), sivil toplum örgütleri ve savunuculuk gruplarından bağımsız medya kuruluşları ve topluluk ağlarına kadar, giderek daha karmaşık bir dijital cephede faaliyet göstermektedir. Dijital araçlar sivil toplumun erişimini, verimliliğini ve etkisini artırırken, aynı zamanda kuruluşları artan siber güvenlik risklerine maruz bırakmaktadır. Sivil toplum dijital olarak daha bağımlı hale geldikçe, dijital olarak da daha savunmasız hale gelmektedir.

Avrupa ve ötesinde, STK'lar dijital ekosistemde yüksek riskli aktörler olarak giderek daha fazla tanınmaktadır. Sivil toplumu hedef alan siber tehditler, artık kimlik avı, fidye yazılımı, casus yazılım ve hizmet reddi saldırılarından, muhalefeti susturmak ve demokratik değerleri zayıflatmak amacıyla devlet destekli sofistike gözetleme faaliyetlerine kadar uzanmaktadır. Genellikle sınırlı teknik kapasiteyle faaliyet gösteren ancak hassas kişisel ve kurumsal verileri yöneten kuruluşlar için dijital güvensizlik, sadece operasyonel riskler değil, aynı zamanda varoluşsal riskler de oluşturmaktadır.

Bu bağlamda, dijital güvenlik artık sadece teknik bir sorun değildir. Bu, misyon açısından kritik bir konudur. Sivil toplum kuruluşlarının çevrimiçi ortamda güvenli bir şekilde faaliyet gösterme yeteneği, ifade özgürlüğünü, şeffaflığı, hesap verebilirliği ve hizmet ettikleri toplulukları koruma yeteneklerinden ayrı düşünülemez. Bu nedenle, sivil toplumda dijital güvenliği güçlendirmek, geçici teknik çözümlerden daha fazlasını gerektirir. Gerçek örgütsel ortamlarda uygulanabilecek yapılandırılmış öğrenme, stratejik planlama ve pratik rehberlik gerektirir.

Bu ihtiyaca yanıt olarak, "Bilgi ve Veri Güvenliği ile Güçlendirilmiş Sivil Toplum Çalışmaları" KA220 Erasmus+ projesi, sivil toplum kuruluşlarının dijital güvenlik kapasitesini artırmak için çok ülkeli bir işbirliği çabası olarak başlatılmıştır. Bu projenin temel sonuçlarından biri, iki tamamlayıcı işlevi kasıtlı olarak tek bir ciltte bir araya getiren bu yayındır.

Bu kitap hem bir müfredat hem de pratik bir rehber olarak tasarlanmıştır.
Bir yandan, sivil toplum için yapılandırılmış bir dijital güvenlik müfredatı işlevi görerek, dijital tehdit ortamını anlamaktan kurumsal politikalar ve olay müdahale mekanizmaları geliştirmeye kadar, bilgileri aşamalı olarak geliştiren tutarlı bir öğrenme yolu sunar. Müfredat odaklı yapısı, farklı ulusal bağlamlarda eğitim, atölye çalışmaları, kapasite geliştirme programları ve eğiticilerin eğitimi faaliyetlerinde kullanıma uygundur.

Diğer yandan, kitap, kuruluşların günlük faaliyetlerinde doğrudan uygulayabilecekleri somut ve eyleme geçirilebilir rehberlik sağlayan pratik bir rehber görevi görmektedir. Teorik düzeyde kalmak yerine, siber güvenlik ilkelerini, sınırlı kaynaklarla çalışan STK'ların ve taban girişimlerinin

gerçeklerine uyarlanmış pratik adımlara, kontrol listelerine, örneklere ve karar verme çerçevelerine dönüştürmektedir.

Bu iki boyutu birleştirerek, kitap öğrenme ve uygulama arasındaki kritik boşluğu doldurmaktadır. Okuyucuların sadece dijital güvenliğin *neden* önemli olduğunu anlamalarını değil, aynı zamanda kendi kuruluşlarında bunu *nasıl* işlevselleştireceklerini de anlamalarını sağlar. Okuyucular kitaba sırayla bir müfredat olarak veya iletişim güvenliği, veri koruma, risk değerlendirme veya dijital güvenlik iç kültürü oluşturma gibi belirli zorlukları ele alan bir referans kılavuzu olarak seçici bir şekilde yaklaşabilirler.

Erişilebilir ancak akademik temelli bir üslupla yazılan bu yayın, proje tabanlı deneyimlerden, saha gözlemlerinden ve siber güvenlik ve sivil toplum kapasite geliştirme alanlarında yerleşik en iyi uygulamalardan yararlanmaktadır. Modüler yapısı, farklı kurumsal ihtiyaçlara, teknik seviyelere ve ulusal düzenleyici ortamlara uyarlanabilmesini sağlamaktadır.

Nihai olarak, bu birleşik müfredat ve kılavuz, sivil toplum kuruluşlarının dijital güvenliklerini sahiplenmelerini sağlamayı amaçlamaktadır. Hem bilgi hem de pratik yetenekleri geliştirerek, STK'ların dayanıklılıklarını güçlendirmelerine, dijital altyapılarını korumalarına ve giderek daha rekabetçi hale gelen dijital alanda daha fazla güven ve sürdürülebilirlikle temel çalışmalarını sürdürmelerine destek olmaktadır.

SETA, Ankara/Türkiye

İÇİNDEKİLER:

1.1 PROJE HEDEFİ:

"***BİLGİ VE VERİ GÜVENLİĞİ İLE GÜÇLENDİRİLEN SİVİL TOPLUM ÇALIŞMALARI***", SETA (Türkiye) tarafından koordine edilen ve Kuzey Makedonya, Norveç, Bosna Hersek, Belçika ve Türkiye'den ortak kuruluşlarla işbirliği içinde yürütülen bir KA220 Erasmus+ projesidir. Proje, Avrupa Komisyonu tarafından Türkiye Ulusal Ajansı aracılığıyla finanse edilmiş ve giderek dijitalleşen bir ortamda sivil toplum kuruluşlarının karşılaştığı artan zorlukları ele almak üzere tasarlanmıştır.

Projenin temel amacı, sivil toplumda dijital okuryazarlığı, siber güvenlik farkındalığını ve veri koruma kapasitelerini artırırken, aynı zamanda kapsayıcılığı, çeşitliliği ve dijital becerilere eşit erişimi teşvik etmekti. Uygulama süresince proje, hem bireylerin hem de kurumların dijital dönüşüm süreçlerinde yol almalarını ve siber tehditlere, yanlış bilgilere ve dezenformasyona karşı dirençlerini güçlendirmelerini destekledi.

Bu çerçeve içinde proje, bir dizi önemli entelektüel ve pratik çıktı üretti. Bunlar arasında, dijital dönüşüm süreçlerinin erişilebilir ve kapsayıcı olmasını sağlayan, **sivil toplum için** kapsamlı bir **Dijital Güvenlik Müfredatı**, dijital okuryazarlık ve siber güvenlik eğitim modülleri yer aldı. Ayrıca, sivil toplum kuruluşlarının etkili dijital dönüşüm stratejileri planlamasına, uygulamasına ve sürdürmesine yardımcı olmak için **Pratik Dijital Dönüşüm Kılavuzu** geliştirildi.

Proje ayrıca, sivil toplum kuruluşlarının siber güvenlik hazırlık durumunu değerlendirmek **için** yazılım tabanlı bir **Çevrimiçi Dijital Güvenlik Test Merkezi** geliştirdi. Bu platform, sivil toplum kuruluşlarının veri koruma uygulamaları, sistem güvenlik yapılandırmaları ve çevrimiçi araçların güvenli kullanımı (ör. alan yapıları, HTTPS kullanımı ve temel dijital altyapı güvenlik önlemleri) gibi unsurları da içeren dijital güvenlik düzeylerini değerlendirmelerine olanak tanıyor. Bu araç sayesinde kuruluşlar, güvenlik açıklarını tespit edebilmekte, mevcut riskler konusunda farkındalık yaratabilmekte ve dijital güvenlik alanında kanıta dayalı kapasite geliştirme ve iyileştirme süreçlerini destekleyebilmektedir.

Eğitim çıktılarının ötesinde, proje aynı zamanda güvenli ve sorumlu dijital uygulamalara odaklanan farkındalık artırıcı materyaller ve kampanyalar da üretti. Ayrıca, ortak ülkeler arasında sağlam bir uluslararası işbirliği ağı kurmayı başardı ve sivil toplum için dijital güvenlik alanında uzun vadeli kapasite geliştirme, bilgi alışverişi ve sürdürülebilir işbirliğinin temellerini attı.

1.2 PROJE ORTAKLARI:

SİYASİ, EKONOMİK VE SOSYAL ARAŞTIRMALAR VAKFI, SETA (KOORDİNATÖR)

Siyasi, Ekonomik ve Sosyal Araştırma Vakfı (SETA), ulusal, bölgesel ve uluslararası konularda doğru ve güncel analizler üretmeye odaklanan, kâr amacı gütmeyen bir düşünce kuruluşudur. Tarihsel ve kültürel bağlamda siyasi, ekonomik, sosyal ve kültürel gelişmeler hakkında politika yapıcıları ve kamuoyunu bilgilendirmeyi amaçlamaktadır. Bir araştırma ve politika önerileri kurumu olarak SETA, akademik standartlar aracılığıyla farklı bakış açılarını bir araya getirerek uluslararası diyaloğu teşvik etmektedir. Araştırma raporları, yayınlar, konferanslar ve politika önerileri yoluyla hükümet, sivil toplum ve iş dünyası liderlerinin bilinçli karar almalarına katkıda bulunur. SETA, siyasi, ekonomik ve sosyo-kültürel konuların birbirine bağlı olduğunu kabul ederek disiplinler arası bir yaklaşım benimser ve barış, adalet, eşitlik ve hukukun üstünlüğüne dayalı bir vizyonu teşvik etmeye çalışır. Misyonu, stratejik tartışmaları zenginleştirmek ve hem kamu hem de özel sektördeki karar alıcılara bağımsız ve güvenilir içgörüler sağlamaktır.

SİYASİ, EKONOMİK VE SOSYAL ARAŞTIRMALAR VAKFI, SETA BRÜKSEL

SETA Siyasi, Ekonomik ve Sosyal Araştırmalar Vakfı, Brüksel merkezli, ulusal, bölgesel ve uluslararası konularla ilgili yenilikçi çalışmalara odaklanan, kâr amacı gütmeyen bir araştırma enstitüsüdür. Amacı, siyaset, ekonomi ve toplum alanlarında doğru bilgi ve analizler üretirken, politika yapıcıları ve kamuoyunu gelişen siyasi, ekonomik, sosyal ve kültürel koşullar hakkında bilgilendirmektir. Araştırma raporları, yayınlar, konferanslar ve politika önerileri yoluyla farklı bakış açılarını bir araya getirerek uluslararası diyaloğu teşvik eder. Vakıf, kamu ve özel sektör liderlerine güvenilir bilgi ve analizler sunarak Türkiye'de bilinçli karar alımını desteklemeyi amaçlamaktadır. SETA'nın disiplinlerarası araştırma yaklaşımı, siyasi, ekonomik ve sosyo-kültürel konuların karşılıklı bağımlılığını ele alarak barış, adalet, eşitlik ve hukukun üstünlüğüne dayalı bir vizyon oluşturmaya çalışmaktadır.

ANKA GELECEK VE İNOVASYON DERNEĞİ

ANKA Gelecek ve Yenilik Derneği (ANKA GLOBAL), Mayıs 2019’da İstanbul’da kurulan, kar amacı gütmeyen ve hükümet dışı bir sivil toplum kuruluşudur.

Dernek, gençlik gelişimi ve sivil toplum alanında faaliyet göstermekte olup özellikle dijital dönüşüm, çevresel sürdürülebilirlik, inovasyon, sosyal kapsayıcılık ve aktif vatandaşlık konularına odaklanmaktadır.

Kuruluşundan itibaren toplum temelli gençlik çalışmaları ve formel olmayan öğrenme yöntemleriyle güçlü bir temel oluşturan ANKA, gençlerin, gençlik çalışanlarının ve toplum temelli örgütlerin kapasitelerini uygulamalı pratik, sektörler arası işbirliği ve uluslararası projeler aracılığıyla güçlendirmektedir.

Zaman içinde Avrupa Gençlik Stratejisi, AB Gençlik Hedefleri, Erasmus+ öncelikleri ve Birleşmiş Milletler Sürdürülebilir Kalkınma Hedefleri doğrultusunda çalışma alanlarını genişleten dernek, bugün gençleri hızla değişen dünyada dijital yetkin, çevre bilinci yüksek, yenilikçi ve kapsayıcı liderler olarak yetiştirmeyi temel misyonu olarak benimsemiştir.

BOSNİAN REPRESENTATİVE ASSOCİATİON FOR VALUABLE OPPORTUNİTİES (BRAVO)

Bosnian Representative Association for Valuable Opportunities (BRAVO), Bosna Hersek merkezli, eğitim, beceri geliştirme ve kapasite geliştirme yoluyla bireyleri ve toplulukları güçlendirmeye odaklanan dinamik bir STK'dır. Misyonu, sosyal içerme, kültürel değişim ve sürdürülebilir kalkınmayı vurgulamaktadır. BRAVO, gençlerin güçlendirilmesi, çevre bilinci, girişimcilik ve teknoloji gibi çeşitli sektörlerde faaliyet göstermektedir. Çok sayıda projede işbirliği yapan, ücretli personel ve gönüllülerden oluşan özel bir ekibi vardır. BRAVO, kültürlerarası anlayışı ve kişisel gelişimi teşvik etmek için gençlik değişim programları düzenlerken, aynı zamanda yenilikçi projelerle çevresel sürdürülebilirliği desteklemektedir. Sosyal etkiye odaklanarak, girişimci adaylarına mentorluk ve kaynaklar sunarak yardımcı olmaktadır. Ayrıca BRAVO, programlama ve web geliştirme gibi dijital beceri atölyeleri sunarak, bireylerin teknoloji alanındaki kişisel ve mesleki gelişimlerini desteklemektedir.

TTB

TtB Norveç merkezli bir sivil toplum kuruluşudur ve sürdürülebilir bir gelecek teşvik etmek için teknoloji ve dijital beceriler konusunda eğitim ve öğretim sağlamaya kendini adamıştır. 6 Ekim 2019'da Trondheim'daki öğrenciler tarafından kurulan TTB, bilgi ve yararlı

beceriler kazanma fırsatları sunarak gençlerin topluma katılımını artırmayı amaçlamaktadır. 15 kişilik ücretli personel ve çok sayıda gönüllüden oluşan bir ekiple TTB, eğitim, çevre ve girişimcilik alanlarında projeler yürütmektedir. Kuruluş, dijital inovasyon, gençlik çalışmaları ve dijital araçların entegrasyonuna odaklanmaktadır. Başlıca faaliyetleri arasında dijital beceri eğitimi, çevre girişimleri ve özellikle teknoloji ve sürdürülebilirlik alanlarında girişimcileri desteklemek yer almaktadır. TTB, açıklık, işbirliği, cesaret ve özeni değerler olarak benimsemekte ve sürdürülebilir, etik ve sosyal sorumluluk sahibi bir ortam yaratmaktadır. Hem bölgesel hem de uluslararası işbirliği faaliyetlerinde bulunmaktadır.

TÜRKİYE GENÇLİK VAKFI (TÜGVA)

2014 yılında kurulan Türkiye Gençlik Vakfı (TÜGVA), 100'den fazla profesyonel ve 300.000 gönüllüden oluşan ekibiyle Türkiye'nin en büyük STK'larından biridir. 39 şehirde robotik kodlama atölyeleri düzenlemekte ve 42 yurt işletmektedir. Vakıf, spor, kadın hakları, girişimcilik, medya, eğitim, kültür ve kariyer gelişimi gibi çeşitli alanlarda 10 koordinatörle faaliyet göstermektedir. Temel misyonu, özellikle Türkiye'de gençlerin fiziksel ve zihinsel sağlığına odaklanarak kapsamlı gelişimini desteklemektir. Vakıf, gençlerin yenilikçi, üretken ve değerli toplum üyeleri olmalarını sağlamayı amaçlamaktadır. 200'den fazla ulusal ve uluslararası projeyi tamamlamış olan vakfın vizyonu, sürekli kendini geliştirme ve kültürel zenginleşme yoluyla medeniyeti yeniden inşa edebilecek ve ilerletebilecek nesiller yetiştirmektir.

ZDRUZENIE NA GRAGJANI MAKEDONSKA ASOCIJACIJA ZA COVECKI RESURSI SKOPJE (MHRA)

Makedonya İnsan Kaynakları Derneği (MHRA), işgücü becerilerinin geliştirilmesi, insan sermayesinin teşvik edilmesi ve informal eğitimin standartlaştırılmasına odaklanan, kar amacı gütmeyen, sivil toplum kuruluşudur. MHRA'nın üyeleri arasında, çoğunluğu kadınlardan oluşan 120'den fazla aktif üye, insan kaynakları alanından 600'den fazla pasif üye ve kamu ve özel sektörden 60'tan fazla şirket bulunmaktadır. Dernek, insan kaynakları yöneticileri, danışmanlar, çalışanlar ve öğrenciler dahil olmak üzere tüm kariyer aşamalarındaki bireyleri bir araya getiren açık bir platform olarak faaliyet göstermektedir. Dernek, hem ulusal hem de yerel düzeyde iş, eğitim ve sosyo-ekonomik konularla ilgili politikaların şekillendirilmesinde rol oynamaktadır.

2012 yılından bu yana Avrupa İnsan Yönetimi Derneği'nin (EAPM) resmi bir üyesi olan MHRA, yerel ve uluslararası girişimlerinde gönüllülüğü de temel bir değer olarak benimsemektedir.

2. PRATİK DİJİTAL DÖNÜŞÜM KILAVUZU

2.1 BÖLÜM 1: STK İÇİN DİJİTAL GÜVENLİK

Dijital Güvenlik Nedir?

Siber güvenlik olarak da bilinen dijital güvenlik, dijital bilgileri, cihazları ve diğer varlıkları yetkisiz erişimden veya zarardan korumak için uygulanan yöntemlerdir. Kişisel verileri, hesapları, dosyaları ve hatta çevrimiçi olarak depolanan veya iletilen finansal kaynakları korumak için alınan önlemleri kapsar. Temel olarak, dijital güvenlik bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamayı amaçlar (genellikle "CIA üçlüsü" olarak özetlenir – Gizlilik, Bütünlük, Kullanılabilirlik).

Dijital Güvenlik Neden Önemlidir?

Günümüzün hiperbağlantılı dünyasında, neredeyse her kuruluş ve birey dijital sistemlere güvenmektedir. CSO'lar ve STK'lar için bu güven, paydaşlarla iletişim kurmak, bağışçı bilgilerini yönetmek ve hizmet sunmak gibi faaliyetleri içerir. Bu dijital faaliyetleri korumak çok önemlidir. Siber saldırılar, operasyonları aksatabilir, hassas verileri ihlal edebilir ve bağışçıların ve toplulukların bir kuruluşa duyduğu güveni zedeleyebilir. Örneğin, 2016 yılında Avustralya Kızılhaçı'nda meydana gelen bir veri ihlali, insan hatası (güvenli olmayan bir yedekleme dosyası) nedeniyle 550.000'den fazla kan bağışçısının kişisel bilgilerini ifşa etti. Bu olay, kuruluşun veri uygulamaları hakkında soruların ortaya çıkmasına neden olmakla kalmadı, aynı zamanda bağışçıların güvenini de kaybetti, siber olayların gerçek insanlara nasıl zarar verebileceğini ve CSO'ların misyonuna olan kamu güvenini nasıl zedeleyebileceğini gösterdi.

Önemli bir nokta, kar amacı gütmeyen kuruluşların siber suçlular ve hatta devlet destekli hackerlar tarafından giderek daha fazla hedef alınmasıdır. Bir Microsoft raporu, insani yardım ve insan hakları CSO'larının, ulus devlet siber saldırılarının en çok hedef aldığı ikinci sektör olduğunu ve 2025 yılında bu tür saldırı bildirimlerinin %31'ini oluşturduğunu ortaya koydu. Cenevre merkezli kar amacı gütmeyen kuruluşlar üzerinde 2023 yılında yapılan bir araştırma, %41'inin son yıllarda siber saldırıya uğradığını ortaya koydu. Ancak bu STK'ların yarısından fazlasının siber güvenlik için ayrılmış bir bütçesi yoktu ve %70'i saldırılara yanıt verecek beceri ve dayanıklılıktan yoksun olduklarını düşünüyordu. Bu rakamlar, dijital güvenliğin artık STK'lar için isteğe bağlı değil, zorunlu olduğunu vurgulamaktadır. Yeterli güvenlik önlemleri alınmazsa, siber olaylar kritik hizmetleri durdurabilir, yararlanıcıların verilerini tehlikeye atabilir ve kuruluşun itibarını zedeleyerek finansmanı tehlikeye atabilir.

Dahası, dijital güvenlik, sivil toplum çalışmalarında fiziksel güvenlik ve insan haklarıyla yakından bağlantılıdır. Aktivistler, gazeteciler ve STK'lar genellikle gözetim veya sindirme amaçlı dijital tehditlerle karşı karşıya kalmaktadır. Bir ihlal veya hackleme, hassas iletişimleri vey 'nin ortaklarının ve yararlanıcılarının kimliklerini açığa çıkararak hayatları veya geçim kaynaklarını tehlikeye atabilir. Bu nedenle, dijital güvenliğe yatırım yapmak, bir kuruluşun çalışmalarının genel dayanıklılığına ve güvenilirliğine yatırım yapmak anlamına gelir.

Dijital Güvenlik Sivil Toplum Kuruluşları İçin Ne Anlama Gelir?

Sivil toplum kuruluşları için *dijital güvenlik*, sosyal misyonlarını yerine getirmelerini sağlayan bilgi ve teknolojinin korunması anlamına gelir. Sivil toplum kuruluşları, destekçilerin ve personelin kişisel bilgileri, stratejik planlar ve araştırmalar gibi hassas verileri rutin olarak toplar ve saklar. Bu verilerin gizliliğini ve bütünlüğünü sağlamak, yanlış ellere geçmemesi veya tahrif edilmemesi için çok önemlidir. Örneğin, bir savunuculuk grubu, aktivistlerin iletişim listelerini veya insan hakları ihlallerine dair kanıtları güvence altına almak zorunda kalabilir. Bu tür bilgiler kötü niyetli kişiler tarafından sızdırılırsa veya değiştirilirse, bireyleri tehlikeye atabilir veya davayı zayıflatabilir.

STK'lar için dijital güvenlik, günlük operasyonların korunmasını da içerir. Birçok kuruluş, faaliyetlerini koordine etmek için e-posta, mesajlaşma uygulamaları ve bulut platformlarına güvenmektedir. Bu hesaplar ele geçirilirse, saldırganlar iletişimi kesintiye uğratabilir veya STK'nın kimliğine bürünebilir. Gerçek bir vakada, bir hayır kurumunun e-posta sistemi, kötü amaçlı yazılım eki içeren bir oltalama e-postası yoluyla hacklendi ve bu da kuruluşun sunucusunu şifreleyen bir fidye yazılımı saldırısına yol açtı. Saldırganlar, şifre çözme anahtarı karşılığında fidye talep etti. Sivil toplum örgütü, yakın zamanda veri yedeklemesi yapmış olduğu ve ödeme yapmamayı tercih ettiği için verilerinin çoğunu geri yükleyebildi, ancak yaklaşık iki haftalık bilgiler kalıcı olarak kayboldu. Bu olay, hem tehdidi hem de hazırlıklı olmanın önemini göstermektedir: güçlü yedeklemeler ve bir müdahale planı olmasaydı, sonuç çok daha kötü olabilirdi.

Hassas siyasi ortamlarda faaliyet gösteren sivil toplum grupları için dijital güvenlik, üyelerinin ve hizmet ettikleri toplulukların güvenliğini korumak açısından ek bir anlam kazanır. Baskıcı kuruluşlar, CSO'ları gözetlemek veya dezenformasyonla hedef almak için siber araçlar

kullanabilir. Bu nedenle, CSO'lar için dijital güvenlik genellikle gizliliği artıran araçları (e-postalar ve mesajlar için şifreleme gibi) ve gözetlemeyi önlemek için güvenli iletişim kanallarını vurgular. Avrupalı bir sivil özgürlükler örgütü olan Liberties'in belirttiği gibi: Aktivizm için dijital araçlar kullanan STK'lar benzersiz tehditlerle karşı karşıyadır ve insanları, süreçleri ve teknolojiyi kapsayan bir "dijital öz savunma" kültürü geliştirmelidir. Pratik olarak bu, personeli ve gönüllüleri güvenlik bilinci konusunda eğitmek, açık politikalar oluşturmak (örneğin, kişisel verilerin işlenmesi veya güvenli uygulamaların kullanılması konusunda) ve teknik korumaları sürekli güncellemek anlamına gelir.

Son olarak, *STK'lar için dijital güvenlik*, güveni sürdürmekle ilgilidir. Bağışçılar ve yararlanıcılar, kuruluşların bilgileri iyi bir şekilde yönetmesini bekler. Kamuoyuna duyurulan bir siber olay, halkın güvenini sarsabilir ve insanların katılımını veya katkısını engelleyebilir. Örneğin, daha önce bahsedilen Kızıl Haç veri sızıntısından sonra, kuruluş kan bağışlarında bir düşüş gözlemledi ve güveni yeniden inşa etmek için çalışmak zorunda kaldı. Dijital güvenliğe öncelik vererek, STK'lar sivil toplum sektörünün temel değerleri olan hesap verebilirlik ve gizlilik konusundaki taahhütlerini gösterirler.

Sivil Toplum Örgütlerine Yönelik Yaygın Dijital Tehditler ve Riskler

Sivil toplum kuruluşları, işletmeler ve bireylerle aynı siber risklerin çoğuyla karşı karşıyadır, ancak genellikle bu riskleri ele almak için daha az kaynağa sahiptir. Yaygın tehditlerden bazıları şunlardır:

- **Hackerlar ve Kötü Amaçlı Yazılımlar:** Saldırganlar, verileri çalmak veya hizmetleri kesintiye uğratmak için bir STK'nın ağına veya cihazlarına sızmaya çalışabilir. Bu, e-posta ekleri, zararlı bağlantılar veya virüslü USB sürücüler aracılığıyla gönderilen kötü amaçlı yazılımlar (virüsler, casus yazılımlar veya fidye yazılımları gibi) yoluyla gerçekleşebilir. Fidye yazılımı, dosyaları şifreleyen ve ödeme talep eden, özellikle zararlı bir kötü amaçlı yazılımdır. Küçük kar amacı gütmeyen kuruluşlardan tüm şehir yönetimlerine kadar her büyüklükteki kuruluşu etkilemiştir. Bir CSO'nun güçlü kötü amaçlı yazılım savunması ve veri yedeklemesi yoksa, fidye yazılımı saldırısı operasyonlarını etkili bir şekilde felce uğratabilir.
- **Kimlik Avı ve Sosyal Mühendislik:** Kimlik avı, saldırganların alıcıları şifrelerini açıklamaya veya kötü amaçlı yazılım indirmeye ikna etmek için meşru görünen sahte e-postalar

veya mesajlar (örneğin, bir iş arkadaşı veya hizmet sağlayıcı gibi davranarak) gönderdikleri bir taktiktir. Kimlik avı, en yaygın tehditlerden biridir ve genellikle daha büyük saldırıların giriş noktasıdır. CSO'lar kimlik avı dolandırıcılıklarının hedefi olmuştur; örneğin, bir eğitim amaçlı kar amacı gütmeyen kuruluş, saldırganların bir ortağı yanlış banka hesabına ödeme yapması için e-postaları taklit etmesiyle neredeyse fonlarını kaybetmiştir (bir tür "iş e-postası dolandırıcılığı"). Kimlik avının yaygın belirtileri arasında acil veya endişe verici dil kullanımı, hassas bilgi talepleri veya hafifçe yanlış yazılmış e-posta adresleri bulunur. Sosyal mühendislik, güvenilir kuruluşları taklit eden telefon görüşmeleri (vishing) veya kısa mesajlar (smishing) yoluyla da gerçekleşebilir.

- **Veri İhlalleri:** Veri ihlali, gizli bilgilere yetkisiz olarak erişildiğinde veya bu bilgiler yetkisiz olarak ifşa edildiğinde meydana gelir. Bu, hackleme, içeriden kötüye kullanım veya hatta kazara ifşa edilme sonucu ortaya çıkabilir. CSO'lar genellikle saldırganlar için cazip olan veya sızdırılabilecek kişisel verileri (ör. yararlanıcı bilgileri, bağışçıların mali kayıtları, sağlık veya hukuk davası bilgileri) elinde bulundurur. Daha önce de belirtildiği gibi, yanlış yapılandırılmış sunucular veya bulut depolama alanları, istemeden veri sızıntısına neden olabilir; Kızıl Haç olayı buna bir örnektir. Bir ihlalin CSO için etkisi ciddidir: verilerdeki kişilerin kimlik hırsızlığına yol açabilir, gizlilik yasalarını ihlal edebilir ve kuruluşun itibarını ve yasal konumunu zedeleyebilir. Ne yazık ki, birçok ihlal insan hatasından kaynaklanmaktadır. Aslında, bir sektör raporu, ihlallerin %74'ünün hatalar veya kimlik avına kurban olmak gibi "insan unsurunu" içerdiğini ortaya koymuştur. Bu, eğitim ve verilerin dikkatli bir şekilde işlenmesi ihtiyacını vurgulamaktadır.

- **Yetkisiz Hesap Erişimi:** Saldırganlar, CSO personelinin kullandığı e-posta, sosyal medya veya bağış toplama platformları gibi hesapları hedef alabilir. Şifreleri çalarak veya tahmin ederek (veya önceki ihlallerden sızan kimlik bilgilerini kullanarak) bu hesapları ele geçirebilirler. Tehlikeye girme belirtileri arasında, tanıdık olmayan konumlardan gelen oturum açma uyarıları, kullanıcının oluşturmadığı yeni e-postalar veya gönderiler ya da oturum açamama (saldırgan tarafından şifre değiştirilmesi) sayılabilir. Örneğin, bir CSO'nun resmi sosyal medya hesabı hacklenirse, bu hesap yanlış bilgi yaymak veya CSO'nun takipçilerini

dolandırmak için kullanılabilir. Güçlü, benzersiz şifreler ve iki faktörlü kimlik doğrulama (Bölüm 2'de ele alınmıştır) kullanmak, hesap ele geçirmelere karşı temel savunma yöntemleridir.

- **Web Sitesi Tahrifatı veya DDoS:** Halka açık web sitelerine sahip CSO'lar, tahrifat (saldırganların mesaj veya propaganda yaymak için sitenin içeriğini değiştirmesi) veya siteyi trafikle doldurarak çevrimdışı hale getiren Dağıtık Hizmet Engelleme (DDoS) saldırılarına maruz kalabilir. Bu saldırılar bazen CSO'ların sesini susturmaya çalışan hacktivistler veya muhalifler tarafından gerçekleştirilir. Bir CSO, saldırganların güvenlik açıklarını istismar etmesinin ardından web sitesinin üçüncü taraf bir siteye yönlendirildiğini keşfetti ve yakın zamanda yedekleme yapmadıkları için siteyi yeniden kurmak dokuz ay sürdü. Web sitesi yazılımının güncel ve yedeklenmiş olmasını sağlamak bu tür riskleri azaltabilir.
- **İçeriden Gelen Tehditler ve İnsan Hatası:** Tüm riskler anonim hackerlardan kaynaklanmaz. Bazen içeridekiler (çalışanlar veya gönüllüler) kazara veya kasıtlı olarak güvenlik olaylarına neden olabilir. Bu, hassas dosyalar içeren güvenli olmayan bir dizüstü bilgisayarın kaybolmasından, bir veritabanının yanlış yapılandırılmasından, memnuniyetsiz bir çalışanın ayrılmadan önce verileri indirmesine kadar değişebilir. CSO'lar, iç erişim kontrollerine ve en az ayrıcalık ilkesine (çalışanlara yalnızca rollerine gerekli olan bilgilere ve sistemlere erişim izni verme) dikkat etmelidir. Ayrıca, güvenlik konusunda bir organizasyon kültürü oluşturmak hataları azaltabilir. Örneğin, insanlar neden kişisel USB sürücüleri kullanmamaları gerektiğini veya veri işleme prosedürlerine uymaları gerektiğini anladıklarında, yanlışlıkla güvenlik açıkları yaratma olasılıkları azalır.

Özetle, CSO'lar, kimlik avı gibi günlük dolandırıcılıklardan sofistike aktörlerin daha hedefli saldırılarına kadar çok çeşitli dijital tehditlerle karşı karşıyadır. 2. bölümde, temel en iyi uygulamalarla bu risklere karşı nasıl korunmaya başlanabileceği ele alınacaktır. Ancak bu giriş aşamasında bile, önemli bir nokta açık olmalıdır: yaygın riskleri tanımak, bunları yönetmenin ilk adımıdır. Neyin yanlış gidebileceğini (çalınan bir şifre, virüs bulaşması veya sızan bir belge gibi) bilerek, kuruluşlar ve bireyler bu senaryoları önlemek ve bunlara yanıt vermek için harekete geçmeye daha hazır hale gelirler.

Bu Kitap Ne Sağlayacak?

Bu kılavuz, sivil toplum kuruluşlarına dijital güvenliklerini iyileştirmek için pratik bilgi ve beceriler kazandırmak amacıyla tasarlanmıştır. Açık üniversite tarzı bir kursa benzer şekilde, öğrenmeyi pekiştirmek için gerçek örnekler, kontrol listeleri ve basit alıştırmalar içeren basit ve *uygulamalı* bir *yaklaşım* benimsemiştir. Bölümleri inceleyerek okuyucular:

- **Temel Bilgileri Anlayın:** Dijital güvenliğin terminolojisini ve temel kavramlarını öğreneceksiniz (endişelenmeyin, hızlı başvuru için Ek'te bir Terimler Sözlüğü bulunmaktadır). Kötü amaçlı yazılımın ne olduğu gibi temel tanımlardan iki faktörlü kimlik doğrulama gibi kavramlara kadar, güvenlik konularını güvenle tartışabilmeniz için jargonu anlaşılır hale getireceğiz.
- **Risklerinizi belirleyin:** Kitap, CSO'nuzun karşılaşabileceği belirli tehditleri ve korunması gereken varlıkları değerlendirmenize rehberlik edecektir. Kısa öz değerlendirme soruları ve senaryolar aracılığıyla, kuruluşunuzun risk profilini belirlemeye başlayacaksınız (Bölüm 3).
- **En İyi Uygulamaları Hayata Geçirin:** Güçlü şifreler oluşturma, cihazlarınızı güvence altına alma ve interneti ve e-postayı güvenli bir şekilde kullanma gibi acil eylemler hakkında açık ve adım adım tavsiyeler sunuyoruz (Bölüm 2). Bunlar, tutarlı bir şekilde uygulandığında güvenlik açıklarınızı önemli ölçüde azaltan siber güvenliğin "hızlı kazançları"dır.
- **Güvenlik Planı Geliştirin:** Bireysel ipuçlarının ötesinde, tüm bunları CSO'nuz için basit ama etkili bir dijital güvenlik planında nasıl bir araya getirebileceğinizi göstereceğiz (Bölüm 3). Buna politika önerileri, ekibiniz için eğitim planları ve verileri yedekleme ve şifreleme yöntemleri dahildir. Kendi planınızı hazırlamanıza veya geliştirmenize yardımcı olmak için şablonlar ve örnekler sunulmaktadır.
- **Güvenlik Araçlarını Kullanmayı Öğrenin:** Bölüm 4'te kullanıcı dostu güvenlik araçları ve yazılımları (şifre yöneticilerinden antivirüs programlarına ve güvenli mesajlaşma uygulamalarına kadar) tanıtılmaktadır. Küçük bir bütçeyle bile kullanımı kolay ve yaygın olarak bulunan araçlara ağırlık veriyoruz. Ele alınan her araç veya yöntem, neden yararlı olduğu ve nasıl kullanılmaya başlanacağı ile ilgili açıklamalarla birlikte sunulmaktadır.
- **Olaylara Hazırlanın:** En iyi çabalarımıza rağmen, olaylar meydana gelebilir. Bölüm 5'te, siber olayların belirtilerini (bilgisayarınızın hacklenmiş olabileceğine dair işaretler gibi) nasıl

tanıyacağınızı ve buna yanıt olarak atmanız gereken acil adımları ele alıyoruz. Bunu bir acil durum tatbikatı olarak düşünün – ne yapmanız gerektiğini bilmek, hasarı önemli ölçüde sınırlayabilir. Ayrıca, kriz anında zamanında destek almak çok önemli olabileceğinden, yardım alabileceğiniz kaynakları ve iletişim bilgilerini de listeliyoruz.

- **İşbirliğini Vurgulayın:** Bu kılavuzun ana temalarından biri, dijital güvenlikle mücadelede yalnız olmadığınızı vurgulamaktır. 6. bölümde, meslektaş desteğinin gücü ele alınmaktadır – CSO'ların uyarıları, ipuçlarını ve hatta eğitim kaynaklarını paylaşarak birbirlerine nasıl yardımcı olabilecekleri anlatılmaktadır. Ayrıca, teknoloji gönüllülerinden yardım hatlarına kadar destek sunan (yerel veya uluslararası) ağlar ve kurumlara da işaret edilmektedir.
- **Gerçek Hayat Örnekleri Sunun:** 7. bölümde, vaka çalışmaları ve yaygın tuzakları sunuyoruz. Siber zorluklarla karşılaşan STK'ların kısa hikayelerini ve bu zorlukları nasıl aştıklarını, ayrıca kuruluşların sıkça yaptığı hataları (böylece bunları önleyebilmeniz için) okuyacaksınız. Ayrıca, güvenliğinizi "test etmek" için birkaç basit alıştırma da ekledik – örneğin, kendi ofisinizi denetlemek için bir kontrol listesi veya ekibiniz için bir oltalama e-postası testi.

Bu e-kitabın sonunda, dijital güvenlikle ilgili konularda kendinizi daha güvende ve yetkin hissedeceksiniz. İçerik, BT konusunda bilgi sahibi olmasanız bile anlayabileceğiniz şekilde düzenlenmiştir. Her bölüm bir önceki bölümün üzerine inşa edilmiştir ve gerektiğinde belirli bölümlere geri dönebilirsiniz. Amaç, sizi bir gecede siber güvenlik uzmanı yapmak değil, yaygın tehditlere karşı korumanızı önemli ölçüde artıracak bilgi ve alışkanlıklar kazandırmaktır. Bunu dijital yol için bir sürücü kılavuzu gibi düşünün – güvenli sürüş için mekanikçi olmanıza gerek yoktur, ancak kuralları öğrenmeniz, doğru araçları (emniyet kemeri gibi) kullanmanız ve tehlikelere karşı uyanık olmanız gerekir.

Ayrıca, bölümler boyunca, öğrendiklerinizi uygulamak için "Biliyor muydunuz?" yan notları ve kısa uygulama ipuçları bulacaksınız. Bunlarla ilgilenmek için biraz zaman ayırın; bunlar, anlayışınızı pekiştirmek ve öğrenme deneyimini daha etkileşimli hale getirmek için vardır. Örneğin, şifreler bölümünden sonra, bir ipucu sizden örnek bir şifrenin gücünü değerlendirmenizi veya yedekleme bölümünden sonra, kuruluşunuzda yedeklenmesi en önemli olan verilerin hangileri olduğunu düşünmenizi isteyebilir.

Sonuç olarak, bu yayın size sivil toplum bağlamına uyarlanmış dijital güvenlik konusunda bir temel sunmaktadır. Bu bölümlere zaman ayırarak, kuruluşunuzun çalışmalarını ve onunla bağlantılı kişileri korumak için önemli bir adım atmış olursunuz. Öyleyse, CSO'nuz için daha güvenli bir dijital geleceğe doğru yolculuğa başlayalım!

Bölüm Özeti

Bu bölüm, CSO'lar için dijital güvenliğin kritik önemini tanıtarak, savunuculuk rollerinden dolayı siber saldırıların başlıca hedefleri olarak savunmasızlıklarını vurgulamaktadır. Kötü amaçlı yazılım, kimlik avı, veri ihlalleri, yetkisiz hesap erişimi, web sitesi tahribatı ve DDoS saldırıları gibi yaygın tehditleri özetleyerek, bunların operasyonlar, güven ve güvenlik üzerindeki etkisini vurgulamaktadır. 550.000 bağışçının bilgilerinin açığa çıktığı 2016 Avustralya Kızılhaçı veri ihlali ve bir hayır kurumuna yapılan fidye yazılımı saldırısı gibi gerçek hayattan örnekler, yetersiz savunmanın sonuçlarını göstermektedir. Bu bölümde, 2025 yılında ulus devlet saldırılarının %31'inin STK'ları hedef aldığı, Cenevre merkezli kar amacı gütmeyen kuruluşların %41'inin saldırılara maruz kaldığı, ancak bunların yarısından fazlasının siber güvenlik bütçesi olmadığı belirtilmektedir. Dijital güvenliğin, hassas verileri (örneğin, yararlanıcıların bilgileri) korumak ve operasyonel sürekliliği sağlamak açısından kritik öneme sahip olduğu vurgulanmaktadır. Hassas siyasi ortamlarda faaliyet gösteren STK'lar için siber güvenlik, fiziksel güvenlikle bağlantılıdır ve gözetleme veya dezenformasyonu önler. Bu bölüm, insanları, süreçleri ve teknolojiyi bir araya getiren bir "dijital öz savunma" kültürünü savunmaktadır. Siber güvenliği sadece bir BT sorunu değil, hayatta kalmak için bir gereklilik olarak çerçeveleyerek e-kitabın temelini oluşturmaktadır ve okuyucuları sonraki bölümlerdeki pratik çözümlere hazırlamaktadır. Önemli çıkarımlar arasında, STK'ların misyonlarını korumak için farkındalık, hazırlık ve güven oluşturma ihtiyacı bulunmaktadır.

CSO'lar için Hızlı Başlangıç Siber Güvenlik Kontrol Listesi

Bu kontrol listesi, kuruluşunuzun dijital güvenliğini artırmak için basit ve acil adımlar sunar. Güvenlik açıklarını azaltmak ve güvenli bir dijital ortam için temel oluşturmak amacıyla bu adımları önümüzdeki hafta içinde tamamlayın. Her adım, sınırlı kaynaklara sahip CSO'lar için düşük maliyetli, kullanıcı dostu ve etkili olacak şekilde tasarlanmıştır.

1. Hesaplarınızı Güvenli Hale Getirin

- İki Aşamalı Kimlik Doğrulamayı (2FA) Etkinleştirin: Tüm önemli hesaplar (ör. e-posta, sosyal medya, bulut depolama) için 2FA'yı bugün etkinleştirin. Ekstra bir koruma katmanı eklemek için bir kimlik doğrulama uygulaması (Google Authenticator veya Authy gibi) veya SMS kodları kullanın .
    - ⇒ Hesap ayarlarını kontrol edin (ör. Gmail: Ayarlar > Güvenlik > 2 Adımlı Doğrulama).
- Güçlü, Benzersiz Şifreler Oluşturun: Önemli hesaplarınızın şifrelerini en az 14 karakter olacak şekilde güncelleyin ve harf, rakam ve sembolleri karıştırın (ör. "sunbird&glass7rain"). Her hesap için farklı bir şifre kullanın.
    - ⇒ Şifreleri güvenli bir şekilde oluşturmak ve saklamak için Bitwarden gibi ücretsiz bir şifre yöneticisi kullanmayı düşünün.
- İhlal Edilen Hesapları Kontrol Edin: "Have I Been Pwned" (haveibeenpwned.com) sitesini ziyaret ederek e-posta adresinizin veya hesaplarınızın veri ihlallerine maruz kalıp kalmadığını kontrol edin. Etkilenen şifreleri hemen değiştirin.
    - ⇒ Sızdırılan kimlik bilgileri, hesaplarınıza saldırmak için kullanılabilir.

2. Cihazlarınızı Koruyun

- Yazılımları Bugün Güncelleyin: Tüm cihazların (bilgisayarlar, telefonlar, tabletler) ve yazılımların (ör. işletim sistemleri, tarayıcılar, uygulamalar) en son güvenlik yamalarıyla güncellendiğinden emin olun.
    - ⇒ Windows Update, macOS Software Update veya uygulama mağazası ayarlarını kontrol ederek bekleyen güncellemeler olup olmadığını kontrol edin.
- Antivirüs Yazılımı Yükleyin: Tüm cihazlara ücretsiz bir antivirüs programı (ör. Windows Defender, Avast Free Antivirus) yükleyin ve programın etkin ve güncel olduğundan emin olun.
    - ⇒ Güvenilir kaynaklardan indirin ve haftalık taramalar planlayın.
- Cihaz Kilidini Etkinleştirin: Cihazları, beş dakika boyunca kullanılmadığında güçlü bir parola veya PIN ile otomatik olarak kilitlenecek şekilde ayarlayın. Şifrelemenin

etkinleştirildiğinden emin olun (çoğu modern cihazda bu özellik varsayılan olarak mevcuttur).

⇒ Kilitler ve şifreleme, cihazların kaybolması veya çalınması durumunda veri hırsızlığını önler.

3. Güvenli İletişim

- Güvenli Mesajlaşma Uygulamaları Kullanın: Hassas iletişim için Signal veya WhatsApp gibi uçtan uca şifrelenmiş uygulamalara geçin. Hassas bilgileri paylaşmadan önce kişileri doğrulayın.

  ⇒ Hassas sohbetler için kaybolan mesajları indirin ve etkinleştirin.

- Oltalama E-postalarını Tespit Edin: Personeli, acil dil, yazım hataları veya tanıdık olmayan gönderenler içeren e-postalardaki bağlantılara tıklamaktan veya bilgileri paylaşmaktan kaçınmaları konusunda eğitin. E-posta adreslerini dikkatlice kontrol edin.

  ⇒ Tıklamadan önce bağlantıların üzerine gelerek URL'leri doğrulayın ve şüpheli e-postaları BT departmanına bildirin.

4. Verileri Koruyun

- Önemli Verileri Yedekleyin: Bu hafta, önemli dosyaları (ör. bağışçı listeleri, proje belgeleri) güvenli bir harici sürücüye veya bulut hizmetine (ör. 2FA özellikli Google Drive) yedekleyin.

  ⇒ Otomatik yedeklemeler planlayın veya dosyaları güvenli bir konuma manuel olarak kopyalayın.

- Veri Erişimi Sınırlayın: Hassas verilere (ör. paylaşılan sürücüler, veritabanları) kimlerin erişimi olduğunu gözden geçirin. Eski çalışanların veya gönüllülerin erişimini kaldırın.

  ⇒ Erişimi kısıtlamak, içeriden gelen tehditlerin veya sızıntıların riskini azaltır.

5. Çevrimiçi Varlığınızı Güvenli Hale Getirin

- Web Sitesi Güvenliğini Kontrol Edin: Web sitenizin HTTPS kullandığını doğrulayın (tarayıcıda asma kilit simgesini arayın). Düzenli yedeklemeler ve güncellenmiş yazılımlar (ör. CMS, eklentiler) için web barındırma sağlayıcınızla iletişime geçin.

  ⇒ Barındırma sağlayıcınıza danışın veya HTTPS için Let's Encrypt gibi ücretsiz araçları kullanın.

- Sosyal Medya Hesaplarınızı Güvenli Hale Getirin: Tüm CSO sosyal medya hesaplarında 2FA ve güçlü şifreler etkinleştirin. Etkin olmayan yöneticilerin erişimini kaldırın.

  $\Rightarrow$ Hesap ele geçirme ve yanlış bilgilendirmeye karşı koruma sağlar.

2.2 BÖLÜM 2: DİJİTAL GÜVENLİĞİN İLK ADIMLARI

Dijital Güvenlikte İlk Adımlar

Bu bölüm, bir kuruluşun her bireyinin temel dijital güvenlik için izlemesi gereken temel uygulamaları ele almaktadır. Bu "ilk adımlar" genellikle önemli güvenlik avantajları sağlayan basit alışkanlıklar ve önlemlerdir. Söylendiği gibi, siber güvenlik siber hijyenle başlar; yani çevrimiçi güvenliğinizi sağlayan günlük rutinler ve önlemlerle. Güçlü şifreler oluşturmayı, interneti dikkatli kullanmayı, iletişiminizi güvence altına almayı ve bilgisayarlarınızı ve akıllı telefonlarınızı korumayı keşfedeceğiz. Başlangıçta sadece bu temel kuralları uygulasanız bile, yaygın tehditlerin büyük bir kısmını ortadan kaldırmış olacaksınız.

Güçlü Parolalar Oluşturma ve Koruma

Dijital güvenliğinizi artırmanın en hızlı yollarından biri, şifrelerinizi güçlendirmektir. Şifreler, hesaplarınızın ve cihazlarınızın anahtarlarıdır. Şifreleriniz zayıfsa veya ele geçirilmişse, saldırganlar e-postanızdan banka bilgilerinize kadar her şeye erişebilir. Ne yazık ki, insanlar genellikle hatırlanması kolay şifreleri tekrar kullanır veya saldırganların tahmin etmesi kolay şifreler seçerler (örneğin "123456" veya "şifre"). Aslında, zayıf veya çalınan şifreler, güvenlik ihlallerinin başlıca nedeni olmaya devam etmektedir.

Güçlü bir şifre nedir?

Siber güvenlik yönergelerine göre, güçlü bir şifre uzun, benzersiz ve karmaşıktır. Microsoft'un güvenlik kılavuzunda, büyük ve küçük harfler, rakamlar ve sembollerden oluşan en az 14 karakterlik bir şifre önerilmektedir. Şifre, kolay kişisel bilgiler (adınız veya doğum tarihiniz gibi) veya yaygın kelimeler içermemelidir. İyi bir uygulama, sizin için hatırlaması kolay ancak başkalarının tahmin etmesi zor olan bir dizi rastgele kelime veya cümleden oluşan bir *parolayı* kullanmaktır. Örneğin, "sunbird&glass7rain" kısa bir parola olan "blue123"ten çok daha güçlüdür, ancak bir cümle olduğu için hatırlanması daha kolay olabilir.

Benzersizlik çok önemlidir: her hesap veya hizmetin kendi şifresi olmalıdır. Şifreleri yeniden kullanırsanız ve bir hesap ihlal edilirse, saldırganlar aynı şifreyi diğer hesaplarınızda da deneyecektir (bu taktik, *kimlik bilgisi doldurma* olarak adlandırılır). Benzersiz şifreler kullanmak, tek bir ihlalin zararını sınırlar. ENISA'nın (AB'nin siber güvenlik ajansı) tavsiye ettiği gibi, *birden fazla hesapta aynı şifreyi kullanmaktan kaçının*. Ayrıca, hesaplarınızın bil e veri ihlallerinde yer

alıp almadığını kontrol etmeyi düşünün ("Have I Been Pwned" gibi web siteleri, ihlal veritabanlarında e-postanızı aramanıza olanak tanır). Eğer öyleyse, bu şifreleri hemen değiştirin.

Şifre yöneticileri: Onlarca uzun ve karmaşık şifreyi ezberlemek gerçekçi değildir. İşte bu noktada şifre yöneticisi araçları devreye girer. Şifre yöneticisi, sizin için güçlü rastgele şifreler oluşturabilen ve bunları şifreli bir kasada saklayabilen bir uygulama (veya güvenli bulut hizmeti) olup, böylece yalnızca bir ana şifreyi hatırlamanız yeterlidir. Birçok güvenlik uzmanı ve kurumu, daha iyi güvenlik için şifre yöneticileri kullanmanızı önerir. Örneğin, Bitwarden (bir şifre yöneticisi şirketi) ENISA'nın, şifreleri benzersiz ve güvenli tutmak için şifre yöneticisi kullanmayı açıkça içeren tavsiyesini övdü. Popüler şifre yöneticileri arasında Bitwarden, LastPass, 1Password ve KeePass (diğerleri arasında) bulunur. Kuruluşunuza uygun birini bulun (bazıları ücretsiz sürümleri vardır) ve tüm zayıf veya tekrarlanan şifreleri yükseltmek için kullanmaya başlayın.

Şifrelerinizi koruma: Güçlü bir şifre bile korunmalıdır. Şifrelerinizi asla e-posta veya mesajlaşma yoluyla paylaşmayın ve şifrenizi istemeden soran kişilere karşı dikkatli olun – meşru destek personeli (BT şirketlerinde bile) gerçek şifrenize ihtiyaç duymaz. Ayrıca, mümkün olduğunda hesaplarınızda İki Aşamalı Kimlik Doğrulama (2FA) özelliğini etkinleştirin. 2FA (çok faktörlü kimlik doğrulama, MFA olarak da bilinir), oturum açarken ikinci bir kimlik kanıtı sağlamanız anlamına gelir. Örneğin, telefonunuza gönderilen veya bir kimlik doğrulama uygulaması tarafından oluşturulan tek kullanımlık bir kod veya parmak izi taraması. Bu şekilde, birisi şifrenizi öğrense bile, ikinci faktör olmadan hesaba erişemez. ENISA'nın en önemli tavsiyesi, oturum açma işlemleri için telefon kodu veya biyometrik gibi "ekstra bir adım" kullanmaktır. Birçok hizmet (Google, Facebook, Microsoft vb.) bir uygulama veya SMS aracılığıyla 2FA'ya izin verir. E-posta hesapları, sosyal medya, bankacılık, bulut depolama ve esasen hacklenirse hassas hale gelebilecek tüm hesaplar için bu özelliği etkinleştirmek akıllıca olacaktır.

Bir başka önemli alışkanlık da cihazlarda veya uygulamalarda varsayılan şifreleri değiştirmektir. Birçok donanım cihazı (Wi-Fi yönlendiriciler gibi) veya yazılım aracı, önceden ayarlanmış yönetici şifreleriyle (genellikle "admin/admin" gibi genel bir şifre) gelir. Bu varsayılan şifreler saldırganlar

tarafından yaygın olarak bilinir, bu nedenle kurulum sırasında her zaman yeni ve güçlü bir şifre belirleyin. Örneğin, CSO'nuz yeni bir ofis yönlendiricisi veya çevrimiçi veritabanı kurarsa, ilk görevlerden biri erişim kimlik bilgilerini özelleştirmek olmalıdır.

Son olarak, şifreleri düzenli olarak güncellemek için bir program oluşturun. Şifrelerin ne sıklıkla değiştirilmesi gerektiği konusunda görüşler farklıdır. Bazı uzmanlar, sık sık zorunlu değişikliklerin ters etki yapabileceğini (kullanıcıların daha basit şifreler seçebileceğini veya sadece bir sayı ekleyebileceğini) söylüyor. Modern kılavuzlar, şifreler güçlü ve benzersiz ise, yalnızca bir güvenlik ihlali belirtisi olduğunda veya periyodik olarak (örneğin, yılda bir kez) yenileme amacıyla değiştirilmesi gerektiğini önerir. Diğer kontroller (2FA gibi) mevcutsa, her üç ayda bir değiştirme kuralı artık zorunlu bir gereklilik değildir. Ancak, herhangi bir hesabın güvenliğinin ihlal edildiğinden şüpheleniyorsanız, o şifreyi ve benzer bir şifreyi kullandığınız diğer tüm yerleri hemen değiştirin.

Özetle, güçlü şifreler + 2FA = güçlü bir savunma. Güçlü, farklı şifreler kullanarak ve ikinci bir oturum açma adımı ekleyerek, birçok saldırı girişimini engelleyebilirsiniz. Bunu, evinizi yüksek kaliteli bir kilit (şifre) ve bir sürgü (2FA) ile kilitlemek gibi düşünün – bir saldırgan, içeri girmek için her ikisini de aşmak zorunda kalır. Ekip olarak, CSO'nuzdaki herkesi bu uygulamaları benimsemeye teşvik edin. 3. bölümde, kuruluş genelinde iyi şifre politikalarının nasıl uygulanacağına değinilecek, ancak bu değişiklik, hesaplarınız için bir şifre yöneticisi ve 2FA kullanarak örnek olarak sizden başlayabilir.

Güvenli İnternet Kullanımı: Dikkat Edilmesi Gerekenler

İnternet, çoğu kuruluş için bilgi ve iletişimin ana damarıdır, ancak dikkatsizce kullanıldığında bir tehdit kaynağı da olabilir. "Güvenli internet kullanımı", web sitelerini gezinirken, çevrimiçi hizmetleri kullanırken ve içerik indirirken dikkatli ve akıllı davranışlar sergilemeyi ifade eder. CSO personelinin uyması gereken temel ilkeler ve ipuçları şunlardır:

***Web Sitesinin Meşruiyetini Doğrulayın*:** Bir web sitesine hassas bilgiler (giriş bilgileri veya kişisel veriler gibi) girmeden önce, sitenin gerçek ve güvenli olduğundan emin olun. URL'nin doğru olduğunu (gerçek olanları taklit eden yazım hataları veya garip alan adlarına dikkat edin) ve bağlantının şifreli olduğunu (tarayıcı adres çubuğunda https:// ve asma kilit simgesi ile gösterilir) kontrol edin. Örneğin, https://secure.CSOportal.org, http://CSO-portal.example.com

adresinden daha güvenilirdir (HTTPS eksikliği bir tehlike işaretidir). Saldırganlar, şifreleri ele geçirmek için genellikle meşru görünen sahte web siteleri oluştururlar (örneğin, bir e-posta giriş sayfasını taklit eden bir site). Giriş yaparken adres çubuğunu her zaman iki kez kontrol edin. Modern tarayıcılar genellikle büyük sitelerin sertifika ayrıntılarında şirket adını vurgular – bu ipuçlarını kullanın. Aldığınız bir bağlantıdan (örneğin, e-posta veya sosyal medya aracılığıyla) şüphe duyuyorsanız, doğrudan tıklamayın. Bunun yerine, Google veya yer imleri aracılığıyla resmi web sitesine gidin veya bağlantının üzerine gelerek URL'yi önizleyin (tıklamadan). Bağlantı şüpheli görünüyorsa veya iddia edilen gönderenle eşleşmiyorsa (örneğin, bir e-posta bankanızdan geldiğini iddia ediyor ancak URL alakasız bir etki alanıysa), muhtemelen kötü amaçlıdır.

Tıklamadan veya İndirmeden Önce Düşünün: Kötü amaçlı bağlantılar ve indirmeler, kötü amaçlı yazılımların başlıca taşıyıcılarıdır. Tanımadığınız siteleri gezerken veya dosya indirme isteği aldığınızda dikkatli olun. İçeriği görüntülemek için bir "kodek" veya "güncelleme" indirmenizi isteyen açılır pencereler genellikle tuzaktır. Belirli bir yazılıma veya belgeye ihtiyacınız varsa, bunu güvenilir bir kaynaktan indirin (örneğin, resmi satıcı sitesinden veya tanınmış bir uygulama mağazasından yazılım). Korsan yazılım veya medya indirmekten kaçının – yasal sorunların yanı sıra, bu tür dosyalar genellikle kötü amaçlı yazılımlar içerir. Ayrıca, tarayıcı ayarlarınızda otomatik indirmeyi devre dışı bırakın; kontrol sahibi olmak, istemediğiniz işlemleri iptal edebileceğiniz anlamına gelir. Tarayıcınız veya güvenlik aracınız bir sitenin güvenli olmayabileceği konusunda uyarı verirse, uyarıyı dikkate alın ve siteyi terk edin. Benzer şekilde, bilinmeyen yayıncılardan gelen tarayıcı uzantılarına veya eklentilerine karşı şüpheci olun. Yalnızca gerçekten ihtiyacınız olan ve resmi web mağazalarından gelen eklentileri yükleyin, çünkü kötü amaçlı bir uzantı faaliyetlerinizi izleyebilir veya reklamlar/virüsler enjekte edebilir.

Güvenli Bağlantılar (Wi-Fi ve VPN) Kullanın: İnternete bağlanırken, özellikle ofis dışında, ağ güvenliğine dikkat edin. Halka açık Wi-Fi ağları (kafeler, havaalanları vb. gibi) riskli olabilir, çünkü aynı ağdaki saldırganlar trafiğinizi ele geçirebilir. Halka açık Wi-Fi kullanmanız gerekiyorsa, bağlantı şifrelenmemişse (HTTPS olup olmadığına bakın) hassas hesaplara erişmekten kaçının. Bununla birlikte, bilgili bir saldırgan, kullanıcıları cezbetmek için cazip bir isimle ("Ücretsiz Havaalanı WiFi") sahte bir Wi-Fi erişim noktası kurabilir. Güvenilir olmayan

ağlarda VPN (Sanal Özel Ağ) kullanmak iyi bir uygulamadır. VPN, tüm internet trafiğiniz için şifreli bir tünel oluşturur ve bu da dinleme olasılığını büyük ölçüde azaltır. Birçok kuruluş, uzaktan çalışma için VPN erişimi sağlar; eğer sizin kuruluşunuz da sağlıyorsa, nasıl kullanılacağını bildiğinizden emin olun. Sağlamıyorsa, seyahat ederken veya halka açık alanlarda çalışırken saygın bir ticari VPN hizmeti kullanmayı düşünün. Ayrıca, ev veya ofis Wi-Fi ağınızın güçlü bir parolayla güvenli olduğundan ve WPA2 veya WPA3 şifrelemesi kullandığından emin olun. Belirtildiği gibi yönlendiricinizdeki varsayılan yönetici parolasını değiştirin ve kesinlikle gerekli olmadıkça uzaktan yönetimi devre dışı bırakın.

E-posta Eklerine ve Bağlantılara Dikkat Edin: E-postalar bir sonraki bölümde daha ayrıntılı olarak ele alınacak olsa da, güvenli internet alışkanlıkları kapsamında, e-postalarda veya web sitelerinde bağlantılara tıklarken dikkatli olunması gerektiğini belirtmek gerekir. Çevrimiçi ortamda yaygın bir dolandırıcılık yöntemi, "Bilgisayarınız virüs bulaşmış! Taramak için buraya tıklayın" gibi sahte uyarılar göndermektir. Bu tür uyarılar genellikle kötü amaçlı yazılımlara yönlendirir. Benzer şekilde, bir şey kazandığınızı veya acil bir güncelleme yapmanız gerektiğini iddia eden banner reklamlara veya pop-up'lara tıklamaktan kaçının. Bunlar, merak veya korkuyu istismar etmeye yönelik sosyal mühendislik girişimleridir. Şu atasözünü unutmayın: Çevrimiçi bir şey gerçek olamayacak kadar iyi (veya korkutucu) görünüyorsa, muhtemelen bir dolandırıcılıktır. Örneğin, "Şimdi 5.000 dolarlık hibe alın – sınırlı süreli!" diyen bir çevrimiçi reklam şüphe uyandırmalıdır. Bu taktikleri tanımayı ve dürtüsel tepki vermemeyi öğrenin.

Kişisel ve Kurumsal Bilgileri Koruyun: Web sitelerinde ve sosyal medyada kamuya açık olarak paylaştığınız bilgilere dikkat edin, çünkü bu bilgiler siber saldırılarda aleyhinize kullanılabilir. Saldırganlar genellikle sosyal medya profillerinden veya web sitelerinden ayrıntılar toplar ve daha ikna edici kimlik avı e-postaları oluşturur (hedefli saldırılarda bu uygulamaya "spear phishing" denir). Örneğin, CSO'nuzun sitesinde çalışanların e-postaları ve ilgi alanları listeleniyorsa, birisi bu bilgileri referans göstererek size e-posta gönderebilir ve güveninizi kazanmaya çalışabilir. Bu nedenle, halka açık forumlarda iç meseleler hakkında ifşa ettiğiniz bilgileri sınırlayın. Web formlarını doldururken, istenen tüm verilerin gerekli olup olmadığını düşünün. Bir site, açık bir ihtiyaç olmadan annenizin kızlık soyadını veya diğer kişisel verilerinizi istiyorsa, iki kez düşünün. Gizlilik açısından, sosyal medyada gizlilik ayarlarını kullanarak

gönderilerinizi kimlerin görebileceğini sınırlayın. Kuruluş için ise, dizinlerin veya hassas belgelerin kendi web sitenizde yanlışlıkla ifşa edilmediğinden emin olun. CSO'nuzun adını düzenli olarak çevrimiçi olarak arayarak hangi bilgilerin mevcut olduğunu kontrol edin. Bu şekilde, ifşa edilmiş bir belge veya sahte bir siteyi tespit edebilirsiniz.

Güncellenmiş Tarayıcılar ve Güvenlik Araçları Kullanın: Güvenli internet kullanımı sadece davranışla ilgili değildir; aynı zamanda güncellenmiş teknolojiyi kullanmakla da ilgilidir. Güncellemeler genellikle güvenlik açıklarını düzeltir, bu nedenle web tarayıcınızın (Chrome, Firefox, Edge vb.) her zaman en son sürümünü kullanın. Tarayıcının yerleşik güvenlik özelliklerini etkinleştirin: çoğu tarayıcı, bilinen kötü web sitelerini engelleyebilen kimlik avı ve kötü amaçlı yazılım korumasına sahiptir. Ayrıca, cihazınızda saygın bir antivirüs/kötü amaçlı yazılımdan koruma programı etkin olmalıdır; bu programlar bazen bir indirmenin veya sitenin kötü amaçlı olup olmadığını tespit edebilir. Modern antivirüs çözümleri genellikle, kimlik avı veya kötü amaçlı yazılım barındırmasıyla bilinen bir siteyi ziyaret etmeye çalıştığınızda sizi uyaran veya engelleyen web korumaları içerir. Örneğin, Microsoft Defender veya Avast, tehlikeli bir siteye erişmeye çalıştığınızda bir uyarı sayfası gösterebilir. Bu uyarılara dikkat edin; bunlar sizi korumak için vardır.

Özetle, interneti güvenli bir şekilde kullanmak, büyük ölçüde çevrimiçi ortamda uyanık ve şüpheci olmakla ilgilidir. Büyük bir şehirde sokak zekası gibi, çevrenizin farkında olun ve şüpheli bir sokağa girmeden önce iki kez düşünün. Çevrimiçi ortamda da, nereye "seyahat ettiğinizi" ve kiminle etkileşimde bulunduğunuzu dikkatle izlemelisiniz. Ekibinizdeki herkesi temkinli bir zihniyet benimsemeye teşvik edin: tıklamadan önce bağlantıların üzerine gelin, yalnızca güvenilir kaynaklardan indirme yapın ve istenmeyen pop-up'ları veya mesajları şüpheyle karşılayın. Bir sonraki bölümde, en yaygın saldırı yolları olan e-posta ve mesajlaşma ile bu iletişimlerin güvenliğini sağlama yöntemlerini daha ayrıntılı olarak ele alacağız.

E-posta ve Mesajlaşma Güvenliği

E-posta, CSO'lar için vazgeçilmez bir araçtır ve mesajlaşma uygulamaları (WhatsApp, Signal veya Telegram gibi) hızlı iletişim için yaygın olarak kullanılmaktadır. Ancak, bu kanallar

phishing, dinleme ve hesap ele geçirme gibi siber saldırıların sık hedefidir. Bu bölüm, daha güvenli iletişim kurma ve yaygın tuzaklardan kaçınma konusunda rehberlik sağlar.

Kimlik Avı Farkındalığı: E-posta kimlik avı, çok yaygın olduğu için daha önce değinilmişti. Tekrarlamak ve genişletmek gerekirse: Beklenmedik e-postaları, özellikle acil eylem gerektiren veya hassas bilgiler isteyen e-postaları her zaman dikkatle inceleyin. Tipik bir kimlik avı e-postası, bir iş arkadaşından, bankadan veya çevrimiçi bir hizmetten gelmiş gibi görünebilir ve "giriş yap" bağlantısı veya açılacak bir ek içerebilir. E-postadaki herhangi bir bağlantıya tıklamadan önce, göndereni ve bağlantının hedefini doğrulayın. Gönderenin adresini dikkatlice kontrol edin – saldırganlar genellikle bir harf farkla farklı bir adres (örneğin, meşru bir Microsoft e-postası yerine john.doe@micros0ft.com) veya iddia edilen kuruluşla eşleşmeyen bir genel e-posta adresi kullanır. Bir e-posta, şifrenizi sıfırlamanız veya bilgi vermeniz gerektiğini iddia ediyorsa, e-postadaki bağlantıya tıklamamak daha güvenlidir. Bunun yerine, resmi web sitesine kendiniz gidin. Ekler için, bilinmeyen veya güvenilir olmayan e-postalardaki dosyaları açmayın. Tanıdık bir kişiden gelmiş olsa bile, beklenmedik ve garipse (örneğin, adresine gönderilen ve beklemediğiniz "Fatura" başlıklı rastgele bir belge), başka bir kanal üzerinden gönderenle doğrulayın. Kural olarak, kaynağına kesinlikle emin olmadıkça Office belgelerinde makroları veya içeriği etkinleştirmeyin – birçok kötü amaçlı yazılım bulaşması, kimlik avı eklerindeki Word/Excel makroları yoluyla gerçekleşir.

CSO'lar, çalışanlarına e-postalara karşı biraz paranoyak olmanın sorun olmadığını (hatta teşvik edildiğini) öğretmelidir – şüphe duyduğunuzda doğrulayın. Sözde gönderen kişiye hızlı bir telefon görüşmesi veya mesaj göndererek, bu isteği gerçekten onların gönderip göndermediğini teyit edebilirsiniz. Tıklayıp pişman olmak yerine iki kez kontrol etmek daha iyidir. Kimlik avının e-posta ile sınırlı olmadığını unutmayın; SMS (kötü bağlantılar içeren metin mesajları) veya mesajlaşma uygulamaları yoluyla da gerçekleşebilir. Örneğin, bir çalışan, çevrimiçi ödeme hizmetinden gelen bir uyarı gibi görünen ve bir bağlantı içeren bir WhatsApp mesajı alabilir. Bu tür mesajları da aynı şekilde, dikkatle ele alın.

E-posta Hesabı Güvenliği: E-posta hesapları diğer şifreleri sıfırlamak için bir kapı olabilir ve hassas yazışmalar içerebilir, bu nedenle e-posta giriş bilgilerinizi güvence altına almak çok

önemlidir. E-posta hesabınız için güçlü bir şifre ve 2FA kullanın (2.1'de tartışıldığı gibi) – Gmail, Outlook veya ProtonMail gibi birçok e-posta sağlayıcısı, bir uygulama veya SMS aracılığıyla iki faktörlü kimlik doğrulamayı destekler. Bu, birisinin e-postanızı hackleme riskini önemli ölçüde azaltır. Ayrıca, paylaşılan veya halka açık bilgisayarlarda e-postanıza erişirken dikkatli olun; her zaman oturumu kapatın ve tarayıcının kimlik bilgilerinizi kaydetmediğinden emin olun. Mümkünse, güvenli e-posta protokolleri kullanın (çoğu modern hizmet varsayılan olarak bunu kullanır): web postasının HTTPS kullandığından emin olun ve bir e-posta istemcisi uygulaması (Outlook, Thunderbird veya telefonunuzdaki gibi) kullanıyorsanız, hem alma (IMAP/POP) hem de gönderme (SMTP) için şifreli bağlantılar (SSL/TLS) kullanacak şekilde ayarlandığından emin olun. BT desteğiniz veya sağlayıcınızın belgeleri bu ayarları doğrulayabilir.

Son derece hassas iletişim için e-posta şifrelemesini düşünün. Standart e-postalar uçtan uca şifrelenmez, yani teorik olarak e-posta içeriği istenmeyen taraflarca (e-posta sağlayıcıları veya hesaba erişim sağlayan herkes gibi) okunabilir. Hassas veriler için PGP/GPG e-posta şifreleme gibi araçlar kullanabilir veya bu iletişim için güvenli mesajlaşma platformlarına geçebilirsiniz. Ancak PGP, günlük kullanım için karmaşık olabilir, bu nedenle başka bir strateji, e-posta gövdesine gizli metinler eklemek yerine, hassas ekler için güvenli dosya paylaşımı kullanmaktır. Bazı CSO odaklı e-posta hizmetleri veya kurumsal paketler, yerleşik şifreleme veya en azından e-postaları veya ekleri parola ile koruma özelliği sunar. Kuruluşunuz son derece hassas bilgilerle (örneğin insan hakları davaları) uğraşıyorsa, şifreleme iş akışını kurmak için bir dijital güvenlik uzmanına danışmalısınız.

Güvenli Mesajlaşma Uygulamaları: Birçok sivil toplum örgütü, hızlı sohbet ve koordinasyon için anlık mesajlaşma kullanır. İletişim kuran kullanıcıların (ve aradaki hiç kimsenin, hatta hizmet sağlayıcının bile) mesajları okuyabilmesini sağlayan uçtan uca şifreleme (E2EE) özelliği sunan mesajlaşma uygulamalarını seçmek önemlidir. Örneğin WhatsApp, Signal ve Telegram'ın "gizli sohbetleri" gibi sohbetler için varsayılan olarak E2EE'ye sahiptir (not: Telegram bulut sohbetleri varsayılan olarak E2EE değildir). Signal, açık kaynaklı, E2EE ve güçlü gizlilik uygulamalarına sahip olduğu için sivil toplum topluluğunda hassas iletişim için yaygın olarak önerilmektedir. Bir diğeri ise yine güvenli ve Avrupa GDPR uyumlu olan **Wire**'dır. **Threema** ve **Element (Matrix)** bazı insan hakları gruplarının kullandığı diğer güvenli mesajlaşma

seçenekleridir. Spesifik uygulama seçimi, bağlamınıza ve muhataplarınızın kullandığı uygulamaya bağlı olabilir, ancak genel kural şudur: hassas konular için düz metin kanallarını (SMS mesajları veya şifrelenmemiş e-postalar) kullanmaktan kaçının ve mümkünse şifreli bir uygulamaya geçin.

Şifreli uygulamalarda bile meta verilere (kim kiminle, ne zaman konuşuyor) dikkat edin. Çoğu E2EE uygulaması, hizmete bazı meta verileri hala ifşa eder (Signal bunu en aza indirmeye çalışsa da). Son derece hassas operasyonlar için, *Session* gibi daha çok anonimliğe odaklanan araçlar kullanılabilir veya Tor üzerinden mesajlaşma kullanılabilir, ancak bunlar ileri düzey senaryolardır. Genel CSO kullanımı için, ana akım bir E2EE uygulaması, şifrelenmemiş kanallara kıyasla güvenliği büyük ölçüde artıracaktır.

Ayrıca, mesajlaşma uygulamalarınızı kilitleyin: Uygulama kilitleme özelliklerini veya cihaz PIN'lerini kullanın, böylece telefonunuz kaybolur veya çalınırsa, başkaları sohbetlerinizi açamaz. Son derece hassas konuşmalar için kaybolan mesajları etkinleştirin – birçok uygulama, mesajların belirli bir süre sonra otomatik olarak silinmesini ayarlamanıza izin verir (Signal, WhatsApp vb.). Bu şekilde, daha sonra birisi hesabınızı ele geçirirse, geçmiş mesajlar çoktan silinmiş olabilir.

Mesajlaşma Dolandırıcılıklarına Dikkat Edin: Kimlik avı dolandırıcılıkları sadece e-postaları kullanmaz. SMS veya uygulamalar aracılığıyla, bir bağlantıya (genellikle kısaltılmış URL'ler) tıklamanızı veya bir şeyi iletmenizi isteyen sahte mesajlar alabilirsiniz. Bunun bir örneği " kodu" dolandırıcılığıdır: istemediğiniz bir giriş kodunu içeren bir SMS alırsınız, ardından hemen bir arkadaşınızdan " sorun yaşıyorum, lütfen az önce aldığın kodu bana gönder" diyen bir WhatsApp mesajı gelir. Bu arkadaşınızın hesabı muhtemelen hacklenmiştir ve saldırgan, WhatsApp hesabınızı ele geçirmek için sizin kodunuzu kullanmaya çalışmaktadır. Bundan çıkarılacak ders: doğrulama kodlarını asla başkalarına vermeyin ve arkadaşlarınızdan gelse bile, sohbetlerdeki acil ve tuhaf taleplere şüpheyle yaklaşın.

Ekler ve Bulut Bağlantıları: E-postaya belge eklemek yerine, çoğu kişi bulut bağlantılarına (ör. Google Drive, Dropbox, OneDrive bağlantıları) geçmiştir. Bunlar kullanışlıdır, ancak kendi güvenlik hususları vardır. Bulut paylaşım bağlantısı gönderirseniz, yalnızca amaçlanan kişilerin erişebildiğinden emin olun (özel bağlantılar kullanın veya e-postalarını

açıkça ekleyin) ve bağlantı için son kullanma tarihi belirlemeyi düşünün. Bir bulut bağlantısı alırsanız, diğer bağlantılarda olduğu gibi dikkatli olun; bağlantının meşru bir bulut hizmeti etki alanından geldiğinden ve beklediğiniz bağlantı olduğundan emin olun. Bir kimlik avı taktiği, Google Drive dosyası gibi görünen ancak sahte bir oturum açma sayfasına yönlendiren bir bağlantı gönderebilir. Her zaman gerektiğinde doğrulayın ve ideal olarak, paylaşılan sürücülere bilinen arayüz üzerinden erişin (örneğin, bir dosyanın sizinle paylaşılıp paylaşılmadığını görmek için doğrudan Google Drive'ınıza giriş yapın).

E-posta Hijyeni ve En İyi Uygulamalar: Birkaç hızlı ipucu daha: Spam filtrelerini kullanın – modern e-posta hizmetleri çoğu gereksiz/oltalama postayı yakalamada oldukça başarılıdır. Yine de, spam klasörünüzü ara sıra yanlış pozitifler için kontrol edin, ancak güvenli olduklarından emin olmadıkça spam klasöründeki e-postalarla etkileşime girmeyin. Saygın kaynaklardan gelmedikçe spam e-postaların aboneliğinden çıkmayın; gerçekten spam olan e-postalarda "abonelikten çık" seçeneğine tıklamak, spam gönderenlere adresinizin aktif olduğunu teyit edebilir. Onları silmek daha iyidir. Büyük gruplara e-posta gönderirken, alıcıların adreslerinin herkes tarafından görülmesini önlemek için BCC'yi kullanın (iletişim listelerinin kazara sızmasını önlemek için). Sağlayıcınız sunuyorsa, e-posta iletme uyarılarını veya oturum açma uyarılarını etkinleştirmeyi düşünün, böylece olağandışı bir etkinlik olup olmadığını bilirsiniz (örneğin, Gmail yeni bir cihazdan yeni bir oturum açıldığında sizi bilgilendirebilir).

Bu uygulamaları takip ederek, kuruluşunuz e-posta veya mesajlaşma tabanlı saldırıların kurbanı olma riskini önemli ölçüde azaltabilir. E-posta genellikle saldırganlar için ilk temas noktası olduğundan, e-posta güvenliğini iyi bir şekilde yönetmek büyük bir güvenlik getirisi sağlar. Bunu güvenli sürüş gibi düşünün: çoğu zaman "yollar" (internet) iyidir, ancak kazaları önlemek için emniyet kemerinizi takmalı (2FA), sinyallere uymalı (şüpheli bağlantılarla ilgili uyarılar) ve dikkatli olmalısınız.

Bilgisayarları ve Telefonları Güvenli Hale Getirmek İçin Temel İpuçları

Dizüstü bilgisayarlar, masaüstü bilgisayarlar ve akıllı telefonlar, modern kuruluşların iş yükünü üstlenen araçlardır. Ayrıca çok sayıda hassas veri depolarlar ve güvenli hale getirilmezlerse saldırganlar için giriş noktaları olabilirler. Bu bölümde, bu cihazları yaygın tehditlerden korumak

için temel ipuçları verilmektedir. Bu ipuçlarının çoğu rutin bakım ve akıllıca kullanım kapsamına girer; bu, kapılarınızı kilitlemek ve düzenli olarak yağ değişimi yaptırmak gibi dijital bir eşdeğerdir.

Yazılımları Güncel Tutun: Tüm cihazlarınızın işletim sistemlerinin ve uygulamalarının en son güvenlik yamalarıyla güncel tutulduğundan emin olun. Yazılım güncellemeleri genellikle saldırganların yararlanabileceği güvenlik açıklarını giderir. Mümkün olduğunca otomatik güncellemeleri etkinleştirin; örneğin, Windows Update veya macOS'un otomatik güncellemelerini etkinleştirin ve iPhone/Android telefonunuzda da sistem ve uygulamalar için aynısını yapın. Ayrıca, uygulamalarınızı (tarayıcılar, ofis programları vb.) düzenli olarak güncelleyin; çoğu, güncelleme mevcut olduğunda uyarı verir – bu uyarıları görmezden gelmeyin. Otomatik güncellenmeyen yazılımlar için, güncellemeleri kontrol etmek üzere tekrarlayan bir hatırlatıcı ayarlayın veya varsa merkezi bir yönetim aracı kullanın. Bunun, tarayıcı eklentilerini ve Java veya Adobe Reader gibi çerçeveleri de içerdiğini unutmayın; bunlar, güncel olmadıkları takdirde tarihsel olarak kötü amaçlı yazılımlar için birer geçit olmuştur. Güncellenmiş bir cihaz, güvenliği artırılmış bir cihazdır.

Antivirüs/Kötü Amaçlı Yazılım Koruması Yükleyin: Bilgisayarlarınızda saygın bir antivirüs çözümü kullanın (ve Android cihazlar için saygın mobil güvenlik uygulamalarından birini de değerlendirin). Modern antivirüs yazılımları gerçek zamanlı koruma sağlar, yani dosyaları aktif olarak tarar ve sistem davranışını izleyerek kötü amaçlı yazılımları engeller. Windows 10/11, güncel tutulduğunda temel kullanım için oldukça iyi olan yerleşik Microsoft Defender ile birlikte gelir. Avast, Bitdefender ve ESET gibi üçüncü taraf seçenekleri (ücretli veya ücretsiz) de düşünülebilir. Önemli olan bir programa sahip olmak ve virüs tanımlarını günlük olarak güncellemek. Aynı anda birden fazla antivirüs programı kullanmaktan kaçının (çakışabilirler). Telefonlarda, iPhone'lar genellikle iOS'un tasarımından dolayı ayrı AV uygulamalarına ihtiyaç duymaz, ancak Android telefonlar, özellikle resmi Play Store dışından uygulamalar yüklediğiniz durumlarda, kötü amaçlı yazılımdan koruma uygulamasından yararlanabilir. Bununla birlikte, telefonlar için en iyi savunma, yalnızca güvenilir uygulama mağazalarından uygulama yüklemek ve uygulama izinlerini kontrol etmektir. Örneğin, bir el feneri uygulamasının kişileriniz veya mesajlarınızı görmesi gerekmez.

Bir şey daha: Asla kolaylık olsun diye güvenlik yazılımınızı devre dışı bırakmayın. Bir eylemi engelliyorsa, basitçe kapatmak yerine nedenini araştırın. Ayrıca, daha önce de belirtildiği gibi korsan yazılım yüklemeyin. Yasalara aykırı olmasının yanı sıra, korsan yazılımlar genellikle antivirüs yazılımlarının yakalayabileceği veya yakalayamayabileceği truva atları ile birlikte gelir.

Cihaz Kilitleri ve Şifreleme Kullanın: Cihazlarınızı kullanmadığınız zamanlarda her zaman PIN, şifre veya biyometrik kilit (parmak izi, yüz tanıma) ile kilitleyin. Kısa bir otomatik kilitleme zaman aşımı süresi ayarlayın (örneğin, beş dakika veya daha az bir süre kullanılmadığında ekran kilitlenir). Bu, birisi cihazınızı fiziksel olarak ele geçirdiğinde yetkisiz erişimi önler. Bir CSO dizüstü bilgisayarı arabadan çalınırsa veya bir konferansta telefon kaybolursa, güçlü bir kilit ekranı verileri meraklı gözlerden koruyabilir, ancak bu sadece kilit ekranı varsa mümkündür. Dizüstü bilgisayarlar için tam disk şifrelemeyi düşünün. Modern işletim sistemleri genellikle bunu varsayılan olarak içerir: Windows'ta BitLocker (Pro sürümleri) veya Aygıt Şifreleme, macOS'ta ise FileVault bulunur. Etkinleştirildiğinde, sabit sürücü çıkarılsa bile, şifre çözme anahtarı (genellikle oturum açma parolanızla bağlantılıdır) olmadan veriler şifreli kalır. Akıllı telefonlarda, hem iOS hem de Android aygıt şifrelemesini destekler (yeni sürümler, PIN/parola kullandığınızda varsayılan olarak şifreler). Şifrelemenin etkinleştirildiğini kontrol edin, özellikle isteğe bağlı olabileceği eski Android sürümlerinde. Şifreleme, hassas veriler için çok önemlidir; örneğin, bir araştırma için katılımcı verilerini içeren bir dizüstü bilgisayar kaybolursa, ancak şifrelenmişse, veriler güvende kalır ve olay bir veri ihlali değil, kayıp cihaz sorunu olarak değerlendirilir.

Düzenli Yedeklemeler: Yedeklemeler öncelikle bir veri kurtarma önlemi olmakla birlikte, aynı zamanda bir güvenlik önlemidir de – fidye yazılımlarından veya cihaz kaybından kurtulmanızı sağlar ve şantaja boyun eğmenize veya tamamen kayba uğramanıza gerek kalmaz. Bölüm 3'te yedekleme stratejileri ayrıntılı olarak anlatılacaktır, ancak temel bir ipucu olarak: önemli dosyaları düzenli olarak yedekleyin ve yedeklemeleri bilgisayarınızdan ayrı güvenli bir yerde saklayın (güvenli bir şekilde saklanan harici sürücü veya bir bulut yedekleme hizmeti). Verileri geri yükleyebildiğinizden emin olmak için bu yedeklemeleri ara sıra test edin. Mobil cihazlar için, önemli fotoğrafları/belgeleri yedeklemeyi düşünün (telefonlar buluta veya bilgisayara yedekleme yapacak şekilde ayarlanabilir). Telefon çalınması durumunda, en azından verileriniz sonsuza kadar kaybolmaz.

Uygulamaların/Programların Güvenli Yüklemesi: Yalnızca güvenilir kaynaklardan yazılım yükleyin. Bilgisayarlarda bu genellikle yazılımın resmi web sitesi veya bilinen bir uygulama mağazası (Microsoft Store veya Mac App Store gibi) anlamına gelir. Telefonlarda Google Play Store, Apple App Store veya F- Droid (açık kaynaklı Android uygulamaları için) kullanın. Bilinmeyen web sitelerinden ücretsiz yardımcı programlara karşı dikkatli olun. Örneğin, bir PDF dönüştürücü veya video oynatıcıya ihtiyacınız varsa, bulduğunuz ilk şeyi indirmek yerine, saygın bir program araştırın. Bazı kötü amaçlı programlar, yararlı araçlar gibi görünür. Ayrıca, yükleme sırasında istemlere dikkat edin ve ekstra araç çubukları yükleme veya arama motorunuzu değiştirme tekliflerini reddedin (ücretsiz yazılım yükleyicilerinde yaygındır). Bunlar tam olarak güvenlik tehditleri değildir, ancak sisteminizi karmaşıklaştırır ve güvenlik açıkları veya gizlilik sorunları yaratabilir.

Güvenli Yapılandırma ve Ayarlar: Cihazlarınızda temel güvenlik ayarlarını yapılandırmak için biraz zaman ayırın. Örneğin, Windows'ta güvenlik duvarının açık olduğundan emin olun (genellikle varsayılan olarak açıktır). Güvenlik duvarı, istenmeyen gelen bağlantıları engellemeye yardımcı olur. Çoğu kullanıcı varsayılan ayarların ötesinde bir ayar yapmaya gerek duymaz, ancak güvenlik duvarı etkin durumda kalmalıdır. Yönlendiricinizde güvenlik duvarı/NAT'ın açık ve uzaktan yönetimin kapalı olduğundan emin olun (güvenli internet bölümünde belirtildiği gibi). Akıllı telefonlarda, her uygulamanın gizlilik ayarlarını kontrol edin – gereksiz izinleri devre dışı bırakın (bir oyunun mikrofonunuza erişmesi gerekir mi? Muhtemelen hayır). Hem Android hem de iOS, her uygulamanın sahip olduğu izinleri görüntülemenize ve aşırı görünen izinleri iptal etmenize olanak tanır.

Cihazların Fiziksel Güvenliği: Dijital güvenlik sadece dijital değildir – cihazların fiziksel güvenliği de önemlidir. Dizüstü bilgisayarları veya telefonları halka açık yerlerde başıboş bırakmayın. Ofiste, masanızdan uzaklaştığınızda ekranları kilitleme politikası uygulayın (Windows ve Mac'te bunun için kısayollar vardır). Seyahat ediyorsanız, havaalanı güvenliğinde veya taksilerde dizüstü bilgisayarlarınıza dikkat edin – birçok güvenlik ihlali, hassas bilgiler içeren cihazların kaybolmasıyla gerçekleşir. Ayrıca, sık sık halka açık yerlerde çalışıyorsanız, dizüstü bilgisayarlar için gizlilik ekranları kullanmayı düşünün (ekranınızı başkalarının görmesini önlemek için). Masaüstü bilgisayarlar için, özellikle CSO'nuzun ziyaretçilere açık bir ofisi veya

ortak alanları varsa, sunucu odalarını kilitlemek veya ekipman için kablo kilitleri kullanmak hırsızlığı önleyebilir.

Kuruluşlar için Mobil Cihaz Yönetimi (MDM) kullanımı: CSO'nuzun kapasitesi varsa (veya büyüdükçe), bir MDM çözümü uygulayabilirsiniz. MDM yazılımı, bir kuruluşun telefon ve dizüstü bilgisayarlarda güvenlik politikalarını merkezi olarak uygulamasına olanak tanır – örneğin, PIN gerektirme, otomatik güncellemeleri zorlama veya kaybolan bir cihazı uzaktan silme. Resmi bir MDM olmasa bile, en azından cihazları uzaktan silebileceğinizden emin olun: Telefonlar için, Find My iPhone veya Android'in Find My Device gibi hizmetler, kaybolan bir telefonu uzaktan bulabilir ve silebilir. Dizüstü bilgisayarlar için, Microsoft hesabına veya kurumsal araçlara bağlı Windows kullanılıyorsa, bazen benzer seçenekler vardır. En azından, kaybolan bir cihazdaki hesapların şifrelerini nasıl değiştireceğinizi ve oturumları nasıl geçersiz kılacağınızı bilin (örneğin, gönüllünüz CSO'nun e-postasına erişimi olan bir telefonu kaybederse, hemen o e-posta şifresini değiştirin ve tüm oturumlardan çıkış yapın).

Arızalar için plan yapın: Bazen donanım arızalanır veya bozulur. "Siber saldırı" olmasa da, bu olaylar veri kaybına veya kesintiye neden olabilir. Temel ipucu: Güvenilir bir antivirüs kullanın, ancak bazı kurtarma araçlarını da elinizin altında bulundurun (antivirüs veya sistem onarım araçları içeren önyüklenebilir temiz bir USB bellek gibi). Önemli dosyaların yalnızca bir dizüstü bilgisayarda depolanmadığından emin olun; donanım arızalanırsa, yedekleriniz veya senkronizasyonunuz hazır olsun.

Bu temel ipuçlarını uygulayarak, kişisel ve iş cihazlarınız için temel bir koruma seviyesi oluşturursunuz. Bunu "uç noktaların" güvenliğini sağlamak olarak düşünün – her telefon veya bilgisayar, zayıfsa istismar edilebilecek bir uç noktadır, ancak toplu olarak CSO'nuzun dijital ortamını oluştururlar. Saldırganlar genellikle en kolay hedefi seçerler. Bu önlemler (güncellemeler, antivirüs, güçlü yapılandırmalar) kolay hedefleri ortadan kaldırarak saldırganları çok daha fazla çaba sarf etmeye zorlar veya ideal olarak onları tamamen caydırır. Bu, ev güvenliğine benzer: kapıları kilitlersiniz, duman alarmları kurarsınız ve belki bir köpeğiniz vardır – bunların hiçbiri güvenliği garanti etmez, ancak riskleri büyük ölçüde azaltır ve uyarılar sağlar. Siber güvenlikte, güvenlik yazılımı ile güncellenmiş, iyi yapılandırılmış cihazınız, kilitleri ve alarmları olan bir ev gibidir – yamalanmamış, korumasız bir sistemden çok daha az çekicidir.

Kişisel ve cihaz güvenliği alışkanlıklarını yerleştirdikten sonra, şimdi kurumsal düzeye geçiyoruz: CSO'nuzda dijital güvenliği destekleyen bir plan ve kültür geliştirmek. Bir sonraki bölümde, riskleri nasıl değerlendireceğiniz ve CSO'nuzun ihtiyaçlarına göre basit ama etkili bir **Dijital Güvenlik Planı** nasıl oluşturacağınız ele alınacaktır.

Bölüm Özeti

Bölüm 2, CSO'lara özel temel siber güvenlik kavramlarına erişilebilir bir giriş sunar ve CIA üçlüsüne odaklanır: gizlilik, bütünlük ve kullanılabilirlik. Gizlilik, verilerin (ör. bağışçı kayıtları) özel kalmasını sağlar, bütünlük yetkisiz değişiklikleri önler ve kullanılabilirlik sistemlerin erişilebilir olmasını sağlar. Bu bölümde, bu ilkeleri açıklamak için sade bir dil ve aktivistlerin iletişim listelerinin güvenliğini sağlamak gibi CSO'larla ilgili örnekler kullanılmaktadır. Riskleri belirlemek ve korumaları önceliklendirmek için bir süreç olan tehdit modellemesini tanıtmaktadır ve bu da onu kaynakları kısıtlı kuruluşlar için uygun hale getirmektedir. Pratik en iyi uygulamalar arasında güçlü şifreler, iki faktörlü kimlik doğrulama (2FA) ve dikkatli internet kullanımı yer alır. Bu bölüm, CSO'ların bütçe kısıtlamalarını ele almak için ücretsiz şifre yöneticileri (örneğin Bitwarden) gibi düşük maliyetli çözümleri vurgular. Ayrıca, ihlallerin %74'ünün kimlik avı dolandırıcılığına kanmak gibi hatalardan kaynaklandığını belirterek insan unsurunu da vurgular. Farkındalığı artırarak, CSO'lar teknik uzmanlık olmadan riskleri azaltabilirler. Bu bölüm, güvenlik altyapısını oluşturmak için basit adımlarla (örneğin, yazılımı güncellemek) başlamayı teşvik etmektedir. Dijital güvenliği CSO'ların misyonlarıyla ilişkilendirerek, verilerin korunmasının güven ve hesap verebilirliği nasıl desteklediğini açıklamaktadır. Örneğin, geçmiş olaylarda görüldüğü gibi, güvenliği ihlal edilmiş bir bağışçı veritabanı halkın güvenini sarsabilir. Bu bölüm, e-kitaba pratik bir ton katarak, okuyuculara güvenlik önlemlerini etkili bir şekilde uygulamak için temel bilgiler sağlamaktadır.

-by-Step Guide for Conducting a Basic Risk Assessment

Bu kılavuz, CSO'ların risk değerlendirme şablonunu doldurmaları için yapılandırılmış bir süreç sunar ve bağışçı veritabanları ve gönüllü kayıtları gibi yaygın CSO varlıklarına özel örnekler içerir. Adımlar, sınırlı teknik uzmanlığa sahip kuruluşlar için erişilebilir olacak şekilde tasarlanmıştır ve müfredatın pratik çerçevelere verdiği önem (Modül 2) ve e-kitabın risk değerlendirmesi ile ilgili kılavuzuyla (Bölüm 5) uyumludur.

Adım 1: Kritik Dijital Varlıkları Belirleyin

- Ne yapmalı: Sivil toplum kuruluşunuzun faaliyetleri için gerekli olan dijital varlıkları (veriler, sistemler, hesaplar) listeleyin. Tehlikeye atıldığında misyonunuzu aksatacak veya paydaşlara zarar verecek unsurlara odaklanın.
- Nasıl yapılır: Küçük bir ekip (ör. liderlik, program personeli, BT irtibat noktası) oluşturarak beyin fırtınası yapın. Verileri (ör. bağışçı listeleri, yararlanıcı bilgileri), sistemleri (ör. e-posta, web sitesi) ve hesapları (ör. sosyal medya, bulut depolama) göz önünde bulundurun.

  Örnek:

  - Bağışçı Veritabanı: Bağışçıların adlarını, iletişim bilgilerini ve bağış tutarlarını içeren bir elektronik tablo veya CRM sistemi.
  - Gönüllü Kayıtları: Gönüllülerin isimleri, iletişim bilgileri ve programlarının paylaşılan bir sürücüde veya bulut platformunda saklandığı dosyalar.
  - E-posta Hesapları: Paydaşlarla iletişim için kullanılan personel Gmail veya Outlook hesapları.

Adım 2: Her Varlığa Yönelik Tehditleri Belirleyin

- Yapılması gerekenler: Her bir varlık için, onu tehlikeye atabilecek potansiyel tehditleri (ör. bilgisayar korsanlığı, kimlik avı, kötü amaçlı yazılım, insan hatası) listeleyin.
- Nasıl yapılır: Saldırganların varlığı nasıl hedef alabileceğini veya neyin yanlış gidebileceğini (ör. kazara sızıntılar, cihaz hırsızlığı) tartışın. E-kitaptaki (Bölüm 1.3) kimlik avı, veri ihlalleri veya fidye yazılımı gibi yaygın tehditlere başvurun.

  Örnek:

  - Bağışçı Veritabanı:

        - Tehdit: Kimlik avı yoluyla veri ihlali (saldırgan, personeli kandırarak giriş bilgilerini ele geçirir).
        - Tehdit: Veritabanını şifreleyen fidye yazılımı.
    - Gönüllü Kayıtları:
        - Tehdit: Zayıf şifreler veya paylaşılan kimlik bilgileri nedeniyle yetkisiz erişim.
        - Tehdit: Dizüstü bilgisayarın çalınması durumunda veri kaybı.

3. Adım: Her Bir Tehdidin Olasılık Derecesini Değerlendirin

- Ne yapmalı: Her bir tehdidin gerçekleşme olasılığını 1 (Nadir) ile 5 (Neredeyse Kesin) arasında bir ölçekte derecelendirin.
- Nasıl yapılır: CSO'nuzun görünürlüğü, geçmiş olaylar veya yaygın saldırı eğilimleri (ör. yaygın olan kimlik avı) gibi faktörleri göz önünde bulundurun. Mümkünse yerel bağlamı kullanın (ör. bölgenizde sık görülen kimlik avı).

  Örnek:
    - Bağışçı Veritabanı:
        - Oltalama: Olasılık = 3 (Oltalama yaygın olduğu için olasıdır, ancak personeliniz bu konuda eğitim almıştır).
        - Fidye yazılımı: Olasılık = 2 (Antivirüs yazılımı varsa olası değildir, ancak imkansız değildir).
    - Gönüllü Kayıtları:
        - Yetkisiz Erişim: Olasılık = 4 (Şifreler zayıfsa veya erişim kısıtlanmamışsa olasıdır).
        - Dizüstü Bilgisayar Hırsızlığı: Olasılık = 2 (Olası değildir, ancak saha operasyonlarında mümkündür).

Adım 4: Her Bir Tehdidin Etkisini Değerlendirin

- Ne yapmalı: Görev kesintisi, veri kaybı veya itibar kaybını göz önünde bulundurarak tehdidin sonuçlarının ciddiyetini 1 (Düşük) ila 5 (Ciddi) arasında derecelendirin.

- Nasıl yapılır: En kötü senaryoyu düşünün (ör. yasal sorunlar, güven kaybı, yararlanıcıların zarar görmesi). E-kitaptaki örnekleri, örneğin Avustralya Kızılhaçı ihlali (Bölüm 1.1) gibi örnekleri referans alın.

  Örnek:

  - Bağışçı Veritabanı:
    - Oltalama/İhlal: Etki = 5 (Bağışçı verilerinin ifşa edilmesi, GDPR cezaları, güven kaybı nedeniyle ciddi).
    - Fidye yazılımı: Etki = 4 (Yüksek, yedekleme olmadan operasyonlar durma noktasına gelebilir).
  - Gönüllü Kayıtları:
    - Yetkisiz Erişim: Etki = 4 (Yüksek, gönüllülerin gizliliğinin ihlali itibara zarar verebilir).
    - Dizüstü Bilgisayar Hırsızlığı: Etki = 3 (Orta, veriler şifrelenmişse ancak kurtarma maliyeti yüksekse).

Adım 5: Risk Puanlarını Hesaplayın ve Önceliklendirin

- Ne yapmalı: Olasılık ile Etkiyi çarpın ve Risk Puanını (1-25) elde edin. Yüksek puanlar, acil dikkat gerektiren riskleri gösterir.
- Nasıl yapılır: Şablonu kullanarak puanları hesaplayın ve riskleri en yüksekten en düşüğe doğru sıralayın. Öncelikle yüksek puan alan riskleri ele almaya odaklanın.

  Örnek:

  - Bağışçı Veritabanı:
    - Kimlik Avı: 3 x 5 = 15 (Yüksek öncelik).
    - Fidye yazılımı: 2 x 4 = 8 (Orta öncelik).
  - Gönüllü Kayıtları:
    - Yetkisiz Erişim: 4 x 4 = 16 (Yüksek öncelik).
    - Dizüstü Bilgisayar Hırsızlığı: 2 x 3 = 6 (Düşük öncelik).

Adım 6: Azaltma Adımları Geliştirin

- Yapılması gerekenler: Düşük maliyetli, pratik önlemlere odaklanarak, her bir tehdidi önlemek veya azaltmak için spesifik, uygulanabilir adımları listeleyin.
- Nasıl yapılır: 2FA, şifreleme veya eğitim gibi çözümler için müfredattan (Modül 1-5) ve e-kitaptan (Bölüm 2-4) yararlan. Adımların CSO'nun kaynakları için uygulanabilir olduğundan emin olun.

  Örnek:

  - Bağışçı Veritabanı:
    - Oltalama: Veritabanı erişiminde 2FA'yı etkinleştirin, dosyaları şifreleyin ve personeli oltalama tespit konusunda eğitin.
    - Fidye yazılımı: Güvenli bir buluta haftalık yedeklemeler planlayın, güncellenmiş antivirüs yazılımı yükleyin.
  - Gönüllü Kayıtları:
    - Yetkisiz Erişim: Güçlü şifreler kullanın, erişimi yetkili personelle sınırlandırın ve izinleri aylık olarak denetleyin.
    - Dizüstü Bilgisayar Hırsızlığı: Cihaz şifrelemesini etkinleştirin, kaybolan cihazlar için uzaktan silme araçlarını kullanın.

7. Adım: Gözden Geçirme ve Güncelleme

- Yapılması gerekenler: Bir ekip üyesini, risk değerlendirmesini yıllık olarak veya önemli değişikliklerden sonra (ör. yeni yazılım, personel değişiklikleri) gözden geçirmekle görevlendirin. Şablonu gerektiği gibi güncelleyin.
- Nasıl yapılır: Varlıklar, tehditler veya hafifletme adımlarında değişiklik olup olmadığını kontrol etmek için bir inceleme toplantısı planlayın. Planın geçerliliğini korumak için güncellemeleri belgelendirin.

  Örnek: 2FA uygulandıktan sonra, gönüllü kayıtlarına yetkisiz erişim olasılığı 2'ye düşer ve risk puanı 8'e iner. Şablonu buna göre güncelleyin.

2.3 BÖLÜM – 3: CSO'LAR İÇİN DİJİTAL GÜVENLİK PLANLARI

CSO'lar için Dijital Güvenlik Planı

Bireysel uygulamaları ele aldıktan sonra, daha geniş bir kurumsal yaklaşıma geçiyoruz. Dijital güvenlik planı, CSO'nuzun dijital varlıklarını nasıl koruyacağı ve tehditlere nasıl yanıt vereceği konusunda stratejik ve operasyonel bir yol haritasıdır. Karmaşık veya uzun bir belge olması gerekmez. Aslında, herkesin anlayabileceği kısa ve öz bir plan, rafta tozlanacak hacimli bir politikadan genellikle daha iyidir. Bu bölüm, **dört temel unsura** odaklanarak temel bir güvenlik planı oluşturmanıza rehberlik eder**:** – Risklerinizi tanımak,

– Uygun önlemlerle planı formüle etmek,

– Eğitim yoluyla farkındalık oluşturmak,

– Yedekleme ve güvenli depolama yoluyla verilerinizi koruma.

Riskleri Tanımak: Kuruluşunuz Hangi Tehditlerle Karşı Karşıya?

Her kuruluş, faaliyetlerine, verilerine ve rakiplerine bağlı olarak kendine özgü bir risk profiline sahiptir. Bir güvenlik planı geliştirmenin ilk adımı, **bu riskleri belirlemek ve değerlendirmektir** – esasen, basit bir dijital risk değerlendirmesi yapmaktır. Bunun için ileri düzeyde bir eğitim gerekmez; sistematik olarak neyin ters gidebileceğini ve bunun operasyonlarınıza ne kadar zarar verebileceğini düşünmek yeterlidir.

Varlıklarınızı ve Verilerinizi Belirleyin: CSO'nuzun sahip olduğu önemli dijital varlıkları ve bilgileri listeleyerek başlayın. Bunlar arasında şunlar bulunur: donanım (bilgisayarlar, telefonlar, sunucular), yazılım ve hizmetler (e-posta hesapları, web siteleri, bulut sürücüler, veritabanları) ve veriler (üye listeleri, finansal kayıtlar, araştırma verileri, iletişimler vb. Şu tür sorular sorun: Hangi veriler kamuya açıklanırsa en fazla zarara yol açar? Günlük çalışmalarımız için hangi sistemler kritik öneme sahiptir? Örneğin, hukuki yardım sağlayan bir CSO, (gizlilik nedeniyle) koruması gereken kritik varlıklar olarak müşteri dosyalarına ve avukatlarla iletişime öncelik verebilir. Bir geliştirme CSO'su, bağışçı veritabanını ve saha araştırma verilerini hayati öneme sahip olarak belirleyebilir. "En değerli varlıklarınızın" neler olduğunu bilmek, güvenlik çabalarınızı odaklamanıza yardımcı olacaktır.

Potansiyel Tehditleri ve Tehdit Aktörlerini Belirleyin: Ardından, kuruluşunuzun dijital altyapısına zarar vermek isteyebilecek kişi veya kurumları düşünün. Bazı yaygın tehditler ayrım gözetmez; örneğin, kâr amacıyla fidye yazılımı yayan rastgele siber suçlular, herkesi vurabilir.

Diğerleri ise daha hedefli olabilir: belki de savunuculuğunuzu desteklemeyen şirketler veya kişiler, hatta hassas konularda çalışıyorsanız, hükümetin gözetlemes . Tehdit kategorilerini listeleyin: finansal kazanç peşinde olan hackerlar, kazara veya kasıtlı olarak güvenliği tehlikeye atabilecek içeriden kişiler (personel veya gönüllüler) ve bağlamınıza özgü tehditler (örneğin, yolsuzluğa karşı kampanya yürüten bir CSO, etkilenen tarafların hedefli kimlik avı veya telefon hackleme girişimlerine maruz kalabilir). Ayrıca, ekipman hırsızlığı veya afetler (sel, yangın - bunlar da BT kesintilerine neden olabilir, bu nedenle tesis dışında yedeklemeler gereklidir) nedeniyle dijital varlıklara yönelik fiziksel tehditleri de göz önünde bulundurun.

Her tehdit için olası senaryoları düşünün: Bu tehdit *nasıl* ortaya çıkabilir? Örneğin:

- Bir siber suçlu, web sitenizi tahrip etmek veya kötü amaçlı yazılım dağıtmak için hacklemeye çalışabilir.
- Düşmanca bir aktör, şifreleri çalmak ve e-postalarınızı okumak için çalışanlarınıza kimlik avı e-postaları gönderebilir.
- Önceki bölümlerde tartışıldığı gibi, fidye yazılımı gibi kötü amaçlı yazılımlar bir personel bilgisayarını enfekte edebilir, dosyaları şifreleyebilir ve fidye talep edebilir.
- Bir gönüllü, şifrelenmemiş hassas veriler içeren bir dizüstü bilgisayarı kaybedebilir.
- Memnuniyetsiz bir eski çalışan, işten ayrılma işlemi düzgün yapılmamışsa hesaba erişmeye devam edebilir ve bu da veri hırsızlığı veya sabotaj riski oluşturur.

Olasılık ve Etkiyi Değerlendirin: Tüm riskler eşit değildir. Bazı olaylar çok düşük olasılıklı olsa da meydana geldiğinde felaketle sonuçlanabilirken, diğerleri olasılığı yüksek ancak etkisi düşük olabilir. Tanımlanan her risk senaryosu için, gerçekleşme olasılığını (düşük, orta, yüksek) ve gerçekleşmesi durumunda etkisini (düşük, orta, yüksek etki) değerlendirin. Örneğin, *kimlik avı saldırıları* çok olasıdır (yüksek olasılık) ve yüksek etkiye sahip olabilir (hesap kimlik bilgileri çalınırsa) – bu nedenle, güçlü önlemler alınması gereken yüksek bir risktir. Öte yandan, *donanım arızası* zamanla oldukça olasıdır (sonunda bir disk arızalanır), ancak yedeklemeleriniz varsa, etkisi düşüktür, bu nedenle yedeklemelerle yönetebileceğiniz orta düzeyde bir risktir. Ya da *devlet destekli hedefli hackleme* yüksek etkiye sahip olabilir (derinlemesine zarar verebilirler),

ancak yüksek profilli kampanyalarınız olmayan küçük bir yerel CSO iseniz, olasılık düşük olabilir – yine de bir miktar koruma gerektirir, ancak birinci önceliğiniz değildir.

Bu tür niteliksel değerlendirmeler önceliklerinizi belirlemenize yardımcı olur. CSO odaklı bir kılavuzda belirtildiği gibi, siber riskleri anlamak ve neyin korunması gerektiğini bilmek, etkili güvenlik için atılması gereken ilk adımlardır. Liberties'in kılavuzunda olduğu gibi bunları soru olarak da ifade edebilirsiniz: "En önemli dijital varlıklarımız nelerdir? Kimler bunları saldırmaya çalışabilir ve neden? X varlığı ihlal edilirse veya kullanılamaz hale gelirse ne olur?" Ekibinizi bu beyin fırtınasına dahil edin – farklı personel farklı endişeleri vurgulayabilir (örneğin, finans sorumlusu banka hesabı kimlik bilgileri konusunda endişelenirken, iletişim sorumlusu sosyal medyanın hacklenmesinden endişe duyabilir, vb.

Yasal ve Uyum Risklerini Dikkate Alın: CSO'lar ayrıca veri koruma yasaları gibi düzenlemeleri de dikkate almalıdır. Örneğin AB'de GDPR, kuruluşların kişisel verileri korumalarını ve ihlalleri bildirmelerini gerektirir. Dolayısıyla, yetersiz güvenliğin bir riski, yasal uyumsuzluk ve para cezalarıdır. CSO'nuz bağışçıların veya yararlanıcıların kişisel bilgilerini işliyorsa, bir ihlal gizlilik yasalarının ihlali anlamına gelebilir. Bu nedenle, risk düşüncesine uyumluluğu da dahil edin – örneğin, "Kişisel veri sızıntısı riski – etkisi, bireylere zarar + yasal cezalar." Bu riskin etkisi açıkça yüksek olacaktır ve çok sayıda kişisel veriniz varsa, belki de orta derecede olasılık, güçlü kontroller gerektirecektir.

Riskleri Belgelendirin ve Sıralayın**:** Kısa bir risk kaydı yazın – basit bir risk senaryoları, olasılık, etki ve mevcut önlemler tablosu bile olabilir. Bunları risk düzeyine göre (olasılık ve etkinin bir kombinasyonu) sıralayın. Bu, kaynakların nereye tahsis edileceğine rehberlik edecektir. Örneğin, "Hesap güvenliğini tehlikeye atan kimlik avı saldırısı"nı en yüksek risk olarak sıralayabilirsiniz, ancak siteniz tartışmalı değilse ve bulut korumalarına sahipse "web sitesine DDoS saldırısı" daha düşük bir risk olabilir. Ya da "Google Drive bağlantısı üzerinden içerdekilerin kazara veri sızdırması" eğitim ve erişim kontrolleriyle ele alınabilecek orta düzeyde bir risk olabilir.

Risk İştahı: *Hiçbir kuruluşun tüm riskleri ortadan kaldıramayacağını* kabul etmek de önemlidir. Risk yönetiminin bir parçası, kaynaklarınızı göz önünde bulundurarak hangi risk düzeyinin kabul edilebilir olduğuna karar vermektir. Buna genellikle "risk iştahı" denir. Küçük bir

CSO, 7/24 çalışan bir BT güvenlik ekibine sahip olmama riskini kabul edebilir ve bunun yerine temel savunma önlemlerine ve gerektiğinde dış desteğe odaklanabilir. Amaç, riskleri sizin için uygun bir düzeye indirmektir. Yüksek riskler için güçlü önlemler alırsınız; daha düşük riskler için ise daha temel önlemler alırsınız veya bunları zaman içinde izlersiniz.

Bu risk tanıma aşamasının sonunda, durumunuzu daha net bir şekilde görebilmelisiniz. Örneğin, şu sonuca varabilirsiniz: *En büyük güvenlik açıklarımız, kimlik avı ve zayıf parolalar (yüksek risk), ayrıca web sitemizdeki eski yazılımlar (orta risk) ve gönüllülerimizin düşük farkındalık düzeyidir (risklere katkıda bulunur). Kayıp cihazlardan kaynaklanan orta düzeyde bir riskimiz var (bazen dizüstü bilgisayarları paylaşıyoruz), ancak şifrelemeyi etkinleştirirsek bu risk azalabilir. Muhtemelen ulus devletler tarafından özel olarak hedef alınmıyoruz, ancak gizli tutulması gereken hassas topluluk bilgilerini işliyoruz.* Bu bilgiler, güvenlik planınızı oluşturmak için zemin hazırlar. Esasen, plan bu belirlenen riskleri uygun önlemlerle ele alacaktır.

Kuruluşunuzun dijital zayıf noktalarını ve bunları en çok istismar etme olasılığı yüksek tehditleri bilerek, savunmanızı verimli bir şekilde planlayabilirsiniz. Bu yaklaşım, siber güvenlik çerçevelerinde önerilen temel bir ilke olan risk temelli karar verme kavramıyla uyumludur. Her şeyi her yerde yapmaya çalışmak yerine, en önemli konulara odaklanmanızı sağlar. Şimdi, bu risk tablosunu göz önünde bulundurarak, bu riskleri azaltmak için politikalar ve uygulamaları kapsayan bir plan oluşturmaya geçelim.

Basit Bir Dijital Güvenlik Planı Oluşturma

Risklerinizi belirledikten sonra, bir sonraki adım bu riskleri yönetmek ve azaltmak için bir plan oluşturmaktır. Bir CSO için dijital güvenlik planı genellikle ana risk alanlarını ele alan politikalar, prosedürler ve kontroller ile rol ve sorumlulukların ana hatlarını içerir. "Plan" terimi sizi korkutmasın; bu, bir kontrol listesi veya kısa bir belge kadar basit olabilir. Önemli olan, planın pratik olması ve kuruluşunuzun büyüklüğüne ve ihtiyaçlarına göre uyarlanmış olmasıdır.

Güvenlik Politikası ve Yönetişim: Öncelikle bazı kılavuz politikalar belirleyin. Bu, kuruluşun dijital güvenliğe olan bağlılığını ve herkesin uyması gereken temel kuralları belirten kısa bir bölüm olabilir. Örneğin, bir Şifre Politikası (ör. tüm kritik hesaplarda belirli uzunlukta güçlü şifreler ve 2FA gerektirme – ayrıntılar için Bölüm 2.1'e bakabilirsiniz), kabul edilebilir

kullanım politikası (ör. iş cihazlarını ve interneti uygun amaçlarla kullanma, yetkisiz yazılım yüklememe vb.) ve bir Veri Koruma Politikası (örneğin, kişisel verilerin işlenmesine ilişkin kurallar, GDPR gibi yasal gerekliliklere uyma ve verilerin hassasiyetine göre sınıflandırma) oluşturun. ENISA, çalışanlara, ICT kaynaklarıyla nasıl davranmaları beklendiğini ve uyulmaması durumunda ne gibi sonuçlar doğacağını özetleyen açık siber güvenlik politikalarının yazılması ve iletilmesi gerektiğini tavsiye etmektedir. Örneğin, politikanızda, çalışanların hesap şifrelerini paylaşmamaları ve şüpheli kimlik avı girişimlerini derhal BT irtibat noktasına bildirmeleri gerektiği belirtilebilir.

CSO'nuz küçükse, birçok şeyi tek bir genel politika belgesinde toplayabilirsiniz – bu sorun değildir. Önemli olan sorumluluğu atamaktır. Ekibinizde güvenlik denetiminden kimin sorumlu olacağına karar verin (bu, bir yönetici direktör veya "güvenlik sorumlusu" olacak teknoloji konusunda bilgili bir çalışan olabilir). ENISA'nın KOBİ kılavuzunda, siber güvenlik için yönetim sorumluluğunun atanmasının başarının temel unsurlarından biri olduğu belirtilmektedir. Bu nedenle, bir rolü açıkça belirtin: örneğin, "Operasyon Müdürü, güvenlik çabalarını koordine etmek ve politikaların uygulanmasını sağlamakla sorumlu Bilgi Güvenliği Sorumlusu olarak görev yapacaktır." Bir yönetim kurulunuz veya liderlik ekibiniz varsa, bu planı onayladıklarından emin olun – liderlik desteği, herkesin desteğini almak için çok önemlidir.

Risk Yönetimi Eylemleri: Belirlenen her bir büyük risk için (3.1'den), bu riskle ilgili ne yapacağınızı özetleyin. Bu, planınızın temelini oluşturur:

- Örneğin, "oltalama" en büyük risk ise, planınız e-postada 2FA'yı uygulamak (daha önce tartışıldı), oltalama farkındalık eğitimi vermek (bkz. 3.3) ve olağandışı talepleri doğrulamak için prosedürler oluşturmak (finansal işlem onay süreci gibi) gibi eylemleri içerebilir.
- "Eski yazılım" bir riskse, planınızda önemli yazılımların envanterini tutmak ve güncellemeler için bir program veya sorumluluk belirlemek (belki güvenlik sorumlusu veya harici BT desteği aylık güncellemeleri sağlar) yer alacaktır.
- "Kişisel bilgilerin veri ihlali" riski tespit edildiğinde: bu verilere erişimi kısıtlama (yalnızca belirli kişiler hassas klasörlere erişebilir), özellikle hassas dosyalar için şifreleme kullanma ve olay müdahale prosedürü oluşturma (ihlal durumunda,

nasıl kontrol altına alınacağı ve bildirileceği - daha fazla bilgi için 5. Bölüm'e bakın) gibi önlemler planlayın.

- "Cihaz kaybı" riski varsa: belirtildiği gibi tam disk şifreleme ve uzaktan silme planlayın, ayrıca paylaşılan cihazlar için cihaz giriş/çıkış günlüğü de ekleyebilirsiniz.

Olay Müdahale Planı: İyi bir plan, basit olsa bile, işlerin ters gidebileceğini öngörür. Bu nedenle, temel bir olay müdahale prosedürü ekleyin: bir siber güvenlik olayı meydana geldiğinde (kötü amaçlı yazılım bulaşması, şüpheli hackleme vb.), personel kime rapor vermeli ve hangi adımları atmalısınız? Bölüm 5 bu konuyu ayrıntılı olarak ele almaktadır, ancak planınızda sadece rolleri özetleyin: örneğin, "Tüm personel, şüpheli güvenlik olaylarını derhal [Ad/Rol]'a bildirmelidir. Etkilenen bilgisayarları ağdan izole edeceğiz, kapsamı değerlendireceğiz ve gerekirse [BT desteği veya harici uzman] ile iletişime geçeceğiz. Ayrıca, yönetimi bilgilendireceğiz ve kişisel veriler söz konusuysa, yasaların gerektirdiği şekilde etkilenen tarafları ve yetkilileri bilgilendirmeye hazırlayacağız." Bunu yazılı olarak belirtmek, kriz anında takip edebileceğiniz bir referansınız olması anlamına gelir, bu da değerli zaman kazanmanızı ve paniği azaltmanızı sağlar.

Erişim Kontrolleri ve Hesap Yönetimi: Plan, kullanıcı hesaplarını ve erişimi nasıl yöneteceğinizi tanımlamalıdır. Bu, hangi sistemlere kimin erişimi olduğunu gösteren bir liste tutmayı, en az ayrıcalık ilkesini kullanmayı (kişilere yalnızca ihtiyaç duydukları erişimi vermeyi) ve, daha da önemlisi, personel/gönüllülerin işe alım ve işten ayrılma prosedürlerini içerebilir. Örneğin, bir kişi kuruluştan ayrıldığında, planınız hesaplarının derhal devre dışı bırakılmasını veya şifrelerinin değiştirilmesini sağlamalıdır. Birçok güvenlik olayı, eski çalışanların veya ortakların hala aktif kimlik bilgilerine sahip olması nedeniyle meydana gelir. "Personel ayrıldığında, BT departmanı 24 saat içinde e-posta, bulut sürücüler ve paylaşılan şifrelere erişimi iptal edecektir" gibi adımları plana dahil edin. Paylaşılan hesaplar veya genel oturum açma bilgileri kullanıyorsanız (bunları en aza indirmeye çalışın), bu şifreleri düzenli olarak veya bilgisi olan bir kişi ayrıldığında değiştirmek için bir planınız olsun.

Üçüncü Taraf Yönetimi: Güvenliğinizin, kullandığınız üçüncü taraf hizmetlerine veya yüklenicilere de bağlı olduğunu unutmayın. "Satıcıları" bir risk olarak belirlediyseniz (örneğin, dış kaynaklı BT desteği veya veritabanınızı barındıran bir bulut sağlayıcısı), bunu yönetmek için

önlemler ekleyin. ENISA'nın kılavuzunda, hassas verilere erişimi olan tüm satıcıların güvenlik gereksinimlerini karşıladığından emin olunması ve güvenlik konusunda sözleşme anlaşmaları yapılması önerilmektedir. Basit bir planda bu, kullandığınız tüm bulut hizmetlerinin saygın ve veri koruma standartlarına uygun olduğunu ve gerektiğinde bunlardan bağımsız yedeklemelerinizin olduğunu doğrulamak anlamına gelebilir. Ayrıca, bir web geliştiricisi veya BT danışmanı işe alırsanız, güvenlik politikalarınızı (örneğin, kimlik bilgilerinizi başka yerlerde yeniden kullanmamak veya verileri gizli tutmak gibi) takip etmeyi kabul eden bir sözleşme imzalamalarını sağlayın.

Temel Kontroller Uygulayın: Uygulayacağınız somut kontrolleri özetleyin (bazıları Bölüm 2'deki ipuçlarıyla örtüşür, ancak burada bunları resmileştirirsiniz):

- **Cihaz Güvenliği**: "Tüm kuruluş dizüstü bilgisayarlarında antivirüs ve güvenlik duvarı etkinleştirilecek ve tam disk şifreleme (BitLocker/FileVault) açılacaktır. Otomatik ekran kilidi, 10 dakika hareketsizlik durumunda devreye girecek şekilde ayarlanacaktır."
- **Parola Güvenliği**: "Parola politikasını uygulayın: en az 12 karakter, yaygın kelimeler kullanmayın, her hesap için benzersiz olsun. Parola yöneticisi kullanımı teşvik edilir ve personel için kurulacaktır. Kritik hesaplarda (e-posta, finans sistemleri vb.) 2FA etkinleştirilecektir."
- **Veri Yedekleme**: “Kritik veriler (ör. bağışçı veritabanı, program dosyaları) haftalık olarak [güvenli bulut/şifreli harici sürücü]'ye yedeklenecektir. Test geri yüklemeleri üç ayda bir yapılacaktır.”
- **Güvenli Yapılandırma**: “Tüm ekipmanlarda varsayılan şifrelerin değiştirildiğinden emin olun. Web sitemizdeki gereksiz hizmetleri devre dışı bırakın ve güncel tutun. Fazla yönetici haklarını kaldırmak için kullanıcı ayrıcalıklarını düzenli olarak gözden geçirin.”
- **Aktarımdaki Veriler için Şifreleme**: “Hassas iletişim için şifreli kanallar kullanın (örneğin, gizli mesajlaşma için Signal veya mümkünse belirli kişiler için PGP e-posta). Web sitemiz SSL sertifikasına (HTTPS) sahiptir ve kullanıcı gönderimlerinin şifrelenmesi için bu sertifikanın kullanımını zorunlu kılacağız.”

Kontrolleri listelerken, çok genel veya ölçülmesi imkansız ifadelerden kaçının ("Tüm saldırıları önleyeceğiz" – gerçekçi değil). Bunun yerine, uygulanabilir kontrollere odaklanın. Bir çerçeveyi kontrol listesi olarak kullanmak yardımcı olabilir – örneğin, CIS Kontrolleri (popüler bir temel siber uygulamalar listesi) veya ISO 27001 alanları ilham kaynağı olabilir. Ancak bunu uygulayabileceğiniz şekilde uyarlayın.

Zaman çizelgesi ve bakım: Planın ne sıklıkla gözden geçirileceğini ve kimin bakımını yapacağını belirtin. Teknoloji ve tehditler gelişir, bu nedenle "Bu güvenlik planı [Rol] tarafından yıllık olarak (veya BT sistemimizde önemli bir değişiklik olduğunda) gözden geçirilecek ve güncellenecektir" gibi bir ifade kullanabilirsiniz. Ayrıca, uygulamaya geçerken her şeyi bir kerede yapmayabilirsiniz. Eylemleri aşamalı olarak önceliklendirmek sorun değildir. Planınızda, acil adımları özetlediğiniz bir "Eylem Planı" bölümü olabilir (ör. 1 ay içinde e-postada 2FA'yı etkinleştirin, gelecek ay eğitim planlayın, 3. çeyrekte yedeklemeleri uygulayın vb.). Bu, planı sadece bir politikadan, son tarihleri olan bir projeye dönüştürür.

İletişim ve Uygulama: Bir plan, ancak insanlar onu bilir ve uygulanırsa işe yarar. Taslak hazırlandıktan sonra, tüm personel ve gönüllülerle paylaşın. Belki de kısa bir toplantı düzenleyerek önemli noktaları açıklayın ("artık bir politikamız var, bunun günlük işleriniz için anlamı şudur"). Geri bildirim alın – belki birisi bir eksiklik görür veya bir önerisi olur. Plana veya ek materyallere, uyulmamasının sonuçlarını dostane bir şekilde ekleyin – örneğin, "Politikalar takip edilmezse, disiplin cezası ile sonuçlanabilir, ancak eğitim ve kaynaklar aracılığıyla herkesin bu en iyi uygulamaları gerçekleştirmesini desteklemeyi amaçlıyoruz." Bu, güvenliğin sadece BT'nin işi değil, herkesin işinin bir parçası olduğu mesajını verir. CyberPeace Institute'tan iyi bir benzetme: siber güvenliği izole bir BT gideri olarak değil, misyonunuzu gerçekleştirmenizi sağlayan bir **araç** olarak değerlendirin. Güvenliği günlük süreçlere dahil ederek, operasyonlarınızda sürekliliği ve güveni sağlarsınız.

Örnek olarak, küçük bir çevre CSO'sunun güvenlik planından bir alıntı düşünün:

- **Risk**: Personel e-postalarının kimlik avı – **Azaltma**: e-posta için zorunlu 2FA, kimlik avını tanıma eğitimi (BT gönüllüsü tarafından verilir) ve şüpheli e-postalar için raporlama protokolü oluşturma.

- **Risk**: Saha dizüstü bilgisayarlarının kaybolması – **Azaltma**: tam disk şifreleme etkinleştirme, internet mevcut olduğunda günlük veri senkronizasyonu, cihaz kilit kodları.
- **Risk**: Web sitesi tahribatı – **Azaltma**: web barındırıcı tarafından düzenli güncellemeler, güvenlik eklentisi veya hizmeti kullanımı, site içeriğinin yedeklenmesi, hacklenme durumunda hızlı geri yükleme planı.
- **Politika**: Tüm yeni gönüllüler temel güvenlik oryantasyonu almalı ve ICT kullanım sözleşmesini imzalamalıdır (hesap paylaşmama vb. konularını kapsar).
- **Sorumluluk**: Bu eylemleri izlemek ve yönlendirmek üzere Jane Doe (Program Yöneticisi) güvenlik koordinatörü olarak atanmıştır.

Eylemleri risklere göre eşleştirerek ve kimin ne yapacağını belirleyerek, planınız uygulanabilir hale gelir. Planınız sadece birkaç sayfa uzunluğunda olabilir, ancak bu sorun değildir. Kısa ve öz olması, net olduğu sürece etkili olabilir. Aslında, ENISA'nın KOBİ kılavuzu, tavsiyeleri işletmeler için mini bir plan görevi gören 12 üst düzey adıma indirger ("İyi bir siber güvenlik kültürü geliştirin – sorumlulukları atayın", "Olaylar için plan yapın" ve "Yedeklemeleri güvence altına alın" gibi). Bunların çoğu burada da yer almaktadır.

Planlamanın son aşaması, bu önlemleri uygulamak ve farkındalığı artırmaktır, bu da bizi bir sonraki bölüme götürür. Planın bileşenlerinden biri genellikle eğitim ve kültür olduğu için, bu konuları tartışırken taslak planınızı elinizin altında bulundurun.

Personel ve Gönüllüler için Farkındalık Eğitimi

Kağıt üzerinde en iyi güvenlik planı bile, kuruluşun çalışanları bu plana destek vermezse veya yeterli bilgiye sahip değilse başarısız olabilir. İnsan davranışı, dijital güvenlikte kritik bir faktördür. Daha önce de belirtildiği gibi, ihlallerin önemli bir çoğunluğu insan unsurunu (hatalar veya sosyal mühendislik) içerir. Bu nedenle, ekibinizi eğitmek ve güvenlik bilinci kültürü oluşturmak, yapabileceğiniz en etkili şeylerden biridir. Personeliniz ve gönüllülerinizin ilk savunma hattı olduğunu (veya tersine, eğitilmedikleri takdirde en zayıf halka olduğunu) düşünün. Bu bölümde, CSO bağlamında etkili güvenlik farkındalığı eğitiminin nasıl oluşturulacağı ve sürdürüleceği özetlenmektedir.

Temel bilgilerle başlayın: Eğitim aşırı teknik olmak zorunda değildir. Aslında, genellikle temel yapılması ve yapılmaması gerekenler, gerçek örnekler ve etkileşimli tartışmalara odaklanmak daha iyidir. İnsanların anlayabileceği şekilde yaygın tehditleri ele alın. Örneğin, bir kimlik avı e-postasının neye benzediğini gösterin (eğitim için temizlediğiniz gerçek bir kimlik avı e-postasını gösterebilirsiniz) ve insanlara kırmızı bayrakları (kötü gramer, garip gönderen adresi, beklenmedik ekler vb.) göstermelerini isteyin. Bir senaryoyu tartışın: "Müdürünüzden acil bir para transferi isteyen bir e-posta alırsanız ne yapmalısınız?" (Cevap: Harekete geçmeden önce her zaman telefonla veya yüz yüze doğrulayın, çünkü bu bir CEO dolandırıcılığı olabilir). Bu pratik alıştırmalar, personelin bir saldırının nasıl gerçekleşebileceğini ve nasıl sakin bir şekilde tepki verebileceğini anlamasına yardımcı olur. ENISA, eğitimin KOBİ'lerin karşılaştığı **gerçek hayattaki durumlara** odaklanmasını önerir; bu, CSO'lar için de geçerlidir. Yetişkin öğrenciler, soyut kurallardan çok senaryolar ve hikayeler aracılığıyla kavramları daha iyi kavrarlar.

Dahil Edilmesi Gereken Ana Konular: En azından, eğitim formunda Bölüm 2'deki konuları ele alın:

- Güvenli şifre uygulamaları ve şifre yöneticilerinin kullanımı.
- 2FA'yı etkinleştirme ve kullanma (belki de bir kimlik doğrulama uygulamasını kurmanın canlı demosu).
- Oltalama e-postalarını, şüpheli bağlantıları tanıma ve ne yapma gerektiği (tıklamayın, bildirin).
- Hassas bilgilerin doğru şekilde ele alınması (ör. gizli veriler için şifreli araçlar kullanmak, iş içeriği için kişisel e-posta kullanmamak vb.
- Cihaz güvenliği: güncellemelerin önemi, yetkisiz uygulamaları yüklememe, ekranları kilitleme ve USB sürücülerine dikkat etme (bilinmeyen USB bellekler tehlikeli olabilir).
- Sosyal medyada dikkatli olunması: Facebook/Twitter'da işle ilgili hassas bilgileri aşırı paylaşmamak, sosyal mühendisliğe karşı dikkatli olmak (örneğin, IT desteği gibi davranan birinin araması).
- Olayları bildirme: Suçlamama kültürünü vurgulayın. İnsanlar, kötü bir şeye tıkladıklarında veya bir cihazı kaybettiklerinde bunu saklamak yerine rahatça

bildirmelidir. Hemen bildirimde bulunmanın çok önemli olduğunu ve dürüst bir hata yaptıkları için cezalandırılmayacaklarını açıkça belirtin – öncelikli olan sorunu çözmektir.

Etkileşimli ve OCSO eğitimi: Farkındalık tek seferlik bir olay değildir. Yenileme oturumları veya en azından periyodik hatırlatmalar planlayın. Birçok kuruluş yıllık güvenlik eğitimi düzenler. Ancak bu eğitimler arasında, personel toplantılarında ipuçları paylaşabilir veya "ayın güvenlik ipucu" e-postası gönderebilirsiniz. Örneğin, Ekim ayında (AB'de ENISA tarafından sıklıkla tanıtılan Siber Güvenlik Farkındalık Ayı), eğlenceli bir quiz düzenleyebilir veya güvenlikle ilgili kısa bir video paylaşabilirsiniz. Eğitim sıkıcı olmak zorunda değildir. Bazı CSO'lar bir güvenlik uzmanını davet eder veya ücretsiz çevrimiçi modüller kullanır (kar amacı gütmeyen kuruluşlar ve küçük işletmelere yönelik birçok ücretsiz siber güvenlik farkındalık kursu ve videosu vardır).

Dış kaynaklardan da yararlanmayı düşünün: Bir BT ortağınız varsa veya yerel bir teknoloji üniversitesi varsa, bazen bunlar atölye çalışması düzenlemenize yardımcı olabilir. Sivil topluma ücretsiz siber farkındalık atölyeleri sunan kar amacı gütmeyen girişimler de vardır (örneğin, TechSoup veya CyberPeace Builders gibi kuruluşların gönüllüleri eğitimlerin düzenlenmesine yardımcı olabilir).

Önemli Roller için Özel Odak: Eğitimin bazı kısımlarını rollere göre uyarlayın. Finans sorumlusunuz, fatura sahtekarlığını tespit etme veya banka giriş bilgilerini güvence altına alma konusunda daha derinlemesine eğitime ihtiyaç duyabilir (çünkü CSO'lar sahte faturalar veya "CEO kimliğine bürünme" e-postaları yoluyla dolandırıcılar tarafından dolandırılmıştır). Sosyal medyayı yöneten iletişim personeliniz, hesap ele geçirmelerini önlemek için ipuçlarına ihtiyaç duyabilir (2FA kullanmak ve kimlik avı DM'lerine karşı dikkatli olmak gibi). Liderlik de kendi rolünü anlamalıdır – yöneticiler genellikle spear phishing ("patron" e-posta hilesi) hedefidir, bu nedenle iyi davranışları örnek almalıdırlar (örneğin, doğrulama yapmadan e-posta ile hassas bilgi veya transfer talep etmemek gibi). Ayrıca, gönüllüler veya kısa süreli çalışanların resmi personel eğitimine katılmayabilecekleri için, en azından güvenlik konusunda mini bir oryantasyon eğitimi almalarını sağlayın. Katıldıklarında "yapılması ve yapılmaması gerekenler" hakkında bir sayfalık bir hile sayfası veya hızlı bir brifing yardımcı olabilir.

Sorgulama Kültürü Oluşturun: Herkesi, garip görünen şeyleri sorgulamanın sorun olmadığını teşvik edin. Örneğin, bir gönüllü, emin olmadığı alışılmadık bir BT talimatı alırsa, soru sormalıdır. Kime soru soracaklarını bilmelerini sağlayın – örneğin, "Şüpheli bir iletişim alırsanız veya bir dosya veya bağlantıdan emin değilseniz, [iletişim] adresinden BT irtibat noktamızla (veya güvenlik koordinatörümüzle) iletişime geçin." Bu, Microsoft'un tavsiyesine geri dönüyor: siber güvenlik bir *takım sporudur* ve bir şey görürseniz, güvenilir bir danışmana bildirin. Birisi, kötü bir bağlantıya tıklamak gibi bir güvenlik hatası yaptığını düşünüyorsa, suçlanmaktan korkmak yerine bunu hemen bildirmekten çekinmemelidir. Hızlı tepki genellikle zararı önleyebilir veya en aza indirebilir (örneğin, kötü amaçlı yazılım şüphesi varsa bilgisayarı kapatmak gibi).

Ölçme ve Güçlendirme: Eğitiminizin ne kadar etkili olduğunu ölçmek faydalıdır. Bunun bir yolu, kaynaklar izin veriyorsa, iç phishing testleri yapmaktır: eğitimden sonra personele zararsız bir "sahte phishing" e-postası göndererek kimin tıkladığını görmek. Tıklayanlar, hafif bir takip eğitimi alabilir. Ancak çok küçük bir kuruluşsanız, gayri resmi soru-cevap ve tartışmalar, anlayışı ölçmek için yeterli olabilir. Hatta personel toplantısında "Tanımadığınız birinden e-posta eki alırsanız ne yaparsınız?" diye sormak ve yanıtları dinlemek, kavrayış düzeyini ortaya çıkarabilir. Ofis ilan panosuna veya Slack kanalına kısa bir güvenlik ipuçları listesi asarak mesajları pekiştirin. Bazı kuruluşlar, güvenliği personel performans değerlendirmelerine veya rutinlerine bile dahil eder ("Yıllık güvenlik sınavını tamamladınız mı?"). Ancak CSO'larda, son derece hassas verilerle çalışmıyorsanız, daha hafif bir yaklaşım genellikle yeterlidir.

Bilgi sahibi olun ve güncellemeleri paylaşın: Tehdit ortamı sürekli değişir. Yeni bir tehdit fark ederseniz, ekibinizi bilgilendirin. Örneğin, bir CSO meslektaşınız sektörünüzdeki kuruluşları hedef alan bir kimlik avı kampanyası bildirdiyse, çalışanlarınızı uyarın: "Dikkatli olun, bir fon sağlayıcıdan geldiğini iddia eden kimlik avı e-postaları dolaşıyor. Bu tür e-postalara tıklamayın ve böyle bir e-posta alırsanız bize bildirin." CSO ağlarının veya güvenlik bilgisi paylaşım gruplarının bir parçası olmak (, Bölüm 6'da göreceğimiz gibi), aktarabileceğiniz bu tür bilgiler sağlayabilir. Bu, güvenlik farkındalığını güncel tutar ve personele tehditlerin sadece teorik değil, gerçek ve kendi ortamlarında meydana geldiğini gösterir.

Özetlemek gerekirse, farkındalık eğitimi, çalışanlarınızı potansiyel yükümlülüklerden güvenlik duruşunuzda varlıklara dönüştürür. Bir siber güvenlik sloganının da belirttiği gibi, "Çalışanlarınız

en iyi güvenlik duvarınızdır." Bilgiyi ve uyanık bir zihniyeti teşvik ederek, maliyetli hataların olasılığını büyük ölçüde azaltabilirsiniz. Unutmayın, teknoloji tek başına yeterli değildir – kullanıcı farkında olmadan saldırganı içeri alırsa, en güçlü güvenlik duvarı bile aşılabilir. Ancak, olumlu bir güvenlik kültürüyle desteklenen, iyi eğitimli bir ekip, birçok olayı başlamadan önce durdurabilir veya erken aşamada yakalayabilir. Bu insan faktörünün güçlendirilmesi, sivil toplum için dayanıklı dijital güvenliğin merkezinde yer alır.

Verilerinizi Koruma: Yedekleme ve Güvenli Depolama

Veriler genellikle kuruluşların "can damarı" olarak tanımlanır. Sivil toplum kuruluşları için veriler, yararlanıcı bilgileri, araştırma bulguları, bağışçı ayrıntıları, mali kayıtlar, proje raporları, fotoğraflar ve daha fazlasını içerebilir. Bu verileri korumak, yalnızca yetkisiz erişimi önlemekle (gizlilik) değil, aynı zamanda verilerin kaybolmamasını (kullanılabilirlik) ve uygunsuz şekilde değiştirilmemesini (bütünlük) sağlamakla da ilgilidir. Bu bölümde, veri korumanın iki temel yönüne odaklanacağız: düzenli yedekleme ve güvenli depolama (hem fiziksel hem de bulutta).

Yedeklemelerin Önemi: En kötü senaryoları düşünün: bir fidye yazılımı saldırısı tüm dosyalarınızı şifreliyor, bir yangın/sel ofis bilgisayarlarınızı yok ediyor veya bir stajyer yanlışlıkla önemli bir klasörü siliyor. Bu durumların her birinde, güncel bir yedeğinizin olması kuruluşunuzu kelimenin tam anlamıyla kurtarabilir. Yedekleme, gerektiğinde geri yükleyebileceğiniz, farklı bir ortamda (ve tercihen farklı bir konumda) tutulan verilerinizin ayrı bir kopyasıdır. Yedeklemeler olmadan, yukarıdaki senaryoların herhangi biri geri dönüşü olmayan bir kayıp anlamına gelebilir. Yedeklemelerle, bir güvenlik ağına sahip olursunuz.

İşte yedekleme için en iyi uygulamalar, bunların çoğu standart tavsiyelerle uyumludur:

Düzenli Sıklık: Önemli verilerinizi düzenli olarak yedekleyin. "Düzenli" terimi, verilerin ne sıklıkta değiştiğine ve ne kadar önemli olduğuna bağlıdır. Oldukça statik veriler için haftalık yedekleme yeterli olabilir; hızla değişen veriler (günlük program günlükleri veya aktif veritabanları gibi) için ise günlük veya hatta günde birden fazla yedekleme daha uygun olabilir. Kurtarma Noktası Hedefinizi (RPO) belirleyin: Ne kadar veri kaybını göze alabiliriz? Bir günlük veri kaybı ise, günlük yedeklemeler yeterlidir. Bir saatlik veri kaybının bile felaket anlamına geleceği durumlarda, daha sık anlık görüntüler almayı hedefleyin.

Otomatikleştirin: İnsanlara bağlı yedekleme süreçleri, unutkanlık veya yoğun programlar nedeniyle sıklıkla başarısız olur. Mümkün olduğunda otomatik yedekleme çözümleri kullanın. Örneğin, dosya sunucunuzu veya NAS'ınızı her gece saat 2'de harici bir sürücüye yedekleyecek şekilde ayarlayın. Veya sürekli veya programlı olarak çalışan bulut yedekleme hizmetlerini (Backblaze, Acronis vb.) kullanın. Google Drive veya OneDrive gibi birçok bulut depolama hizmeti, dosya düzenlemeleri veya silme işlemleri için bir tür yedekleme görevi görebilen dosyaların önceki sürümlerini de saklar.

Birden Çok Kopya ve Tesis Dışı: 3-2-1 kuralı gibi bir şeyi izleyin: 2 farklı ortamda 3 kopya veri (birincil + iki yedek), bunlardan 1'i tesis dışında. Bu, çok küçük bir CSO için aşırı olabilir, ancak fikir mantıklıdır. Örneğin, ofisteki harici bir sabit sürücüde bir yedek ve bir bulut hizmetinde başka bir şifreli yedek bulundurabilirsiniz. Tesis dışında olması, ofis yanarsa tesis dışındaki (veya buluttaki) yedeklemenin güvende olacağı anlamına gelir. Bulut yedeklemeleri doğası gereği tesis dışındadır. Fiziksel ortam kullanıyorsanız, bir sürücüyü yönetim kurulu üyesinin evinde veya bir kasa dairesinde saklamayı ve düzenli olarak güncellemeyi düşünün.

Yedeklemelerinizi Güvenli Hale Getirin: Yedekleme, hassas verilerinizin bir kopyasıdır, bu nedenle onu koruyun. Harici bir sürücü kullanıyorsanız, o sürücüyü şifreleyin (birçok yedekleme aracı veya Windows BitLocker gibi işletim sistemi harici diskleri şifreleyebilir). Bulut yedekleme kullanıyorsanız, hizmetin verileri şifrelediğinden emin olun (çoğu şifreler, ancak ekstra güvenlik için dosyaları yüklemeden önce şifrelemeyi de seçebilirsiniz). Yedeklere erişebilecek kişileri sınırlayın. Örneğin, yedekleme sürücüsünü çevrimiçi bir sisteme sürekli bağlı bırakmayın; fidye yazılımı saldırısı durumunda bu sürücü de şifrelenebilir. İdeal olarak, sürekli bağlı olmayan yedeklemeler (çevrimdışı yedeklemeler) ağınızdaki kötü amaçlı yazılımlara karşı bağışıklık kazanır. Yedeklemeler için ağ sürücüsü kullanıyorsanız, sürüm kontrolü veya kötü amaçlı yazılımların eski yedeklemeleri hemen bozamayacağı bir koruma önlemi olduğundan emin olun.

Geri yüklemeyi test edin: Yedeklemeler, gerektiğinde çalışmazsa bir anlam ifade etmez. Yılda en az birkaç kez geri yükleme sürecini test edin. Yedekten bir dosyayı kurtarmaya çalışın ve dosyanın doğru şekilde açılıp açılmadığını kontrol edin. Yangın tatbikatı yapın: "Ana paylaşımlı sürücümüz bozulursa ne olur? Dün geceki yedeği yeni bir cihaza kolayca geri yükleyebilir miyiz?"

Testler, bozuk yedekler, eksik şifreleme anahtarları veya iyileştirilmesi gereken prosedürler gibi sorunları ortaya çıkaracaktır. Birçok kuruluş, kriz anında yedeklemelerinin eksik olduğunu veya uzun zaman önce sessizce başarısız olduğunu fark etmiştir. Bunun size de olmasına izin vermeyin.

Yedekleme Prosedürlerini Belgelendirin: Neyin, nasıl ve nereye yedeklendiğini yazın. Ayrıca, yedeklemeleri denetlemekle ve kurtarmayı gerçekleştirmekle kimin sorumlu olduğunu da not edin. Örneğin: "Salesforce bağışçı veritabanımız, Salesforce'un kendi günlük dışa aktarımıyla ve ayrıca her ayın 1'inde John tarafından şifreli bir USB sürücüsüne manuel olarak dışa aktarılmasıyla yedeklenir." John ayrılırsa, başka biri bunu okuyabilir ve uygulamaya devam edebilir. Ayrıca, yedeklemeler için gerekli kimlik bilgilerini (tabii ki güvenli bir şekilde) belgelendirin, böylece acil bir geri yükleme sırasında şifreyi bulmak için uğraşmak zorunda kalmazsınız.

Güvenli Depolama ve Erişim Kontrolü: Yedeklemelerin ötesinde, verileri korumak aynı zamanda günlük kullanımda güvenli bir şekilde depolamak anlamına da gelir. Bu, hem fiziksel depolama (basılı dosyalar, USB sürücüler ve sunucular gibi) hem de bulut depolama çözümlerini içerir:

Fiziksel Dosyalar ve Cihazlar: Fiziksel formda hassas bilgileriniz varsa (kağıt belgeler, USB bellekler, harici sabit sürücüler), bunları kilitli dolaplarda veya kasada saklayın. Kişisel veriler içeren belgeleri masaların üzerinde bırakmayın. Örneğin, gönüllü kayıt formları veya yararlanıcı formları aktif olarak kullanılmadığında dosyalanmalıdır. Hassas belgeleri imha etmeden önce parçalayın. Cihazlar için, daha önce de belirtildiği gibi, tam disk şifreleme kullanın, böylece bir bilgisayar veya sürücü kaybolduğunda verilere kolayca erişilemez. Cihazların envanterini tutun – kimin hangi dizüstü bilgisayara veya telefona sahip olduğunu bilin. Bir cihaz hassas veriler içeriyorsa, güvenli olmayan yerlerde bırakılmaması için politikalar oluşturun (örneğin, ofis çekmecesinde kilitli tutmak veya personelin eve götürüp güvenli bir şekilde saklamasını sağlamak). Seyahat sırasında, gizlilik ekranı filtreleri kullanın ve cihazları yanınızda tutun (mümkünse dizüstü bilgisayarları bagaja vermeyin).

Bulut Depolama (Google Drive, Dropbox vb.): Bulut hizmetleri çok kullanışlıdır ve yerleşik yedeklilik özelliğine sahiptir, ancak güvenlik için bunları doğru şekilde yapılandırmanız

gerekir. İlk olarak, yetkisiz oturum açmaları önlemek için bulut hesaplarında 2FA'yı etkinleştirin. İkinci olarak, paylaşım izinlerini dikkatli bir şekilde yönetin. Tüm sürücüyü açık bir şekilde paylaşmak yerine, klasörleri/dosyaları yalnızca erişime ihtiyaç duyan belirli kişilerle paylaşın. Google Drive veya Dropbox'ınızda kimin neye erişimi olduğunu düzenli olarak gözden geçirin ve artık erişime ihtiyacı olmayan kişileri (projeleri sona eren harici işbirlikçileri de dahil) kaldırın. "Bağlantı yoluyla paylaş" özelliklerine dikkat edin; bir dosyaya genel bir bağlantı oluştururursanız, teorik olarak bu bağlantıyı bulan herkes dosyaya erişebilir (bazı sistemler artık parola korumalı bağlantılar veya süreli bağlantılar sunmaktadır; gerekirse bunları kullanın). Son derece hassas dosyalar için, yüklemeden önc i bir istemci tarafı şifreleme kullanmayı düşünün (bazı araçlar Dropbox/Google Drive ile entegre olarak dosyaları yerel olarak şifreler, böylece birisi bulut hesabınızı hacklese bile, anahtarınız olmadan anlamsız karakterler görür).

ENISA'nın KOBİ'ler için bulut konusunda verdiği rehberlik bu noktaları yinelemektedir: bulutun kendine özgü risklerini anlayın ve saygın sağlayıcıları seçtiğinizden emin olun. Özellikle, verilerle ilgili yasaları ihlal etmeyen sağlayıcıları kullandığınızdan emin olun (örneğin, AB dışındaki kişisel verilerin güvenli önlemler alınmadan depolanmasına ilişkin GDPR kısıtlamaları). Örneğin, CSO'nuz AB'de faaliyet gösteriyor ve kişisel verileri depoluyorsa, bulut sağlayıcınızın verileri nerede depoladığını doğrulamalı ve mümkünse Veri İşleme Anlaşmaları imzalamalısınız. Dropbox veya Google gibi hizmetleri kullanıyorsanız, bu hizmetlerin uyumluluğunu inceleyin ve güvenilir bölgelerde sunucuları olan hizmetleri tercih edin veya gerekirse Avrupa'daki alternatifleri kullanın.

Aktarım ve Depolama Sırasında Şifreleme: Verilerin sadece disklerde değil, aktarım sırasında da şifrelenmesini sağlayın. Çoğu bulut sağlayıcı, sunucularında depolanan verileri şifreler ve aktarımlar için HTTPS kullanır, bu da iyidir. Herhangi bir veriyi kendi sunucunuzda barındırıyorsanız (örneğin, internet üzerinden erişilebilen bir yerinde NAS), bir VPN kurun veya en azından web bağlantılarının HTTPS üzerinden yapıldığından emin olun. Ayrıca, son derece hassas bilgiler için şifreleme katmanları oluşturabilirsiniz. Örneğin, bir belgeyi şifreli bir bulut klasörüne yüklemeden önce bir şifre ile şifreleyin (çift şifreleme). Bu, örneğin düşmanca bir bölgedeki aktivistlerin listeleri için geçerli olabilir.

Veri Segmentasyonu: CSO'daki herkes otomatik olarak tüm verilere erişebilmemelidir. Verileri segmentlere ayırmak için erişim denetimlerini kullanın. Örneğin, İK dosyaları veya personel tıbbi bilgileri yalnızca İK personeli ile sınırlandırılabilir. Finansal kayıtlar sadece finans ekibine açıktır. Proje dosyaları sadece o projede çalışanlara açıktır, vb. Birçok bulut platformu, izin kademeleri ve grup tabanlı erişim sağlar. Bu şekilde, bir kullanıcının hesabı ele geçirilirse, saldırgan her şeyi ele geçirmek zorunda kalmaz, sadece o kullanıcının erişebildiği bilgileri ele geçirir. Bu ayrıca iç kötüye kullanım riskini de azaltır – insanlar kendi görevleriyle ilgisi olmayan verileri gözetleyemezler.

Veri Saklama ve İmha Planı: Güvenli depolamanın bir parçası, verileri gereğinden fazla saklamamaktır. Değiştirilen bilgisayarlardaki eski sabit diskler güvenli bir şekilde silinmeli veya imha edilmelidir (sadece dosyaları silmek yeterli değildir; yazılım kullanarak diski üzerine yazın veya fiziksel olarak imha edin). Artık kullanılmayan USB bellekler için de aynı şey geçerlidir. CSO'nuz gereksiz yere onlarca yıllık kişisel veri biriktiriyorsa, eski kayıtları arşivlemek veya silmek için bir politika oluşturmayı düşünün. Bu, bir ihlalde açığa çıkabilecek hassas bilgilerin miktarını azaltır ( ) ve veri koruma yasalarının ilkeleriyle uyumludur (veri saklamayı en aza indirgemek). Örneğin, beş yıl önce bir eğitim düzenlediyseniz ve hala katılımcıların kimlik kopyalarına sahipseniz, bunlara gerçekten ihtiyacınız olup olmadığına karar verin.

Yedeklilik ve İş Sürekliliği: Yedeklemeler veri sürekliliğini sağlar, ancak operasyonel sürekliliği de düşünün. Ofis sunucunuz çökerse, veri yedeklemesi ilk adımdır, ancak ikinci adım işlevselliği geri yüklemektir. Planınız yedek bir cihaza veya bulut yedekleme sistemine sahip olmayı içerebilir. Birçok küçük CSO için, kritik işlevler (e-posta, belgeler vb.) için bulut hizmetlerinden çalışmak, doğası gereği süreklilik sağlar – bir cihaz arızalanırsa, başka bir cihazdan herhangi bir yerden çalışmaya devam edebilirsiniz. Ancak, tekil arıza noktalarını belirleyin. Yedeklemelere nasıl erişileceğini tek bir kişi biliyorsa, bu bir risktir – başka birini de bu konuda eğitin veya belirtildiği gibi bunu belgelendirin.

Uygulama örneği: CSO'nuzun ofisteki bir NAS cihazında tüm proje dosyaları için paylaşılan bir sürücüsü olduğunu varsayalım. Bu NAS'ın her gece yedeklemesini, yöneticinizin hafta sonları eve götürdüğü (ofis dışına) şifreli bir harici HDD'ye yaparsınız. Ayrıca, kritik alt klasörler, işbirliği ve ofis dışı güvenlik için gerçek zamanlı olarak güvenli bir bulut (Google Drive

veya Nextcloud gibi) ile senkronize edilir. CRM'nizden bağışçı veritabanınızın yedeklemelerini planlar ve aylık olarak bir kopyasını indirir, şifreler ve bulutta saklarsınız. İmzalı yararlanıcı onay formları gibi fiziksel dosyalar için, bunları tarayıp yükleyin (böylece yedeklenirler) ve orijinallerini kilitli bir dolapta saklayın. Tüm dizüstü bilgisayarlar için BitLocker'ın açık olduğundan emin olun ve her birinde BIOS/ürün yazılımı şifresi olsun, böylece hırsızlar USB'den önyükleme yaparak şifrelemeyi kolayca atlatamazlar. Her üç ayda bir, yedeklemelerinizden geri yükleme yapabildiğinizden emin olmak için bir veri kaybı senaryosu simüle edin.

Tüm bunları yaparak dayanıklılık elde edersiniz: bir siber felaket yaşansa veya donanım arızalansa bile verileriniz güvende olur ve en az kesinti ile çalışmaya devam edebilirsiniz. CyberPeace Institute, kar amacı gütmeyen kuruluşların siber güvenliği (ve dolayısıyla veri koruma önlemlerini) sosyal etki için teknolojiyi güvenli bir şekilde kullanmalarını sağlayan bir araç olarak görmeleri gerektiğini vurgulamıştır. Güvenli veriler ve yedeklemeler, kritik bilgileri kaybetme korkusu olmadan dijital araçları kullanabileceğiniz anlamına gelir.

Sonuç olarak, yedeklemeler ve güvenli depolama, dijital operasyonlarınızın emniyet kemeri ve hava yastıkları gibidir – acil bir durumda onlara asla ihtiyaç duymamanızı umarsınız, ancak ihtiyaç duyduğunuzda, kuruluşunuzu felaketle sonuçlanabilecek kayıplardan kurtarabilirler. Bunu önceki bölümlerde bahsedilen proaktif önlemlerle (şifre hijyeni ve erişim kontrolleri gibi) birleştirerek, CSO'nun bilgi varlıkları için güçlü bir kalkan oluşturursunuz. Şimdi, oluşturduğumuz plan ve politikaları tamamlayarak, uygulamada güvenliğinizi daha da güçlendirebilecek bazı kullanımı kolay araçları inceleyeceğiz.

Bölüm Özeti

Bu bölüm, CSO'lara günlük operasyonlar ve güven için kritik öneme sahip iletişim ve hassas verileri güvence altına almak için pratik rehberlik sunar. E-posta, mesajlaşma ve veri depolama için şifrelemeyi kapsar ve güvenli sohbetler için Signal, web trafiği için HTTPS gibi araçlar önerir. E-posta veya bulut platformları (ör. Google Drive) gibi hesaplara yetkisiz erişimi önlemek için güçlü şifreler ve 2FA gibi güçlü erişim kontrolleri vurgulanır. Bu bölüm, fidye yazılımı veya veri kaybından kurtulmak için güvenli konumlara (örneğin şifreli sürücüler) düzenli yedeklemeler yapılmasını savunur ve yedeklemelerin bir CSO'yu fidye yazılımı saldırısından kurtardığı bir vakayı örnek olarak verir. Yararlanıcı verilerini korumak için şifreli bulut hizmetleri gibi güvenli dosya paylaşım yöntemleri vurgulanır. Bu bölüm, GDPR uyumluluğunu ele alır ve yasal veri işleme ve rızayı vurgular. Gmail'de 2FA'yı etkinleştirme veya ücretsiz şifreleme araçlarını kullanma gibi uygulanabilir adımlar içerir ve teknik bilgiye sahip olmayan personel için erişilebilir hale getirir. Bir hayır kurumunun e-postasının kimlik avı yoluyla hacklenmesi gibi örnekler, dikkatli olunması gerektiğini vurgulamaktadır. Bu bölümde ayrıca, CSO'ların uzaktan veya yüksek riskli ortamlarda güvenli bir şekilde iletişim kurabilmelerini sağlamak için güvenli video konferans ve sosyal medya uygulamaları da ele alınmaktadır. CSO'lar bu önlemleri uygulayarak hassas bilgileri korur, operasyonel sürekliliği sağlar ve bağışçıların güvenini kazanır.

Siber Güvenlik Planı CSO'lar için Yıllık İnceleme ve Güncelleme Kontrol Listesi

Bu kontrol listesi, varlıkları, tehditleri, politikaları ve olay müdahale stratejilerini yıllık olarak veya önemli değişikliklerden sonra (ör. yeni sistemler, personel değişimi) gözden geçirerek CSO'nuzun siber güvenlik planının güncel ve etkili kalmasını sağlar. Bu adımları tamamlamak, misyonunuzu ve paydaşlarınızı korumak için sağlam bir dijital güvenlik duruşu sağlar:

1 . Dijital Varlıkları Gözden Geçirin ve Güncelleyin

- ⇒ Son gözden geçirme tarihinden bu yana eklenen yeni veya değiştirilen dijital varlıkları (ör. yeni bağışçı veritabanı, bulut depolama, sosyal medya hesapları) belirleyin.
- ⇒ Planı eski varlıkları (örneğin, kullanımdan kaldırılan yazılımlar, eski e-posta hesapları) kaldırın.
- ⇒ Örnek: Bağışçı yönetimi için yeni bir CRM sistemi mi eklediniz? Bunu risk değerlendirmesine dahil edin. Eski bir gönüllü veritabanını kullanımdan mı kaldırdınız? Bunu plandan kaldırın.

2. Yeni veya Gelişen Tehditleri Değerlendirin

- ⇒ CSO'larla ilgili son siber güvenlik eğilimlerini veya tehditlerini gözden geçirin (ör. artan kimlik avı, fidye yazılımı veya yerel gözetim riskleri).
- ⇒ Güncellemeler için yerel kaynaklara (ör. ulusal CERT, CSO ağları) veya küresel raporlara (ör. Microsoft'un CSO saldırı istatistikleri) başvurun.
- ⇒ Risk değerlendirme şablonunu, yeni tehditleri veya olasılık/etki değişikliklerini yansıtacak şekilde güncelleyin.
- ⇒ Örnek: Bölgenizdeki CSO'ları hedef alan kimlik avı e-postalarında artış fark ettiniz mi? Risk değerlendirmenizde kimlik avı olasılık puanını artırın.

3. Son Olayları veya Kaza Tehlikelerini Gözden Geçirin

- ⇒ Son incelemeden bu yana meydana gelen tüm siber güvenlik olaylarını veya kıl payı kaçırılan olayları (ör. kimlik avı girişimleri, kötü amaçlı yazılım uyarıları) belgelendirin.
- ⇒ Tepkinizde nelerin iyi gittiğini ve nelerin başarısız olduğunu analiz edin (örneğin, yedeklemeler işe yaradı mı? Olay derhal rapor edildi mi?).
- ⇒ Gelecekteki yanıtları iyileştirmek için öğrenilen derslerle planı güncelleyin.
- ⇒ Örnek: Bir çalışan bir kimlik avı bağlantısını tıkladı, ancak 2FA erişimi engelledi. 2FA eğitimini güçlendirmek ve e-posta filtrelerini güncellemek için bir not ekleyin.

4. Olay Müdahale Prosedürlerini Güncelleyin

- ⇒ Olay müdahale planının güncel adımları, rolleri ve sorumlulukları (ör. kim tespit eder, kim kontrol altına alır, kim iletişim kurar) içerdiğini doğrulayın.
- ⇒ Dahili müdahale ekipleri (ör. BT personeli, liderlik) ve harici destek ekipleri (ör. yerel CERT, hukuk danışmanı) için iletişim listelerini güncelleyin.
- ⇒ Planı bir masaüstü tatbikatıyla (ör. fidye yazılımı saldırısı simülasyonu) test ederek eksiklikleri belirleyin.
- ⇒ Örnek: Yeni BT yöneticisi mi var? Kaza müdahale lideri olarak rolünü güncelleyin. Eski CERT iletişim bilgileri mi güncel değil? Güncel bilgilerle değiştirin.

5. Güvenlik Politikaları ve Uyumluluğu Kontrol Edin

- ⇒ Yeni araçları, düzenlemeleri veya uygulamaları yansıtmak için güvenlik politikalarını (ör. kabul edilebilir kullanım, veri koruma, BYOD) gözden geçirin ve güncelleyin.
- ⇒ Veri koruma yasalarına (ör. GDPR, yerel düzenlemeler) uyumu onaylayın ve gerekirse prosedürleri güncelleyin (ör. onay formları, ihlal raporlama).
- ⇒ Örnek: GDPR, ihlallerin 72 saat içinde bildirilmesini gerektirir. Politikanızda bu süre ve belirlenen raporlama irtibat kişisi bilgilerinin yer aldığından emin olun.

6. Teknik Korumaları Doğrulayın

- ⇒ Güvenlik önlemlerini (ör. 2FA, antivirüs, yedeklemeler, şifreleme) denetleyerek tüm cihazlarda ve hesaplarda etkin ve güncel olduklarından emin olun.
- ⇒ Araçlarda (ör. bulut platformları, e-posta sağlayıcıları) yeni güvenlik özellikleri olup olmadığını kontrol edin ve varsa bunları etkinleştirin.
- ⇒ Örnek: Google Workspace, paylaşılan sürücüler için yeni bir güvenlik özelliği mi ekledi? Bu özelliği etkinleştirin ve erişim denetimlerini güncelleyin.

7. Personel Eğitimi ve Farkındalık Planlayın

- ⇒ Tüm personel ve gönüllüler için siber güvenlik eğitimi veya yenileme kursları (ör. kimlik avı farkındalığı, şifre yönetimi) planlayın.
- ⇒ Son tehditlere veya olaylara dayalı yeni konular ekleyin (ör. AI destekli kimlik avı, bulut güvenliği).
- ⇒ Örnek: Yerel bir fidye yazılımı saldırısı dalgasının ardından, fidye yazılımı uyarı işaretlerini tanımaya yönelik 30 dakikalık bir oturum ekleyin.

8. Yedeklemeleri ve Kurtarmayı Test Edin

- ⇒ Yedeklemelerin planlandığı gibi çalıştığını ve güvenli bir şekilde saklandığını (ör. şifreli bulut veya harici sürücü) doğrulayın.
- ⇒ Verilerin hızlı ve doğru bir şekilde kurtarılabildiğinden emin olmak için bir yedekleme geri yükleme testi yapın.
- ⇒ Örnek: Geçen ayın yedeklemesinden bir örnek dosyayı geri yükleyerek erişilebilir ve bozulmamış olduğunu doğrulayın.

9. Liderlik ve Paydaşları Dahil Edin

- ⇒ Güncellenen plan ve gerekli kaynaklar (ör. yeni araçlar için bütçe, eğitim için zaman) hakkında liderlere bilgi verin.
- ⇒ Güvenlik uygulamalarınıza olan güveni güçlendirmek için önemli güncellemeleri paydaşlarla (ör. bağışçılar, ortaklar) paylaşın.
- ⇒ Örnek: Bağışçılara, GDPR'ye uymak için veri korumasını güçlendirdiğinizi ve şeffaflığı artırdığınızı bildirin.

10. Bir Sonraki Gözden Geçirmeyi Belgelendirin ve Planlayın

⇒ Siber güvenlik planındaki tüm güncellemeleri kaydedin ve güvenli, erişilebilir bir yerde (ör. şifreli paylaşımlı sürücü) saklayın.

⇒ Bir sonraki yıllık incelemeyi planlayın veya önemli değişikliklerden sonra (ör. yeni yazılım, ofis taşınması) incelemeyi başlatın.

⇒ Örnek: Bu süreci tekrarlamak için yıllık takvim hatırlatıcısı ayarlayın.

2.4 BÖLÜM 4: KULLANICI DOSTU GÜVENLİK ARAÇLARI

Kullanıcı Dostu Güvenlik Araçları

Şimdiye kadar uygulamaları ve planlamayı ele aldık. Bu bölümde, güvenliği uygulamayı kolaylaştırabilecek araçlara ve teknolojilere odaklanacağız. İyi haber şu ki, sağlam bir koruma seviyesi elde etmek için teknoloji uzmanı olmanıza veya çok pahalı çözümlere yatırım yapmanıza gerek yok. Dijital güvenliğinizi önemli ölçüde artırabilecek, genellikle kar amacı gütmeyen kuruluşlar veya küçük işletmeler için tasarlanmış, **kullanıcı dostu ve uygun maliyetli** birçok **araç** mevcuttur. Araçların kategorilerini inceleyeceğiz: güvenli uygulamaları belirleme, güvenli gezinme yardımcıları, bulut depolamayı güvence altına alma ve bilgisayarlarınızı ve telefonlarınızı korumak için araçlar. Her alt bölümde, pratiklik ve kullanım kolaylığına vurgu yapılarak temel araçlar veya yöntemler tanıtılmaktadır.

Güvenli Uygulamaları Tanıma

Sayısız yazılım ve uygulama varken, hangilerinin "güvenli" olduğunu nasıl anlarsınız? Burada, güvenlik ve gizliliği önceliklendiren uygulamaları seçmenize yardımcı olacak bazı kriterler ve örnekler özetlenmiştir.

Bir Uygulamayı Güvenli Kılan Nedir? Güvenli bir uygulama genellikle aşağıdaki özelliklere sahiptir:

- Saygın bir geliştirici veya kaynaktan gelir ve aktif olarak bakım yapılır (hataları gidermek için düzenli olarak güncellenir).
- Aktarım ve depolama sırasında verileri korumak için şifreleme kullanır (özellikle iletişim ve depolama uygulamaları için önemlidir).
- İyi bir erişim kontrolüne sahiptir (örneğin, güçlü kimlik doğrulama, hesaplar için 2FA gibi).
- Güvenlik açıklarına yanıt verme konusunda geçmiş performansı vardır (geliştiriciler yamalar yayınlar) ve ideal olarak güvenlik denetimlerinden geçmiştir.
- Uygulama gizliliğe saygı duyar (aşırı veri toplamaz veya kötü amaçlı yazılım enjekte edebilecek şüpheli reklamlar sunmaz).

Örneğin, Signal gibi mesajlaşma uygulamaları, açık kaynaklı yazılım oldukları (herkes arka kapı kodunu inceleyebilir), varsayılan olarak uçtan uca şifreleme kullandıkları ve gereksiz meta verileri toplamadıkları için güvenli kabul edilir. Öte yandan, bazı ücretsiz uygulamalar kullanışlı görünebilir, ancak güvenli olmayabilir – örneğin, şifrelenmemiş rastgele bir dosya paylaşım uygulaması veya 2FA seçeneği olmayan bir şifre yöneticisi, alternatiflerinden daha az güvenli olacaktır.

Önemli Görevler için Yazılım Seçimi*:* İşte güvenli öneriler içeren bazı yaygın uygulama kategorileri:

***Şifre Yönetimi*:** Bahsedildiği gibi özel bir şifre yöneticisi uygulaması kullanın. İyi seçenekler arasında Bitwarden (açık kaynaklı, bulut tabanlı, temel kullanım için ücretsiz), LastPass (popüler, ücretsiz bir seviyesi var, ancak 2022'de bir güvenlik ihlali yaşadı, bu da güçlü ana şifreler kullanmanın gerekliliğini vurguluyor), 1Password (ücretli, kullanıcı dostu) veya KeePass (açık kaynaklı, çevrimdışı) sayılabilir. Bu uygulamalar, giriş bilgilerinizi güvenli bir şekilde saklamak için güçlü şifreleme özelliğine sahiptir ve çoğu, kasayı açmak için 2FA'yı destekler. Ayrıca sizin için rastgele şifreler de oluşturabilirler. Bunlardan herhangi birini kullanmak, şifreleri bir elektronik tabloda saklamaktan veya tekrar kullanmaktan çok daha üstündür.

Güvenli Mesajlaşma ve E-posta: Mesajlaşma için, daha önce de belirtildiği gibi: En güvenli iletişim için Signal; WhatsApp da uçtan uca şifrelenmiştir (Meta'ya ait olmasına rağmen yaygın olarak kullanılmaktadır ve güçlü şifreleme temellerine sahiptir). Avrupa'da barındırılan bir çözüm istiyorsanız, Wire veya Threema kurumsal kullanım için iyi seçenekler olabilir. E-posta için, daha yüksek güvenlik ihtiyacınız varsa, uçtan uca şifreleme sunan ProtonMail veya Tutanota gibi sağlayıcıları değerlendirin (özellikle iç e-postalar veya aynı hizmetin kullanıcıları arasındaki e-postalar için). Gmail veya Outlook.com'u kullanmaya devam edecekseniz, 2FA ile kullanıldığında makul düzeyde güvenlidirler, ancak hassas e-postalar şifreli bir kanal üzerinden veya GnuPG/PGP gibi şifreleme araçları kullanılarak gönderilmesi daha iyi olabilir (ancak PGP pratikte karmaşıktır).

Antivirüs/Kötü Amaçlı Yazılımdan Koruma: Bahsedildiği gibi, tanınmış ve iyi yorumlar almış antivirüs çözümlerini kullanın. Windows Defender (Windows 10/11'de yerleşik olarak

bulunur) sağlam bir temel oluşturur ve sorunsuz çalışır. Üçüncü taraf bir ürün istiyorsanız: Avast, AVG, Bitdefender, Kaspersky (bazıları Kaspersky'nin kökeni nedeniyle endişe duyuyor, ancak teknik olarak güçlüdür), ESET vb. Bunların çoğunun temel koruma için ücretsiz sürümleri vardır. Sisteminizi aşırı derecede yavaşlatmayan ve iyi bir algılama oranına sahip olanı seçin (bağımsız AV test laboratuvarları bu konuda rehberlik edebilir). Güncel tutun.

Güvenlik Duvarı ve Ağ Güvenliği: Çoğu durumda, işletim sisteminin yerleşik güvenlik duvarı yeterlidir. Daha fazla kontrol ve görsel ipucuya ihtiyacınız varsa (ileri düzey kullanıcılar için), Windows'ta ZoneAlarm veya TinyWall gibi araçlar daha kullanıcı dostu bir arayüzde uygulama düzeyinde güvenlik duvarı yönetimi sunar. Yönlendiricinizde güvenlik duvarının açık olduğundan emin olun. Bazı CSO'lar, ofis ağları varsa donanım güvenlik duvarları veya UTM cihazlarını tercih ederler, ancak bunlar karmaşık olabilir; genellikle, iyi bir yönlendirici (güncellenmiş ürün yazılımı ile) temel bir güvenlik duvarı görevi görür. Bir web sitesi işletiyorsanız, Cloudflare gibi bir hizmet veya barındırıcınızın güvenlik eklentilerini kullanarak web saldırılarına karşı bir güvenlik duvarı sağlayabilirsiniz.

Güvenli Tarayıcılar ve Uzantılar: Modern ve güvenli bir tarayıcı (Chrome, Firefox, Edge, Brave) kullanın. Hepsi oldukça güvenlidir; Brave, gizlilik varsayılanları (izleyicileri engelleme) ile bilinir. Firefox açık kaynaklıdır ve gizlilik açısından yüksek düzeyde yapılandırılabilir. Chrome güvenlik açısından çok sağlamdır (Google Project Zero, istismarları ve yamaları agresif bir şekilde bulur), ancak verileri Google'a gönderir (çoğunlukla zararsız kullanım istatistikleri olsa da). Edge de iyidir (Chrome'un motoru üzerine Microsoft güvenlik özellikleriyle inşa edilmiştir). Herhangi bir tarayıcıyı uzantılarla geliştirebilirsiniz: örneğin, HTTPS Everywhere (çoğu site otomatik olarak HTTPS kullandığı için artık büyük ölçüde gereksizdir, ancak mümkün olduğunda şifreleme sağlar), uBlock Origin veya Privacy Badger, kötü amaçlı reklamları ve izleyicileri engellemek için (bu da kötü amaçlı reklam riskini azaltır) ve tarayıcının kendi pop-up engelleyicisi ve kimlik avı önleme filtresi açık olmalıdır. Bazıları NoScript kullanır (varsayılan olarak tüm komut dosyalarını engeller), ancak bu gelişmiş bir özelliktir ve siteleri bozabilir; komut dosyası tabanlı saldırılardan endişe duyan ileri düzey kullanıcılar için isteğe bağlıdır. Flash/Java için tıklayarak oynatmayı etkinleştirin (çoğu tarayıcı artık Flash'ı tamamen devre dışı bırakıyor, bu da iyi bir şey).

VPN Hizmetleri: Ekibiniz sık sık halka açık Wi-Fi kullanıyorsa veya uzaktan çalışıyorsa, VPN kullanmak güvenliği artırabilir. *İyi* bir VPN hizmeti, internet trafiğinizi şifreler ve yerel ağda gözetlemeyi önleyebilir. Ayrıca IP adresinizi gizleyerek gizliliğinizi artırabilir. Ancak, yalnızca saygın ücretli/ücretsiz olanları kullanın (bazı ücretsiz VPN'lerin gizliliğin tam tersini yaptığı, yani reklamları kaydettiği veya eklediği tespit edilmiştir). Alternatif olarak, BT kapasiteniz varsa, ekibiniz için bir bulut sunucusunda kendi VPN'inizi kurabilirsiniz. Daha basit: Artık birçok yönlendirici, ev ofis VPN'i oluşturmayı desteklemektedir, böylece personel yurtdışındayken ofis ağına güvenli bir şekilde bağlanabilir.

Disk Şifreleme Araçları: İşletim sisteminin yerleşik şifrelemesinin yanı sıra, şifreli konteynerler oluşturabilen veya tüm sürücüleri şifreleyebilen VeraCrypt (TrueCrypt'in ücretsiz, açık kaynaklı halefi) gibi araçlar da vardır. USB bellekleri şifrelemek veya herhangi bir yerde (hatta bulutta) depolayabileceğiniz ve güvenli olduğunu bildiğiniz şifreli bir klasör (konteyner dosyası) oluşturmak istiyorsanız kullanışlıdır. VeraCrypt biraz teknik bir araçtır ancak iyi belgelenmiştir. Telefonlar ve bilgisayarlar için belirli dosyaları şifre ile koruyan ve şifreleyen daha basit kasa uygulamaları da vardır (örneğin, 7-Zip dosyalar için şifreli arşivler oluşturabilir).

Güvenli Alternatifler ve Güncellemeler: Güvenli uygulamaları tanımak, bazen riskli bir uygulamayı daha güvenli bir alternatifle değiştirmek anlamına gelir. Örneğin, birisi güvenlik açıkları olduğu bilinen eski bir uygulama sürümünü kullanıyorsa (örneğin, bir web sitesi için eski bir CMS veya eski bir Adobe Acrobat), bunu güncelleyin veya alternatiflere geçin (örneğin, kötü amaçlı yazılımların sık hedef aldığı eski Adobe Reader yerine Chrome'un PDF görüntüleyicisini veya SumatraPDF'yi kullanın). Kullanım ömrü dolmuş yazılımları değiştirin (artık güncelleme almayan Windows 7 gibi – bütçe kısıtlıysa Windows 10/11'e yükseltin veya hafif bir Linux kullanın).

Mobil Uygulamalar: Telefonlara, vurgulandığı gibi yalnızca resmi uygulama mağazalarından uygulamalar yükleyin. Güvenli iletişim için yine Signal, WhatsApp (yedeklemeler konusunda dikkatli olun, çünkü WhatsApp bulut yedeklemeleri, yeni şifreli yedekleme özelliğini seçmediğiniz sürece şifrelenmemiş olabilir). Telefonlarda güvenli depolama için, yerleşik güvenli klasör özelliklerini (Samsung Secure Folder) veya Android için **KeePassDX** gibi uygulamaları kullanarak şifreleri çevrimdışı olarak yönetin.

Araçlar Hakkında Eğitim: Yeni uygulamaların tanıtımı, ancak kullanıcılar bunları doğru şekilde kullandığında faydalıdır. Bu nedenle, herhangi bir aracı (şifre yöneticisi veya VPN gibi) kullanıma sunmanın bir parçası, kısa bir eğitim veya hile sayfası sunmaktır. Birçok araç sezgiseldir, ancak başlangıçta verilen rehberlik, doğru kullanımı sağlar (örneğin, şifreleri e-posta yerine yönetici aracılığıyla güvenli bir şekilde paylaşmayı gösterir).

Güvenli uygulamaları dikkatlice seçip kullanarak güvenlik açıklarını azaltabilirsiniz. Ancak dengeyi koruyun: "en güvenli" bazen daha az kullanıcı dostu anlamına gelir ve bu da risk oluşturan geçici çözümlerin ortaya çıkmasına neden olabilir (örneğin, güvenli bir mesajlaşma uygulaması çok hantal ise, personel kolaylık için açık e-postayı kullanmaya geri dönebilir). Ekibinizin rahatlıkla benimseyebileceği araçları seçin – genellikle, iyi yapılandırılmış yaygın araçlar hem güvenlik hem de kullanılabilirlik sağlar. Örneğin, Google Workspace veya Microsoft 365, 2FA ve uygun yönetici kontrolleriyle kurulursa, e-posta/belgeler için güçlü güvenlik sağlar ve kullanıcı dostudur. Bazı niş çözümler kadar kilitli olmayabilirler, ancak kullanıcılar bu araçlarda güvenlik uygulamalarını gerçekten takip ederse, yeterli ve entegrasyonu daha kolay olabilirler.

Esasen, güvenli uygulamaları tanımak, yeni bir şey yüklemeden önce biraz araştırma yapmak ve güvenlikle tanınan uygulamaları tercih etmekle ilgilidir. Birçok sivil toplum kuruluşu, önerilen araçların listelerini adresinde paylaşmaktadır (örneğin, araç kılavuzları sunan Front Line Defenders'ın Security-in-a-Box uygulaması). Sonraki bölümlerde, her biri için özel ipuçları ve araçlar içeren belirli alanları (web tarama, bulut, cihazlar) vurgulayacağız.

İnternette Daha Güvenli Tarama

Web tarama o kadar yaygın bir faaliyettir ki, potansiyel tehlikeleri unutmak kolaydır. Bu bölüm, 2. Bölümdeki güvenli internet kullanımı uygulamalarını temel alır ve web'de gezinmeyi daha güvenli ve daha gizli hale getirebilecek araçlara ve tarayıcı ayarlarına odaklanır.

Tarayıcı Güvenlik Ayarları: Öncelikle, web tarayıcınızın yerleşik güvenlik özelliklerini yapılandırdığınızdan emin olun:

- Tarayıcıyı güncel tutun (çoğu varsayılan olarak otomatik güncellenir; bunu devre dışı bırakmayın).

- Kimlik avı ve kötü amaçlı yazılım korumayı etkinleştirin (Chrome, Firefox ve Edge gibi tarayıcılarda bu özellik varsayılan olarak etkindir; ziyaret edilen URL'leri bilinen kötü listelerle karşılaştırır ve bir sitenin kimlik avı şüphesi varsa veya kötü amaçlı yazılım içeriyorsa büyük kırmızı bir uyarı gösterir).
- "İzleme" özelliğini etkinleştirin (bu özellik büyük ölçüde tavsiye niteliğinde olsa da, bazı siteler bu özelliği dikkate alır).
- Varsa, tarayıcının sanal alanı veya site izolasyon özelliklerini kullanmayı düşünün (Chrome, belirli saldırıları azaltmak için site izolasyonuna sahiptir – genellikle yüksek riskli alan adları için varsayılan olarak açıktır).
- Chrome'da, tehdit değerlendirmesini iyileştirmek için Google ile daha fazla veri paylaşan "Gelişmiş Güvenli Tarama" modunu da kullanabilirsiniz (bu verileri Google'a güveniyorsanız isteğe bağlıdır).

Reklam engelleyiciler ve komut dosyası engelleyiciler: Belirtildiği gibi, birçok kötü amaçlı yazılım bulaşması, güvenliği ihlal edilmiş sitelerdeki kötü amaçlı reklamlar veya kötü amaçlı komut dosyaları yoluyla gerçekleşir. **uBlock Origin** veya **Adblock Plus** gibi saygın bir reklam engelleyici uzantısı kullanmak, yaygın kötü amaçlı yazılım dağıtım vektörlerini keserek yalnızca gizlilik ve estetiğe değil, aynı zamanda güvenliğe de yardımcı olur. Bu uzantılar, bilinen reklam etki alanlarını engeller ve şüpheli komut dosyalarının yüklenmesini önleyebilir. **Privacy Badger** (EFF'den) gibi gizlilik odaklı uzantılar, izleyicileri engellemeyi öğrenir ve bu süreçte genellikle kötü amaçlı üçüncü taraf içeriklerini ortadan kaldırır. Çok endişeliyseniz veya riskli siteleri ziyaret ediyorsanız, **NoScript** (Firefox) veya **ScriptSafe** (Chrome) varsayılan olarak tüm komut dosyalarını engelleyebilir. Bu, yüksek güvenlik sağlar ancak meşru siteler için manuel beyaz listeye ekleme gerektirir işlevselliği, teknoloji konusunda bilgili değilseniz zahmetli olabilir. Daha hafif bir yaklaşım kullanabilirsiniz: **Firefox**'un sıkı Gelişmiş İzleme Koruması modu veya varsayılan olarak birçok komut dosyasını ve reklamı engelleyen **Brave** tarayıcısı.

Güvenli Bağlantılar ve Uzantılar: Her zaman web sitelerinin HTTPS sürümlerini kullanmaya çalışın. *HTTPS Everywhere* uzantısı (EFF'den), mümkün olduğunda otomatik olarak HTTPS'ye yönlendirir, ancak günümüzde çoğu büyük site zaten varsayılan olarak HTTPS kullanmaktadır. Tarayıcının asma kilit simgesi sizin dostunuzdur – sertifika ayrıntılarını

incelemek veya en azından şifre veya hassas veriler girdiğiniz herhangi bir sitede mevcut olduğundan emin olmak için bu simgeye tıklayın. Sık sık halka açık Wi-Fi kullanıyorsanız, şifrelemeyi sağlamak için **HTTPS Everywhere** gibi bir uzantı kullanmayı düşünün (VPN kullanmıyorsanız) veya manuel olarak dikkatli olun. Bazı modern tarayıcılar (Chrome, Firefox) artık form içeren HTTPS olmayan sayfaları adres çubuğunda "Güvenli değil" olarak işaretliyor – bu uyarıya dikkat edin.

Arama Motorları ve İzleme: Google arama motoru güçlüdür, ancak sorguları izler. Hedefli reklamlardan veya profil oluşturulmasından kaçınmak istiyorsanız, **DuckDuckGo'yu** varsayılan arama motorunuz olarak kullanmayı düşünün. Bu arama motoru aramaları izlemez ve genel sorgular için iyi sonuçlar verir. Ayrıca, sitelerin gizlilik uygulamalarını derecelendiren ve şifrelemeyi uygulayan bir uzantı da sunar. Alternatif olarak, **Startpage** Google sonuçlarını verir, ancak kimlik bilgilerini kaldırır. Bunlar, arama kalitesinden çok fazla ödün vermeden gizliliği biraz artırabilir.

Zehirli Arama Sonuçlarından Kaçınmak: Bazen kötü amaçlı yazılım siteleri veya kimlik avı sayfaları arama sonuçlarında görünür (ör. sahte teknik destek siteleri). Personeli, belirsiz arama sonuçlarına tıklarken dikkatli olmaları konusunda eğitin ve indirmeler için bilinen web sitelerine bağlı kalmalarını sağlayın (ör. yazılımları rastgele bir toplama sitesinden değil, resmi bir kaynaktan edinin). **Web of Trust (WOT)** veya **Bitdefender TrafficLight** gibi bir uzantı kullanmak, arama sonuçlarının yanında itibar simgeleri göstererek bir sitenin topluluk/algoritma tarafından güvenli kabul edilip edilmediğini belirtebilir – ancak bu tür araçların kendileri de tartışmalara konu olmuştur (WOT'un kullanıcı verilerini topladığı tespit edilmiştir, bu nedenle dikkatli kullanın).

Özel Tarama Modu: Uygun olduğunda tarayıcılarda "Gizli" veya özel modu kullanın. Bu, sizi internette anonim hale getirmez, ancak kapattıktan sonra çerezleri, geçmişi veya önbelleği kaydetmez. Bu, paylaşılan bir bilgisayarda bir hizmete giriş yapıyorsanız veya belirli bir oturumdan hiçbir kalıntı kalmamasını sağlamak istiyorsanız (örneğin, web sitenizin yeni bir kullanıcıya nasıl göründüğünü test etmek gibi) yararlıdır. Not: Bu, dış tehditlere karşı bir güvenlik aracı değildir, ancak aynı bilgisayarı kullanan diğer kullanıcıların oturumlarınızı gözetlemesini engelleyebilir.

Anonim Tarama için Tor Tarayıcı: Yüksek düzeyde anonimlik gerektiren durumlarda veya yerel internet sansürünü atlatmak için **Tor Tarayıcı** dikkate alınması gereken bir araçtır. Trafiğinizi Tor ağı üzerinden yönlendirir, IP adresinizi gizler ve ağ içindeki trafiği şifreler (ancak HTTPS kullanılmadıkça trafik şifrelenmeden hedefe ulaşır). CSO'lar, gazeteciler ve aktivistler bazen engellenen sitelere ulaşmak veya gözetimden kaçınmak için Tor'u kullanır. Dezavantajı, daha yavaş olması ve bazı sitelerin Tor çıkış düğümlerini engellemesidir. Ancak baskıcı ortamlarda veya hassas araştırmalar için araç setinizin bir parçası olabilir. Yalnızca torproject.org adresinden resmi Tor Browser'ı kullanın ve kullanım kurallarını anlayın (örneğin, Tor Browser'a ekstra tarayıcı eklentileri yüklemeyin, Tor'u atlayabilecekleri için çevrimiçi iken belgeleri açmayın vb.). Bağlamınız için gerekli değilse, VPN ile iyi yapılandırılmış normal bir tarayıcı yeterli olabilir.

Tarayıcı Seçimi ile İlgili Hususlar: Çeşitli tarayıcılar kullanmak bazen etkinlikleri sanal ortama taşıyabilir. Örneğin, hassas hesaplara giriş yapmak için özel olarak bir tarayıcı (ve minimum uzantılarla, yalnızca güvenlik uzantıları) ve gündelik gezinme için başka bir tarayıcı kullanabilirsiniz. Bu şekilde, sıradan tarayıcıda tüm deneysel uzantıları kullanabilir veya zaman zaman daha az güvenli siteleri ziyaret edebilirsiniz, ancak "güvenli tarayıcı"yı (örneğin Firefox) dikkatli kullanabilirsiniz (gereksiz uzantılar yok, sıkı ayarlar, yalnızca banka, e-posta vb. gibi bilinen sitelere girme). Bu, kritik oturum çerezlerinin veya verilerin açığa çıkmasını sınırlar.

E-posta/Web Entegrasyonu: Birçok modern e-posta hizmeti, bağlantıları veya ekleri bir tür sanal alan veya güvenli görüntüleyici içinde açar (Google, ekler için "Korunan görünüm" özelliğine sahiptir; Outlook Web, yöneticiler tarafından etkinleştirildiğinde güvenli bağlantılar sunar). Bu özelliklere sahipseniz, bunları açık tutun; bunlar, içeriği kontrollü bir ortamda açarak ek bir güvenlik katmanı sağlar.

Eklentileri ve Eklentileri Güncel Tutun veya Kaldırın: Flash veya Java gibi tarayıcı eklentileri, belirtildiği gibi, mümkünse kaldırılmalıdır. Çoğu web sitesi artık bunlara ihtiyaç duymamaktadır. Herhangi bir nedenle Flash veya diğerlerine kesinlikle ihtiyacınız varsa, otomatik olarak çalışmamaları için "Etkinleştirmeyi sor" olarak ayarlayın. Kullanılmayan tarayıcı uzantılarını kaldırın; yalnızca güvendiğiniz ve ihtiyacınız olanları saklayın, çünkü kötü amaçlı veya güvenliği ihlal edilmiş uzantılar taramayı ele geçirebilir.

Güvenilir Siteleri Yer İmlerine Ekleyin: Önemli siteler için (bağış platformu giriş bilgileri veya CSO'nuzun kullandığı devlet portalları gibi) yer imlerini/favorileri kullanmayı teşvik edin. Bu, yazım hatası nedeniyle yanlış adrese yönlendirilmeyi (yourbank.com yerine yanlışlıkla yourbank-secure.com adresine gitmeyi) önlemeye yardımcı olur. Ayrıca tanıma sürecini hızlandırır – kullanıcılar her seferinde siteyi yeniden yazmak veya Google'da aramak yerine bilinen yer imini tıklarlar (bu da onları yanlış yönlendirebilir).

Pop-up'lar ve Dolandırıcılık Hakkında Eğitim: "Virüs bulaşmış, bu numarayı arayın" diyen "teknik destek" pop-up'ları gibi dolandırıcılıkları tamamen engelleyen bir araç yoktur. Bu nedenle, farkındalığınızı koruyun: bu tür bir pop-up penceresi açılırsa veya bir indirme işlemi aniden başlarsa, tarayıcıyı veya sekmeyi kapatın. Modern tarayıcılar çoğu pop-up penceresini engeller, ancak bazı reklamlar bunları taklit eder. Bir reklam engelleyici kullanmak bunları çoğunlukla ortadan kaldırır. Ayrıca, modern işletim sistemleri akıllıdır: Windows 10'un SmartScreen özelliği, bilinen kötü amaçlı indirmeleri genellikle engeller veya bir uygulama yaygın olarak indirilmiyorsa sizi uyarır.

Bu araçları ve ayarları birleştirerek, günlük tarama önemli ölçüde daha güvenli hale gelir. Amaç, katmanlı bir savunma oluşturmaktır: bir uzantı kötü bir reklamı engelleyebilir, tarayıcı aldatıcı bir site hakkında uyarı verebilir ve geri kalanı sizin dikkatiniz halleder. Bir şey gözden kaçarsa, antivirüsünüz onu indirirken yakalayabilir. Tek bir katman kusursuz değildir, ancak birlikte riskleri büyük ölçüde azaltırlar.

Bulut Depolama: Google Drive, Dropbox ve Güvenlikleri

Google Drive, Dropbox, Microsoft OneDrive ve diğerleri gibi bulut depolama hizmetleri, CSO'ların işbirliği yapma ve veri depolama yöntemlerinde devrim yarattı. Varsayılan olarak kolaylık ve yedekleme sağlarlar, ancak güvenlikle ilgili hususları da beraberinde getirirler. Bu bölümde, bu hizmetleri güvenli bir şekilde kullanma yöntemi açıklanmaktadır.

Erişim Kontrolü ve Paylaşım Ayarları: Bulut depolamanın en büyük risklerinden biri, kazara aşırı paylaşımdır. Dosya veya klasörleri nasıl paylaştığınızı her zaman iki kez kontrol edin. Varsayılan olarak, belgeleri kuruluşunuz veya belirli kullanıcılar için özel tutun. Örneğin, Google Drive "Bağlantıya sahip herkes" ile paylaşıma izin verir; bunu yalnızca gerekli olduğunda kullanın ve şifre veya son kullanma tarihi eklemeyi düşünün (Google, bağlantılara şifre sunmaz, ancak

OneDrive for Business ve Dropbox ücretli hesaplar için sunar). Bunun yerine, belirli kişilerin e-postalarıyla paylaşmayı tercih edin (bu kişiler oturum açmaları gerekecek, bu da daha güvenlidir). Dropbox ve Google, bir klasörün paylaşılıp paylaşılmadığını gösteren simgeler gösterir. Bu göstergeleri öğrenin ve düzenli olarak kontrol edin. Google'ın **"Benimle paylaşılanlar"** bölümü ve Dropbox'ın paylaşılan klasör listesi, nelerin açık olduğunu gözden geçirmenize yardımcı olabilir.

CSO'nuz G Suite/Google Workspace veya Microsoft 365 kullanıyorsa, yönetim ayarlarından yararlanın: harici paylaşımı kısıtlayabilir veya en azından izleyebilirsiniz. Belki de harici paylaşım yapabilecek kişileri sınırlayabilir veya kuruluş dışındaki bağlantı paylaşımının kapalı olduğu bir varsayılan ayar belirleyebilirsiniz. Bu şekilde, bir çalışan kamuya açık paylaşım yapmak için kasıtlı olarak bu ayarı geçersiz kılmalıdır. Kişisel/ücretsiz bir Google hesabı kullanıyorsanız, bu hesaplarda yönetici denetimi olmadığı için çok dikkatli olun, çünkü bir dosya yanlışlıkla tüm dünyaya açık hale gelebilir.

Bulut Hesaplarında İki Aşamalı Kimlik Doğrulamayı Etkinleştirin: 2FA'yı defalarca vurguladık ve hesabınızın ihlali birçok veriyi açığa çıkarabileceğinden, bulut depolama için bu çok önemlidir. Google, Dropbox, Microsoft, Box vb. tümü 2FA'yı destekler (genellikle kimlik doğrulama uygulamaları veya SMS yoluyla). Erişimi olan ekibinizdeki her kullanıcının bunu yaptığından emin olun. Birçok ihlal, oturum açma kimlik bilgilerinin çalınması nedeniyle gerçekleşir, ancak 2FA saldırganı durdurabilir.

Cihaz Yönetimi ve Uzaktan Silme: Cihazları yönetmek için seçenekleri kullanın. Örneğin, Dropbox ve OneDrive bağlı tüm cihazları (bilgisayarlar, telefonlar) listeler. Bir cihaz kaybolursa veya birisi ayrılırsa, uzaktan bağlantıyı kaldırabilir ve Dropbox'ta yerel olarak ayarlanmış dosyaları uzaktan silebilirsiniz. Google Drive (Yedekleme ve Senkronizasyon veya yeni Masaüstü için Drive), yerel dosyaları tamamen silmez çünkü bunlar genellikle sadece önbellekte bulunur, ancak erişimi iptal etmek yine de önemlidir. Google'ın yönetici paneli (Workspace için), cihaz yönetimini ayarlarsanız, bir kullanıcının mobil cihazındaki Drive'daki verileri silebilir. Otomatik silme yapamasanız bile, şifreyi değiştirip tüm oturumlardan çıkış yapmak (genellikle bir hesap güvenlik ayarıdır), kaybolan bir dizüstü bilgisayarın yeni verileri senkronize edememesini veya hesaba erişilememesini sağlamaya yardımcı olur.

Hassas Verilerin Şifrelenmesi: Daha önce de belirtildiği gibi, bu hizmetler sunucularındaki verileri şifrelerken, anahtarları da saklarlar (uçtan uca şifrelenmiş ancak daha az kullanılan MEGA veya SpiderOak gibi belirli ürünler hariç). Google Drive veya Dropbox'a özellikle hassas veriler koyuyorsanız, kendi şifreleme katmanınızı ekleyebilirsiniz. Seçenekler:

- **VeraCrypt** gibi araçları kullanarak şifreli bir konteyner oluşturun ve bu dosyayı Drive/Dropbox'ta saklayın. Daha sonra, şifre ile açmak için VeraCrypt'e ihtiyacınız olacaktır. Dezavantajları: Değişiklik yapıldığında tüm konteynerin yeniden senkronize edilmesi gerekir ve konteyner içinde eşzamanlı işbirliği yapmak kolay değildir.
- Dışarıdan paylaşmayı planladığınız belirli dosyaları yüklemeden önce **7-Zip** veya **WinZip** kullanarak şifreleyin. Güçlü bir şifre kullanın ve bu şifreyi farklı bir kanal üzerinden paylaşın.
- Bazı bulut hizmetleri, şifreli bir "kasayı" veya "kilitli dolabı" bir özellik olarak sunar (örneğin, Dropbox Professional'da Vault vardır). Aracınızın özelliklerini öğrenin.
- Office 365 kullanıyorsanız, dosyaları şifreleyen hassasiyet etiketleri uygulayabilir ve böylece yalnızca belirli hesapların dosyaları açabilmesini sağlayabilirsiniz (ancak bu, daha gelişmiş bir kurumsal özelliktir).
- Google kullanıyorsanız, Google teknik olarak bu dosyalara erişebildiğinden, gerekli olmadıkça Google Docs metinlerine son derece hassas içerik eklemekten kaçının. Belki çevrimdışı şifreli formatlar kullanıp bunları orada saklayabilir veya **Cryptomator** gibi bir araç kullanabilirsiniz. Cryptomator, buluta senkronize etmeden önce dosyaları istemci tarafında şifrelemek için tasarlanmış bir araçtır (sanal bir sürücü oluşturur; bu sürücüye bırakılan dosyalar şifrelenir ve ardından senkronize edilir). Cryptomator, Dropbox, Google Drive vb. ile iyi çalışır ve özel sunucu yazılımı gerektirmez (bulut, anlamsız dosyalar görür). Son derece gizli bilgileri işleyen bir CSO için, bu, verilerin bir alt kümesi için uygulanmaya değer olabilir.

İzleme ve Uyarılar: Bazı hizmetler etkinlik izlemeye izin verir. Örneğin, Dropbox hesap sayfasında paylaşım olaylarının ve oturum açma işlemlerinin bir günlüğünü gösterir. Google Workspace yöneticisi, "dışarıdan paylaşılan dosya" veya "şüpheli oturum açma girişimi" gibi durumlar için uyarılar ayarlayabilir. Mümkünse, bunları yapılandırın. Kişisel hesaplarda bile, Google Hesap Güvenliği yeni cihaz oturum açma girişimleri konusunda sizi uyarır – bu e-postalara veya uyarı mesajlarına ("X cihazından oturum açtınız mı?") dikkat edin.

Sosyal Mühendislik Hakkında Bilgilendirin: Saldırganlar Google'ı doğrudan hacklemeyebilir, ancak sizi kimlik avına uğratabilir. Örnek: Bir iş arkadaşınızdan Google Drive paylaşımı gibi görünen bir e-posta alırsınız, ancak bu aslında sahte bir Google giriş sayfasına yönlendiren, ustaca gizlenmiş bir kimlik avı bağlantısıdır. Google Drive kimlik avı, insanların Drive/Docs paylaşım e-postalarına güvendikleri için bilinen bir taktiktir. Bu nedenle, beklenmedik paylaşımları, giriş yapmadan önce doğrulayın. Google, Docs'a güvenlik taramaları ekleyerek iyileştirmeler yaptı, ancak yine de dikkatli olmak gerekir. Benzer şekilde, bulut şifrenizi beklenmedik bir şekilde açılan pencerelere girmeyin; istenirse drive.google.com adresine manuel olarak gidin.

Sürüm Geçmişi ve Fidye Yazılımı ***Koruması:*** Bulut depolamanın bir avantajı sürüm geçmişidir. Fidye yazılımı yerel dosyalarınızı şifreler ve bunlar buluta anlamsız bir şekilde senkronize edilirse, Dropbox ve OneDrive gibi hizmetler eski sürümleri birkaç gün boyunca saklar. Birçok dosyanın önceki sürümlerini geri yükleyebilirsiniz (Dropbox Pro'da genişletilmiş sürüm geçmişi seçeneği bile vardır). Bu süreci öğrenin. OneDrive (işletme) ayrıca, fidye yazılımı olayından sonra toplu olarak kurtarma yapmak için "Tüm dosyaları önceki bir zamana geri yükle" özelliğine sahiptir. Bu özelliğin var olduğunu bilin, ancak önlem almak, bu özelliğe ihtiyaç duymamanın anahtarıdır.

Kurumsal Hesaplar ve Kişisel Hesaplar: Mümkünse, bulut depolama için bir dizi kişisel hesap yerine, kuruluş tarafından yönetilen bir hesap kullanın. Örneğin, Google Workspace for Nonprofits (genellikle CSO'lar için ücretsiz/indirimli) ile Drive'da yönetilen hesaplar ([name]@CSO.org gibi) elde edersiniz. Bu şekilde, veriler kuruluşun mülkiyetinde olur ve birisi ayrıldığında bunları kontrol edebilirsiniz. Kişisel hesaplar verileri bireylere bağlar ve bu, kişi ayrıldığında karışıklığa neden olabilir. Ayrıca, kuruluşlar için Google Workspace ve Microsoft

365, ücretsiz hesaplara göre tasarım açısından daha iyi güvenlik kontrollerine sahiptir. Bu kar amacı gütmeyen kuruluşlara yönelik teklifleri (Google for Nonprofits, Microsoft for Nonprofits) inceleyin, çünkü bunlar düşük maliyetle veya hiç maliyet olmadan güvenliği (ve işbirliğini) önemli ölçüde artırabilir.

Düzenli Denetimler: Belki üç ayda bir veya altı ayda bir, zaman ayırarak bulut sürücülerinizi denetleyin. Artık ihtiyacınız olmayan eski verileri silin (maruz kalma riskini azaltır). Önemli klasörlerin paylaşım ayarlarını kontrol edin. Artık erişime ihtiyacı olmayan kullanıcıların erişimini kaldırın. Bu bakım, bulut ortamınızın düzenli ve güvenli kalmasını sağlar.

Özetle, Google Drive ve Dropbox gibi hizmetler akıllıca kullanıldığında CSO'lar için güvenli olabilir: hesapları güçlü kimlik doğrulama ile koruyun, paylaşımı dikkatlice yapılandırın ve çok hassas dosyalar için ek şifreleme ekleyin. Kolaylık ve işbirliği avantajları çok büyüktür, bu nedenle esas olarak araçların güvenlik özelliklerini en iyi şekilde kullanmak önemlidir. Bu platformlarda meydana gelen olayların çoğu, sağlayıcıların ihlal edilmesinden ziyade insan hatasından (yanlışlıkla bir bağlantıyı herkese açık olarak paylaşmak veya zayıf bir parola kullanmak gibi) kaynaklanmaktadır. Bu insan faktörlerini ve teknik ayarları ele alarak buluttan güvenle yararlanabilirsiniz.

Telefonunuzu ve Bilgisayarınızı Koruma

Önceki bölümlerde genel cihaz güvenliği uygulamalarını ele aldık. Burada, tüm dijital kaynaklarınıza eriştiğiniz uç noktalar olan bilgisayarlarınızı ve mobil cihazlarınızı daha da güvenli hale getirmek için bazı özel araçlar ve ayarlara değineceğiz.

f Tüm dizüstü bilgisayarlarda ve mobil cihazlarda FDE'nin etkinleştirildiğinden emin olun. Modern bilgisayarlarda, bunun için genellikle sadece özelliği açmak yeterlidir:

- Windows 10/11: **BitLocker'ı** (Pro sürümlerinde) veya Home'daki Aygıt Şifreleme'yi (varsa) kullanın. Etkinleştirildiğinde, tüm sürücüyü şifreler ve şifre çözme işlemini şifrenize/PIN kodunuza (ve TPM yongasına) bağlar. BitLocker, USB sürücüleri de şifreleyebilir (bunun için BitLocker To Go'yu kullanabilirsiniz).
- macOS: Güvenlik ayarlarında **FileVault'u** etkinleştirin; Mac'in diskini şifrelemek için tek bir tıklama yeterlidir.

- Linux: Linux kullanıyorsanız, LUKS şifrelemeyi etkinleştirerek yükleyin veya cryptsetup gibi bir araç kullanın. Birçok kullanıcı dostu dağıtım, yükleme sırasında şifrelemeyi etkinleştirmeye izin verir.
- Android: Çoğu modern Android cihaz, varsayılan olarak depolama alanını şifreler (özellikle Android 7.0+ sürümlerinden itibaren). Şifreleme, kilit ekranı kadar güçlü olduğundan, güçlü bir PIN/parola/desen belirlediğinizden emin olun.
- iPhone/iPad'ler: Bir şifre belirlediğiniz sürece otomatik olarak donanım şifrelemesi yapılır. Bu nedenle her zaman bir şifre kullanın (ve kolaylık için Touch/Face ID'yi kullanın, ancak bu şifreye yedek olarak kilitlenir).

Mobil Cihaz Güvenlik Uygulamaları: Android için, saygın bir güvenlik uygulaması yüklemeyi düşünün. Seçenekler: **Google Play Protect** yerleşiktir ve uygulamaları tarar (Play Store ayarlarında etkinleştirildiğinden emin olun). **Avast Mobile**, **Bitdefender Mobile** veya **Lookout** gibi üçüncü taraf AV uygulamaları, kimlik avı koruması ve telefonumu bulma özellikleri ekleyebilir. Ayrıca, Play Protect'in bulduklarından daha fazla kötü amaçlı uygulamayı tarayabilirler (Google'ın uygulaması da iyidir). iOS için, sanal alan nedeniyle ayrı güvenlik uygulamalarına daha az ihtiyaç vardır (ancak Lookout gibi uygulamalar, telefonunuzu bulmaya veya iOS'unuzun jailbreak yapılıp yapılmadığını kontrol etmeye yardımcı olabilir).

***Cihazımı Bul*:** Bulma ve uzaktan silme hizmetlerini her zaman etkinleştirin:

- Android: **Cihazımı Bul** (bir Google hizmeti) özelliğini kullanın – telefonunuzda bir Google hesabınız varsa bu özellik genellikle açıktır. Bu özelliği test edin (Google'da "cihazımı bul" yazın ve telefonunuzun bulunup bulunmadığını kontrol edin).
- Samsung cihazlarda ayrıca daha fazla özelliğe sahip bir alternatif olan **Find My Mobile (**Mobil Cihazımı Bul**)** özelliği de vardır.
- iPhone: **iPhone'umu Bul özelliğinin** açık olduğundan emin olun (iCloud ayarlarında). Bu, kaybolan bir telefonu bulmanızı veya silmenizi sağlar.
- Dizüstü bilgisayarlar: Hırsızlık endişeniz varsa, bir dizüstü bilgisayar izleme yazılımı kullanmayı düşünün. PreyProject (Prey), üç cihaza kadar ücretsiz bir plan sunar ve kaybolan/çalınan bir dizüstü bilgisayarı bulmanıza, hatta fotoğraf

çekmenize veya mesaj göndermenize yardımcı olabilir. Bazı iş dizüstü bilgisayarlarında hırsızlık önleme özelliği yerleşik olarak bulunur (Computrace/LoJack gibi). Ancak özel bir yazılım olmasa bile, dizüstü bilgisayar kaybolursa, erişimi olan hesapların şifrelerini hemen değiştirin ve şifrelenmişse en azından verilerin güvende olduğunu bilin.

Bilgisayarlarda Güvenlik Duvarı: Windows Güvenlik Duvarı varsayılan olarak açıktır – açık tutun. İstenmeyen gelen trafiği engelleyerek sessizce görevini yerine getirir. Gerekirse belirli uygulamaların giden trafiğini engellemek için de kullanabilirsiniz (CSO senaryosu için daha az yaygındır). Mac'te, Güvenlik tercihlerinde güvenlik duvarını açın. Muhtemelen üçüncü taraf güvenlik duvarı yazılımına ihtiyacınız yoktur; yerleşik olanlar yeterlidir ve teknoloji konusunda çok bilgili olmayanların yine de izin verebileceği kafa karıştırıcı uyarıları önler.

Firmware ve BIOS Güvenliği: Yüksek güvenlik gereksinimleri için, dizüstü bilgisayarlarda BIOS/UEFI şifresi belirlemeyi düşünün (böylece harici medyadan önyükleme yapmak veya önyükleme ayarlarını değiştirmek için şifre gerekir). Ayrıca Güvenli Önyükleme'yi etkinleştirin (rootkit'leri önlemek için). Bu adımlar, fiziksel erişimi olan bir saldırganın, örneğin canlı bir işletim sistemi önyükleyerek sistem güvenliğinizi atlamasını önler. Bununla birlikte, FDE ve güçlü bir şifreniz varsa, saldırganlar yine de içeri giremez. Ancak BIOS şifresi, makinenin kurcalanmasına veya kullanılmasına karşı bir katman daha ekler.

Cihaz Güncellemeleri Otomasyonu: İşletim sistemi güncellemelerinden bahsettik; ek olarak:

- Uygulamaları güncel tutun, örneğin Microsoft Office veya LibreOffice'in güncel olduğundan emin olun (Office genellikle Office 365 varsa otomatik olarak güncellenir, yoksa Windows Update veya Office'in güncellemesini kontrol edin).
- PDF okuyucu: Acrobat Reader kullanıyorsanız, onu güncelleyin. Veya **SumatraPDF** veya tarayıcınızın PDF görüntüleyicisi gibi daha güvenli, daha basit ve daha az istismar edilen bir okuyucu kullanın.
- Java: Eğer kullanmanız gerekiyorsa, otomatik olarak güncellenmesini ayarlayın. İhtiyacınız yoksa, tamamen kaldırın.

- Telefonlarda, güncellemeler mevcut olduğunda Play Store/App Store üzerinden uygulamaları güncelleyin (kolaylık sağlamak için Wi-Fi üzerinden otomatik güncellemeyi etkinleştirin).

Gereksiz Özellikleri Devre Dışı Bırakın: Kullanılmayan açık kapılar kapatılabilir:

- Windows'ta, RDP (Uzak Masaüstü) veya dosya paylaşımı gibi özelliklere ihtiyacınız yoksa, saldırı yüzeyini azaltmak için bunları kapatın.
- Telefonlarda Bluetooth ve NFC'ye dikkat edin – kullanmadığınız zamanlarda kapalı tutun (Bluetooth saldırıları artık yamalar sayesinde daha az yaygın, ancak yine de özellikle kamusal alanlarda iyi bir güvenlik önlemi).
- Telefonlarda kullanmadığınız bloatware uygulamalarını, özellikle arka planda çalışabilen veya izinlere sahip olanları kaldırın (bazı Android telefonlarda veri madenciliği yapabilen önceden yüklenmiş uygulamalar bulunur).
- Herhangi bir sistemde, günlük kullanım için yönetici olarak oturum açmayın. Rutin işler için standart bir kullanıcı hesabı ve yazılım yüklemek için bir yönetici hesabı oluşturun. Bu şekilde, kötü amaçlı yazılım çalışırsa, derin değişiklikler yapmak için yönetici haklarına sahip olmayabilir. Kuşkusuz, birçok kişi bunu görmezden gelir, ancak bu Windows ve Linux'ta önerilen bir uygulamadır. Mac'te, ilk kullanıcı yöneticidir, ancak Mac, ayrıcalıkları ayırmaya benzer şekilde çalışan şifre yükseltme isteğinde bulunur.

İyi bir güvenlik yazılımı paketi kullanın: Bütçe izin veriyorsa veya ücretsiz seçenekler yeterliyse, kapsamlı bir güvenlik paketi kullanın. Örneğin, **Microsoft Defender** aslında sadece kötü amaçlı yazılımdan koruma değil, aynı zamanda Kontrollü Klasör Erişimi (bilinmeyen uygulamaların belgelerinizi düzenlemesini engelleyen fidye yazılımı koruması) ve etkinleştirildiğinde bulut tabanlı koruma da içerir. Üçüncü taraf paketler şifre yöneticisi, VPN deneme sürümü vb. içerebilir. Yalnızca bu ekstra özelliklere ihtiyacınız varsa yatırım yapın; aksi takdirde, katmanlı bireysel araçlar da işe yarar.

Cihazda E-posta Güvenliği: Outlook veya Thunderbird gibi bir e-posta istemcisi kullanıyorsanız, güncellendiğinden emin olun. Açtığınız ek dosyalara dikkat edin. Modern e-

posta istemcileri bazı sanal alanlara sahiptir (örneğin Outlook, varsayılan olarak görüntüleri yüklemez veya makroları çalıştırmaz ve bir uygulama e-posta verilerine erişmeye çalıştığında uyarı verir). Bazı entegrasyonlar için gerekli olmadıkça "programlı erişime izin ver" seçeneğini etkinleştirmeyin.

Fiziksel Korumalar: Dizüstü bilgisayarlar – paylaşılan bir alanda bırakıyorsanız (fırsatçı hırsızları caydırmak için) Kensington kilit kablosu kullanmayı düşünün. Telefonlar için, halka açık yerlerde hassas bilgilerle çalışıyorsanız koruyucu kılıflar ve belki de gizlilik ekran koruyucuları kullanın (omuz üzerinden bakmayı önler).

Cihazlar için Veri Yedeklemeleri: Yedeklemelerden bahsettik, ancak bir husus daha var: mobil cihazlar için verilerinizi de yedekleyin (bulut yedekleme veya manuel). iPhone'lar için iCloud veya yerel iTunes yedeklemelerini kullanın; Android için, kritik veriler için Google'ın yedekleme hizmetlerini veya uygulamalarını kullanın. Bu şekilde, cihazınızı kaybetmeniz veri kaybı anlamına gelmez ve verilerinizin kaydedildiğini bilerek tereddüt etmeden uzaktan silebilirsiniz.

Hırsızlık Önleyici Etiketleme: Bazen en basit çözümler en iyisidir: Cihazlarınızı iletişim bilgileriyle etiketleyin. Kayıp bir cihazı bulan kişi, kolay olursa onu iade edebilir ("Bulursanız, [CSO numarası]'nı arayın" yazan bir etiket gibi). Bu, güvenlikten çok kurtarma ipucudur, ancak günü kurtarabilir.

Cihaz Değiştirme Planı: Bir cihazın güvenliği ihlal edildiğinde veya eski olduğunda basit bir planınız olsun. Örneğin, bir bilgisayar artık güncelleme almıyorsa (Windows 7, eski Android), onu kullanımdan kaldırın veya hassas görevlerden uzak tutun. Gerekirse eski bir şey için çevrimdışı olarak kullanabilirsiniz. Ancak güvenlik için donanımı desteklenen ömrü boyunca kullanmaya yatırım yapın.

Telefonlarınızda ve bilgisayarlarınızda yukarıdaki yöntemleri ve araçları kullanarak, kişisel ve iş verilerinizin etrafında güçlü bir savunma çemberi oluşturursunuz. Cihazınızı güvenli bir kasa olarak düşünün: onu kilitlediniz (güçlü oturum açma), alarm kurdunuz (antivirüs ve güvenlik duvarı), güçlendirdiniz (güncellemeler ve şifreleme) ve çalınması durumunda içeriğini bulmak veya yok etmek için bir yol ayarladınız (cihazımı bul, uzaktan sil). Bu tür önlemlerle, tehditler

ortaya çıksa bile, bunları engellersiniz veya felaketle sonuçlanacak bir kayıp yaşamadan yanıt vermeye hazır olursunuz.

Bu, araçlar ile ilgili bölümü sonlandırır. Güvenli uygulamaları benimseyerek (4.1), güvenli gezinmeyi uygulayarak (4.2), bulut depolamayı doğru kullanarak (4.3) ve cihazları güçlendirerek (4.4), CSO'nuz çok daha güçlü bir dijital güvenlik duruşuna sahip olacaktır. Şimdi, tüm bunlara rağmen bir siber sorun meydana gelirse ne yapmanız gerektiğini ele alacağız. Hiçbir savunma %100 mükemmel olamayacağından, bir müdahale planına sahip olmak hayati önem taşır.

Bölüm Özeti

4. bölüm, bilgisayarlar, ağlar ve web siteleri dahil olmak üzere CSO'ların kullandığı teknolojinin güvenliğini sağlamaya odaklanmaktadır. Yazılımları güncel tutarak güvenlik açıklarını gidermeyi, kötü amaçlı yazılımlarla mücadele etmek için antivirüs araçları (ör. Avast Free) kullanmayı ve WPA2/WPA3 şifreleme ile Wi-Fi güvenliğini sağlamayı önermektedir. Web siteleri için ise, HTTPS'yi etkinleştirmeyi, düzenli yedeklemeler yapmayı ve İçerik Yönetim Sistemlerini (ör. WordPress) güncellemeyi, böylece tahrifat veya DDoS saldırılarını önlemeyi tavsiye etmektedir. Eski yazılım nedeniyle bir CSO'nun web sitesinin üçüncü taraf bir siteye yönlendirilmesi vakası, bu riskleri göstermektedir. Bu bölüm, saha personeli için hayati önem taşıyan kamuya açık Wi-Fi ağlarında güvenli bağlantı için VPN'leri (ör. ProtonVPN) önermektedir. CSO'ların bütçelerine uygun, Let's Encrypt aracılığıyla ücretsiz HTTPS gibi düşük maliyetli çözümleri vurgulamaktadır. Teknik bilgiye sahip olmayan personel, BT uzmanlığı gerektirmeden ayarları doğrulamaları (örneğin, HTTPS kilitlerini kontrol etmeleri) konusunda yönlendirilir. Bu bölümde ayrıca hırsızlık veya kayıplara karşı koruma sağlamak için cihaz şifreleme ve güçlü parolalar da ele alınmaktadır. Altyapıyı güvenli hale getirerek, CSO'lar kesintileri ve veri ihlallerini önler ve misyonun sürekliliğini sağlar. Otomatik güncellemeleri planlamak gibi bu bölümdeki pratik adımlar, uygulamayı kolaylaştırır ve e-kitabın erişilebilir siber güvenlik hedefiyle uyumludur.

CSO'lar için Sosyal Medya Hesabı Güvenlik Kontrol Listesi

Bu kontrol listesi, CSO'ların sosyal medya hesaplarını (ör. Twitter/X, Facebook, Instagram) güvence altına almalarına yardımcı olarak çevrimiçi varlıklarını ve itibarlarını ele geçirilme, yanlış bilgilendirme veya yetkisiz erişimden korur. Bu adımlar, teknik uzmanlığı minimum düzeyde olan program personeli ve gönüllüler tarafından bir veya iki saat içinde tamamlanacak şekilde tasarlanmıştır. Her bir maddeyi inceleyin ve tamamlanan görevleri işaretleyin. Emin değilseniz, sosyal medya yöneticinize, BT irtibat kişinize veya platform desteğine yardım isteyin. Güvenli bir çevrimiçi varlığı sürdürmek için bulguları ekibinizle paylaşın.

1. İki Aşamalı Kimlik Doğrulamayı (2FA) Etkinleştirin

⇒ Tüm sosyal medya hesapları için 2FA'yı etkinleştirerek ikinci bir doğrulama adımı (ör. telefonunuza veya uygulamanıza gönderilen bir kod) gerektirin.

⇒ Platform İpuçları:

- Twitter/X: Ayarlar > Gizlilik ve Güvenlik > İki Aşamalı Kimlik Doğrulama'ya gidin. Bir kimlik doğrulama uygulaması (ör. Google Authenticator) veya SMS seçin.
- Facebook: Ayarlar > Güvenlik ve Giriş > İki Aşamalı Kimlik Doğrulama'ya gidin. Bir kimlik doğrulama uygulaması veya kısa mesaj seçin.
- Instagram: Ayarlar > Güvenlik > İki Aşamalı Kimlik Doğrulama'ya gidin. Uygulama tabanlı veya SMS kimlik doğrulamasını etkinleştirin.

⇒ Örnek: Hacklenen bir CSO Twitter hesabı sahte mesajlar yayınladı. 2FA, daha fazla yetkisiz erişimi engelledi.

⇒ Her hesaba giriş yapın, 2FA'yı etkinleştirin ve ekibinizin cihazlarıyla test edin.

2. Güçlü, Benzersiz Parolalar Kullanın

⇒ Şifreleri en az 14 karakter olacak şekilde güncelleyin, harfleri, rakamları ve sembolleri karıştırın (ör. "sunbird&glass7rain"). Her hesap için farklı bir şifre kullanın.

⇒ Şifreleri güvenli bir şekilde saklamak için ücretsiz bir şifre yöneticisi (ör. Bitwarden) kullanmayı düşünün.

⇒ Platform İpuçları:

- Twitter/X: Ayarlar > Şifreyi Değiştir bölümünden güncelleyin. Diğer platformlardaki şifreleri tekrar kullanmaktan kaçının.
- Facebook: Ayarlar > Güvenlik ve Giriş > Şifreyi Değiştir seçeneğine gidin. E-posta veya diğer hesaplardan farklı ve benzersiz bir şifre olduğundan emin olun.
- Instagram: Ayarlar > Güvenlik > Şifre bölümüne gidin. Daha kolay hatırlamak için bir şifre cümlesi kullanın.

⇒ Örnek: Bir CSO'nun Instagram hesabı, yeniden kullanılan e-posta şifresi nedeniyle ele geçirildi. Benzersiz bir şifre ile sorun çözüldü.

⇒ Tüm hesapların şifrelerini değiştirin ve bir şifre yöneticisinde saklayın.

3. Kullanılmayan Yönetici Hesaplarını Silin

⇒ Sosyal medya hesaplarınıza yönetici veya editör erişimi olan kişileri kontrol edin ve eski çalışanları, gönüllüleri veya aktif olmayan kullanıcıları kaldırın.

⇒ Platform İpuçları:

- Twitter/X: Ayarlar > Yaratıcı Abonelikleri > Ekibi Yönet seçeneğine giderek yöneticileri inceleyin ve kaldırın.
- Facebook: Sayfa Ayarları > Sayfa Rolleri'ne gidin ve gereksiz yöneticileri veya editörleri görüntüleyin ve silin.
- Instagram: Ayarlar > Yetkili Uygulamalar veya İşletme Ayarları > Kullanıcılar'a gidin ve kullanılmayan hesapların erişimini iptal edin.

⇒ Örnek: Eski bir gönüllünün yönetici erişimi, yetkisiz içerik yayınlamak için kullanıldı. Eski yöneticileri kaldırmak, bunun tekrarını önledi.

⇒ Sosyal medya yöneticinize şunu sorun: "Eski yönetici hesaplarını inceleyip kaldırabilir miyiz?"

4. Kurtarma E-postası/Telefonunu Ayarla ve Doğrula

⇒ Her hesabın, kilitlendiğinde veya hacklendiğinde hesap kurtarma için güvenilir personel tarafından kontrol edilen güncel bir kurtarma e-postası veya telefon numarası olduğundan emin olun.

- Platform İpuçları:
    - Twitter/X: Ayarlar > Hesabınız > Hesap Bilgileri'nden güncelleyin. Kurtarma e-postasının aktif olduğunu doğrulayın.
    - Facebook: Ayarlar > Güvenlik ve Giriş > İletişim bölümüne gidin ve kurtarma e-postası/telefon numarasını ekleyin veya güncelleyin.
    - Instagram: Ayarlar > Güvenlik > Hesap Kurtarma bölümüne gidin ve geçerli bir e-posta veya telefon numarasını onaylayın.

⇒ Örnek: Bir CSO, kurtarma e-postasını kullanarak hacklenmiş Facebook hesabını geri aldı. Bu e-posta olmasaydı, kurtarma işlemi haftalar sürerdi.

⇒ Kurtarma bilgilerini ekleyin veya güncelleyin ve kurtarma kodu isteyerek test edin.

5. Hesap Etkinliğini İzleyin

⇒ Olağandışı etkinlikleri (ör. sizin oluşturmadığınız gönderiler, bilinmeyen konumlardan yapılan oturum açma girişimleri) düzenli olarak kontrol edin.

⇒ Şüpheli etkinliklerle ilgili bildirimler almak için mevcutsa oturum açma uyarılarını etkinleştirin.

⇒ Platform İpuçları:

- Twitter/X: Ayarlar > Gizlilik ve Güvenlik > Bağlı Hesaplar bölümünde tanıdık olmayan cihazlar veya uygulamalar olup olmadığını kontrol edin.

- Facebook: Ayarlar > Güvenlik ve Giriş > Giriş Yaptığınız Yerler bölümüne giderek aktif oturumları inceleyin. Giriş uyarılarını etkinleştirin.
- Instagram: Ayarlar > Güvenlik > Oturum Açma Etkinliği'ne gidin ve oturum açma konumlarını görün ve bildirimleri etkinleştirin.

⇒ Örnek: Bir CSO, başka bir ülkeden yapılan bir oturum açma işlemini fark etti ve zarar vermeden hesabı kilitledi.

⇒ Etkinlik günlüklerini haftalık olarak inceleyin ve olağandışı davranışları platform desteğine bildirin.

6. Üçüncü Taraf Uygulama Erişimi Sınırlayın

⇒ Artık kullanılmayan veya güvenilir olmayan üçüncü taraf uygulamaların veya araçların (ör. planlama araçları, analiz uygulamaları) erişimini kaldırın.

⇒ Platform İpuçları:

- Twitter/X: Ayarlar > Gizlilik ve Güvenlik > Bağlı Hesaplar bölümüne giderek uygulama izinlerini iptal edin.
- Facebook: Kullanılmayan veya şüpheli uygulamaları kaldırmak için Ayarlar > Uygulamalar ve Web Siteleri'ne gidin.
- Instagram: Ayarlar > Güvenlik > Uygulamalar ve Web Siteleri'ne giderek gereksiz uygulamaların erişimini iptal edin.

⇒ Örnek: CSO'nun Twitter hesabında spam göndermek için eski erişim iznine sahip bir planlama uygulaması kullanıldı. Erişim izni iptal edilerek sorun çözüldü.

⇒ Hesap ayarlarında gereksiz uygulama bağlantılarını inceleyin ve kaldırın.

7. Personeli Güvenli Sosyal Medya Kullanımı Konusunda Eğitin

⇒ Personel ve gönüllülere, hesap bilgilerini paylaşmamalarını, şüpheli bağlantılara tıklamamalarını veya sosyal medyada hassas verileri (ör. bağışçı bilgileri) paylaşmamalarını hatırlatın.

⇒ Bir ipucu paylaşın: "Paylaşılan veya halka açık cihazlarda hesaplardan çıkış yapın."

⇒ Örnek: Bir gönüllü, halka açık bir Instagram gönderisinde hassas kampanya ayrıntılarını paylaştı. Eğitim, gelecekte benzer hataların tekrarlanmasını önledi.

⇒ Ekibe bir e-posta gönderin: "Sosyal medya giriş bilgilerinizi asla paylaşmayın. Paylaşılan cihazlarda kullandıktan sonra oturumu kapatın."

8. Yanlış Bilgilendirme veya Hesap Ele Geçirme Durumları için Plan Yapın

⇒ Hacklenen hesaplar veya yanlış bilgiler için basit bir müdahale planı geliştirin (ör. platform raporu, takipçilere açıklama yayınlama).

⇒ Hazır bir açıklama taslağı bulundurun: "Hesabımız ele geçirildi. Lütfen son gönderileri dikkate almayın. Bu sorunu çözüyoruz."

⇒ Platform İpuçları:

- Twitter/X: Hacklemeleri help.twitter.com/forms/security adresinden bildirin.
- Facebook: Facebook.com/hacked adresini kullanarak ele geçirilen hesapları bildirin.
- Instagram: Sorunları Ayarlar > Yardım > Hacklenmiş Hesabı Bildir üzerinden bildirin.

⇒ Örnek: Bir CSO, Facebook'ta hacklenmiş bir gönderiyi hızlı bir şekilde açıklığa kavuşturarak yanlış bilginin yayılmasını engelledi.

⇒ Hızlı erişim için bir yanıt metni hazırlayın ve platform destek bağlantılarını kaydedin.

BÖLÜM 5: ÖRNEK SİBER GÜVENLİK OLAY SENARYOLARI

Siber Olay Yaşarsanız Ne Yapmalısınız

Önleme konusunda en iyi çabaları göstermenize rağmen, olaylar yine de meydana gelebilir. Hızlı, sakin ve metodik bir yanıt, siber olayın neden olduğu zararı önemli ölçüde azaltabilir. Bu bölümde, olayın belirtilerini tanıma, hemen atılması gereken adımlar, yardım için kiminle iletişime geçilmesi gerektiği ve olaydan sonra güvenliği nasıl geri kazanabileceğiniz konusunda rehberlik edilmektedir. Esasen, bu bölüm dijital alem için acil durum eylem planınızdır.

Siber Saldırının Belirtilerini Tanımak

Bir sorun olduğunu ne kadar çabuk fark ederseniz, o kadar hızlı tepki verebilirsiniz. Siber saldırılar çeşitli şekillerde ortaya çıkabilir; bazıları bariz, bazıları ise daha belirsizdir. Aşağıda, bir sorunu işaret edebilecek yaygın uyarı işaretleri bulunmaktadır:

F***idye Yazılımı Mesajı veya Kilitli Ekran:*** Çok açık bir işaret – bilgisayarınız aniden dosyalarınızın şifrelendiğini belirten bir mesaj görüntüler veya sisteminizin kilidini açmak için fidye talep eder. Dosyaları açamayabilirsiniz ve dosyalar garip uzantılara sahip olabilir. Genellikle arka plan talimatlarla değişebilir veya dosyaları ve ödeme talimatlarını listeleyen bir pencere açılabilir. Bunu görürseniz, neredeyse kesin olarak bir fidye yazılımı saldırısıdır.

Antivirüs Uyarıları veya Sahte AV Açılır Pencereleri: Antivirüsünüz bir şey yakalarsa, bunu ciddiye alın. Tersine, "Bilgisayarınız virüs bulaşmış! Taramak için buraya tıklayın" diyen sahte bir açılır pencere görürseniz ve bu, antivirüsünüzden değil bir web sitesinden geliyorsa, bu sizi kötü amaçlı yazılım yüklemeye yönlendirmek için kullanılan bir taktiktir. Farkı anlayın: Gerçek antivirüs yazılımınız tanıdık bir arayüze sahiptir ve rastgele bir tarayıcı reklamı yoluyla uyarı vermez.

Beklenmedik Araç Çubukları veya Tarayıcı Davranışı: Tarayıcınızda aniden yeni araç çubukları belirir, ana sayfanız/arama motorunuz sizin müdahaleniz olmadan değişir veya aramalarınız garip sitelere yönlendirilir. Bu, reklam yazılımı veya kötü amaçlı yazılımın yüklendiğini gösterir. Benzer şekilde, çevrimdışı olduğunuzda veya normalde reklam göstermeyen sitelerde sık sık açılan reklamlar da bir enfeksiyonun göstergesi olabilir.

Tanıdık Olmayan Programlar veya İşlemler: Hiç yüklemediğiniz bir uygulama fark edersiniz. Ya da bilgisayarınızın fanı yüksek hızda çalışıyor ve bilgisayarınız yavaşlıyor ve Görev

Yöneticisi/Etkinlik Monitörü, CPU'yu meşgul eden bilinmeyen işlemler gösteriyor. Bazı kötü amaçlı yazılımlar görünmez bir şekilde çalışabilir, ancak çoğu kaynak tüketir (kripto madenciliği gibi, sisteminizi yavaşlatır). Kısa bir süre açılıp sonra kaybolan bir program veya masaüstünde yeni simgeler görürseniz, araştırın.

Arkadaşlarınız Sizden Garip Mesajlar Alıyor: İş arkadaşlarınız veya arkadaşlarınız sizden göndermediğiniz garip bir e-posta veya sosyal medya mesajı aldıklarını söylüyorsa, hesabınız ele geçirilmiş olabilir. Örnekler: adresinizden gönderilen spam e-postalar veya WhatsApp'ınızın grup sohbetlerinde şüpheli bir bağlantı göndermesi. Bu, cihazınızın veya hesabınızın ele geçirildiğinin bir işaretidir.

Şifre Çalışmıyor: Şifre değiştirildiği için (ve siz değiştirmediğiniz halde) bir hesaba aniden giriş yapamamanız çok endişe verici bir işarettir. Bildiğiniz doğru şifre reddediliyorsa ve hesap kurtarma işlemi bir değişiklik olduğunu gösteriyorsa, o hesabın ele geçirildiğini varsayabilirsiniz.

Olağandışı Ağ veya Sistem Etkinliği: Bu, ortalama bir kullanıcı için fark edilmesi daha zor olabilir, ancak bir ağ izleme aracınız veya BT yöneticiniz varsa: örnekler arasında giden trafiğin artması, ağda bilinmeyen cihazlar veya hiçbir şey yapmadığınız halde sabit sürücü ışığının sürekli yanıp sönmesi sayılabilir (bu, verilerin sızdırıldığı veya dosyalarınızı tarayan bir virüs olduğu anlamına gelebilir). Ayrıca, güvenlik duvarı uyarılarını (varsa) veya Windows Defender günlüklerini tekrarlanan engellenen eylemler için kontrol edin.

Kayıp veya Değiştirilmiş Dosyalar: Dosyaların açıklanamayan bir şekilde silindiğini veya içeriğinin değiştirildiğini fark ederseniz, bu endişe vericidir. Veriler bir saldırgan tarafından silinmiş veya tahrif edilmiş olabilir. Ayrıca, isimleri bozuk olan veya kilitli veya şifreli gibi uzantıları olan dosyalar görürseniz, bu fidye yazılımının varlığını gösterir.

Garip İmleç veya Kontrol: Aşırı durumlarda, fareniz kendi kendine hareket ediyorsa veya pencereler açılıyorsa ve bunu siz yapmıyorsanız, birisi uzaktan kontrol sahibi olabilir (uzaktan masaüstü veya RAT kötü amaçlı yazılımı çalışıyormuş gibi). Bu durumda, derhal internet bağlantısını kesin.

Sistem Uyarıları veya Çökme Ekranları: Tekrarlanan çökmeler veya mavi ekranlar sadece donanım/yazılım sorunları olabilir, ancak bazen rootkitler veya derin kötü amaçlı

yazılımlar kararsızlığa neden olur. Diğer belirtilerle birlikte bu durum ortaya çıkmaya başladıysa, kötü amaçlı yazılım olasılığını göz önünde bulundurun.

Tarayıcı Yönlendirmeleri: Yaygın siteleri (banka veya Gmail gibi) ziyaret etmeye çalıştığınızda sürekli olarak biraz farklı bir URL'ye yönlendiriliyorsanız veya beklenmedik bir şekilde sertifika uyarıları görüyorsanız, kötü amaçlı yazılım veya DNS kaçırma sorunu yaşıyor olabilirsiniz. Örneğin, facebook.com adresine gitmeye çalışırken her zaman doğru görünmeyen bir sayfaya yönlendiriliyorsanız, bu bir sorun olduğunu gösterir.

Uygulamada, bu belirtilerin çoğu birbiriyle örtüşür. Örneğin, bir fidye yazılımı saldırısı şifrelenmiş dosyalar (açamayacağınız) ve muhtemelen her klasörde bir fidye notu metin dosyası ve belki de bunu duyuran değiştirilmiş bir masaüstü duvar kağıdı oluşturur. Kimlik avı hesap ihlalleri genellikle başkaları size garip mesajlar bildirdiğinde veya olağandışı yerlerden oturum açma uyarıları aldığınızda keşfedilir.

Bir sorun olduğundan şüpheleniyorsanız ancak emin değilseniz, tedbirli davranın:

- Potansiyel bir virüsse, tam bir antivirüs taraması yapın.
- Bir hesap ele geçirilmiş olabilirse, farklı bir güvenli cihazdan oturum açmayı deneyin ve hala mümkünse şifreyi değiştirin veya hesap etkinlik günlüklerini kontrol edin.
- Ağ kullanımını takip edin (Windows 10'da, Görev Yöneticisi'nde de uygulama başına ağ kullanımını görebilirsiniz).
- Cihazınızda bir tanılama veya güvenlik tarama aracı (Windows Güvenlik veya üçüncü taraf bir araç gibi) varsa, bunu kullanın.

Önemli olan uyanık olmaktır. Bir CSO uygulaması, personeli "bilgisayarları garip davranıyorsa" bunu bildirmeleri için teşvik etmektir. Gerçek bir ihlali gözden kaçırmaktansa, yanlış alarmları araştırmak daha iyidir. Potansiyel damgalama nedeniyle bildirim yapılmasına engel olmayın; güvenlik eğitiminde, zamanında bildirim yapmanın çok önemli olduğunu ve endişelerini dile getirdikleri için suçlanmayacaklarını vurgulayın.

Artık neye dikkat etmeniz gerektiğini bildiğinize göre, bir sonraki adım, bir sorun olduğunda hemen harekete geçmektir. Aşağıdaki bölümlerde acil müdahale adımları, kime yardım çağrısı yapılacağı ve nasıl kurtarma işlemi yapılacağı ele alınacaktır.

Adım Adım Müdahale: Bir Sorun Olduğunda Ne Yapmalı

Bir siber olayın meydana geldiğini fark ettiğiniz anda, sorunu kontrol altına almak ve araştırmak için bilinçli adımlar atmak çok önemlidir. Paniklemek veya yanlış şeyler yapmak (örneğin, hemen fidye ödemek veya kanıtları silmek) durumu daha da kötüleştirebilir. İşte CSO ortamı için basitleştirilmiş terimlerle standart olay müdahale aşamalarına (tespit etme, kontrol altına alma, ortadan kaldırma, kurtarma) uygun adım adım kılavuz:

1. **Panik Yapmayın, Durumu Değerlendirin: Derin** bir nefes alın ve neler olduğunu anlamaya çalışın. Belirtiler ve kapsam nedir? Örneğin, bir bilgisayar mı yoksa birden fazla bilgisayar mı garip davranıyor? Hesap sorunu mu yoksa cihaz sorunu mu? Olayın niteliğini belirlemek, sonraki adımları yönlendirir. Gözlemlediklerinizi (zaman, belirtiler) not alın. Gerekirse, şüpheli mesajların veya hata ekranlarının fotoğraflarını veya ekran görüntülerini telefonunuzla hızlıca çekin (kanıt olarak ve daha sonra uzmanlara danışmak için yararlıdır).

2. **Etkilenen Sistemlerin Bağlantısını Kesin:** Aktif bir kötü amaçlı yazılımdan şüpheleniyorsanız, özellikle veriler çalınıyor olabilirse veya daha fazla sistem enfekte olmuşsa, makineyi derhal ağdan izole edin. Ethernet kablosunu çıkarın veya Wi-Fi'yi kapatın. Bu, yayılmayı önler (örneğin, bazı solucanlar veya fidye yazılımları ağ sürücülerine atlamaya çalışır) ve saldırganın uzaktan kontrolünü veya veri sızdırmasını durdurur. Ancak, mecbur kalmadıkça sistemi kapatmayın; sadece ağ bağlantısını kesin. Burada bir nüans vardır: sistemi kapatmak kötü amaçlı yazılımı durdurur, ancak geçici kanıtları da silebilir. Çoğu CSO senaryosunda, sistemi açık ve bağlantısı kesik bırakıp taramaları çalıştırmak uygundur. Ancak fidye yazılımı gözünüzün önünde aktif olarak dosyaları şifreliyorsa, bunu durdurmak için sistemi hızlıca kapatabilirsiniz. Kendi kararınızı verin; şüpheniz varsa, ağ bağlantısını kesmek iyi bir ilk adımdır.

3. **Hesaplarınızı Güvenli Hale Getirin:** Bir hesap (e-posta veya sosyal medya gibi) ele geçirilmişse, **kontrolü geri kazanmaya çalışın**. Hesap kurtarma akışlarını kullanın: şifreleri hemen sıfırlayın. Tüm aktif oturumlardan çıkış yapın (çoğu hizmetin "tüm cihazlardan çıkış yap" işlevi vardır). Henüz etkinleştirmediyseniz 2FA'yı etkinleştirin (hacker hala oturum açmış olsa bile, onu dışarı attığınızda 2FA yeniden oturum açmasını engellemeye yardımcı olacaktır). Hesabın ele geçirildiğini iş arkadaşlarınıza bildirin, böylece son mesajları potansiyel olarak sahte olarak değerlendirmeleri gerekir. Erişimi geri kazanamıyorsanız (hacker şifreyi değiştirip sizi

dışarı kilitlediyse), hemen hizmet sağlayıcının destek birimine başvurarak hesap ele geçirilmesini bildirin.

4. **Sorumlu Kişiyi (ve Mümkünse Herkesi) Bilgilendirin:** Güvenlik planınıza (3. Bölüm) göre, olaylar için bir sorumlu kişi veya ekip belirlemelisiniz. Onları hemen bilgilendirin. Bu kişi sizseniz, ilgili kişileri toplayın. Örneğin, paylaşılan bir sunucu saldırıya uğradıysa, tüm kullanıcıları bir sonraki duyuruya kadar sunucuyu kullanmamaları konusunda uyarın. Bir çalışanın bilgisayarı virüs bulaşmışsa, diğerlerine o bilgisayardan gelen e-postaları açmamaları konusunda uyarıda bulunabilirsiniz. **Olayı gizli tutmayın**; gizlemek hasarı daha da kötüleştirebilir. Hızlı iletişim, diğerlerinin tetikte olmasını veya koruyucu önlemler almasını sağlar (gerekirse şifrelerini değiştirmek gibi). Ayrıca, BT desteğiniz varsa (şirket içi veya sözleşmeli), onları erken arayın. Teknik önlemler veya daha derinlemesine analizlerle yardımcı olmaya başlayabilirler.

5. **Hasarı Sınırlayın:** Ağı kesmenin ötesinde, **hasarı** sınırlamak için atabileceğiniz adımlar şunlardır:
    - PC'de kötü amaçlı yazılım varsa, mümkünse güvenli modda veya önyüklenebilir kurtarma diski kullanarak antivirüs taraması yapın. Bu, kötü amaçlı yazılımı karantinaya alarak daha fazla zarar görmesini engelleyebilir. Ancak, önce sınırlayın (ağı kapatın), sonra tarayın – aktif bir saldırgan izliyor olabilir veya ek yükler indirilebilir, bu nedenle çevrimiçi durumdayken tarama yapmayın.
    - Fidye yazılımı varsa ve dosyalar şifrelenmişse, durdurulmuş mu yoksa hala çalışıyor mu belirleyin. Şüpheli işlemleri görürseniz Görev Yöneticisi aracılığıyla sonlandırın (bazıları açık isimler kullanır, diğerleri rastgeledir). Ancak bu aşamada, şifreleme muhtemelen hızlı bir şekilde yapılmıştır. Sınırlama, o bilgisayarı karantinaya almak ve dosyalara dokunmamak anlamına gelir (böylece adli tıp uzmanları veya şifre çözme araçları kurtarmayı deneyebilir).
    - Bir web sitesi saldırı altındaysa (tahrip edilmiş veya hacklenmişse), ziyaretçilere daha fazla zarar gelmesini önlemek ve düzeltme için zaman kazanmak için mümkünse siteyi çevrimdışı hale getirin (örneğin, bir bakım sayfası yayınlayın veya barındırma sağlayıcısından siteyi geçici olarak askıya almasını isteyin).

- E-posta ihlallerinde, şifreyi değiştirmenin yanı sıra, kişilerinize e-posta göndererek hesabınızdan gelen olası kimlik avı saldırıları konusunda onları uyarmayı düşünün.
- Veriler sızdırılmışsa (örneğin, veritabanınızı bir yapıştırma sitesinde bulursanız), istismar yolunu anlayıp düzeltme yapana kadar bu sistemlere erişimi kısıtlayın.

6. **Her şeyi belgelendirin:** Yukarıdakileri yaparken notlar alın. Zamanları, yaptığınız işlemleri ve kime bildirimde bulunduğunuzu yazın. Şüpheli bir dosya veya işlem adı bulursanız, bunu not edin. Bu belgeler daha sonra kurtarma, raporlama ve güvenlik planınızı iyileştirme konusunda yardımcı olacaktır. Ayrıca, kolluk kuvvetlerini veya bir olay müdahale uzmanını devreye sokarsanız, olayların sırasını bilmek isteyeceklerind

7. **Gerekirse Yardım İsteyin:** Dışarıdan yardım almaktan çekinmeyin. Siber güvenlikle ilgili bir irtibat kişiniz varsa (başka bir CSO'nun BT departmanı, gönüllü bir uzman veya siber güvenlik yardım hattı gibi), onları arayın. Birçok ülkede, küçük kuruluşlara bile yardım veya danışmanlık sağlayabilecek CERT'ler (Bilgisayar Acil Durum Müdahale Ekipleri) bulunmaktadır. Ücretsiz topluluk kaynakları da mevcuttur; örneğin, bir fidye yazılımı vakasında, "No More Ransom" web sitesini ziyaret ederek, sizin virüs türünüz için bir şifre çözme aracı olup olmadığını kontrol edebilirsiniz. Ancak yalnızca saygın araçları kullanın – çevrimiçi tavsiyelerde, bunların meşru olduğundan emin olun. Emin değilseniz, güvendiğiniz BT danışmanlarınıza danışın.

8. **Kanıtları Saklayın (Özellikle Ciddi Olaylarda):** Olay suç içerebiliyorsa (örneğin, kasıtlı bir hack, önemli bir hırsızlık), daha sonra kolluk kuvvetlerini devreye sokabilirsiniz. Bu gibi durumlarda, günlükleri ve kanıtları saklamak çok önemlidir. Sorun anlaşılana ve çözülene kadar sistem günlüklerini silmeyin veya sistemi temizlemeyin. Sistemi yeniden kurmanız gerekiyorsa, önce diskin bir görüntüsünü almayı düşünün. Daha az kritik durumlarda da kanıtlar öğrenme açısından yararlıdır – örneğin, birisini kandıran kimlik avı e-postasını saklayarak inceleyin ve diğerlerini bilgilendirin.

9. **Tehdidi ortadan kaldırın:** Tehdit kontrol altına alındıktan sonra, kaldırma işlemine geçin. Kötü amaçlı yazılımlar için: AV kullanarak tamamen kaldırın veya inatçı durumlarda işletim sistemini yeniden biçimlendirin/yeniden yükleyin (yedekleriniz varsa ve çok

zahmetli değilse, baştan başlamak en güvenli yoldur). Güvenliği ihlal edilmiş hesaplar için: arka kapı olup olmadığını iki kez kontrol edin (örneğin, saldırganın e-postaları gizlice iletmek için yeni iletme kuralları belirlemediğinden emin olun, bu genellikle gözden kaçan bir hiledir). Diğer hesapları da kontrol edin, çünkü bazen bir kimlik bilgisi birçok hesaba erişim sağlar – örneğin, tarayıcı şifreleri kaydetmişse, saldırgan bunları ele geçirebilir, bu nedenle diğer hesapların şifrelerini de değiştirmeniz gerekebilir.

Olay bir güvenlik açığıysa (örneğin, web sitenizde istismar edilen eski bir eklenti varsa), bunu düzeltin veya kaldırın. Sorun, kötü niyetli bir içerdekiden kaynaklanıyorsa, elbette, bu kişinin erişimini kaldırın.

10. **Kurtarma ve Geri Yükleme:** Acil tehdidi ortadan kaldırdıktan sonra, normale dönmeye başlayın:

- Yedeklemelerden kaybolan veya bozulan verileri geri yükleyin. Yedeklemelerin temiz olduğunu doğrulayın (mümkünse geri yüklemeden önce antivirüs ile tarayın).
- Sistemleri dikkatlice yeniden bağlayın. Örneğin, bir bilgisayarı temizledikten sonra, onu ağa geri bağlayın ve şüpheli giden trafiğin devam edip etmediğini izleyin (devam ediyorsa, kötü amaçlı yazılım tamamen ortadan kaldırılmamış olabilir).
- Hesapları yeniden etkinleştirdiyseniz veya kimlik bilgilerini değiştirdiyseniz, herkesin yeni güvenli parolalarla ihtiyaç duydukları bilgilere tekrar erişebildiğinden emin olun.
- İşlemler durdurulduysa (örneğin, bir sunucuyu çevrimdışı hale getirdiyseniz), test etmek için yoğun olmayan bir saatte sunucuyu yeniden başlatın ve herhangi bir kalıntı sorun olmadığından emin olun.

11. **Güncellemeleri İletin:** Personeli olan biten ve yapılanlar hakkında bilgilendirin. Şeffaflık, güven ve işbirliği sağlar. Ayrıca, uygunsa, dış paydaşları da uygun şekilde bilgilendirin (kiminle iletişime geçileceği konusunda bir sonraki bölüme bakın, örneğin, verileri ihlal edilmişse bağışçılar vb. Ancak, genel olarak, dışa raporlama ihtiyacı veya yükümlülüğü olmadığı sürece, iç sorunlar içerde tutulabilir.

Bu süreç boyunca, suçlama değil öğrenme tutumunu koruyun. Saldırılar en iyilerimizin başına bile gelebilir. Kimin neyi tıkladığına odaklanmak yerine (bu bilgiyi eğitimi iyileştirmek için kullanmak dışında), çözüme ve tekrarının önlenmesine odaklanın.

Bu yapılandırılmış müdahale – tanımlama, kontrol altına alma, ortadan kaldırma, kurtarma – uzmanların önerilerini yansıtmaktadır. Küçük STK'lar için, bu adımlar birden fazla görevi üstlenen tek bir kişi tarafından gerçekleştirilebilir, ancak ilke aynı kalır.

Şimdi, bir olayı ele almak sadece kuruluşunuzdan daha fazla tarafı içerebileceğinden, kimi aramanız veya kime rapor etmeniz gerektiğini daha ayrıntılı olarak inceleyelim.

Yardım için Kime Başvurulmalı: Destek Kaynakları ve Yardım Alma

Bir siber olayla karşılaştığınızda, bunu tek başınıza halletmek zorunda değilsiniz. Yardım, tavsiye ve raporlama için başvurabileceğiniz birçok yer ve kişi vardır. Destek kaynaklarının bir dökümü aşağıda verilmiştir:

Dahili Ekip ve BT Desteği: İlk olarak, kuruluşunuz içinde BT veya güvenlikten sorumlu kişileri (teknik personeliniz/gönüllüleriniz veya sistemlerinizi kuran kişi) sürece dahil edin. BT yönetilen hizmet sağlayıcınız veya gönüllü BT danışmanınız varsa, hemen onlarla iletişime geçin ve durumu açıklayın. Muhtemelen benzer sorunlarla karşılaşmışlardır ve teknik adımlar konusunda size yol gösterebilirler. Teknoloji konusunda bilgili bir yönetim kurulu üyesi veya ortak kuruluşun BT personeli bile zor durumlarda değerli bir müttefik olabil .

Akran Ağları ve Diğer STK'lar: Kardeş kuruluşlara veya ağlara gizlice ulaşmayı düşünün. Genellikle, STK ağları (örneğin, bir insan hakları ağı veya bir STK çatı kuruluşu) ortak kaynaklara veya en azından kolektif bilgiye sahip olabilir. Sektörünüzde veya bölgenizde yaygın tehditleri biliyor olabilirler ve önerilerde bulunabilirler (örneğin, "Evet, diğer iki STK da aynı kimlik avı e-postasını aldı; biz şöyle yaptık"). Burada işbirliği çok etkili olabilir. Ancak, dışarıya ne kadar ayrıntı paylaşacağınızı iyi düşünün – resmi açıklama yapılana kadar itibar riskinden kaçınmak için hassas ayrıntıları güvenilir kişilerle paylaşın.

Sivil Toplum için Siber Güvenlik Yardım Hatları: Sivil topluma dijital güvenlik acil durumlarında yardımcı olmak için özel girişimler vardır. Bunlardan dikkate değer biri, dünya çapındaki STK'lara, aktivistlere ve gazetecilere 7/24 ücretsiz yardım sağlayan **Access Now'un Dijital Güvenlik Yardım Hattıdır**. Web sitesi saldırıları, hesap ele geçirmeleri vb. durumlarda

yardımcı olabilirler, genellikle uzman gönüllülerle bağlantı kurar veya özel rehberlik sağlarlar. Kendi kapasitenizin ötesinde ciddi bir durumla karşı karşıya kalırsanız, bu tür bir yardım hattına e-posta göndermeyi veya aramayı tereddüt etmeyin (Access Now'un yardım hattı ). Bu hatlar gizliliği korur ve acil durumları ele almaya alışkındır.

Başka bir örnek: **CyberPeace Institute'un CyberPeace Builders** programı, kurumsal gönüllüler tarafından STK'lara ücretsiz siber güvenlik yardımı sunar. Zaten kayıtlıysanız veya onlarla bağlantınız varsa, bu kanalı kullanın. Değilse, gelecekte bunu dikkate alabilirsiniz.

Kolluk Kuvvetleri: Bu, olayın niteliğine bağlıdır:

- Kişisel verilerin çalınması veya kasıtlı bir hackleme gibi önemli bir veri ihlali söz konusuysa, yerel kolluk kuvvetlerine veya siber suç birimine bildirmeyi düşünebilirsiniz. Özellikle bağışçıların parası veya hassas bilgileri çalındıysa veya şantaj (fidye yazılımı talepleri gibi) söz konusuysa, bunlar soruşturma yapabilir. Ancak deneyimler değişiklik gösterir; bazı yerlerde polis yardımcı olurken, diğer yerlerde öncelik vermez veya uzmanlığa sahip olmayabilir.
- Zorunlu ihlal bildirim yasaları olan ülkelerde (AB'deki GDPR gibi, ciddi kişisel veri ihlalleri 72 saat içinde veri koruma yetkililerine bildirilmelidir), bu düzenlemelere uymalısınız. Bu, ilgili Veri Koruma Otoritesini ( ) ve muhtemelen etkilenen kişileri bilgilendirmek anlamına gelir (bu konuda daha fazla bilgi bir sonraki bölümde verilmiştir).
- Saldırganın belirli bir bölgeden olduğunu veya birden fazla kuruluşu etkileyen bir model olduğunu düşünüyorsanız, kolluk kuvvetleri bunları bir araya getirebilir.
- Not: CSO'nuz, yetkililerin dostça davranmayabileceği veya bu bilgileri kötüye kullanabileceği bir ülkede hassas konular üzerinde çalışıyorsa (örneğin, saldırı devlet destekli olabilirse), kolluk kuvvetlerini devreye sokmayı dikkatlice değerlendirmelisiniz. Bu gibi durumlarda, başlangıçta uluslararası kuruluşlara (örneğin, tarafsız bir ülkedeki CERT veya sadece CSO yardım hatlarını kullanmak) danışmak tercih edilebilir.

Ulusal CERT/CSIRT: Birçok ülkede, genellikle hükümet veya akademik kurumlar çatısı altında bir Bilgisayar Acil Durum Müdahale Ekibi (CERT) veya CSIRT bulunmaktadır. Bu ekipler bazen kuruluşlara (sadece kritik altyapılara değil) yardım ederler. Bazıları küçük işletmeler veya kar

amacı gütmeyen kuruluşlar için özel birimlere sahiptir. Örneğin, **AB'deki CERT'ler** genellikle olaylara müdahale eder ve tavsiyelerde bulunur veya kolluk kuvvetleriyle koordinasyon sağlar. Bir irtibat kişiniz varsa veya web siteleri üzerinden kolayca bildirimde bulunabiliyorsanız, bu faydalı olabilir. Ayrıca, başkalarını uyarabilir veya bir kötü amaçlı yazılım kampanyasının yayılmasını takip edebilirler.

Bağışçılar veya Ortaklar: Bir proje veya bağışçı verileri söz konusuysa veya hizmet sunumu etkilenmişse, ortakları bilgilendirmeniz gerekebilir. Örneğin, ortak bir proje yürütüyor ve hackerlar proje web sitesini tahrip ediyorsa, diğer STK'dan ortağa durumu bildirmek, onların haberdar olmasını ve yardımcı olmasını veya en azından hazırlıksız yakalanmamasını sağlar. Fonlar etkilenmişse (örneğin, finansal dolandırıcılık), bağışçılar raporlama gereklilikleri olabilir. Destekleyici tarafta, bazı bağışçılar (özellikle büyük bağışçılar veya siber güvenlik kapasitesini finanse edenler) size yardımcı olacak kaynaklara sahip olabilir. Ancak iletişimi dikkatli bir şekilde yönetin – güveni korumak için sadece soruna değil, sorunu çözmek için yapılanlara odaklanın.

Sigorta: Siber olayları kapsayan siber sigortanız veya genel sorumluluk sigortanız varsa, sigorta şirketinin olay hattını mümkün olan en kısa sürede bilgilendirin (genellikle sigorta kapsamı için gereklidir). Sigorta şirketi, profesyonel olay müdahale ekibi gönderebilir veya sonraki adımlar konusunda rehberlik edebilir. Birçok sigorta poliçesi, fidye ödeme kararları gibi konularda sigorta şirketinin koordinasyonunu gerektirir. Sigortanız yoksa, bu durum elbette geçerli değildir.

Topluluk ve Çevrimiçi Kaynaklar: **Reddit r/cybersecurity veya r/techsupport** veya **StackExchange Security** gibi, profesyonellerin bazen yardım ettiği çevrimiçi forumlar vardır. Ancak, halka açık forumlarda hassas bilgileri ifşa etmemeye dikkat edin. Bunun yerine, bu forumları arayarak başkalarının belirli bir kötü amaçlı yazılım veya hatayla başa çıkıp çıkmadığını görebilirsiniz (genellikle birisi o belirli fidye notu veya virüs davranışı hakkında bir şey yayınlamıştır ve bu da çözüm için ipuçları verebilir). **BleepingComputer** gibi web sitelerinde, kötü amaçlı yazılımların kaldırılmasına yardımcı olmak için özel bölümler ve belirli fidye yazılımı destek konuları bulunur ve bu bölümler genellikle mağdurlara ücretsiz olarak yardım eden uzmanlar tarafından yönetilir. Bu siteler genellikle NoMoreRansom projesiyle de işbirliği yapar. Bu yolu seçerseniz, onların yönergelerini izleyin (genellikle günlük dosyalarını paylaşmanızı

isterler, ancak kendinizi rahat hissetmediğiniz hiçbir şeyi yapmayın; durumunuzu kamuya açık bir şekilde tartışıyorsanız, takma ad kullanabilirsiniz).

Etkilenen Kişileri/Kamuoyunu Ne Zaman ve Nasıl Bilgilendirmeli: Bu daha çok "kime bildirimde bulunulacağı" ile ilgilidir: yararlanıcıların veya paydaşların kişisel verileri sızdırılırsa, etik ve muhtemelen yasal yükümlülükler, bu kişilerin kendilerini koruyabilmeleri için onları bilgilendirmenizi gerektirebilir (örneğin, e-postaları sızdırılmışsa şifrelerini değiştirmeleri, kimlik hırsızlığına karşı dikkatli olmaları). Bu tür iletişimlerin hazırlanması zor olabilir; dürüst, özür dileyen ve rehberlik sağlayan bir üslup kullanılmalıdır (örneğin, "E-posta adresinizin ifşa olmuş olabileceği bir güvenlik olayı yaşadık. Şüpheli e-postalara karşı uyanık olun ve şifrenizi tekrar kullandıysanız değiştirmeyi düşünün ..."). Emin değilseniz, bir iletişim veya hukuk danışmanına danışın – doğru üslubu kullanmak ve yanlışlıkla sorumluluğu kabul etmek gibi hatalar yapmamak istersiniz.

Psikolojik Destek: Bu konu dışı gibi gelebilir, ancak ciddi bir olay stres yaratabilir. İnsanlar kendilerini ihlal edilmiş veya suçlu hissedebilir (phishing'e tıklayan kişi kendini çok kötü hissedebilir). Morali ele almaya değer. Herkesin hataların olabileceğini bildiğinden emin olun ve ileriye bakmaya odaklanın. Aşırı stresliyseniz, kısa bir mola verin veya konuşacak birini bulun (benzer bir deneyim yaşamış başka bir CSO'daki bir meslektaşınıza dertlerinizi anlatmak bile sizi rahatlatabilir). Durum yatıştıktan sonra, destekleyici bir değerlendirme toplantısı düzenlemeyi düşünün: olanları tartışın ve birbirinize nasıl yardımcı olabileceğinizi ve güçlenebileceğinizi konuşun.

Dış kuruluşlarla yapılan tüm iletişimlerde, kiminle ne zaman iletişime geçtiğinizi, vaka/referans numaralarını veya verilen tavsiyeleri kaydedin. Bu, belgelemenin bir parçasıdır ve takip işlemlerine yardımcı olur.

Son olarak, bu destek kanallarını sadece olay sırasında değil, sonrasında da iyileştirme amacıyla kullanın. Örneğin, Access Now yardım hattı, gelecekte benzer olayların tekrarlanmasını önlemek için atılması gereken adımlar konusunda tavsiyelerde bulunabilir veya CERT size raporunu ve önerilerini gönderebilir.

Güvenliği Geri Kazanma: Kurtarma Adımları

Olayı kontrol altına aldıktan ve yardım aldıktan sonra, son aşama sistemleri normal çalışır duruma getirmek ve tekrarını önlemek için önlemler almaktır. Kurtarma sadece verileri geri yüklemekle ilgili değil, aynı zamanda ortamınızın tekrar temiz ve güvenli olduğuna dair güveni geri kazanmakla da ilgilidir.

Sistemleri Temizleme ve Yeniden Oluşturma: Herhangi bir makine virüs bulaşmışsa, kötü amaçlı yazılımları kaldırdıktan sonra işletim sisteminin tamamen yeniden yüklenmesi gerekip gerekmediğini değerlendirin. Genellikle güvenlik uzmanları, ciddi güvenlik ihlalleri (rootkitler veya bilinmeyen kötü amaçlı yazılımlar gibi) için, sistemin temiz olduğundan emin olmak için en güvenli yolun silme ve yeniden oluşturma olduğunu önerir. Evet, uygulamaları yeniden yüklemek ve dosyaları geri yüklemek zaman alıcıdır, ancak gizli bir arka kapı kalmadığından emin olmanızı sağlar. Bunu yapmamayı tercih ederseniz, en azından birden fazla tarama aracı çalıştırın (bir antivirüs programı bir şeyi kaçırabilirken, başka bir program onu yakalayabilir). Malwarebytes, HitmanPro vb. araçlar, ikinci bir görüş için ana antivirüs programınıza ek olarak çalıştırılabilir. Temizleme işleminden sonra işletim sisteminin tamamen yamalandığından emin olun.

Hesaplar için, erişimi yeniden kazandıktan sonra hesap ayarlarını gözden geçirin: Saldırgan herhangi bir yönlendirme kuralı oluşturdu mu, kurtarma e-postaları veya kendi 2FA cihazlarını ekledi mi? (Bu yaygın bir durumdur: örneğin, bir Gmail korsanının kendi e-postasını kurtarma e-postası olarak eklemesi ve böylece şifre değiştirildikten sonra bile hesap kurtarmayı denemesi gibi.) Bu tür yetkisiz değişiklikleri kaldırın. Posta filtrelerini, uygulama şifrelerini, bağlı uygulamaları, kısacası hesap ayarlarında erişimin devam etmesine izin verebilecek her şeyi kontrol edin.

Bir web sitesi saldırıya uğradıysa, güvenlik açığını giderip içeriği geri yükledikten sonra, daha güvenli bir sunucuya taşıma veya bir web uygulaması güvenlik duvarı (WAF) eklemeyi düşünün. Özel bir siteyse, kodun güvenlik denetimini yapın. Ayrıca, tehlikeye girmiş olabilecek tüm veritabanı ve FTP şifrelerini değiştirin.

Yedeklemelerden Verileri Geri ***Yükleyin:*** Kayıp verileri geri getirin. Örneğin, bir bilgisayarı silmek zorunda kaldıysanız, yedeklemeden kullanıcı dosyalarını geri alın (ancak,

belgelerde virüslü bir dosya bulunma ihtimaline karşı önce bunları tarayın). Bir veritabanı silinmiş veya şifrelenmişse, en son yedeklemeyi kurtarın. Geri yüklenen verilerin sağlam olduğunu ve bunları kullanan sistemlerin düzgün çalıştığını test edin. Bazen yedeklemeler istediğimiz kadar güncel olmayabilir, bu nedenle biraz iş kaybedebilirsiniz. Kurtarma işleminden sonra, personelden eksik bir şey olup olmadığını hızlıca kontrol etmelerini isteyin ve varsa, yeniden girilip girilemeyeceğini veya yeniden toplanıp toplanamayacağını kontrol edin.

Fidye yazılımı söz konusuysa ve yedeğiniz yoksa, kurtarma işlemi daha zordur. Şifre çözme araçları için uzmanlara veya NoMoreRansom'a danışın; bazen belirli fidye yazılımı türleri için ücretsiz çözümler mevcuttur. Fidye ödemek genellikle önerilmez (suçlulara para kazandırır ve garanti yoktur), ancak bazı kuruluşlar bu zor seçimi yapar. Ödeme yapmadan önce kolluk kuvvetlerine başvurun, çünkü bazen anahtarları olabilir veya tavsiyede bulunabilirler. Sonuçta veri kaybı varsa, bu verileri nasıl yeniden oluşturacağınızı planlayın (belki ortaklarınızla iletişime geçerek size sahip oldukları dosyaların kopyalarını göndermelerini isteyebilirsiniz, vb.

Güvenlik Önlemlerini İyileştirin ve Güncelleyin: Bir ihlalden sonra, savunmayı güçlendirmek gerekir. Bu, istismar edilen açıkları düzelttiğiniz "dersler" aşamasıdır:

- Phishing saldırısıysa, açıkça daha fazla eğitim ve belki de teknik kontroller (daha iyi bir spam filtresi veya MFA uygulaması gibi) gereklidir. Örneğin, tüm e-posta hesaplarında 2FA'nın etkinleştirilmesini zorunlu kılın ve belki de harici gönderenler için bir e-posta uyarısı uygulayın (bazı sistemler, sahtekarlığı tespit etmeye yardımcı olmak için, posta dışarıdan gelirse konu başlığına "[Harici]" ibaresini ekler).
- Zayıf bir parola veya yeniden kullanılan kimlik bilgileri söz konusuysa, parola politikalarını (daha uzun, benzersiz) sıkılaştırın ve bunu desteklemek için kuruluş genelinde bir parola yöneticisi kullanmayı düşünün. Ve kesinlikle kritik her şeyde 2FA kullanın.
- Kötü amaçlı yazılım yamalanmamış yazılım yoluyla geldiyse, güncellemelerin daha hızlı uygulanmasını sağlayın. Eksik yamaları izlemek için bir araç kullanın veya yazılımınızla ilgili güvenlik bültenlerine abone olun.
- Belirli bir hizmet açığa çıkmışsa (brute force saldırısına uğrayan açık bir RDP bağlantı noktası gibi), onu kapatın veya bir VPN arkasına yerleştirin.

- Güvenlik duvarı kurallarınızın sıkılaştırıldığını ve gereksiz hizmetlerin devre dışı bırakıldığını kontrol edin (4.4'te ele aldığımız gibi).
- Ağınızı veya verilerinizi bölümlere ayırmayı düşünün: örneğin, gelecekte yedeklemeleri her zaman bağlı olmayan bir cihazda saklayarak fidye yazılımlarının onlara ulaşmasını engelleyin veya hassas verileri herkesin erişemeyeceği bir sürücüye ayırın.
- Daha iyi izleme uygulayın: sistem günlüğünü etkinleştirin ve uyarılar ayarlayın (ücretsiz günlük izleme araçları veya hatta Windows Olay İletimi gibi, birden fazla başarısız oturum açma gibi belirli olayları izlemek için araçlar mevcuttur).
- Henüz yoksa resmi bir olay müdahale prosedürü planlayın – temel olarak bu sefer yaptıklarınızı yazın ve bir dahaki sefere iyileştirin (güvenlik planı güncellemelerinin bir parçası).

Paydaşlarla iletişim kurun: Olayı insanlara bildirmek zorunda kaldıysanız, çözüldükten sonra takip edin. Örneğin, yönetim kurulunuza veya bağışçılarınıza "X olayını yaşadık, Y adımlarını attık ve şimdi operasyonlar yeniden başladı. Bunun tekrar yaşanmaması için Z'yi uyguluyoruz." Bu güvence ve hesap verebilirlik, şeffaf ve yetkin bir şekilde yapıldığında güveni güçlendirebilir. Benzer şekilde, gönüllüler veya yararlanıcılar daha önce dikkatli olmaları konusunda bilgilendirildiyse, daha sonra sorunun çözüldüğünü onlara bildirin: örneğin, "Web sitemiz artık güvenli ve tekrar çevrimiçi. Sabrınız için teşekkür ederiz."

Psikolojik İyileşme: Bir ihlalden sonra, ekip morali düşebilir. İnsanlar tedirgin hissedebilir ("Hackerların hala içeride olmadığından emin miyiz?") veya suçluluk duyabilir. Neler olduğunu açıkça tartışmak için bir değerlendirme toplantısı düzenleyin ve bunu bir cadı avı olarak değil, bir öğrenme fırsatı olarak değerlendirin. Hasarı sınırlayan hızlı raporlama veya eylemleri övün. Belki de herkese yeni önlemlerin neler olduğunu bildirdiğiniz küçük bir "öğrenilen dersler" atölyesi düzenleyin, bu da onlara artık her şeyin daha güvenli olduğunu garanti edecektir. Ton şu şekilde olmalıdır: Bir zorlukla karşılaştık ve onu aştık, şimdi daha güçlüyüz.

Belgeleme ve Raporlama: Olay hakkında bir iç rapor yazın – sadece bir sayfa olsa bile. Zaman çizelgesini, temel nedeni (biliniyorsa), alınan önlemleri ve önerileri belgelendirin. Bu, hafızanız için (altı ay sonra, benzer bir olay olursa önemli ayrıntıları unutabilirsiniz) ve herhangi bir dış raporlama görevi için yararlıdır. Yönetmelik (örneğin, GDPR) gerektiriyorsa, bu ayrıntıları da içeren resmi raporu yetkili makama sunun. Bir şemsiye kuruluşuyla koordinasyon

halindeyseniz veya bağışçılara karşı yükümlülüğünüz varsa (bazı hibeler, risk yönetiminin bir parçası olarak ciddi olayların raporlanmasını gerektirir), iç raporu uygun şekilde iletişim kurmak için kullanın.

Planları Test Edin ve Güncelleyin: Her şey normale döndüğünde, güvenlik planınızı ve olay müdahale planınızı iyileştirmek için mükemmel bir zamandır. İletişim listelerinizi güncelleyin (belki CERT'in numarasını elinizin altında tutmadığınızı fark ettiniz – şimdi kaydedin). Belirli bir araç, olayı daha erken tespit etmeye veya durdurmaya yardımcı olsaydı, bunu uygulamayı düşünün. Hatta gelecekte küçük bir "yangın tatbikatı" yapmayı düşünün – örneğin, yedeklemeleri geri yüklemeyi test edin veya yeni eğitimin işe yarayıp yaramadığını görmek için simüle edilmiş bir kimlik avı testi yapın.

Tam kurtarma sürecinin güveni yeniden kazanmayı da içerdiğini unutmayın. Çalışanlarınızın sistemlere olan güveni, dış ortakların sizin yönetimize olan güveni. Şeffaflık, eylem ve takip, bu güveni yeniden inşa etmeye yardımcı olur. Bu, sorunu ciddiye aldığınızı ve iyileştirmeler yaptığınızı gösterir.

Son olarak, uygunsa bilgileri (hassas ayrıntılar olmadan) toplulukla paylaşmaya değer. Örneğin, CSO'ları hedef alan yeni bir dolandırıcılık tespit ettiyseniz, bir posta listesi veya ağ aracılığıyla diğerlerini uyarmak, onların kurban olmasını önleyebilir – bu, yaşadığınız zorlu deneyimin olumlu bir sonucu olur.

Bu kurtarma adımlarını titizlikle uygulayarak, sadece normale dönmekle kalmaz, ideal olarak daha sağlam bir güvenlik duruşuna da kavuşursunuz. Birçok kuruluş, bir ihlalin kendilerini uyandıran bir uyarı olduğunu ve sonuçta gelecek için daha iyi hazırlıklı hale geldiklerini fark eder (ancak bir olayın acısını yaşamadan iyileştirmek her zaman daha iyidir!).

Bu noktada, olayların kendisinin nasıl ele alınacağını ele aldık. Şimdi, sivil toplum için siber güvenliğin genellikle yeterince değerlendirilmeyen bir yönü olan, güvenliği sağlamada işbirliği ve topluluğun gücüne geçeceğiz.

Bölüm Özeti

Bu bölüm, siber güvenliğin insani yönünü vurgulamakta ve eğitim ve politikalar yoluyla güvenlik bilincine sahip bir kültürün oluşturulmasını savunmaktadır. İhlallerin %74'ünün kimlik avı gibi insan hatasından kaynaklandığını vurgulayarak, personel eğitiminin kritik önemini ortaya

koymaktadır. CSO'lar, kimlik avı testleri gibi alıştırmalar kullanarak, şifre yönetimi ve kimlik avı e-postalarını tespit etme gibi temel siber güvenlik eğitimleri düzenlemeye yönlendirilmektedir. Bu bölüm, cihazlar ve veriler için kabul edilebilir kullanım politikaları hazırlama konusunda tavsiyelerde bulunarak, personel ve gönüllüler için net kurallar sağlanmasını garanti altına almaktadır. Ayrıca, olay raporlama protokollerini özetleyerek, ihlalleri kontrol altına almak için hızlı iletişimi teşvik etmektedir. Örnekler arasında, CSO'nun şüpheli e-postaları raporlamaları için personeli eğitmesi ve kötü amaçlı yazılım saldırılarını önlemesi sayılabilir. Bu bölüm, çabaları meşrulaştırmak için güvenli uygulamaları (ör. 2FA kullanımı) modellemede liderliğin rolünü vurgulamaktadır. Alışkanlıkları pekiştirmek için, phishing'i bildiren personeli övmek gibi uyanıklığı ödüllendirmeyi önerir. CSO'lar, güvenliği günlük iş akışlarına dahil ederek dayanıklı bir kültür oluşturur. Bu bölümün basit ve kapsayıcı uygulamalara odaklanması, tüm personel için erişilebilirliği sağlar ve müfredatın eğiticileri eğitme modeliyle ve e-kitabın uzun vadeli güvenlik alışkanlıklarını teşvik etme hedefiyle uyumludur.

-Teknik Olmayan CSO'lar için Web Sitesi Güvenlik Kontrol Listesi

Bu kontrol listesi, program personeli ve gönüllülerin teknik uzmanlık gerektirmeden CSO'nuzun web sitesi güvenliğini doğrulamasına ve iyileştirmesine olanak tanır. Bu adımlar, web sitenizi saldırılardan (ör. tahrifat, DDoS) korumaya ve misyonunuz için güvenilir bir platform olmaya devam etmesini sağlamaya yardımcı olur:

1. Web sitenizin HTTPS kullanıp kullanmadığını kontrol edin

- ⇒ Web sitenizi ziyaret edin ve tarayıcının adres çubuğunda (URL'nin önünde) bir asma kilit simgesi veya adresin başında "https://" yazısı olup olmadığını kontrol edin.
- ⇒ "http://" veya "Güvenli Değil" uyarısı görürseniz, HTTPS'yi etkinleştirmek için web barındırıcınızla iletişime geçin (örneğin, ücretsiz Let's Encrypt sertifikası isteyin).
- ⇒ Örnek: Siteniz "www.CSOexample.org" adresindedir. Adres çubuğunda "https://www.CSOexample.org" yazdığından ve asma kilit simgesi bulunduğundan emin olun.
- ⇒ HTTPS eksikse, web barındırıcınıza e-posta gönderin: "Lütfen web sitemiz için HTTPS'yi etkinleştirin."

2. Düzenli Yedeklemeleri Onaylayın

- ⇒ Web barındırıcınıza veya web sitesi yöneticinize, web sitenizin düzenli olarak (örneğin, günlük veya haftalık) yedeklendiğini ve yedeklemelerin nerede saklandığını (örneğin, bulut veya harici sunucu) sorun.
- ⇒ Yedeklemelerin çalıştığından emin olmak için bir test geri yüklemesi isteyin (örneğin, "Sitemizi geçen haftaki sürümüne geri yükleyebilir misiniz?" diye sorun).
- ⇒ Örnek: Web siteniz bir saldırıdan sonra çevrimdışı kaldı. Son yedekleme sayesinde siteyi hızlı bir şekilde geri yükleyebilirsiniz.
- ⇒ Barındırma sağlayıcınızla iletişime geçin: "Otomatik web sitesi yedeklemelerimiz var mı? Ne sıklıkla yapılıyor?"

3. Web Sitesi Yazılım Güncellemelerini Doğrulayın

⇒ İçerik Yönetim Sistemi (CMS, örneğin WordPress, Joomla) ve eklentiler/temaların düzenli olarak güncellenip güncellenmediğini web barındırıcınıza veya web sitesi yöneticinize danışın.

⇒ Güncellemelerin otomatik olup olmadığını veya aylık olarak kontrol edilip edilmediğini sorun.

⇒ Örnek: Güncel olmayan bir WordPress eklentisi, bir CSO'nun sitesinin hacklenmesine neden oldu. Düzenli güncellemeler bunu önler.

⇒ Barındırma sağlayıcınıza e-posta gönderin: "CMS ve eklentilerimiz güncel tutuluyor mu? Değilse, lütfen otomatik güncellemeleri etkinleştirin."

4. Yönetici Erişiminin Güvenliğini Sağlayın

⇒ Yalnızca güvenilir personelin web sitesi yönetici erişimine sahip olduğundan emin olun. Eski personel veya gönüllülerin erişimini kaldırmak için web sitesi yöneticinize danışın.

⇒ Yönetici hesaplarının güçlü şifreler (ör. 14+ karakter, "sunbird&glass7rain" gibi) ve iki faktörlü kimlik doğrulama (2FA) kullandığını doğrulayın.

⇒ Örnek: Eski bir gönüllünün eski giriş bilgileri bir siteyi tahrip etmek için kullanıldı. Kullanılmayan hesapları kaldırmak bunu önler.

⇒ Web sitesi yöneticinize şunu sorun: "Yönetici erişimi kimlerde var? Eski hesapları kaldırabilir ve 2FA'yı etkinleştirebilir miyiz?"

5. Şüpheli web sitesi değişikliklerini kontrol edin

⇒ Web sitenizi ziyaret edin ve olağandışı içerik (örneğin, garip metinler, tanıdık olmayan resimler veya diğer sitelere yönlendirmeler) olup olmadığını kontrol edin.

⇒ Herhangi bir garip davranışı web barındırıcınıza veya BT irtibat kişinize hemen bildirin.

⇒ Örnek: Bir CSO'nun ana sayfası, bir hack saldırısı nedeniyle dolandırıcılık sitesine yönlendirildi. Erken bildirim sayesinde sorun hızla çözüldü.

⇒ Sitenizi tarayın ve olağandışı herhangi bir şeyi not edin. Barındırma sağlayıcınızla iletişime geçin: "Sitemizde [sorun] var; lütfen araştırın."

6. DDoS Saldırılarına Karşı Koruma

⇒ Web barındırıcınıza, trafik yoğunluğu sırasında sitenizi çevrimiçi tutmak için DDoS (Dağıtık Hizmet Engelleme) koruması sağlayıp sağlamadığını sorun.

⇒ Temel korumaların (ör. Cloudflare'in ücretsiz planı) etkinleştirilip etkinleştirilmediğini onaylayın.

⇒ Örnek: Bir insan hakları CSO'sunun sitesi, bir DDoS saldırısı sırasında çevrimdışı kaldı. Ücretsiz DDoS koruması, sitenin çalışmaya devam etmesini sağladı.

⇒ Barındırma sağlayıcınıza e-posta gönderin: "DDoS korumamız var mı? Cloudflare gibi ücretsiz bir hizmeti etkinleştirebilir miyiz?"

7. Hassas Sayfalara Genel Erişimi Sınırlayın

⇒ Hassas web sitesi sayfalarının (ör. yönetici girişi, iç belgeler) şifre korumalı olup olmadığını veya genel erişimden gizli olup olmadığını kontrol edin.

⇒ Web sitesi yöneticinizden erişimi yalnızca yetkili kullanıcılarla sınırlandırmasını isteyin.

⇒ Örnek: Bir STK'nın bağışçı listesi yanlışlıkla kamuya açık hale geldi. Sayfayı şifre ile korumak sorunu çözdü.

⇒ Şunu sorun: "Yönetici girişleri gibi hassas sayfalar korunuyor mu? Gerekirse şifre ekleyebilir miyiz?"

8. Personeli Güvenli Web Sitesi Kullanımı Konusunda Eğitin

⇒ Personel ve gönüllülere, yönetici kimlik bilgilerini paylaşmamalarını veya web sitesinde hassas bilgiler (ör. bağışçı verileri) yayınlamamalarını hatırlatın.

⇒ Hızlı bir ipucu paylaşın: "Kullanımdan sonra her zaman web sitesi yönetici panelinden çıkış yapın."

⇒ Örnek: Bir personel, bir e-postada yönetici şifresini paylaştı ve bu da bir hacklemeye yol açtı. Eğitim, bunun önlenmesini sağlar.

⇒ Ekibe bir e-posta gönderin: "Web sitesi giriş bilgilerini asla paylaşmayın. Siteyi düzenledikten sonra oturumu kapatın."

BÖLÜM 6: DİJİTAL GÜVENLİK İÇİN İŞBİRLİĞİ VE DESTEK

Birlikte Daha Güçlü: İşbirliği ve Destek

Dijital güvenlik yalnızca bireysel veya kurumsal bir çaba değildir; kolektif bir çabadır. Sivil toplum kuruluşları, siber tehditler karşısında birlikte çalışarak, bilgi paylaşarak ve birbirlerini destekleyerek büyük fayda sağlayabilirler. Bu bölümde, işbirliğinin güvenliği nasıl artırabileceğini ele alıyoruz – benzer STK'larla bilgi paylaşmaktan ve toplumda bir güvenlik kültürü oluşturmaktan, halkı eğitmeye ve yerel ve uluslararası destek ağlarından yararlanmaya kadar.

Diğer Sivil Toplum Örgütleriyle Bilgi Paylaşımı

Hiçbir STK, özellikle dijital alanda, bir ada değildir. Çoğu zaman, bir kuruluşu hedef alan saldırılar veya riskler, aynı sektördeki veya bölgedeki diğer kuruluşları da etkileyebilir. Tehditler ve en iyi uygulamalar hakkında bilgi paylaşarak, STK'lar savunmalarını toplu olarak iyileştirebilirler.

Neden Paylaşmalı? Utanç veya güvenlik açığını ortaya çıkaracağı korkusuyla güvenlik olaylarını paylaşma konusunda tereddüt edilebilir. Ancak, doğru ortamda yapıldığında, faydalar genellikle risklerden daha ağır basar. CSO'nuz bir kimlik avı kampanyasının kurbanı olduysa, diğerlerini bilgilendirmek onların bu tuzağa düşmesini önleyebilir. Bu, mahalle bekçiliğine benzer: bir ev dolandırıcılığın hedefi olursa, komşuları uyarırlar. Siber güvenlikte, bu **bilgi paylaşımı** kavramı bazı sektörlerde ISAC'ler (Bilgi Paylaşımı ve Analiz Merkezleri) aracılığıyla resmileştirilmiştir. Finans veya sağlık gibi sektörler için resmi ISAC'ler mevcut olsa da, CSO'lar kendi gayri resmi paylaşım çevrelerini veya gruplarını oluşturabilirler.

Ne ve Nasıl Paylaşılmalı:

- **Tehdit Uyarıları:** Belirli bir kimlik avı e-postası, kötü amaçlı yazılım dosyası veya şüpheli bir yaklaşımla (örneğin, bağışçı kılığına giren biri) karşılaşırsanız, göstergeleri paylaşabilirsiniz: örneğin, "X adresinden Y konulu kötü amaçlı bir e-posta aldık. Dikkatli olun." Diğerlerinin bunu tanıyabilmesi için yeterli ayrıntı sağlayın. Bazı CSO ağları, bu tür uyarılar için e-posta listeleri veya güvenli sohbet grupları oluşturur.

- **Taktikler ve Dersler:** Bir olay veya tatbikat yaşadıktan sonra, öğrendiklerinizi paylaşın, hassas kısımları anonim hale getirebilirsiniz. Örneğin, şunu paylaşabilirsiniz: "Tüm hesaplarımızda iki faktörlü kimlik doğrulama uyguladık ve bu, birçok yetkisiz oturum açma girişimini engelledi. Bu çabaya değdi." Bu, diğerlerini de benzer önlemleri almaya motive eder.
- **Politikalar ve Eğitim Materyalleri:** Örnek güvenlik politikaları veya eğitim slaytları gibi kaynakları paylaşmak karşılıklı olarak faydalı olabilir. Bir CSO, herkesin tekerleği yeniden icat etmek yerine, başkalarının uyarlayabileceği harika bir temel "Personel için Siber Güvenlik 101" sunumu hazırlamış olabilir.
- **Yardım için İletişim Bilgileri:** Bir güvenlik danışmanı veya BT gönüllüsüyle iyi bir deneyiminiz varsa, bu kişiyi ihtiyacı olan bir CSO meslektaşınızla paylaşabilirsiniz (tabii ki izniyle). Benzer şekilde, bir CSO üyesi bir siber güvenlik atölyesine veya web seminerine katılırsa, katılamayan meslektaşlarına önemli bilgileri aktarabilir.
- **Ortak Tatbikatlar:** Birden fazla kuruluşun katıldığı bir güvenlik eğitimi veya birkaç CSO arasında simüle edilmiş bir kimlik avı tatbikatı gibi ortak etkinlikler düzenleyebilirsiniz. Bu, becerileri geliştirmekle kalmaz, katılımcılar arasında güveni de artırır.

Paylaşım için Güven Oluşturma: Güvenlik bilgileri hassastır. Açıkça paylaşmak için ("X yöntemiyle hacklendik, Y verilerini kaybettik"), meslektaşlarınızın bu bilgileri kötüye kullanmayacağına veya sert bir şekilde yargılamayacağına güvenmeniz gerekir. Gizlilik normu oluşturun. Belki de daha geniş bir ölçeğe geçmeden önce, küçük, güvenilir bir grup oluşturun (örneğin, birbirini tanıyan CSO'lardan oluşan bir koalisyon veya çalışma grubu gibi). Bazı topluluklar Chatham House Kuralı'nı benimser (bilgileri kullanabilirsiniz, ancak kimin söylediğini açıklamayabilirsiniz). Bazıları, paylaşılan bilgileri dikkatli bir şekilde ele almaya yönelik basit bir mutabakat metni bile imzalayabilir. Zamanla, faydalı paylaşımlar oldukça güven artar.

Platformların kullanımı: Bazı platformlar ve araçlar güvenli paylaşımı kolaylaştırabilir:

- Şifreli e-posta listeleri (tüm katılımcılar yönetebiliyorsa hizmetler veya PGP kullanarak, ancak PGP kullanımı zordur).
- Acil konular hakkında hızlı bilgi vermek için Signal veya benzer uygulamalardaki mesajlaşma grupları.

- Muhtemelen **Rocket. Chat** veya **Matrix/Element** gibi bir platform kullanarak, CSO'lar için (kendi barındırdıkları veya güvenilir bir sunucuda) kamuoyunun gözünden uzak bir şekilde güvenlik konularını tartışabilecekleri kapalı bir forum oluşturun.
- Bazı ağlar, CERT'lerle ortaklık kurarak onlara anonim bilgiler sağlayabilir ve karşılığında tavsiyeler alabilir.

Başarılı Örnekler: **"CyberPeace Cafe"** veya güvenlik konusunda STK buluşmaları gibi girişimler olmuştur. Ayrıca, **NetHope** (insani yardım STK'larının oluşturduğu bir konsorsiyum) sivil toplum altyapısını kritik öneme sahip olarak ele alarak, ortak siber güvenlik kılavuzları ve olay bilgileri üzerinde çalışmaktadır. Bir diğeri ise bazılarının ortaya attığı "Sivil Toplum Örgütleri için Bilgi Paylaşımı ve Analiz Örgütü (ISAO)" konseptidir. Avrupa'da, AB projeleri kapsamında (belki de bu müfredatın bağlamında olduğu gibi), ortak sivil toplum örgütleri bu amaç için özel olarak paylaşılan bir olay günlüğü veya Slack kanalı kurabilirler.

Zamanında bilgi paylaşarak, STK'lar **birine yönelik saldırıyı tümü için erken bir uyarıya dönüştürebilir**. Bu, kıt uzmanlığın verimli kullanımını da sağlar – önde gelen bir STK'daki bir BT uzmanı, bilgi alışverişi yoluyla birkaç ortağa etkili bir danışmanlık hizmeti verebilir.

Güvenlik için Bir Topluluk Oluşturmak

Reaktif bilgi paylaşımının ötesinde, CSO'lar dijital güvenliği önceliklendiren bir topluluk kültürü proaktif olarak oluşturabilirler. Destekleyici bir topluluk, kaynakları bir araya getirebilir, öğrenmeyi teşvik edebilir ve daha iyi güvenlik araçları ve politikaları için savunuculuğu güçlendirebilir.

Güvenlik Şampiyonları Ağı: Yerel sivil toplumda siber güvenlikle ilgilenen veya bu alanda becerileri olan kişileri belirleyin. Bunlar teknoloji konusunda bilgili personel, BT geçmişi olan gönüllüler veya bu alana ilgi duyan akademisyenler olabilir. Sorunları ve çözümleri tartışmak için düzenli olarak (sanal olarak da olabilir) bir araya gelen yerel bir "güvenlik şampiyonları" grubu oluşturun. Bu şampiyonlar daha sonra kendi kuruluşlarında irtibat kişisi olarak görev yapabilirler. Örneğin, bir CSO'nun BT sorumlusu diğerlerine Wi-Fi ağlarını nasıl güçlendireceklerini öğretirken, GDPR hakkında bilgi sahibi olan bir başkası uyumluluk ipuçları paylaşabilir.

Atölye Çalışmaları ve Eğitim Etkinlikleri: Birden fazla CSO'yu davet ederek topluluk eğitim oturumları düzenleyin. Belki de "Şifre Yöneticilerini Kullanma", "Mobil İletişimi Güvenli Hale Getirme" veya "Siber Olaylara Nasıl Müdahale Edilir" gibi konularda üç ayda bir atölye çalışması düzenleyebilirsiniz. Bu konuların çoğu bu kitabın içeriğinden alınmıştır. Birlikte eğitim alarak, CSO personeli sadece bilgi edinmekle kalmaz, aynı zamanda meslektaşlarıyla da tanışır ve bu da daha önce bahsettiğimiz bilgi paylaşımı için güven temeli oluşturur. 'da, CSR veya topluluk hizmeti kapsamında, kar amacı gütmeyen kuruluşlar için düşük maliyetli veya ücretsiz olarak bu atölyeleri düzenleyecek uzmanlar (üniversitelerden, şirketlerden veya devlet CERT'lerinden) bulabilirsiniz. Sayıların gücü vardır – bir kurumsal eğitmen, beş kişilik bir CSO için ücretsiz bir oturum düzenlemeyebilir, ancak çeşitli CSO'lardan 50 kişilik bir topluluk için bunu yapabilir.

Akran Desteği ve Mentorluk: Arkadaşlık sistemini teşvik edin: IT desteği olmayan daha küçük bir STK'yı, IT departmanı olan daha büyük bir STK ile mentorluk için eşleştirebilirsiniz. Örneğin, bulut güvenliğini başarıyla uygulayan bir STK, bu işe yeni başlayan başka bir STK'ya mentorluk yapabilir. Bu gayri resmi olabilir, ancak gerektiğinde hızlı yardım sağlar ("Hey, tüm personel için 2FA'yı nasıl uyguladınız? Bize gösterebilir misiniz?").

Kaynak Havuzu: Ortak satın alma veya araçların paylaşılmasını düşünün. Bir grup CSO, güvenlik yazılımında toplu indirim alabilir veya aboneliği paylaşabilir (lisans koşulları dahilinde). Alternatif olarak, bir CSO'nun yedek sunucusu veya güvenlik cihazı varsa, diğerleri de bu kapasiteyi kullanabilir. Bazı durumlarda, CSO'lar, her birinin tek başına sağlayabileceğinden daha yüksek kaliteli güvenlik sağlamak için ortak BT hizmetleri (ortak bir güvenli e-posta sunucusu veya üç veya dört kuruluş arasında paylaşılan bir BT yardım masası gibi) kurmuştur.

Topluluk Savunuculuğu: STK'ların daha iyi siber güvenlik koşulları için toplu olarak savunuculuk yapma rolü de vardır. Örneğin, bağışçı topluluğuna siber güvenlik kapasitesinin geliştirilmesi için fon sağlaması için lobi yapmak veya yazılım sağlayıcılarını daha iyi kar amacı gütmeyen kuruluşlara yönelik fiyatlandırma veya özellikler sunmaya zorlamak (bazı kar amacı gütmeyen koalisyonlar, Microsoft veya Google'ın STK'lar için ücretsiz güvenlik eklentileri eklemesini sağlamıştır). Ayrıca, internet servis sağlayıcıları veya yetkililerle sivil topluma yönelik tehditler (aktivistleri hedef alan sofistike kimlik avı gibi) hakkında farkındalık yaratmak, daha

geniş koruma önlemlerine yol açabilir. NetHope'un tanımladığı "kritik altyapı olarak sivil toplum" kavramını düşünün – CSO'lar bir araya gelerek, hükümet veya endüstriye benzer bir korumaya ihtiyaçları olduğunu savunabilir ve böylece destek çekebilirler.

Olaylara Müdahale Konusunda Dayanışma: Büyük bir olay meydana geldiğinde (örneğin, bir STK ciddi bir saldırıya uğradığında veya çevrimiçi tacizle karşı karşıya kaldığında vb. Diğer STK'lar insan gücüyle yardımcı olabilir, kamuoyuna mesaj verme yükünü paylaşabilir veya geçici hizmetler sağlayabilir. Örneğin, bir insan hakları grubu DDoS saldırısına uğradığında, diğerleri web sitesi içeriğini yansıtarak erişilebilirliğini sürdürmüştür (dijital dayanışma gibi). Bu tür işbirliğine dayalı savunma, düşmanlara birine saldırmanın diğerlerini harekete geçireceğini gösterir ve bu da caydırıcı olabilir.

Başarı Hikayelerini Paylaşma: Olumlu bir topluluk oluştururken, başarı hikayelerini de paylaşın (Bölüm 7'de vurgulanacağı gibi). Bir CSO, eğitim sayesinde bir kimlik avı girişimini başarıyla engellediğinde, bunu topluluk bülteninde kutlayın. Bu, güvenliğe yatırım yapmanın karşılığını aldığını herkese gösterir. Güvenliğe katkıda bulunanları takdir edin ve onlara teşekkür edin (örneğin, yıllık CSO konferansında, farklı CSO'lara gidip ücretsiz antivirüs yükleyen o gönüllü BT çalışanını övün – bu tür moral desteği, sürekli desteği teşvik eder).

Güvenlik konusunda sıkı sıkıya bağlı bir topluluk oluşturarak, CSO'lar izole, savunmasız hedeflerden dayanıklı bir ağa dönüşürler. Saldırganlar (suçlular veya baskıcı rejimler) genellikle izole kuruluşları hedef alırlar; birleşik bir cephe, saldırganların taktikleri hakkındaki bilgilerin hızla yayılması ve yanıtların koordine edilebilmesi anlamına gelir. Bir atasözünde de söylendiği gibi, "Dayanışmada güvenlik vardır."

Halkı Bilgilendirmek: Dijital Güvenlik Bilincini Artırmak

Sivil toplum kuruluşları genellikle topluluk eğitimcileri ve savunucuları olarak hizmet eder. Dijital güvenlik sadece iç bir sorun değildir; birlikte çalıştığınız birçok kişi (yararlanıcılar, topluluk üyeleri, aktivistler vb.) de daha iyi güvenlik bilincinden faydalanabilir. Dijital güvenlik bilgisini daha geniş bir topluluğa yayarak, etkiyi katlar ve daha güvenli bir sivil toplum ortamı yaratmaya yardımcı olursunuz.

Topluluk Atölyeleri ve Eğitimleri: Hedef kitleniz için temel dijital güvenlik konusunda halka açık atölyeler veya web seminerleri düzenlemeyi düşünün. Örneğin, bir gençlik

örgütüyseniz, gençler ve ebeveynleri için gizlilik ayarları, siber zorbalık, kimlik avı vb. konuları kapsayan "Sosyal Medyada Güvende Kalmak" başlıklı bir oturum düzenleyin. İnsan hakları savunucuları ile çalışıyorsanız, güvenli iletişim (Signal kullanımı, gözetimden kaçınma) konusunda bir eğitim düzenleyebilirsiniz. Bu oturumlar, düzenli programınıza entegre edilebilir. Birçok STK zaten ilgili konularda (örneğin, medya okuryazarlığı, çevrimiçi gizlilik) eğitimler düzenlemektedir – bu müfredattan modüller ekleyebilirsiniz. Bu tür bir eğitim sağlamak sadece topluma yardımcı olmakla kalmaz, aynı zamanda STK'nızı güncel sorunları ele almada lider konumuna getirir, bu da itibarınızı ve güvenilirliğinizi güçlendirebilir.

Basit Eğitim Materyalleri Geliştirin: Güvenlik ipuçları hakkında broşürler, infografikler veya blog yazıları oluşturabilir veya uyarlayabilir ve bunları kamuoyuyla paylaşabilirsiniz. Örneğin, etkinliklerde veya sosyal medyada dağıtabileceğiniz, kolay adımlar içeren (güçlü şifreler kullanın, şüpheli bağlantılara tıklamayın, yazılımları güncelleyin vb.) "Çevrimiçi Kendinizi Korumanın 5 Yolu" başlıklı bir sayfalık bir belge. Görsel, teknik olmayan dili, genel kitle için en uygunudur. Ulusal siber güvenlik farkındalık kampanyalarının içeriğini uyarlayabilirsiniz (Ekim Siber Güvenlik Ayı materyalleri genellikle ENISA veya diğer kaynaklar aracılığıyla birden fazla dilde ücretsiz olarak mevcuttur). Materyallerin yerel dilde ve bağlamsal olarak alakalı olduğundan emin olun (insanların karşılaştığı yerel dolandırıcılıkları, yerel destek irtibatlarını belirtin). Bu, kuruluşunuzun misyonuyla da bağlantılı olabilir – örneğin, çevrimiçi dolandırıcılıktan kaçınmayı öğreten bir tüketici hakları CSO'su.

***Halkı Bilgilendirme Kampanyaları*:** Kaynaklar izin veriyorsa, dijital güvenlikle ilgili bir kampanya düzenleyin. Bu kampanya, Güvenli İnternet Günü gibi bir etkinliğe veya ilgili yerel gelişmelere (örneğin, bölgenizde SMS dolandırıcılıklarının artması) bağlanabilir. İletişim kanallarınızı kullanarak takipçilerinize düzenli olarak güvenlik konusunda hatırlatmalarda bulunun (güvenlik ipuçlarını tweetleyin, dikkat edilmesi gereken güncel dolandırıcılık haberlerini paylaşın vb.). Bazı STK'lar, telekom şirketleri veya medya ile işbirliği yaparak güvenlikle ilgili kamu spotu mesajları yayınlamaktadır. Facebook sayfanızda haftalık "Güvenlik İpucu Salısı" yayınlamak gibi küçük ölçekli bir kampanya bile yavaş yavaş farkındalığı artırabilir.

Medya ve Hikaye Anlatımını Kullanın: İnsanlar hikayeler aracılığıyla anlarlar. Uygunsa, dijital olayların ve bunların nasıl aşıldığının anonim hikayelerini paylaşın (belki bir blog veya

konuşma kapsamında). Örneğin, bir topluluk liderinin e-postasının nasıl hacklendiği ve sahte mesajlar göndermek için kullanıldığı ve bundan ne öğrenildiği gibi bir hikaye. Bu, sorunu insancıllaştırabilir ve başkalarını dikkatli olmaları konusunda uyarabilir. Medya, bir eğilim varsa (örneğin, çevrimiçi olarak STK'ların veya aktivistlerin hedef alınmasının artması gibi) da ilgilenebilir; konuyla ilgili STK'nızla yapılan bir röportaj, dijital güvenliğin önemini daha geniş bir kitleye vurgulayabilir.

Daha İyi Politikalar ve Destek için Lobi Faaliyetleri: Daha üst düzeyde, kamuoyunu ve politika yapıcıları sivil toplumun siber güvenlik ihtiyaçları hakkında bilgilendirin. STK'lar, STK'lara siber güvenlik konusunda yardımcı olan hükümet programlarını toplu olarak savunabilirler (bazı ülkelerde hibe programları veya CERT özel yardım programları vardır). Ayrıca, teknoloji ürünlerinde kullanıcı dostu güvenlik için savunuculuk yapın – örneğin, yazılım şirketlerini güvenli ayarları varsayılan olarak yapmaya zorlayarak, kullanıcıların kapsamlı uzmanlık gerektirmeden daha güvenli olmalarını sağlayın. Örneğin AB'de, sivil toplumu siber tehditlerden korumaya yönelik diyaloglar vardır; bu forumlarda STK'ların sesleri, politika önlemlerinin onları da içermesini sağlar (finansman ve eğitim gibi).

Okullar ve Kütüphanelerle İşbirliği Yapın: Dijital okuryazarlık ve güvenlik konusunda ortak oturumlar düzenlemek için yerel eğitim kurumları veya kütüphanelerle ortaklık kurabilirsiniz. Birçok halk kütüphanesi bilgisayar dersleri düzenlemektedir; güvenlik konulu bir bölüm sunmak memnuniyetle karşılanabilir. Okullar, çevrimiçi güvenliği öğretme ihtiyacını giderek daha fazla hissetmektedir; uzmanlığa sahip STK'lar bu müfredatı destekleyebilir. Gençleri ve genel halkı eğitmeye yardımcı olarak, daha güvenlik bilincine sahip bir toplum oluşturursunuz, bu da dolaylı olarak STK'nızı da korur (kuruluşunuzun spear phishing saldırılarına maruz kalmasına neden olabilecek kişisel hesapların sayısının azalması vb.

Bildirim ve Diyaloğu Teşvik Edin: Etkileşimde bulunduğunuz halkı siber suçları veya şüpheli olayları bildirmeleri için teşvik edin. Birçok kişi sessizce acı çekiyor veya çok utanıyor (sanki bir dolandırıcılığın kurbanı olmuş gibi). İnsanların yardım isteyebileceği bir ortam yaratın – belki CSO'nuz, çevrimiçi taciz veya dolandırıcılık kurbanı olan kişileri polise veya yardım hatlarına yönlendirmek için arabulucu olarak hizmet edebilir. Bazı CSO'lar, güvenlik bilinciyle ilişkili olan

toplumdaki gizlilik veya gözetim gibi konuları vurgulayarak dijital haklar savunucusu rolünü üstlenir.

Misyonunuzla uyumlu olun: Tutarlılık için kamu güvenliği eğitimini misyonunuzla uyumlu hale getirin. Örneğin, CSO'nuz kadın haklarıyla ilgileniyorsa ve kadın aktivistlerin çevrimiçi tacize maruz kaldığını biliyorsanız, farkındalığı bu konuya ve bununla nasıl başa çıkılacağına (engelleme/bildirme özellikleri, gizliliği koruma) odaklayın. Çevresel bir CSO iseniz, yanlış bilgilerin çevrimiçi olarak nasıl yayıldığını ve temel doğrulama uygulamalarını vurgulayabilirsiniz – bu, güvenlikle ilgili bir konudur (bilgi bütünlüğü).

Halkı bilgilendirerek, STK'lar iki yönlü bir hizmet sunar: seçmenlerini korur ve faaliyet gösterdikleri ortamın genel güvenlik "hijyenini" artırarak kendi güvenliklerini güçlendirir. Bu, bilinçli bir topluluğun siber olayların taşıyıcısı veya kurbanı olma olasılığının daha düşük olduğu bir döngü yaratır.

Özetle, bilgi güçtür ve CSO'lar, güvenilir topluluk kuruluşları olarak, bu gücü geniş çapta yaymak için uygun konumdadır.

Yerel ve Uluslararası Destek Kaynakları

Akran işbirliği ve kamu bilincinin yanı sıra, yerel, bölgesel ve uluslararası düzeylerde CSO'lara sunulan resmi destek kaynakları da bulunmaktadır. Bunların neler olduğunu ve bunlara nasıl erişebileceğinizi bilmek, özellikle sofistike tehditlerle karşı karşıya kaldığınızda veya kapasitenizin ötesinde kaynaklara ihtiyaç duyduğunuzda çok gerekli olan yardımı sağlayabilir.

Yerel Kaynaklar:

- Ul**usal Siber Güvenlik Ajansları/CERT'ler:** Daha önce de belirtildiği gibi, birçok ülkede rehberlik hizmeti sunan ulusal bir CERT (Bilgisayar Acil Durum Müdahale Ekibi) veya siber güvenlik ajansı bulunmaktadır. Bazıları CSO'lara veya küçük işletmelere odaklanan programlara sahiptir. Örneğin, Birleşik Krallık'ın Ulusal Siber Güvenlik Merkezi (NCSC), kuruluşların güvenliğini artırmak için ücretsiz rehberlik ve hatta bazı ücretsiz hizmetler (web kontrolü, posta kontrolü gibi) sunmaktadır. Ülkenizin CERT'inin sizin dilinizde bir sosyal yardım programı veya kaynakları olup olmadığını kontrol edin (genellikle takip edebileceğiniz uyarı bültenleri yayınlarlar).

- **Kolluk Kuvvetleri Siber Suç Birimleri:** Çevrimiçi dolandırıcılık, taciz veya hedefli saldırı gibi sorunlarla karşılaşırsanız, yerel polis siber birimleri yardımcı olabilir. Bazı ülkelerde sivil toplumla çalışan özel birimler vardır (özellikle gazetecileri veya aktivistleri korumak amacıyla). Mümkünse bir ilişki kurun; örneğin, bir memuru CSO forumuna siber olayları bildirme konusunda konuşma yapmaya davet ederek süreci anlaşılır hale getirebilirsiniz.
- **Akademik Kurumlar:** Yerel üniversiteler, özellikle BT veya siber güvenlik bölümleri olanlar, müttefikiniz olabilir. Profesörler veya öğrenciler, araştırma veya gönüllü projelerin bir parçası olarak CSO güvenliğini üstlenebilir. Örneğin, bir üniversite BT kulübü, sınıf projesi olarak CSO'nuz için bir güvenlik denetimi yapabilir (izin ve denetim altında). Bazı üniversiteler siber güvenlik klinikleri işletir veya sosyal teknoloji çözümleri için kuluçka merkezleri vardır.
- **Teknoloji Şirketlerinin Yerel Ofisleri:** Büyük teknoloji şirketleri genellikle yerel varlığa ve kurumsal sosyal sorumluluk (CSR) programlarına sahiptir. Bazen dijital okuryazarlık veya güvenlik atölyeleri düzenlerler (Google'ın çevrimiçi güvenlik eğitimi, Meta'nın dijital okuryazarlık kampanyası vb.). CSO personelinizin veya yararlanıcılarınızın bu ücretsiz eğitimlere dahil edilmesi için onlarla iletişime geçin. Ayrıca güvenlik ürünleri bağışlayabilir veya indirimli satabilirler. Örneğin, Cisco bazı kar amacı gütmeyen kuruluşlara ortaklıklar aracılığıyla güvenlik duvarı donanımı bağışlamıştır.
- **CSO Destek Kuruluşları:** Teknoloji federasyonları veya dernekleri gibi kuruluşlar (örneğin, güvenlik paketleri dahil olmak üzere indirimli yazılım sağlayan küresel bir CSO olan TechSoup; Avrupa'da ise belki de Avrupa Sivil Toplum Güvenliği Ağı vb. mevcuttur). TechSoup, özellikle , sadece yazılım değil, aynı zamanda kapasite geliştirme kaynakları ve bazen güvenlikle ilgili web seminerleri de sunmaktadır. Ulusal CSO ağları da ICT ile ilgili çalışma gruplarına sahip olabilir ve bu gruplardan tavsiye alabilirsiniz.

Uluslararası Kaynaklar:

- **Access Now'un Dijital Güvenlik Yardım Hattı:** Daha önce de belirtildiği gibi, bu hat sivil toplum için 7/24 hizmet veren, küresel çapta erişilebilir bir hızlı müdahale ekibidir. Birden fazla dilde hizmet vermektedir (7/24 İngilizce, İspanyolca, Fransızca ve diğer dillerde). Kötü amaçlı yazılımların kaldırılmasına yönelik rehberlikten DDoS saldırılarının etkisinin

azaltılmasına ve hesapların kurtarılmasına kadar her konuda yardımcı olabilirler. Hizmet ücretsiz ve gizlidir.

- **CyberPeace Institute:** Bu kuruluş**,** sivil topluma yönelik siber saldırıları analiz etmekle kalmaz, aynı zamanda yardımları da koordine eder. CyberPeace Builders programı, teknoloji şirketlerinden gönüllülerin dünya çapındaki sivil toplum kuruluşlarına ücretsiz yardım sunmasını sağlar. Programın yararlanıcıları arasına katılmak için başvurabilirsiniz. Bu sayede, güvenli altyapı veya politikalar oluşturma konusunda yardım gibi düzenli uzmanlık desteği alabilirsiniz.
- **Uluslararası İfade Özgürlüğü/Dijital Haklar Kuruluşları:** Front Line Defenders, The Engine Room, EFF (Electronic Frontier Foundation) ve diğerleri gibi gruplar genellikle kılavuzlar yayınlar veya sizi uzmanlarla buluşturabilir. Örneğin, Front Line Defenders'ın insan hakları savunucuları için özel olarak tasarlanmış bir "Dijital Koruma" programı ve Security in a Box araç seti (araçlar ve taktikler içeren) bulunmaktadır.
- **Bağışçılar Tarafından Finanse Edilen Programlar:** Bazen, özellikle STK'ların siber dayanıklılığını artırmak için bağışçılar tarafından finanse edilen projeler vardır. Örneğin, AB'de Erasmus+ veya CEF kapsamında, kar amacı gütmeyen kuruluşlar için güvenlik dahil olmak üzere dijital becerilerin geliştirilmesine odaklanan projeler vardır (belki de başlığınızda bahsettiğiniz KA220 projesi bunlardan biridir). Bu tür projeler kapsamındaki çağrılara veya ağlara dikkat edin; bunlar genellikle araç setleri üretir, eğitimler düzenler veya katılan STK'lara danışmanlık hizmeti sunar.
- **Forumlar ve Konferanslar:** Uluslararası düzeyde, RightsCon, İnternet Yönetişim Forumu (IGF) veya bölgesel siber güvenlik konferansları gibi konferanslarda bazen sivil toplum oturumları düzenlenir. Bu konferanslara katılmak sizi küresel bir topluluğa ve kaynaklara bağlayabilir. Özellikle RightsCon, aktivistlerin dijital hakları ve güvenliği ile ilgilidir. Birçok oturumda, uygulanabilir tavsiyeler verilir veya güvenlik iyileştirmelerinizi destekleyebilecek fon sağlayıcılarla tanışabilirsiniz.
- **Fon Olanakları:** Uluslararası vakıflar, siber güvenliği sivil toplum için kritik bir kapasite olarak kabul etmiştir. Örneğin, Ford Vakfı ve Açık Teknoloji Fonu, STK'ların siber güvenlik girişimlerine fon sağlamıştır. AB, Horizon veya Digital Europe gibi programlar

kapsamında, ortaklık kurarsanız veya başvurursanız kapasite geliştirmeyi destekleyebilecek fonlar sunmaktadır. Ciddi iyileştirmelere (BT güvenlik personeli işe almak veya BT altyapısını yenilemek gibi) ihtiyacınız varsa, bunu temel destek için hibe tekliflerine dahil etmeyi düşünün. Bunu gerekli risk azaltma önlemi olarak gerekçelendirin – birçok bağışçı artık bu konuda daha bilinçlidir ve bunun için bütçeyi onaylayabilir.

Dil ve Kültürel Alaka: Yardım ararken, mümkünse kendi dilinizde veya bağlamınızda bulmaya çalışın. Küresel kaynaklar harikadır, ancak İngilizce olabilir veya çok genel olabilir. Bu nedenle yerel uzmanlar ve uluslararası kılavuzların yerel dillere çevrilmesi önemlidir. Örneğin, CSO'nuz Türkiye'deyse (mesajda İstanbul saat dilimini görüyorum), yerel bir Türk kaynağı (Türkçe CERT danışmanlığı veya Türkçe dijital güvenlik eğitimi gibi) kullanmak personel için daha kolay olabilir. Dilinizde bir kaynak bulamıyorsanız, ilgili bir kılavuzu çevirmek için gönüllü olun – bu da bir topluluk katkısıdır.

Teknoloji Bağışları: Destek konusunda, Google for Nonprofits'ın ücretsiz G Suite, Microsoft for Nonprofits'ın ücretsiz O365 lisansları, Okta'nın ücretsiz tek oturum açma çözümleri sunduğunu ve bazı güvenlik sağlayıcılarının kar amacı gütmeyen bağış programları olduğunu (örneğin, NortonLifeLock bazı CSO desteği sağlar) unutmayın. Bunlar, üst düzey güvenlik araçlarını kullanmanın maliyet engellerini azaltabilir.

Güncel Kalın: Tehdit ortamı sürekli değişmektedir. Bazı güvenlik haber kaynaklarını takip etmeyi veya posta listelerine katılmayı (bazıları CSO'lar için hazırlanmıştır) bir alışkanlık haline getirin. Örneğin, CIVICUS Siber Güvenlik posta listesi (varsa) veya sosyal medyada güvenilir kaynakları takip etmek (örneğin, AB haberleri için Twitter'da @enisa_eu veya yerel siber güvenlik şirketlerinin blogları).

Özetle, yalnız değilsiniz. Yerelden küresele kadar bir destek ağı vardır. Sakin zamanlarda (sadece kriz sırasında değil) bu kaynaklarla proaktif olarak bağlantı kurmak faydalıdır. Önemli kişilerle ilişkiler kurun (bir sorun olduğunda saat 10'da kimi arayacağınızı bilin). Aynı şekilde, bilgi veya kaynak edindiğinizde, bu ağlara katkıda bulunun – bu, ağların sağlam kalmasını ve ihtiyaç duyan bir sonraki CSO için kullanılabilir olmasını sağlar.

İşbirliğinden yararlanarak (bölüm 6.1, 6.2), halkı eğiterek (6.3) ve destek sistemlerine ulaşarak (6.4), CSO'lar dijital güvenliği zorlu bir tek başına mücadele olmaktan çıkarıp topluluk destekli

bir çaba haline getirebilirler. Bir sonraki bölümde, gerçek dünya deneyimlerinden daha fazla ders çıkarmak için somut örnekler ve yaygın tuzaklara bakacağız.

Bölüm Özeti

Bölüm 6, CSO'ların riskleri proaktif olarak belirlemeleri ve siber olaylara hazırlanmaları için çerçeveler sunar. Kuruluşlara, basit risk değerlendirme şablonlarını kullanarak kritik varlıkları (ör. bağışçı veritabanları) ve güvenlik açıklarını değerlendirmeleri için rehberlik eder ve phishing veya fidye yazılımı gibi tehditleri önceliklendirir. Bu bölüm, olay müdahale planı oluşturmayı özetler ve tespit, sınırlama, iletişim ve kurtarma adımlarını ayrıntılı olarak açıklar. Örneğin, bir müdahale planına sahip bir CSO, fidye yazılımı saldırısından sonra verileri hızlı bir şekilde geri yükleyerek hasarı en aza indirebilir. Olaylardan ders çıkarmak için olayları belgelemeyi ve planları yıllık olarak güncellemeyi vurgular. Bu bölüm, GDPR'nin 72 saatlik ihlal bildirim kuralını ele alarak uyumluluğu sağlar. Pratik adımlar arasında rol atama (örneğin, Veri Koruma Görevlisi) ve masa başı tatbikatları yoluyla planları test etme yer alır. Bu bölümün hazırlığa odaklanması, CSO'ların hızlı bir şekilde kurtarma yapmasına yardımcı olarak operasyonel ve itibar zararını azaltır. Açık ve düşük maliyetli çerçeveler sunarak, teknik olmayan personelin dayanıklılığa katkıda bulunmasını sağlar ve kaynakları kısıtlı kuruluşlar için siber güvenliği ulaşılabilir hale getirme misyonuyla uyumludur.

CSO'lar için Veri Koruma Politikası Şablonu

Kuruluş Adı: [CSO Adını Girin]

Yürürlük Tarihi: [Tarihi girin]

Son Güncelleme: [Tarihi girin veya "İlk politika için geçerli değil"]

Bu Veri Koruma Politikası, [CSO Adı]'nın gizlilik, güvenlik ve geçerli yasalara (ör. GDPR, [Yerel Veri Koruma Yasasını ekleyin]) uyumu sağlamak için kişisel verileri nasıl topladığını, sakladığını, eriştiğini ve koruduğunu özetler. Kişisel verileri işleyen tüm personel, gönüllüler ve ortaklar için geçerlidir ve yararlanıcılarımızın, bağışçılarımızın ve paydaşlarımızın güvenini korur.

Bu politika, [CSO Adı] tarafından yönetilen tüm kişisel verileri (örneğin, isimler, iletişim bilgileri, sağlık veya finansal bilgiler) kapsar; buna yararlanıcılar, bağışçılar, personel ve gönüllülerle ilgili veriler de dahildir.

1. Veri Toplama

Misyonumuz ve programlarımız için gerekli olan kişisel verileri toplarız ve gerektiğinde bilgilendirilmiş onam alırız. Veriler yasalara uygun, şeffaf ve belirli amaçlar için toplanır.

Prosedürler:

⇒ Veri toplanmadan önce, verilerin neden toplandığı ve nasıl kullanılacağı açıkça açıklanır (örneğin, onay formları veya gizlilik bildirimleri yoluyla).

⇒ Amaca ulaşmak için minimum düzeyde veri toplayın (veri minimizasyonu ilkesi).

⇒ Toplamanın amacını belgelendirin ve uygun olduğu durumlarda onay alın (örneğin, imzalı formlar, çevrimiçi onay kutuları).

2. Veri Depolama

Yetkisiz erişim, kayıp veya hırsızlığı önlemek için kişisel verileri şifreleme ve korumalı sistemler kullanarak güvenli bir şekilde saklarız.

Prosedürler:

⇒ Verileri güvenli platformlarda saklayın (ör. 2FA ile Google Drive gibi şifreli bulut hizmetleri veya kilitli fiziksel dosyalar).

⇒ Hassas verileri depolandıkları yerde (ör. dizüstü bilgisayarlar, harici sürücüler) ve aktarım sırasında (ör. HTTPS veya güvenli e-posta kullanarak) şifreleyin.

⇒ Veri kurtarmayı sağlamak için düzenli yedeklemeler yapın (ör. haftalık olarak güvenli bir bulut veya harici sürücüye).

⇒ Artık ihtiyaç duyulmadığında verileri güvenli bir şekilde imha edin (örneğin, kağıt kayıtları parçalayın, dijital dosyalar için güvenli silme araçları kullanın).

3. Erişim Kontrolü

Kişisel verilere erişim, en az ayrıcalık ilkesine göre, görevleri için bu verilere ihtiyaç duyan yetkili personel ile sınırlıdır.

Prosedürler:

⇒ İş rollerine göre erişim atayın (örneğin, yalnızca program yöneticileri yararlanıcı verilerine erişebilir).

⇒ Kişisel verilere erişimi olan tüm hesaplar için güçlü parolalar ve iki faktörlü kimlik doğrulama (2FA) kullanın.

⇒ Eski personel veya gönüllülerin erişimini kaldırmak için erişim izinlerini düzenli olarak (örneğin, aylık olarak) denetleyin.

⇒ Personel ve gönüllülere güvenli veri işleme konusunda eğitim verin (örneğin, şifreleri paylaşmama, kullanımdan sonra oturumu kapatma).

4. İhlal Bildirimi

Zararı en aza indirmek ve yasal yükümlülükleri yerine getirmek için veri ihlallerini derhal tespit eder, bunlara yanıt verir ve rapor ederiz (örneğin, GDPR'nin 72 saatlik bildirim kuralı).

Prosedürler:

⇒ İhlalleri ele almak üzere bir Veri Koruma Görevlisi veya sorumlu kişi (örneğin, [Ad/Rol Ekle]) atayın.

⇒ Şüpheli ihlalleri derhal belirlenen kişiye bildirin (ör. [E-posta adresini girin] adresine e-posta yoluyla).

⇒ İhlal bireylere zarar verme riski taşıyorsa, 72 saat içinde ilgili veri koruma otoritesine (ör. [Yerel Otorite Adını Girin]) bildirin.

⇒ Gerekirse etkilenen kişileri (ör. yararlanıcılar, bağışçılar) bilgilendirin ve sonraki adımlar hakkında net talimatlar verin.

⇒ Gelecekte önlemlerin alınmasını iyileştirmek için tüm ihlalleri ve bunlara verilen yanıtları belgelendirin (ör. risk değerlendirmesini güncelleyin).

5. Sorumluluklar

Liderlik: Politikanın uygulanmasını onaylayın ve finanse edin (örneğin, eğitim ve araçlar için bütçe ayırın).

Personel ve Gönüllüler: Bu politikayı takip edin, sorunları derhal bildirin ve veri koruma eğitimine katılın.

Veri Koruma Görevlisi/Sorumlu Kişi: Politika uyumluluğunu denetleyin, ihlalleri yönetin ve yıllık incelemeleri koordine edin.

6. Uyum ve İnceleme

Uyum: Bu politika GDPR ve [Yerel Veri Koruma Yasasını ekleyin] ile uyumludur. Uyumsuzluk, disiplin cezası veya yasal yaptırımlarla sonuçlanabilir.

Bu politikayı yıllık olarak veya önemli değişikliklerden sonra (ör. yeni programlar, düzenlemeler) gözden geçirin ve güncelleyin. Sonraki gözden geçirme: [Tarih ekleyin, ör. Kasım 2026].

Tüm personel ve gönüllüler, işe başlarken ve her yıl veri koruma eğitimi alır.

7. İletişim

Sorularınız veya ihlalleri bildirmek için iletişim kurun: [Veri Koruma Görevlisi/Sorumlu Kişinin Adı, E-posta, Telefonu ekleyin].

Yerel Veri Koruma Kurumu: [Ad ve İletişim Bilgilerini Ekleyin, örneğin, "Türkiye Kişisel Verileri Koruma Kurumu (KVKK), [iletişim bilgileri]".

Onaylayan: [Yönetim Adı/Görevi, ör. İcra Direktörü]

Tarih: [Tarihi ekleyin]

Özelleştirme Notları: Yer tutucuları (ör. [CSO Adı], [Yerel Veri Koruma Yasası]) kuruluşunuzun bilgileriyle değiştirin. Gerektiğinde yerel uyumluluk gerekliliklerini veya belirli araçları ekleyin.

2.7 BÖLÜM 7: CSO'LARDA GÜVENLİK BAŞARILARI

Gerçek Hikayeler: CSO'larda Güvenlik Başarıları

Benzer kuruluşların güvenlik sorunlarını nasıl aştığını öğrenmek cesaret vericidir. İşte, iyi güvenlik uygulamaları sayesinde olumlu sonuçlar elde edilen birkaç anonim ama gerçekçi senaryo:

Eğitimle Engellenen Kimlik Avı Girişimi: Doğu Avrupa'daki bir insan hakları CSO'su, bir meslektaşından Google Docs paylaşımı gibi görünen bir e-posta aldı. Personel kimlik avı farkındalık eğitimi almış olduğu için, bir ekip üyesi bir şeylerin ters olduğunu fark etti (gönderenin e-postasında küçük bir yazım hatası vardı) ve bağlantıya tıklamadı. Bunun yerine, BT irtibat görevlisine haber verdi. Bunun kimlik bilgilerini çalmak için yapılan bir kimlik avı girişimi olduğunu doğruladılar. Sonuç olarak, hiçbir hesap ele geçirilmedi. Bu olay, eğitimin değerini pekiştirdi. CSO'nun direktörü, bir sonraki personel toplantısında, bu çalışanın ihtiyatlı davranışının herkesi koruduğunu vurgulayarak bunu bir ders olarak değerlendirdi. Uyanık bir personel sayesinde saldırı sıfır hasarla önlendiği için bu olay bir başarı olarak değerlendirildi.

Yedeklemeler Sayesinde Ransomware Saldırısından ***Kurtulma:*** Afrika'da orta ölçekli bir sağlık CSO'su bir sabah ransomware saldırısına uğradı – personel, dosyalarının şifrelenmiş olduğunu ve ekranlarında bir fidye notu olduğunu fark etti. Başlangıçta kaos yaşandı. Ancak, kuruluşun sağlam bir yedekleme sistemi vardı: tüm kritik veriler her gece harici bir sunucuya yedekleniyordu. Birkaç saat içinde, BT danışmanları virüs bulaşmış makineleri izole etti, silip temizledi, yazılımları yeniden yükledi ve önceki gecenin yedeklemesinden verileri geri yükledi. En fazla birkaç belgenin bir günlük çalışmasını kaybettiler. Fidyeyi ödemediler ve olayı bildirdiler. Bu deneyim, paylaştıkları bir güvenlik başarı öyküsüne dönüştü: yedekleme ve kurtarma planlamasına yaptıkları yatırım karşılığını verdi ve bunun ne kadar önemli olduğunu kanıtladı. Daha sonra, bu vakayı bir web seminerinde sunarak diğer CSO'ları çevrimdışı yedeklemeler uygulamaya teşvik ettiler.

Güvenli İletişim Korunan Hassas Planlar: Bir savunuculuk koalisyonu, yoğun gözetim altında olan bir ülkede bir kampanya düzenliyordu. İletişimlerinin izlendiğinden şüpheleniyorlardı. Dijital güvenlik danışmanının rehberliğinde, uçtan uca şifreli mesajlaşma (Signal) ve en hassas ekler için PGP ile e-posta kullanmaya geçtiler. Kampanya sırasında, rakiplerinin stratejilerini önceden engellemeye çalıştıklarını fark ettiler, ancak kritik detaylar

hiçbir zaman sızdırılmadı. Kampanya sonrası analizler, güvenli iletişime geçtikten sonra muhalefetin "içeriden bilgi" avantajını kaybettiğini gösterdi. Koalisyon, planlarını koruyan ve kampanyanın başarısına katkıda bulunan güvenli araçlara teşekkür etti. Bu, gelecekteki operasyonlar için şifreli kanalları kullanma kararlılıklarını pekiştirdi ve ağlarındaki diğerlerine örnek oldu.

İki Faktörlü Kimlik Doğrulama Hesap Ele Geçirmeyi Engelledi: Güney Asya'daki bir kadın hakları CSO'su, çalışanlarından birinin Gmail hesabının spear-phishing e-postası ile hedef alındığını fark etti. Çalışan, yanlışlıkla sahte bir Google giriş sayfasına şifresini girdi. Bu şifre saldırganın eline geçti. Kısa bir süre sonra, başka bir ülkeden saldırgan, çalışanın Google hesabına giriş yapmaya çalıştı, ancak STK tüm hesaplarda iki faktörlü kimlik doğrulamayı zorunlu kıldığından, giriş için çalışanın telefonundan bir doğrulama kodu istendi. Saldırgan bu koda sahip olmadığı için engellendi. Google, kullanıcıya engellenen giriş girişimi konusunda uyarıda bulundu. Çalışan ne olduğunu hemen fark etti, durumu bildirdi ve şifresini değiştirdi. Sonuçta, 2FA, ciddi bir güvenlik ihlali olabilecek bir durumu, hiçbir zarar verilmeden sadece bir korkuya dönüştürdü. Bu gerçek olay, tüm ekibe, biraz can sıkıcı olan 2FA istemlerinin neden değerli olduğunu gerçekten anlattı. O gün, güvenlik önlemlerinin başarısı ve rahatlama günüydü.

Topluluk İşbirliği DDoS'yi Durdurdu: Bir çevre CSO'ları ağı, bazı rakiplerin öfkesini çeken bir kampanya başlattı ve rakipler, ağın ortak web sitesine Dağıtık Hizmet Engelleme (DDoS) saldırısı düzenledi (trafiği aşırı yükleyerek siteyi çevrimdışı hale getirdi). CSO'lar, bunu hafifletmek için bireysel olarak sınırlı BT kaynaklarına sahipti. Ancak, bir teknoloji dayanışma kanalı aracılığıyla, bir CSO lideri hızlı bir şekilde yardım istedi. Bir teknoloji şirketindeki ortak kuruluş, DDoS koruma hizmetinin (Cloudflare) geçici olarak kullanılmasını sağladı ve başka bir STK'nın BT personeli, bu koruma aracılığıyla sitenin yeniden yönlendirilmesine yardımcı oldu. Birkaç saat içinde, saldırıya rağmen web sitesi yeniden açıldı ve kampanya devam etti. Bu işbirliğine dayalı müdahale, müttefiklerin desteğinin büyük siber tehditlere bile nasıl karşı koyabileceğini gösteren bir başarı öyküsüydü. Ayrıca, bundan sonra her zaman açık olan Cloudflare korumasını kurmayı da öğretti. Daha sonra, yardım edenlere teşekkür etmek ve diğerlerine DDoS ile başa çıkma konusunda rehberlik etmek için bu vakayı bir blogda yazdılar.

Bu hikayeler, CSO'lar siber tehditlerin hedefi olsa bile, **hazırlıklı olmak ve hızlı hareket etmek başarılı bir savunma veya hızlı bir kurtarma sağlayabileceğini** göstermektedir. Ortak noktalar şunlardır: güvenlik önlemlerine (eğitim, yedeklemeler, 2FA) önceden yatırım yapmak, hızlı tanıma ve müdahale ve destek ağlarından yararlanmak. CSO'lar bu tür başarıları paylaşarak ve inceleyerek, neyin gerçekten işe yaradığını öğrenebilir ve benzer durumlarla başa çıkabileceklerine dair güven kazanabilirler.

Yaygın Hatalar ve Bunları Önleme Yöntemleri

Başkalarının hatalarından (veya kendi hatalarımızdan) ders almak, güvenliği artırmak için çok önemlidir. CSO'ların sıkça karşılaştığı bazı tuzaklar ve bunları önlemek için stratejiler şunlardır:

Zayıf veya Varsayılan Parolalar Kullanmak: Belki de en yaygın hata, kolay parolalar kullanmak (örneğin "123456", "password") veya cihazlarda varsayılan parolaları değiştirmeden bırakmaktır (örneğin, yönlendiriciler genellikle "admin/admin" parolasıyla gelir). Bunlar saldırganlar için birer hediyedir. Önleme: Güçlü, benzersiz parolalar gerektiren bir parola politikası oluşturun ve bunları yönetmek için parola yöneticileri kullanın. Eğitim sırasında, kötü ve iyi şifrelerin örneklerini gösterin. Yeni donanım/yazılım kurduğunuzda, varsayılan kimlik bilgilerini hemen değiştirin (ve bunları güvenli bir şekilde belgelendirin). Ara sıra denetimler yapın – bir araç veya komut dosyası kullanarak herhangi bir hesabın zayıf şifreye sahip olup olmadığını kontrol edin (bazı kuruluşlar ihlal veritabanlarını veya denetim araçlarını kullanır). Gözden kaçan zayıf şifreleri telafi etmek için 2FA'yı vurgulayın.

Düşünmeden Tıklama (Oltalama Başarısı): Birçok ihlal, birisinin kötü amaçlı bir bağlantıya veya eki dikkatlice incelemeden tıklamasıyla başlar. Hata, e-postanın veya mesajın gerçekliğini doğrulamak yerine, e-posta veya mesajın dürtüsüyle hareket etmektir (özellikle aciliyet veya merak uyandıranlar). Önleme: Eğitim, eğitim, eğitim. Simüle edilmiş kimlik avı testleri gerçekleştirerek kimin daha fazla pratiğe ihtiyacı olduğunu belirleyin. Yavaşlayıp talepleri doğrulamanın normal olduğu bir kültür oluşturun – örneğin, "Bir e-posta acil görünüyor ve para veya kimlik bilgileri istiyorsa, bir telefon görüşmesi veya ayrı bir e-posta ile tekrar kontrol etmek normaldir (hatta teşvik edilir)." Basit kontrol listeleri sağlayın: gönderen adresini dikkatlice kontrol edin, yazım hataları olup olmadığına bakın, beklenmedik ekleri indirmeyin vb.

Ayrıca, iyi spam filtreleri ve bağlantı taraması gibi teknik savunma yöntemleri, bariz dolandırıcılıkları filtrelemeye yardımcı olur.

***Yazılımı Zamanında Güncellememek*:** Yaygın bir senaryo: Bir CSO web sitesi WordPress üzerinde çalışıyor ancak bir yıldır eklentileri güncellemedi ve bir saldırgan bilinen bir açığı kullanarak siteyi tahrip etti. Ya da personel bilgisayarları hala yamalanmamış güvenlik açıkları olan eski işletim sistemi sürümlerini çalıştırıyor. Hata, güncellemeleri geciktirmek veya görmezden gelmektir (bazen bir şeyi bozabileceği korkusundan, bazen de sadece unutmaktan). Önleme: Mümkün olduğunda otomatik güncellemeleri etkinleştirin. Otomatik güncellemeyi etkinleştire e izin vermeyen sistemlerde, aylık kontrol görevini birine verin. Güncelleme ihtiyaçlarını toplayan araçlar kullanın (sadece "Güncellemeleri kontrol et" bildirimlerini etkinleştirmek bile yeterlidir). Web siteleri için, güncellemeleri yöneten yönetilen barındırma hizmetlerini değerlendirin veya eklenti güvenliği posta listelerine abone olun. "Yama Salı" veya başka bir rutin uygulamayı vurgulayın. Kaynaklar izin veriyorsa, kritik yazılımların envanterini tutun ve yama durumlarını takip edin (eksik yamaları vurgulayan ücretsiz tarayıcılar mevcuttur). Ayrıca, güncelleme yapmamanın güvenlik risklerini göstererek "güncellemeler bilgisayarımı yavaşlatıyor" gibi mitleri ortadan kaldırın.

Yedekleme Yapmama (veya Yedeklemeleri Test Etmeme): Bazı kuruluşlar, veri kaybı yaşadıktan sonra yedeklemelerin önemini anlar. Hatalar arasında hiç yedekleme yapmama veya yedeklemeler yapıp bunları test etmeme (daha sonra ihtiyaç duyulduğunda bunların eksik veya bozuk olduğunu fark etme) sayılabilir. Önleme: 3-2-1 yedekleme stratejisi uygulayın (birden fazla kopya, farklı ortamlar, bir tanesi şirket dışında). Yedeklemeleri planlayın ve otomatikleştirin. Daha da önemlisi, düzenli olarak test geri yüklemeleri yapın. Basit bir tatbikat: rastgele bir dosya seçin ve işlemin çalıştığından emin olmak için yedekten geri yüklemeyi deneyin. Ayrıca, yedeklemelerin kendilerinin de güvenli olduğundan emin olun (şifrelenmiş ve normal ağdan erişilemez, böylece fidye yazılımları onlara ulaşamaz). Birçoğu, herkesin erişebileceği bir ağ sürücüsündeki yedeklemenin şifreleme kötü amaçlı yazılımlarından güvenli olmadığını zor yoldan öğrenmiştir. Çözümler: çevrimdışı yedeklemeler veya en azından sürümlenmiş bulut yedeklemeleri şifrelemeye karşı bağışıktır.

Aşırı Ayrıcalık ve Paylaşılan Hesaplar: Hata: "daha kolay olduğu için" tüm kullanıcılara yönetici hakları vermek veya kolaylık olması için birden fazla kişi arasında tek bir oturum açma bilgisini paylaşmak. Bu, büyük sorunlara yol açabilir – bir kişi yönetici haklarıyla yanlışlıkla kötü amaçlı yazılım yükleyebilir veya işten ayrılan bir çalışan paylaşılan hesabın şifresini hala biliyor olabilir. Hesaplar paylaşıldığında hesap verebilirlik kaybolur (kimin ne yaptığını bilemezsiniz). Önleme: En az ayrıcalık ilkesini uygulayın. Herkes için ayrı hesaplar oluşturun ve onlara yalnızca ihtiyaç duydukları erişimi verin. Dosyalar ve sistemler için rol tabanlı izinler kullanın. Evet, başlangıçta biraz daha fazla kurulum gerektirir, ancak modern sistemler kullanıcıları yönetmeyi oldukça kolaylaştırır. Ayrıca, erişimin sistematik olarak verilmesi ve iptal edilmesi için net bir işe alım/işten ayrılma kontrol listesi oluşturun. Yönetici görevleri için ayrı bir yönetici hesabı oluşturun – yönetici kullanıcısı olarak internette gezinmeyin veya e-posta okumayın. Bu şekilde, bir kullanıcı kandırılsa bile, hasar kullanıcı düzeyinde sınırlı kalabilir.

Güvenlik Uyarılarını veya En İyi Uygulamaları Göz Ardı Etmek: İnsanlar bazen tarayıcı uyarılarını ("Bu sitenin sertifikası güvenilir değil") göz ardı eder veya güvenlik özelliklerini devre dışı bırakır, çünkü bunlar can sıkıcı görünür ("bu uygulamanın çalışması için güvenlik duvarını kapatayım"). Bu, saldırılara kapı açabilir. Başka bir örnek: alışkanlıktan dolayı eski, güvenli olmayan protokoller (SFTP yerine FTP gibi) kullanmak. Önleme: Uyarıların neden var olduğunu açıklayın. Örneğin, sertifika uyarısının ne anlama geldiğini ve bunun sahte bir site veya dinlemeyi işaret edebileceğini açıklayın. Bir güvenlik önlemi bir şeyi engellediğinde, personel bunu devre dışı bırakmak yerine uygun çözümler (bilinen güvenli bir iç site ise istisna eklemek gibi) istemesini sağlayacak bir ortam yaratın. Rehberlik sağlayın: Antivirüs bir dosyayı işaretlerse, sinirlenip onu beyaz listeye eklemeyin; gerçekten güvenli olup olmadığını analiz etmek için BT departmanına başvurun. Basit iç SSS'ler yazın: "Bir güvenlik uyarısı görürseniz, X'i yapın." Ayrıca, yeni araçlar kurarken, personel güvenli olmayan geçici çözümler kullanmaya yönelmemesi için bunu baştan itibaren güvenli bir şekilde yapın.

Olay Müdahale Planının Olmaması: Birçok CSO, bir olay sırasında ne yapacağını bilemez ve kimi arayacağını veya hangi adımları atacağını bilemez, bu da değerli zamanın boşa harcanmasına neden olur. Hata: Önceden tanımlanmış olay planı veya tatbikatların olmaması. Önleme: Temel bir olay müdahale planı geliştirin (Bölüm 5'te yapıldığı gibi) ve herkesin bu

planın temellerini bildiğinden emin olun. Bu plan tek sayfalık bir belge olabilir: "Garip bir şey olursa: internet bağlantısını kesin, bu kişiyi arayın, vb." Ayrıca, en azından bir masaüstü tatbikatı yapın: "Ya fidye yazılımı bize saldırırsa, ne yaparız?" gibi varsayımsal bir senaryoyu tartışarak eksiklikleri tespit edin. Bir planın olması, yanlış sistemi kapatmak veya paniğe kapılmak gibi gerçek krizler sırasında hataları azaltır.

Bu yaygın hataların farkında olarak, bir CSO bu tuzaklara düşmemek için proaktif önlemler alabilir. Genellikle davranış veya politikadaki küçük değişiklikler büyük fark yaratır – güncellemeleri uygulama veya tıklamadan önce iki kez kontrol etme alışkanlığı gibi. **"Herkesin güvenlik konusunda paydaşı olduğu"** felsefesini teşvik edin**,** böylece hatalar kolektif özenle yakalanabilir veya önlenebilir (örneğin, şüpheli e-postaların meslektaşlar tarafından incelenmesi – "Hey meslektaşım, bu sana meşru geliyor mu?" hatayı önleyebilir).

Özetle: zayıf şifreleri güçlendirin, tıklamadan önce düşünün, her şeyi güncel tutun, özenle yedekleyin, ayrıcalıkları sınırlayın, uyarılara kulak verin ve en kötüsüne hazırlıklı olun. Bu yaygın hatalardan kaçınmak, oldukça düşük bir maliyetle güvenlik durumunuzu önemli ölçüde iyileştirecektir.

Kendi Güvenliğinizi Test Edin: Basit Alıştırmalar

Güvenlik hakkında okumak bir şeydir, bunu uygulamaya koymak başka bir şeydir. İşte, güvenlik hazırlığınızı ölçmek ve iyileştirmek için siz (ve ekibiniz) yapabileceğiniz birkaç basit öz değerlendirme ve alıştırma. Bunları "güvenlik tatbikatları" veya kontroller olarak düşünün:

Oltalama Tatbikatı: Ekibinizin farkındalığını test etmek için zararsız bir "sahte oltalama e-postası" hazırlayın. Örneğin, kuruluşunuzun adresinden olmayan bir e-posta gönderin, ancak ekranda kuruluşunuzun adını kullanın, konu başlığını "Acil güncelleme gerekli" olarak belirleyin ve bir Google Form bağlantısı ekleyin (bu formda sadece "Tebrikler, bu bir testti!" yazıyor). Kimlerin tıkladığını veya bilgi gönderdiğini görün. Amaç eğitmektir, tuzağa düşürmek değil: sonrasında bunu açıklayın ve bunun phishing olduğunu gösteren ipuçlarını tartışın (belki adresin hafif bir farkı, acil tonu vb.). Çok az kişi tuzağa düşerse, harika – bazıları düşerse, bunu nazik bir eğitim fırsatı olarak kullanın. Alternatif olarak, Google'ın phishing testi veya Phishing Simülasyon araçları (bazı AV paketlerinde bu özellik vardır) gibi ücretsiz araçları kontrollü bir şekilde kullanın.

Parola Gücü Kontrolü: Bazı parolalara bakın (kimseye parolasını göstermesini istemeden, yaygın kalıpları simüle edebilirsiniz). Parola gücü ölçer (çoğu çevrimiçi, örneğin Passwordmeter.com) kullanarak tipik parolaları önerilen parolalarla karşılaştırın. Daha da iyisi, bir şifre yöneticisi kullanıyorsanız, zayıf/tekrar kullanılan şifreleri rapor edip etmediğini kontrol edin – çoğunda güvenlik denetimi özelliği vardır. Bir alıştırma olarak, herkesten dört rastgele kelimeden oluşan güçlü bir şifre cümlesi oluşturmasını isteyin (örneğin, "apple caravan tiger dance") ve bunun gücünü "Winter2020!" gibi bir şifre ile karşılaştırın – sonuçlar genellikle şifre cümlesinin daha güçlü ve hatırlanması daha kolay olduğunu gösterir. Bu, iyi şifre oluşturma alışkanlıklarını pekiştirir.

Yedekleme Geri Yükleme Tatbikatı: Yedeklemenizi test edin. Bir senaryo simüle edin: "X dosyasını kaybettik, ne yapmalıyız?" Aslında, yedekleme konumunuza gidin, dosyayı alın ve sağlam olduğundan emin olmak için açın. Veya bir tarih seçin ve her şeyi o tarihteki haline geri döndürmeniz gerektiğini varsayın – o tarihin yedeklemesini alabilir misiniz? Temsili bir veri kümesini geri yüklemek ne kadar sürer? Bu, yedeklemeleri doğrulamakla kalmaz, aynı zamanda yedeklemeler için talimatların/kimlik bilgilerinin hazır olup olmadığını ortaya çıkararak sizi

gerçek olaylara hazırlar. Belki de başka birine (her zamanki BT personeli değil) yalnızca belgelenmiş adımları kullanarak geri yüklemeyi denemesini isteyerek sürecin yeterince açık olup olmadığını kontrol edebilirsiniz.

Cihaz Güvenliği Denetimi: Ofis bilgisayarlarınızı ve telefonlarınızı hızlı bir şekilde denetleyin (tabii ki izin alarak). Kontrol edin: Tüm işletim sistemleri güncellenmiş mi (Windows Update veya eşdeğerini açın, son güncelleme tarihine bakın)? Antivirüs çalışıyor ve güncellenmiş mi? Güvenlik duvarları açık mı? Hala varsayılan şifreleri kullanan cihaz var mı (örneğin, ofis yönlendiricisine giriş yapın ve varsayılan kimlik bilgilerinin çalışıp çalışmadığını kontrol edin – çalışıyorsa, bunu değiştirmek için büyük bir işaret)? Ekranlar boşta kaldığında otomatik olarak kilitleniyor mu? Basit bir kontrol listesi hazırlayabilir ve her bilgisayara puan verebilirsiniz. Ardından, bulunan sorunları giderin ve çoğu şey varsayılan olarak güvenliyse bunu kutlayın (bu, yapılandırma uygulamalarınızı doğrular).

E-posta Sahtekarlığı Testi: İlginç bir alıştırma: e-postaları sahtecilik yapmanın ne kadar kolay olduğunu göstererek şüpheciliği artırın. Kontrollü bir ortam kullanarak (kendi özel adresinizden e-posta göndermenize izin veren bir hizmet veya Gmail'de "Gönderen" adını değiştirmenize izin veren bir hizmet gibi), kendinize örneğin "" adresinden gönderilmiş gibi görünen bir e-posta gönderin (ancak bu e-posta başka bir etki alanından gönderilmiştir). Personele, ilk bakışta e-postanın ikna edici göründüğünü, ancak e-posta başlıklarının veya gerçek adresin gerçeği gösterdiğini gösterin. Bu alıştırma genellikle insanları şok eder ve bundan sonra e-posta adreslerini daha dikkatli kontrol ederler.

İzinlerin Temizlenmesi: Paylaşılan bir klasörü veya Google Drive'ı alın ve kimin erişimi olduğunu denetleyin. Eski gönüllülerin hala erişimi olduğunu veya bazı dosyaların yanlışlıkla herkese açık bağlantı olarak paylaşıldığını keşfedebilirsiniz. "Mini alıştırma" olarak, gereksiz erişimleri iptal edin ve bunu belgelendirin. Bu, erişim hakları için bahar temizliği gibidir. Bu, bunu periyodik olarak yapmanız gerektiğini hatırlatır.

Olay Rol Oyunu: Bir senaryo seçin (örneğin, "kafeden dizüstü bilgisayar çalındı" veya "sunucuda fidye yazılımı var") ve nasıl tepki vereceğinizi sözlü olarak anlatın (kimi arayacağınızı, hangi adımları atacağınızı). Personel ile rol oyunu: Birisi panikleyen kullanıcıyı, diğeri BT müdahale ekibini oynar vb. Bu düşük profilli prova, eksiklikleri ortaya çıkarabilir ("E-posta ele

geçirildiğinde hesapları dondurmak için bankanın numarasını elimizde yok" veya "LastPass'e erişilemediğinde web sitemizin yönetici şifresini ezbere bilmediğimizi fark ettik"). Gerçek bir kriz sırasında öğrenmektense şimdi öğrenmek daha iyidir.

Her tatbikat basit ve zaman alıcı olmamakla birlikte çok bilgilendirici olmalıdır. Bunu siber tehditler için yangın tatbikatı gibi düşünün – düşük riskli bir ortamda tatbikat yaparsınız, böylece gerçek bir acil durumda ne yapmanız gerektiğini bilirsiniz ve daha önce benzer bir şey yaptığınız için daha az endişeli hissedersiniz.

Her alıştırmadan sonra, sonuçları suçlamadan açıkça tartışın. Bir şeyler ters giderse (örneğin, ekibin yarısı kimlik avı testinde başarısız olursa), bunu kolektif bir öğrenme olarak değerlendirin: belki de kimlik avı e-postası gerçekten çok kurnazdı – artık herkes bir dahaki sefere bu tuzağa karşı dikkatli olacağını biliyor. Bir alıştırma ciddi bir zayıflığı ortaya çıkarırsa, bunu ortaya çıkardığı için sürece teşekkür edin ve düzeltmeye kararlı olun.

Bu tür egzersizleri düzenli olarak yapmak, insanların zihninde güvenliği canlı tutar ve sürekli iyileştirme kültürünü teşvik eder. Güvenliği anlaşılır hale getirir (çünkü sadece politikaları dinlemekle kalmaz, aktif olarak bir şeyler yaparsınız). Hatta bir bakıma eğlenceli bile olabilir – bazı kuruluşlar bunu oyunlaştırarak, phishing'i fark edenlere veya denetimlerde en az sorun yaşayanlara küçük ödüller verir.

Dijital Güvenliği Günlük Rutine Entegre Etmek

Nihai hedef, iyi güvenlik uygulamalarının ikinci bir doğa haline gelmesidir – sizin ve kuruluşunuzun işleyişinin normal bir parçası haline gelmesidir. CSO'da dijital güvenliği günlük hayata sorunsuz bir şekilde entegre etmek için ipuçları:

Güne Güvenliği Düşünerek Başlayın: Basit sabah alışkanlıklarını teşvik edin. Örneğin, bilgisayarınızı başlattığınızda, işe koyulmadan önce güncellemeleri yüklemesine izin verin ("ertele" düğmesine basmak yerine, güncelleme yapılırken kahvenizi alın). Veya güvenlik bildirimlerini ("Windows Defender: sorun bulunamadı" veya yazılım güncelleme uyarısı gibi) kontrol edin ve bunları erken aşamada ele alın. Bu, görev çubuğunuzdaki küçük kalkanları ve ünlem işaretlerini görmezden gelmek yerine, güvenli bir ortamda çalışmaya başlamanızı sağlar.

Her Gün Şifre Yöneticisi: Şifre yöneticisini kullanmayı oturum açma işlemlerinin rutin bir parçası haline getirin. Düzgün bir şekilde ayarlandığında, kimlik bilgilerini otomatik olarak

doldurabilir, böylece personel bunun avantajını hızlı bir şekilde görebilir (daha hızlı oturum açma, şifre sıfırlama zahmeti yok) ve bu, onların oturum açma şekli haline gelir. Günlük rutin, "şifreleri hatırlamak veya yazmak"tan "güçlü bir parolayla yöneticinin kilidini bir kez açmak ve ardından tıklayarak her yere oturum açmak"a dönüşür. Zamanla, şifre yöneticisi olmadan hayatı hayal edemeyecek hale gelirler. Bazı yöneticiler, zayıf şifreleri güncellemeyi de isterler. Belki her Cuma birkaç dakika ayırarak işaretlenen bir şifreyi güncelleyebilirsiniz. Yavaş yavaş, tüm hesaplar daha güçlü şifrelere sahip olur.

Ekip Hatırlatmaları ve Kültürü: Düzenli ekip toplantılarına veya şirket içi haber bültenlerine güvenlikle ilgili bilgiler ekleyin. Örneğin, haftalık toplantıda gündem maddelerinden biri, bir dakikalık güvenlik ipucu veya haber olabilir (ör. "Bilginiz olsun, şu anda WhatsApp'ta bir dolandırıcılık dolaşıyor; doğrulama kodlarını paylaşmamayı unutmayın"). Bu, konuyu normalleştirir. 'ın hakim olması gerekmez, sadece rutin bir kontrol yeterlidir. Bazı CSO'lar duvara veya Slack kanalına "Ayın Güvenlik İpucu" posteri asarak farkındalığı pasif olarak günlük görüş alanında tutar.

Ekranları Kilitleyin ve Masaları Temizleyin: Bir dakikalığına bile olsa, bilgisayarınızdan uzaklaştığınızda ekranı kilitlemeyi (Windows'ta Win+L, Mac'te Ctrl+Cmd+Q) bir alışkanlık haline getirin. Herkes bunu yaparsa, paranoyakça değil, normal bir şey olarak algılanır. Aynı şey, hassas belgeleri veya USB sürücüleri ortalıkta bırakmamak için de geçerlidir (eski "masayı temiz tutma politikası"). Bunu bir şeye bağlarsanız rutin olarak yapmak daha kolay olur: örneğin, günün sonunda, son olarak: dosyaları yedekleyin, tüm dolapları kilitleyin, sistemlerden çıkış yaptığınızı kontrol edin – böylece hazır olduğunuzu bilirsiniz. Belki de ofisi güvenli bir şekilde kapatmak için (dijital ve fiziksel) personel tarafından her gün takip edilecek ve ikinci bir doğa haline gelene kadar uygulanacak basılı bir kontrol listesi oluşturabilirsiniz.

Güvenliği İş Akışlarına Entegre Edin: Hangi araçları kullanırsanız kullanın, varsayılan olarak güvenlik özelliklerini kullanın. Örnek: Bir dosyayı bulut üzerinden paylaşıyorsanız, bağlantı yerine rutin olarak "belirli kişilerle paylaş" seçeneğini kullanın. E-postalarını yazmak belki 10 saniye daha fazla zaman alır, ancak bu, insanların paylaşım yapmasının tek yolu haline gelirse, bu normal bir durumdur. Veya proje kapanışının bir parçası olarak periyodik izin incelemeleri planlayın: örneğin, bir proje bittiğinde, kapanış kontrol listesinin bir parçası "proje

klasörlerinden tüm harici erişimi inceleyin ve kaldırın"dır. Bu şekilde, güvenlik bakımı proje yönetimi yaşam döngüsüne dahil edilir.

Salı günü (veya seçilen bir gün) güncelleme: Birçok kuruluş, bakım görevlerini ne zaman yapacaklarını planlar. Belki de Salı sabahları, BT/atanmış kişi tüm cihazlarda işletim sistemi ve uygulamaların güncellendiğinden emin olur veya her kullanıcı haftalık olarak telefon güncellemelerini kontrol eder. Beklenen ve planlanmışsa, bu bir kesinti olarak değil, rutin bir işlem olarak görülür (her Pazartesi bitkileri sulamak gibi, sistemleri güncelleriz). Bulut hizmetleri kendilerini günceller, ancak belki de aylık olarak yönetici konsolunu herhangi bir uyarı veya etkinleştirilecek yeni güvenlik özelliği olup olmadığını kontrol etmek gerekir (sağlayıcılar sık sık yeni güvenlik ayarları ekler; bunları düzenli olarak entegre etmek için zaman ayırmak iyidir).

Sürekli Öğrenme: Personeli ara sıra kısa çevrimiçi kurslara veya testlere katılmaya teşvik edin. Belki herkes her üç ayda bir çevrimiçi güvenlik kursunun bir modülünü tamamlar (bazıları etkileşimli ve kısadır). Bunun için örneğin bir saatlik çalışma süresi ayırırsanız, bu organizasyonun taahhüdünü gösterir. Bu, bilginin güncel kalmasını sağlar ve güvenliğin isteğe bağlı bir görev değil, mesleki gelişimin bir parçası olduğunu gösterir.

Örnek Olun: Liderlik, güvenlik davranışlarını açıkça örneklemelidir. Müdür her zaman 2FA jetonu kullanır ve "Bunun ne kadar güvenli ve kolay olduğunu seviyorum" diye övünürse, diğerleri de onu takip eder. Liderlik dolandırıcılıklara kanarsa veya zayıf uygulamalar kullanırsa, diğerleri bilinçaltında bunun normal olduğunu düşünür. Bu nedenle, bunu en üst düzeyde entegre edin. Örneğin, bir çalışan hassas verileri kişisel e-postayla gönderirse, yönetici bunu nazikçe düzeltmelidir: "Lütfen resmi hesabımızı kullanın veya dosyayı şifreleyin, burada işler böyle yürür." Zamanla, grup normları değişir.

Otomasyonu Kullanın: Günlük insan çabası olmadan güvenlik sağlamak için bir yol otomasyondur. Örneğin, tüm bilgisayarları beş dakika kullanılmadığında otomatik olarak kilitlenecek şekilde ayarlayın. Böylece personel bu düzene alışır (ve belki de beş dakikanın çok kısa olduğunu düşünerek, cümlenin ortasında kilitlenmek yerine, odadan çıkarken proaktif olarak kilitler). Otomatik güncellemeleri, otomatik taramaları kullanın (haftalık öğle molası için tam AV taramaları planlayın). Bu, hafızaya veya motivasyona olan bağımlılığı azaltır; sistem rutini destekler. Benzer şekilde, varsa tek oturum açma (SSO) çözümü kullanmak güvenliği

entegre edebilir (tek bir güçlü oturum açma, birden fazla uygulamanın kilidini açar, böylece kullanıcılar her zaman zayıf yöntemlerle uğraşmak yerine bu tek sağlam yöntemle oturum açarlar).

Ödüllendirin ve pekiştirin: Olumlu pekiştirme alışkanlıkların oluşmasına yardımcı olur. İyi güvenlik davranışları için küçük ödüller veya takdirler düşünün. Örnek: Bir kimlik avı e-postasını bildiren veya güvenliği artırmak için bir fikir bulan kişiye "Ayın Güvenlik Yıldızı" ödülü verin. Sadece kamuya açık bir övgü bile, "Olağandışı e-postayı fark ettiği için Alice'e teşekkürler – detaylara çok dikkat ediyor!" herkesi dikkatli olmaya teşvik eder. Bu, güvenlik bilincinin sadece beklenen değil, takdir edilen bir şey olduğunu gösterir.

Bu uygulamaları günlük iş akışlarına dahil ederek, dijital güvenlik sporadik bir proje olmaktan çıkar ve organizasyon kültürünün bir parçası haline gelir. Yeni çalışanlar, "burada işler böyle yürür" diye ilk günden itibaren bunu benimserler. Bu, güvenliği gizemli bir şey olmaktan çıkarır – güvenlik, özel bir teknik konu değil, ofis kapısını kilitlemek veya kimlik kartı takmak gibi herkesin rutin iş görevlerinin bir parçasıdır. Zamanla, bu küçük günlük alışkanlıklar neredeyse görünmez bir şekilde güçlü bir kale oluşturur. Rutin ve kolay olduğu için ne kadar güvenli hale geldiğinizi fark etmeyebilirsiniz bile. Hedef budur: güvenlik bir yük olarak değil, her gün daha akıllı ve daha güvenli çalışmanın entegre bir parçası olarak.

Bölüm Özeti

Bu bölüm, CSO'ların dijital güvenliği artırmak için işbirliğini ve dış kaynakları nasıl kullanabileceklerini araştırıyor. Hiçbir kuruluşun siber tehditlerle tek başına yüzleşmediğini vurgulayan bölüm, bilgi ve ağların paylaşılmasını savunuy . Bölüm, bütçe kısıtlamalarını ele almak için CSO'lar için Google Workspace veya dijital güvenlik yardım hatları gibi ücretsiz veya topluluk odaklı araçları öne çıkarıyor. Tehdit istihbaratı ve başarı hikayelerini paylaşmak için güvenlik forumlarına ve koalisyonlarına katılmayı teşvik ediyor. Örnekler arasında, sunucuların güvenliğini sağlamak için teknoloji gönüllüleriyle ortaklık kuran veya ulusal CERT'lerden ücretsiz kaynaklara erişen CSO'lar yer almaktadır. Bu bölümde ayrıca, daha güvenli bir dijital ekosistem savunmak için hükümet, akademi ve teknoloji endüstrileriyle işbirliği yapılması teşvik edilmektedir. Akranlarıyla bağlantı kurarak CSO'lar savunmalarını güçlendirmektedirler. Bu, paylaşılan uyarıların bir kimlik avı kampanyasını durdurduğu bir vakada görüldüğü gibi. Güvenlik

bültenlerine abone olmak gibi bu bölümdeki pratik rehberlik, küçük CSO'ların erişilebilirliğini sağlar. Müfredatın eğitmen eğitimi modeliyle uyumlu olup, dayanıklılık ve kolektif savunma konusunda topluluk odaklı bir yaklaşımı teşvik eder.

3. EĞİTİM MODÜLLERİ

Giriş ve Bağlam

Günümüzün dijital çağında, sivil toplum kuruluşları (STK'lar) ve sivil toplum örgütleri (STÖ'ler) misyonlarını yerine getirmek için giderek daha fazla dijital araçlara güvenmektedir. Ne yazık ki, bu durum onları siber tehditler için cazip hedefler haline getirmektedir. Aslında, 2025 yılında STK'ların %50'si siber saldırıların hedefi olmuştur ve kar amacı gütmeyen kuruluşlar artık ulus devletlerin siber saldırılarının en çok hedef aldığı ikinci sektör konumundadır (tüm vakaların %31'i). Bu riske rağmen, birçok STK hazırlıksızdır: Beş STK'dan dördü herhangi bir siber güvenlik planına sahip değildir ve %70'i siber saldırılara yanıt vermek için gerekli bilgi veya becerilere sahip olmadığını düşünmektedir. Bu istatistikler, kar amacı gütmeyen sektörde dijital güvenlik kapasitesinin güçlendirilmesinin acil bir ihtiyaç olduğunu vurgulamaktadır.

Dijital güvenlik sadece bir BT sorunu değildir; bir kuruluşun topluma hizmet etme yeteneğini de etkiler. Tek bir güvenlik ihlali veya fidye yazılımı saldırısı, kritik hizmetleri aksatabilir, hassas yararlanıcı verilerini tehlikeye atabilir ve kamu güvenini zedeleyebilir. Sınırlı kaynaklarla çalışan STK'lar için, bu tür olaylardan kurtulmak, değerli fonları ve zamanı asıl görevlerinden uzaklaştırabilir. Bu nedenle, sivil toplumun dijital güvenlik altyapısını güçlendirmek, bu kuruluşların güvenli ve etkili bir şekilde çalışabilmesini sağlamak için çok önemlidir.

Müfredatın Amacı

Projemizin temel amaçlarından biri, kapsamlı bir "Sivil Toplum için Dijital Güvenlik Müfredatı" geliştirmektir. Amaç, STK'lara ve sivil toplum gruplarına dijital güvenlik altyapılarını iyileştirmek için gerekli bilgi ve becerileri kazandıracak yapılandırılmış bir eğitim programı oluşturmaktır. Altyapı derken, güvenli teknolojiler ve uygulamalardan politikalara ve personel kapasitelerine kadar bir kuruluşun dijital güvenlik duruşunun tüm yelpazesini kastediyoruz. Bu müfredat, STK'ların verilerini, sistemlerini ve iletişimlerini nasıl koruyacaklarını öğrenmelerine yardımcı olacak ve böylece siber tehditlere karşı savunmasızlıklarını azaltacak pratik bir araç seti olarak tasarlanmıştır.

Bu hedef, Avrupa genelinde dijital güvenliği artırmak olan projemizin daha geniş hedefiyle uyumludur. Sivil toplum düzeyinde kapasite geliştirerek, kıtasal ölçekte siber güvenliği güçlendirmek için aşağıdan yukarıya bir yaklaşım benimsiyoruz. İyi eğitilmiş STK'lar sadece kendi faaliyetlerini korumakla kalmayacak, aynı zamanda hizmet ettikleri topluluklar için daha güvenli

bir dijital ortama katkıda bulunacaklar. Esasen, müfredat sivil toplum aracılığıyl 'da siber güvenliği güçlendirmek için stratejik bir adım olacak ve daha küçük kuruluşların bile güçlü dijital savunma uygulamalarını sürdürebilmelerini sağlayacaktır.

Bu müfredatın sonunda katılımcılar şunları yapabileceklerdir:

- *Sivil toplum kuruluşlarına yönelik başlıca dijital güvenlik tehditlerini belirlemek ve temel koruma önlemlerini açıklamak.*
- *Kuruluşlarının dijital varlıklarına ilişkin temel bir risk değerlendirmesi yapmak ve basit bir siber güvenlik planı taslağı hazırlamak.*
- *Cihazlar, ağlar ve iletişimde temel güvenlik önlemlerini uygulamak (ör. güçlü şifreler, güvenlik duvarları, güvenli Wi-Fi).*
- *Veri koruma ilkelerini uygulamak ve ilgili veri gizliliği düzenlemelerine (ör. GDPR) uymak.*
- *Kuruluşun itibarını ve bilgilerini korumak için güvenli sosyal medya ve çevrimiçi araçlar kullanın.*
- *Temel BT güvenlik politikaları (şifre, yedekleme ve kabul edilebilir kullanım politikaları gibi) geliştirin ve uygulayın ve temel bir olay müdahale prosedürü yürütün.*

Müfredat Genel Bakış

"Sivil Toplum için Dijital Güvenlik Müfredatı", sivil toplum kuruluşları ve STK'ların dijital güvenlik altyapılarını güçlendirmek için izledikleri stratejik bir araç seti olarak tasarlanmış yapılandırılmış bir öğrenim programıdır. Müfredat, proje ortaklarının kendi ülkelerinde uyarlayıp uygulayabilecekleri modüler bir eğitim paketi olarak sunulmaktadır.

Müfredatın temel özellikleri şunlardır:

- **Kapsamlı İçerik:**

  Müfredat, temel seviyeden ileri seviyeye kadar konuları kapsar ve önceden bilgisi sınırlı olan kuruluşların dijital güvenlik kapasitelerini adım adım geliştirmelerini sağlar.
- **Pratik Odaklılık:**

  Müfredat, teorik yaklaşımlardan ziyade uygulamalı becerileri ve gerçek hayattaki senaryoları vurgular. Modüller, kimlik avı girişimlerine yanıt verme, çevrimiçi toplantıları

güvenli hale getirme ve örgütsel verileri koruma gibi pratik durumları ele alır. Her modül , STK'ların günlük faaliyetlerinde doğrudan uygulayabilecekleri eyleme geçirilebilir kılavuzlar, araçlar ve kontrol listeleri sağlar.

- **Özelleştirme ve Yerel Alaka:**
  Müfredat, ulusal bağlamlara uyarlanabilir şekilde tasarlanmıştır. Proje ortakları, örnekleri, vaka çalışmalarını ve seçilen içeriği yerel düzenlemelere, ihtiyaçlara ve operasyonel gerçeklere göre uyarlar, ancak temel ilkeler ve öğrenme hedefleri tüm ortak ülkelerde tutarlı kalır.
- **Biçim ve Sunum:**
  Eğitim materyalleri arasında slayt sunumları, kısa açıklayıcı metinler ve alıştırmalar ve testler gibi etkileşimli bileşenler bulunmaktadır. Müfredat, farklı büyüklükteki ve teknik kapasitedeki kuruluşların erişebilirliğini sağlamak için çevrimiçi formatlar ve/veya yüz yüze atölye çalışmaları aracılığıyla sunulmaktadır. Eğitici eğitimi yaklaşımı teşvik edilerek, proje ortaklarının ve yerel uzmanların eğitimleri kendi ulusal dillerinde sunmaları sağlanmaktadır.
- **Sonuç Odaklı Yapı:**
  Müfredatı tamamlayan katılımcılar, kuruluşlarının dijital risklerini değerlendirebilir, temel güvenlik önlemlerini uygulayabilir, iç dijital güvenlik politikaları geliştirebilir ve yaygın siber tehditlere güvenle yanıt verebilir. Müfredat, kuruluşların dijital güvenlik hazırlık düzeylerini değerlendirmelerine olanak tanıyan öz değerlendirme araçları ve göstergeler içerir.

Sivil Toplum Kuruluşları Neden Dijital Güvenlik Kapasitesine İhtiyaç Duyar?

- ***Yüksek Risk, Düşük Kaynaklar***: STK'lar genellikle hassas verilerle (örneğin, yararlanıcıların ve bağışçıların kişisel bilgileri) çalışır, ancak siber güvenlik önlemlerini kısıtlayan sınırlı bütçelerle faaliyet gösterir. Saldırganlar, birçok STK'nın "siber açıdan fakir ama hedef açısından zengin" olduğunu bilir – veri ve fon açısından zengin, ancak savunma açısından fakir.
- ***Büyüyen Tehdit Ortamı***: Dijitalleşmenin artması (pandemi ile hızlanan) ve üçüncü taraf çevrimiçi hizmetlere bağımlılığın artmasıyla, CSO'ların saldırı yüzeyi büyümüştür. Sivil

topluma yönelik kimlik avı, kötü amaçlı yazılım, fidye yazılımı ve DDoS saldırıları artmaktadır.

- ***Farkındalık ve Eğitim Eksikliği***: Birçok STK çalışanı ve lideri resmi siber güvenlik eğitimi almamıştır. Kar amacı gütmeyen kuruluşların yaklaşık %90'ı çalışanlarına düzenli olarak siber hijyen eğitimi vermemektedir. Bu eksiklik, saldırganların istismar ettiği güvensiz uygulamalara (zayıf şifreler veya kimlik avı dolandırıcılıklarına kanmak gibi) yol açmaktadır.
- ***Resmi Politikaların Olmaması***: Rehberlik olmadan, çok az sayıda STK güvenlik politikaları veya olay müdahale planları oluşturmaktadır ve bu da olaylar sırasında yönsüz kalmalarına neden olmaktadır. STK'ların yaklaşık %80'i siber güvenlik politikası/planı uygulamamaktadır. Bir müfredat, kuruluşların bu iç politikaları ve müdahale stratejilerini oluşturmalarına yardımcı olabilir.
- ***Yasal Baskı***: Dünyanın en kapsamlı veri koruma yasası olan AB Genel Veri Koruma Yönetmeliği (GDPR) gibi veri koruma yasaları, kuruluşların kişisel verileri korumalarını gerektirir. CSO'lar, şirketler gibi bu yasalara uymak zorundadır, aksi takdirde yasal ve itibar açısından risklerle karşı karşıya kalırlar. Bu tür düzenlemeler hakkında bilgi sahibi olmak, dijital güvenlik kapasitesinin önemli bir parçasıdır.
- Bu zorluklar, özel bir müfredatın neden gerekli olduğunu ortaya koymaktadır. Bu müfredat, bilgi eksikliğini giderecek, güvenlik kültürünü teşvik edecek ve CSO'lara kendi siber güvenlik planlarını, politikalarını ve korumalarını geliştirmeleri için bir yol haritası sunacaktır.

Hedef Kitle ve Paydaşlar

Müfredatın birincil hedef grubu, aşağıdaki profilleri içeren sivil toplum kuruluşları (STK'lar) ve STK'lardan oluşmaktadır:

- ***CSO Liderlik ve Yönetim Kadrosu:***

  Dijital güvenlik riskleri ve kurumsal sorumluluklar hakkında net bir anlayışa sahip olması gereken, organizasyonel strateji, risk yönetimi ve kaynak tahsisinden sorumlu kişiler.

- ***BT Personeli veya Teknik Odak Noktaları:***

  Teknik güvenlik önlemlerinin uygulanmasından ve kuruluş içinde güvenli dijital uygulamaların desteklenmesinden sorumlu personel.
- ***Program ve Operasyon Personeli:***

  Günlük veri akışlarını, yararlanıcı bilgilerini, mali kayıtları ve dijital iletişimi yöneten personel, güvenli dijital uygulamalar konusunda güçlü bir farkındalığa sahip olmalıdır.
- ***Gönüllüler ve Saha Personeli:***

  Saha ortamında kurumsal cihazları kullanan veya hassas bilgileri işleyen ve güvenli dijital davranış konusunda rehberliğe ihtiyaç duyan kişiler.
- ***Ortak Ağlar ve Topluluk Kuruluşları:***

  Sivil toplum kuruluşlarıyla işbirliği veya koalisyon halinde çalışan ve dijital güvenlik uygulamalarının kurumsal ağlara yayılmasını sağlayan kuruluşlar.

Müfredatın geliştirilmesi ve uygulanmasında yer alan paydaşlar arasında, katılımcı ülkelerden proje ortağı kuruluşlar ile siber güvenlik ve dijital güvenlik uzmanları bulunmaktadır. Uzmanlar ve kurumların katkıları, müfredatın dijital güvenlik ve veri korumada uluslararası düzeyde tanınan en iyi uygulamalarla uyumlu olmasını sağlamaktadır.

Müfredattaki Temel Modüller ve Konular

Müfredat, her biri dijital güvenliğin kritik bir yönüne odaklanan birkaç modülden oluşmaktadır. Aşağıda, dahil etmeyi planladığımız temel konuların bir özeti bulunmaktadır:

1. Dijital Güvenlik Temelleri: Tehdit Ortamını ve Temel Hijyen Kurallarını Anlamak – Dijital güvenliğin sivil toplum kuruluşları için neden önemli olduğunu anlatır. Tehdit türlerini (kötü amaçlı yazılım, kimlik avı, hackleme, DDoS vb.), tehdit aktörlerini (suçlular, sivil toplumu hedef alan düşman hükümetler) ve temel en iyi uygulamaları kapsar. Güvenlik bilinci ve temel alışkanlıklar (güçlü şifreler, iki faktörlü kimlik doğrulama, düzenli yazılım güncellemeleri, şüpheli e-postalardan kaçınma) oluşturmaya vurgu yapar.

2. Risk Değerlendirmesi ve Planlama: Organizasyonel Riskleri Değerlendirme ve Güvenlik Planı Oluşturma – CSO'lara dijital varlıklarını ve güvenlik açıklarını belirleme konusunda rehberlik eder. Basit bir risk değerlendirmesi nasıl yapılır (başkaları saldırı yapabilecek neye sahibiz? Bunu

nasıl yapabilirler? Sonuçları ne olabilir?). Bu modül, kuruluşların siber güvenlik planlarını hazırlamalarına veya iyileştirmelerine yardımcı olacaktır (şu anda %80'i böyle bir plana sahip değildir) – veri işleme, erişim kontrolü ve olay müdahale prosedürü politikaları dahil.

3. Cihazları ve Altyapıyı Güvenli Hale Getirme: Bilgisayarları, Ağları ve Web Sitelerini Koruma – CSO'ların kullandığı teknolojinin güvenliğini sağlamaya odaklanır. Konular arasında cihaz güvenliği (antivirüs, cihazların şifrelenmesi, güvenli cihaz yapılandırması), Wi-Fi ve ağların güvenli kullanımı, uygun durumlarda VPN'lerin ( ) kullanımı ve web sitelerinin güvenliği (web barındırma güvenliğinin temelleri, yedeklemeler, HTTPS kullanımı, tahrifat veya DDoS'ye karşı koruma) yer alır. Gerçek saldırı örnekleri (örneğin, bir CSO'yu aylarca çevrimdışı bırakan bir web sitesi tahrifatı vakası) bu önlemlerin önemini gösterecektir.

4. Güvenli İletişim ve İşbirliği: Güvenli E-posta, Mesajlaşma ve Uzaktan Çalışma – Hem şirket içinde hem de dış paydaşlarla güvenli iletişim kurmayı öğretir. E-posta güvenliği (oltalamayı tanıma, şifreli e-posta veya güvenli e-posta sağlayıcıları kullanma), mesajlaşma uygulamaları (Signal gibi güvenli uygulamaları seçme, uçtan uca şifrelemeyi etkinleştirme) ve güvenli dosya paylaşımını kapsar. Ayrıca uzaktan çalışmanın zorluklarını da ele alır: güvenli bağlantılar kullanma, video konferansları koruma ve evden veya hareket halindeyken hesapları/kimlik bilgilerini yönetme.

5. Veri Koruma ve Gizlilik Uyumluluğu: Verileri Koruma ve Yasal Yükümlülükleri Anlama – CSO'ların topladığı hassas verilerin (yararlanıcı verileri, bağışçı bilgileri vb.) korunmasını vurgular. Veri koruma ilkelerini tanıtır: veri minimizasyonu, depolanan ve aktarılan verilerin şifrelenmesi, güvenli depolama/yedekleme ve uygun veri imhası. Avrupa'nın önde gelen veri koruma çerçevesi olan GDPR gibi ilgili yasaları ve CSO'lar için uyumluluğun ne anlama geldiğini (ör. onay alma, kişisel verilerin güvenliğini sağlama, ihlalleri bildirme) vurgulayacağız. Bu modül, kuruluşların veri işleme konusunda hem etik hem de yasal sorumluluklarını anlamalarını sağlar.

6. Sosyal Medya ve Çevrimiçi Varlık Güvenliği: Kuruluşun İtibarını ve Hesaplarını Koruma – Birçok CSO, sosyal medyayı erişim için kullanır. Bu konu, sosyal medya hesaplarının güvenliğini

(güçlü şifreler, iki faktörlü kimlik doğrulama, birden fazla yönetici için rol tabanlı erişim), hesap ele geçirilmesine karşı koruma ve çevrimiçi taciz veya yanlış bilgi kampanyalarıyla başa çıkmayı kapsar. Ayrıca, CSO'nun itibarını koruyan web sitesi içeriği yönetimi, güvenlik ve güvenli çevrimiçi davranışlarla ilgili kılavuzlar da içerir.

7. Güvenlik Kültürü Geliştirme: Personel Eğitimi, Politikalar ve Olaylara Müdahale – İnsan faktörleri ve kurumsal önlemlere odaklanır. Her personelin siber güvenlikteki rolünü anladığı bir kültürün nasıl geliştirileceği. Basit BT güvenlik politikaları (kabul edilebilir kullanım politikası, kendi cihazını getir kuralları vb.) yazma, düzenli personel farkındalık eğitimleri düzenleme (oCSOing eğitimi, personelin %90'ının zayıf halka olmasını önlemek için hayati önem taşır) ve olay müdahale planı oluşturma (ihlal durumunda atılacak adımlar, roller ve sorumluluklar, siber kriz sırasında iletişim stratejisi) konusunda rehberlik. Ayrıca, yetkililere olayları bildirme ve olaylardan ders çıkarma konusunda temel bilgileri de ele alacağız.

Müfredatın Uygulama Stratejisi

Bu müfredatın geliştirilmesi ve uygulanması, işbirliğine dayalı ve aşamalı bir süreç olarak gerçekleştirilmiştir.

Müfredatın Gözden Geçirilmesi ve Yerelleştirilmesi:

İlk taslağın hazırlanmasının ardından, proje ortakları müfredat materyallerini yerel bağlamlarla uygunluğunu sağlamak için gözden geçirdiler. Bu aşamada ortaklar, temel terminolojinin çevirisi, ülkeye özgü vaka çalışmalarının dahil edilmesi ve önerilerin ulusal mevzuat ve yaygın uygulamalarla uyumlu hale getirilmesi gibi uyarlamalar önerdiler. Sonuç olarak, müfredat, her katılımcı ülke için isteğe bağlı yerelleştirilmiş bölümlerle tamamlanan bir temel çerçeve ile yapılandırıldı.

Pilot Eğitim:

Müfredat, seçilen ortak ülkelerdeki küçük bir STK katılımcı grubuyla pilot olarak uygulandı. Pilot uygulama, kısa modül bölümleri (modül başına yaklaşık 15-20 dakika) veya tam gün süren bir atölye çalışması olarak gerçekleştirildi. Bu aşamada toplanan geri bildirimler, içeriğin netliği, uzunluğu ve pratik yararı üzerine odaklandı ve müfredat buna göre iyileştirildi.

Eğitici Eğitimi Oturumları:

Ölçeklenebilirlik ve sürdürülebilirliği sağlamak için, her ülkede proje ortakları ve belirlenen STK temsilcileri için eğiticilerin eğitimi oturumları düzenlendi. Bu oturumlar sadece müfredat içeriğini değil, aynı zamanda rehberli kolaylaştırma tekniklerini, etkileşimli alıştırmaları ve tartışma konuları da kapsadı ve eğiticilerin materyali daha geniş kitlelere güvenle sunmalarını sağladı.

Sivil Toplum Kuruluşlarına Sunum (Kapasite Geliştirme):

Eğitici eğitimi aşamasının ardından, ortak kuruluşlar yerel STK'lar ve sivil toplum aktörleri için ulusal düzeyde eğitimler düzenledi. Bu eğitimler web seminerleri, yüz yüze seminerler aracılığıyla verildi veya mevcut kapasite geliştirme faaliyetlerine entegre edildi. Yerel ihtiyaçlara bağlı olarak, eğitimler 15-20 dakikalık bireysel modüller halinde yapılandırıldı veya birden fazla modülü kapsayan daha uzun atölye çalışmalarına dönüştürüldü.

Kaynaklar ve OCSOing Desteği:

Tüm müfredat materyalleri ve beraberindeki el kitabı, erişilebilir formatlarda, öncelikle indirilebilir PDF kaynakları olarak derlenip paylaşıldı. Ayrıca, katılımcıların ve eğitmenlerin sorular sorabilmeleri, deneyimlerini paylaşabilmeleri ve yeni ortaya çıkan tehditler veya iyi güvenlik uygulamalarıyla ilgili güncellemeleri paylaşabilmeleri için bir çevrimiçi iletişim kanalı oluşturuldu. Bu akran öğrenme ortamı, resmi eğitim oturumlarının ötesinde sürekli katılımı destekledi**.**

İzleme ve Değerlendirme:

Uygulama süreci boyunca, müfredatın etkisini değerlendirmek için izleme ve değerlendirme faaliyetleri yürütüldü. Göstergeler arasında eğitilen STK'ların sayısı, eğitim öncesi ve sonrası değerlendirmeler arasında gözlemlenen değişiklikler ve örgütsel iyileştirmelerle ilgili niteliksel geri bildirimler (siber güvenlik politikalarının veya yeni veri koruma prosedürlerinin benimsenmesi gibi) yer aldı. Bu bulgular, müfredatın katılımcı kuruluşlar arasında dijital güvenlik uygulamalarının güçlendirilmesine etkili bir şekilde katkıda bulunmasını sağlamak için projenin genel izleme çerçevesine entegre edildi.

Bu yaklaşımı izleyerek, müfredat geliştirme ve uygulama süreci kapsayıcı ve yinelemeli oldu ve farklı ulusal bağlamlardaki sivil toplum kuruluşlarının ihtiyaçlarına iyi uyarlanmış bir nihai ürün ortaya çıktı**.**

3.1 MODÜL 1: DİJİTAL GÜVENLİK TEMELLERİ – TEHDİT ORTAMINI VE TEMEL HİJYENİ ANLAMAK

Bu modülün sonunda katılımcılar şunları yapabileceklerdir:

- *Sivil toplum kuruluşları için dijital güvenliğin neden kritik olduğunu açıklamak ve temel siber hijyen uygulamalarını tanımlamak.*
- *Sivil toplumu hedef alan yaygın siber tehditleri (kötü amaçlı yazılım, kimlik avı, DDoS vb.) tanımak.*
- *Temel güvenlik alışkanlıklarını (güçlü şifreler, iki faktörlü kimlik doğrulama, yazılım güncellemeleri, şüpheli e-postalara karşı dikkatli olma) uygulamak.*

Öğrenim Hedefleri:

- Dijital güvenliğin STK'lar için neden kritik öneme sahip olduğu ve sivil toplumu hedef alan belirli siber tehditler konusunda farkındalık yaratmak.
- Sivil toplum kuruluşlarının karşılaşabileceği yaygın siber saldırı türlerini (ör. kötü amaçlı yazılım, kimlik avı, hackleme, DDoS) ve tehdit aktörlerini (suç grupları, düşman hükümetler) belirleyin.
- Temel siber güvenlik en iyi uygulamalarını ve alışkanlıklarını benimseyin (örneğin, güçlü şifreler oluşturmak, iki faktörlü kimlik doğrulamayı etkinleştirmek, yazılımları güncel tutmak ve şüpheli iletişimleri tanımak).

Ana Konular:

- Sivil toplum kuruluşları için dijital güvenliğin önemi – siber olayların operasyonları nasıl aksatabileceği ve hassas verileri nasıl tehlikeye atabileceği.
- Tehdit ortamına genel bakış: kötü amaçlı yazılım, kimlik avı, hackleme, DDoS vb. gibi yaygın saldırı türleri ve sivil topluma karşı artan sıklıkları.
- Sivil toplum kuruluşlarını hedef alan tehdit aktörleri: finansal kazanç peşinde olan siber suçlulardan, sivil toplum kuruluşlarının faaliyetlerini izlemek veya aksatmak isteyen düşman devlet destekli gruplara kadar.
- Temel siber hijyen uygulamaları: güçlü şifreler ve şifre yöneticisi kullanmak, iki faktörlü kimlik doğrulamayı etkinleştirmek, yazılımları/antivirüsleri güncel tutmak ve şüpheli e-postalara veya bağlantılara karşı dikkatli olmak.

- Personel arasında güvenlik bilinci oluşturmak – herkesin dijital güvenlikten sorumlu olduğu bir kültür ve uyanıklığı teşvik etmek.

Örnek Faaliyetler veya Alıştırmalar:

- **Tehdit Beyin Fırtınası:** Katılımcılar, kuruluşlarına yönelik potansiyel siber tehditleri listeler ve her bir tehdidin çalışmalarını nasıl etkileyebileceğini tartışır.
- **Şifre Yarışması:** Katılımcılar örnek şifrelerin gücünü değerlendirir ve güçlü şifreler oluşturmayı ve yönetmeyi öğrenir (ör. şifre cümleleri, şifre yöneticisi kullanma).
- **Oltalama Testi:** Örnek e-postalar (bazıları oltalama, bazıları meşru) sunun ve katılımcılardan oltalama girişimini gösteren uyarı işaretlerini belirlemelerini isteyin.
- **Vaka Çalışması Tartışması:** CSO'ları etkileyen yakın tarihli bir yerel siber olayı açıklayın – Bu olayda neler olduğunu analiz edin ve hangi temel güvenlik önlemlerinin bunu önleyebileceğini tartışın.

Modül 1 Vaka Çalışması Örneği: Bir Topluluk CSO'suna Yönelik Kimlik Avı Saldırısı

- **Bağlam:** Savunmasız nüfus gruplarına gıda ve yardım sağlayan küçük bir topluluk CSO'su, e-posta ve çevrimiçi bağış platformlarına güvenmektedir. Personel, asgari düzeyde siber güvenlik eğitimi almıştır ve yalnızca temel e-posta güvenliğine güvenmektedir.
- **Sorun:** Bir sabah, CSO'nun finans sorumlusu, büyük bir bağışçı gibi davranan birinden acil bir e-posta aldı. E-posta, ödeme bilgilerini güncellemek için şüpheli bir bağlantı içeriyordu. Yetkili, bağlantıya tıklayarak CSO'nun banka hesabı web sitesine giriş bilgilerini girdi, bunun bir kimlik avı sitesi olduğunun farkında değildi. Birkaç saat içinde, CSO'nun hesabından toplamda binlerce dolar tutarında yetkisiz para çekme işlemi gerçekleştirildi. CSO, fonları geri kazanıp hesapları güvence altına alırken faaliyetlerini geçici olarak durdurmak zorunda kaldı.
- **Sonuç:** Olayın ardından, CSO teknoloji konusunda bilgili bir gönüllünün yardımıyla bu güvenlik ihlalini inceledi. Hemen temel siber güvenlik önlemleri uyguladılar: güçlü, benzersiz şifreler kullanmayı zorunlu hale getirdiler ve tüm hesaplarda iki faktörlü kimlik doğrulamayı etkinleştirdiler. Ayrıca, kimlik avı e-postalarını tanımak için (yazım hatalarını aramak, gönderen adreslerini kontrol etmek vb.) düzenli personel eğitimi

vermeye başladılar. Sonraki aylarda, CSO benzer dolandırıcılıkları başarıyla önledi ve iyileştirmeler konusunda şeffaf davranarak bağışçıların güvenini geri kazandı.

Tartışma Soruları:

- *Bu durumda kimlik avı saldırısını hangi temel siber güvenlik uygulaması önleyebilirdi?*
- *Personel üyesi neden kimlik avı e-postasına kanmış ve personel gelecekte bu tür dolandırıcılıkları tanımak için hangi adımları atabilir?*
- *CSO bu olaydan nasıl kurtuldu ve sonrasında güvenliği güçlendirmek için hangi önlemleri aldı?*

Modül 1 Değerlendirmesi

- Bu modül, beş kısa soru ve bir küçük görevle değerlendirilecektir. Geçmek için en az %70 puan alınması gerekir.

Modül 1 – Değerlendirme: Kısa Sorular

1. Sivil toplum kuruluşları için dijital güvenlik neden özellikle önemlidir? (Siber olayların STK'ların faaliyetlerini veya yararlanıcılarını nasıl etkileyebileceğini kısaca açıklayın.)
2. Sivil toplum kuruluşlarını sık sık hedef alan iki yaygın siber tehdidi sayın. (Örnek: kimlik avı, kötü amaçlı yazılım, DDoS vb.)
3. Kimlik avı nedir ve genellikle kullanıcıları nasıl kandırmaya çalışır? (Temel yöntemi bir veya iki cümle ile açıklayın.)
4. Hesapların ele geçirilmesini önlemeye yardımcı olan iki temel siber hijyen uygulamasını sıralayın. (Örnek: güçlü şifreler, iki faktörlü kimlik doğrulama, düzenli güncellemeler.)
5. Bir e-postanın kimlik avı girişimi olabileceğine dair açık bir uyarı işaretinden bahsedin. (Örnek: acil dil, şüpheli gönderen adresi, beklenmedik bağlantılar veya ekler.)

Pratik Görev: Kimlik Avı Riskinin Belirlenmesi

Katılımcılara CSO'nun çalışmalarıyla ilgili kısa bir örnek e-posta (veya senaryo) verilir (ör. bağış güncellemesi, fon sağlayıcı mesajı veya iç talep).

Katılımcılardan şunlar istenir:

- Mesajın meşru mu yoksa şüpheli mi olduğuna karar verin.
- Mesajda en az iki uyarı işareti (kırmızı bayrak) belirleyin.
- Bağlantıya tıklamak veya doğrudan yanıt vermek yerine almaları gereken somut bir önlemi yazmak (ör. başka bir kanal üzerinden doğrulamak, amirine bildirmek).

Değerlendirme Kriterleri:

- E-postayı şüpheli veya riskli olarak doğru bir şekilde tanımlar.
- En az iki kırmızı bayrağı doğru bir şekilde belirtir,
- Uygun ve güvenli bir yanıt önerir.

3.2 MODÜL 2: RİSK DEĞERLENDİRME VE PLANLAMA – KURUMSAL RİSKLERİ DEĞERLENDİRME VE GÜVENLİK PLANI OLUŞTURMA

Bu modülün sonunda katılımcı şunları yapabilecektir:

- *Kuruluşun kritik dijital varlıklarını ve potansiyel güvenlik açıklarını tanımlayabilir.*
- *Bu varlıklara yönelik tehditlerin olasılığını ve etkisini tahmin ederek temel bir risk değerlendirmesi yapmak.*
- *Veri işleme, erişim kontrolü ve olay müdahale planını kapsayan basit bir siber güvenlik planı veya politikası taslağı hazırlamak.*

Öğrenim Hedefleri:

- Kuruluşun kritik dijital varlıklarını (veriler, sistemler, hesaplar) ve potansiyel güvenlik açıklarını nasıl belirleyeceğini anlamak.
- Bu varlıklara yönelik tehditleri ve kuruluş üzerindeki potansiyel etkisini değerlendirmek için temel bir risk değerlendirmesi yapın.
- Veri işleme prosedürleri, erişim kontrolleri ve olaylara müdahale hazırlığı gibi önemli alanları kapsayan bir siber güvenlik planı/politikası geliştirin veya iyileştirin.

Ana Konular:

- Dijital varlıkları ve verileri belirleme: CSO'nun hangi bilgileri ve sistemleri kullandığını (ör. bağışçı veritabanları, e-posta hesapları, web siteleri) ve bunların neden hedef alınabileceğini belirleme.
- Güvenlik açıkları ve tehditler: zayıflıkları (eski yazılımlar, yedekleme eksikliği vb.) nasıl tespit edeceğinizi anlayın ve tehdit senaryoları hayal edin (Saldırganlar neyi hedef alabilir? Bunu nasıl yapabilirler? Sonuçları ne olabilir?).
- Risk değerlendirme süreci: farklı tehdit senaryolarının olasılığını ve etkisini değerlendirmek ve öncelikle ele alınması gereken riskleri önceliklendirmek.
- Siber güvenlik planı oluşturma: veri koruma uygulamalarını, kullanıcı erişim kontrolünü ve olay müdahale prosedürünü kapsayan bir kurumsal güvenlik politikası taslağı hazırlamak (CSO'ların yaklaşık %80'inin şu anda resmi bir güvenlik planı olmadığı için bu özellikle önemlidir).

- Planı güncel tutma: Kuruluş büyüdükçe veya tehdit ortamı değiştikçe güvenlik planını periyodik olarak gözden geçirme ve güncelleme sorumluluğunu atama.

Örnek Faaliyetler veya Alıştırmalar:

- **Varlık Envanteri:** Katılımcılar, CSO'larının güvendiği temel dijital varlıkları (ör. veritabanları, e-posta hesapları, cihazlar, bulut hizmetleri) listeler ve her biriyle ilişkili hassas bilgileri belirler.
- **Risk Haritalama:** Listelenen her varlık için grup, olası tehditleri veya arıza senaryolarını belirler ve bunların olasılığını ve etkisini derecelendirir (yüksek öncelikli riskleri görselleştirmek için basit bir risk matrisi oluşturur).
- **Plan Geliştirme:** Katılımcılar, ekipler halinde çalışarak örnek bir CSO için temel bir siber güvenlik planı taslağı hazırlar. Bu taslak, veri işleme politikaları, verilere kimlerin erişebileceği ve bir güvenlik olayı meydana geldiğinde atılması gereken adımlar ile ilgili bölümleri içermelidir. Ekipler daha sonra planlarını paylaşarak geri bildirim alır.
- **Yerel Risk Senaryosu:** (Vaka senaryosu örnekleri, ülkeye özgü yerelleştirme bölümlerinde yer almaktadır.) Katılımcılar bu senaryoyu tartışır ve güvenlik planının unsurlarını (politikalar, önleyici tedbirler, müdahale adımları) kullanarak riski nasıl azaltacaklarını beyin fırtınası yapar.

Modül 2 Vaka Çalışması: Göz Ardı Edilen Güvenlik Açığı Veri Kaybına Yol Açar

Bağlam: Orta ölçekli bir CSO, bağışçı ve yararlanıcı verilerini depolayan bir iç sunucuyu yönetmektedir. Sunucunun önemli olduğunu bilmelerine rağmen, yedeklemeleri veya riskleri hakkında resmi bir belgeleri yoktur. Personel, "daha önce kötü bir şey olmadığından" verilerin güvende olduğunu varsaymıştır.

Sorun: Yakındaki bir fırtına nedeniyle ani bir elektrik dalgalanması CSO'nun sunucu donanımına zarar vererek verileri bozmuştur. Sunucu aylardır yedeklenmediği için tüm bağışçı kayıtları, proje dosyaları ve finansal veriler kaybolmuştur. CSO, programlarını haftalarca durdurmak zorunda kalmıştır. Bağışçılar bilgileri yeniden göndermek zorunda kalmış ve birçok kayıt kurtarılamamış, bu da kafa karışıklığına ve güven kaybına yol açmıştır.

Sonuç: Bu arızanın ciddiyetinin farkına varan CSO, dışarıdan yardım alarak kapsamlı bir risk değerlendirmesi gerçekleştirdi. Önemli varlıkları (veritabanları, web sitesi, e-posta hesapları) ve

tehditleri (elektrik kesintisi, donanım arızası, siber saldırılar) belirlediler. Off-site yedekleme sistemine yatırım yapmaya ve düzenli bir yedekleme programı oluşturmaya öncelik verdiler. CSO, veri yedekleme ve kurtarma prosedürlerini içeren temel bir siber güvenlik planı hazırladı. Daha sonra, küçük sistem sorunları meydana geldiğinde, kesintiye uğramadan yedeklemelerden verileri başarıyla geri yüklediler.

Tartışma Soruları:

- *Felaketten önce CSO'nun savunmasız olduğuna dair uyarı işaretleri nelerdi?*
- *CSO, benzer bir kaybı önlemek için yeni siber güvenlik planına hangi unsurları dahil etmelidir?*
- *Risk değerlendirmesi yapmak, CSO'nun güvenliğini ve operasyonlarını iyileştirmesine nasıl yardımcı oldu?*

Modül 2 Değerlendirme

Bu modül, beş kısa soru ve bir küçük görevle değerlendirilecektir. Geçmek için en az %70 puan alınması gerekir.

Modül 2 – Değerlendirme: Kısa Sorular

- CSO bağlamında dijital varlık olarak neler kabul edilir? (İki örnek verin.)
- Bir kuruluşun "daha önce kötü bir şey olmadı" varsayımına güvenmesi neden risklidir?
- Temel risk değerlendirmesinde değerlendirilen iki ana faktör nedir? (Kısaca açıklayın.)
- CSO'larda siber güvenlik risklerini artırabilecek iki yaygın güvenlik açığını belirtin.
- Siber güvenlik planını düzenli olarak gözden geçirmek ve güncellemek neden önemlidir?

Pratik Görev: Temel Risk Değerlendirmesi Alıştırması

Katılımcılardan, varsayımsal veya gerçek bir CSO için aşağıdaki adımları tamamlamaları istenir:

- Bir kritik dijital varlık listeleyin (ör. bağışçı veritabanı, e-posta sistemi, web sitesi).
- Bu varlığa yönelik olası bir tehdidi belirleyin (ör. elektrik kesintisi, kimlik avı saldırısı, donanım arızası).
- Riski azaltabilecek bir önleyici tedbiri kısaca açıklayın (ör. yedeklemeler, erişim kontrolleri, iki faktörlü kimlik doğrulama).

Değerlendirme Kriterleri:

- Varlık açıkça tanımlanmıştır,
- Tehdit gerçekçi ve ilgili,
- Önerilen önleyici tedbir uygundur.

3.3 MODÜL 3: CİHAZ VE ALTYAPI GÜVENLİĞİ – BİLGİSAYAR, AĞ VE WEB SİTELERİNİN KORUNMASI

Bu modülün sonunda katılımcılar şunları yapabileceklerdir:

- *Bilgisayarları ve mobil cihazları güvenli hale getirmek için en iyi uygulamaları hayata geçirebilecek (güncellemeleri yükleme, kötü amaçlı yazılımdan koruma ve şifreleme).*
- *Kurumsal ağları yapılandırmak ve korumak (güvenli Wi-Fi, uzaktan erişim için VPN kullanımı).*
- *Web sitesi ve sunucu güvenliğini artırmak (HTTPS'yi etkinleştirmek, düzenli yedeklemeler yapmak ve defacement veya DDoS gibi yaygın saldırılara karşı savunma sağlamak).*

Öğrenim Hedefleri:

- Bilgisayarları ve mobil cihazları güvenli hale getirmek için en iyi uygulamaları uygulamak (ör. kötü amaçlı yazılımdan koruma yazılımı yüklemek, cihaz şifrelemesini etkinleştirmek ve güvenlik ayarlarını doğru şekilde yapılandırmak).
- Güvenli Wi-Fi uygulamaları ve güvenli bağlantıların kullanımı (uzaktan erişim için VPN'ler gibi) yoluyla kurumsal ağları ve internet erişimini korumak.
- Modern koruma önlemleri (HTTPS, yedeklemeler, DDoS koruması vb.) kullanarak ve yaygın saldırılara nasıl yanıt verileceğini anlayarak CSO'nun web sitesinin ve çevrimiçi altyapısının güvenliğini güçlendirin.

Ana Konular:

- Cihaz güvenliği temel unsurları: tüm bilgisayarlara antivirüs/kötü amaçlı yazılımdan koruma yazılımı yüklemek ve güncellemek, güvenlik duvarlarını etkinleştirmek ve veri hırsızlığını önlemek için dizüstü bilgisayarlarda ve akıllı telefonlarda disk şifreleme kullanmak.
- Güvenli cihaz yapılandırması: güçlü cihaz oturum açma parolaları/PIN'leri uygulamak, gereksiz uygulamaları ve hizmetleri kaldırmak veya devre dışı bırakmak ve güvenlik yamalarını veya güncellemeleri düzenli olarak uygulamak.

- Ağ güvenliği temelleri: Wi-Fi'yi güvenli kullanma (güvenilir ağları kullanma, güçlü parolalar ve şifreleme ile ofis Wi-Fi'sini güvenli hale getirme) ve şifreli bağlantılar için VPN'leri ne zaman kullanma (özellikle kamu ağlarında).
- Web sitesi ve sunucu güvenliği: web sitesi yazılımını (CMS, eklentiler) güncel tutmak, web trafiğini şifrelemek için HTTPS kullanmak, site verilerinin düzenli yedeklemelerini yapmak ve defacement veya DDoS gibi yaygın saldırılara karşı korumalar uygulamak.
- Altyapı saldırılarının gerçek hayattan örnekleri: örneğin, bir CSO'yu aylarca çevrimdışı bırakan bir web sitesi defacement vakası, proaktif savunmanın önemini vurgulamaktadır.

Örnek Etkinlikler veya Alıştırmalar:

- **Cihaz Güvenliği Denetimi:** Katılımcılar, bir kontrol listesi kullanarak örnek bir cihazı (veya uygunsa kendi cihazlarını) temel güvenlik korumaları açısından incelerler – antivirüs yüklemesi ve güncellemeleri, güvenlik duvarı durumu, şifreleme etkinliği ve son güvenlik güncellemeleri kontrol edilir.
- **Wi-Fi Güvenliği Demosu:** Eğitmen, güvenli olmayan halka açık Wi-Fi kullanmanın risklerini gösterir (örneğin, trafiği izlemenin ne kadar kolay olduğunu). Ardından, güvenliği sağlamak için atılması gereken adımları tartışır: güvenli bir ev/ofis Wi-Fi ağı yapılandırmak ve halka açık ağlarda VPN veya güvenli uygulamalar kullanmak.
- **Web Sitesi Güvenlik İncelemesi:** Birkaç güvenlik açığı olan (eski yazılım, HTTPS yok, zayıf yönetici şifresi) hayali bir CSO web sitesi senaryosu sunun. Küçük gruplar sorunları belirler ve web sitesinin güvenliğini artırmak için düzeltmeler önerir.
- **Yerel Vaka Çalışması:** CSO web sitesinin tahrif edilmesi veya siber saldırıya uğraması ile ilgili yerel bir vakayı açıklayın. Bu olayda neler olduğunu ve gelecekte böyle bir olayın yaşanmasını önlemek için (modülün ana konularından) hangi önleyici tedbirlerin alınabileceğini tartışın.

  Modül 3 Vaka Çalışması: Web Sitesi Tahribatı ve Hizmet Kesintisi

  Bağlam: Bir sivil toplum kuruluşu, program güncellemeleri ve bağış toplama amacıyla halka açık bir web sitesi işletmektedir. Site, açık kaynaklı bir içerik yönetim sistemi (CMS)

üzerine kurulmuştur. Teknik bakım, siteyi ara sıra güncelleyen tek bir gönüllü tarafından yapılmaktadır.

Sorun: Hackerlar, STK'nın web sitesindeki eski bir eklentiyi istismar ederek ana sayfayı tahrip etmiş ve yerine siyasi bir mesaj yerleştirmiştir. STK, personel siteyi düzenli olarak kontrol etmediği için değişikliği hemen fark etmemiştir. Tahribat birkaç gün boyunca kalmış, destekçiler arasında kafa karışıklığına neden olmuş ve bağışçıları geçici olarak caydırmıştır. Ziyaretçiler uygunsuz içerik gördü ve kuruluşun adresindeki güvenilirliği zarar gördü. Ayrıca, hackerlar web sitesinin dosyalarına erişim sağladı ve bağışçı verilerinin güvenliği konusunda endişeler uyandırdı (ancak herhangi bir ihlal doğrulanmadı).

Sonuç: Sorunu keşfettikten sonra, CSO temizlik için web sitesini çevrimdışı hale getirdi ve kötü amaçlı içeriği kaldırdı. CMS ve tüm eklentileri en son sürümlere güncellediler. CSO, bundan sonra düzenli site yedeklemeleri uyguladı ve web sitesinin haftalık kontrollerini planladı. Ayrıca, otomatik güncellemeler ve HTTPS şifrelemesi sunan bir yönetilen barındırma sağlayıcısına geçiş yaptı. Sonraki aylarda site güvenli kaldı ve CSO, olay ve bunu önlemek için atılan adımlar hakkında şeffaf bir şekilde iletişim kurarak güveni yeniden kazandı.

Tartışma Soruları:

- *Yazılımı güncel tutmak ve düzenli yedeklemeler yapmak bu saldırının sonucunu nasıl değiştirebilirdi?*
- *CSO, web sitesinin tahrif edildiğini fark ettiğinde hangi acil önlemleri almalıydı?*
- *CSO, web altyapısını güvence altına almak için hangi uzun vadeli önlemleri uyguladı?*

Modül 3 Değerlendirme

Bu modül, beş kısa soru ve bir küçük görevle değerlendirilecektir. Geçmek için en az %70 puan alınması gerekir.

Modül 3 – Değerlendirme

Kısa Sorular

1. CSO'lar tarafından kullanılan dizüstü bilgisayarlar ve akıllı telefonlar için cihaz şifrelemesi neden önemlidir?
   (Bir veya iki cümle ile cevaplayın.)
2. Tüm kurumsal cihazlarda etkinleştirilmesi gereken iki temel güvenlik önlemini belirtiniz.
3. Ek koruma olmadan güvenli olmayan halka açık Wi-Fi kullanmanın başlıca riskleri nelerdir?
4. Eski CMS eklentileri CSO web siteleri için neden ciddi bir güvenlik riski oluşturur?
5. Düzenli yedeklemeler, web sitesi tahribatı veya siber saldırıların etkisini nasıl azaltır?

Pratik Görev: Temel Cihaz veya Web Sitesi Güvenlik Kontrolü

Katılımcılar aşağıdaki seçeneklerden birini seçerler:

Seçenek A – Cihaz Güvenliği

- Bir iş cihazına (bilgisayar veya akıllı telefon) şu anda uygulanan **üç güvenlik önlemini** listeleyin
  (ör. antivirüs, şifreleme, ekran kilidi, güncellemeler)
- **Eksik veya zayıf bir önlemi** belirleyin ve nasıl iyileştirilebileceğini kısaca açıklayın.

Seçenek B – Web Sitesi Güvenliği

- Bir CSO web sitesi için uygulanması gereken **iki temel güvenlik kontrolünü** belirleyin. *(ör. HTTPS, düzenli güncellemeler, yedeklemeler, güçlü yönetici şifreleri)*
- Bu kontroller uygulanmadığında ortaya çıkabilecek **bir riski** kısaca açıklayın.

Değerlendirme Kriterleri:

- Belirlenen önlemler modülle ilgilidir.
- Riskler veya iyileştirmeler gerçekçi ve açık bir şekilde açıklanmıştır.

Geçerlilik Koşulu:

Katılımcı, en az iki geçerli güvenlik önlemini ve bir ilgili riski veya iyileştirmeyi doğru bir şekilde tanımlamalıdır.

3.4 MODÜL 4: GÜVENLİ İLETİŞİM VE İŞBİRLİĞİ – GÜVENLİ E-POSTA, MESAJLAŞMA VE UZAKTAN ÇALIŞMA

Bu modülün sonunda katılımcı şunları yapabilecektir:

- *Yaygın e-posta tabanlı tehditleri (örneğin kimlik avı) tanımak ve önlemek ve güvenli e-posta uygulamalarını (güçlü parolalar, 2FA) uygulamak.*
- *Şifreleme sağlayan güvenli mesajlaşma ve dosya paylaşım araçlarını kullanmak.*
- *Güvenli uzaktan çalışma uygulamalarını hayata geçirmek (kamu ağlarında VPN kullanmak, sanal toplantıları şifrelerle güvenli hale getirmek).*

Öğrenim Hedefleri:

- Yaygın e-posta tabanlı tehditleri (örneğin, kimlik avı dolandırıcılığı) tanımak ve önlemek ve günlük işlerde güvenli e-posta uygulamaları kullanmak.
- Hassas bilgileri korumak için mesajlaşma ve dosya paylaşımı için güvenli iletişim araçları (ör. uçtan uca şifrelenmiş uygulamalar, güvenli belge işbirliği platformları) seçin ve kullanın.
- Uzaktan çalışma ve sanal işbirliği için güvenlik önlemleri uygulayın (güvenli ağlar kullanın, çevrimiçi toplantıları koruyun ve şirket dışında çalışırken hesapları/cihazları yönetin).

Ana Konular:

- **E-posta güvenliği:** Kimlik avı girişimlerini (örneğin, şüpheli gönderenler veya bağlantılar, acil, olağandışı istekler) nasıl tespit edebilirsiniz ve e-posta hesapları için güçlü parolalar ve 2FA kullanmanın önemi. Hassas veriler alışverişi yapılıyorsa, şifreli e-posta hizmetlerini veya eklentileri kullanmayı düşünün.
- **Güvenli mesajlaşma:** Uçtan uca şifreleme sunan güvenilir mesajlaşma uygulamalarını (örneğin, Signal veya diğer güvenli mesajlaşma uygulamaları) seçmek ve kaybolan mesajlar gibi güvenlik özelliklerini etkinleştirmek. Kişileri doğrulama ve güvenli olmayan kanallarda hassas bilgileri paylaşmama konusunda rehberlik.
- **Dosya paylaşımı ve işbirliği:** Şifreleme özelliği sunan güvenli bulut depolama veya dosya paylaşım hizmetlerini kullanın. Hassas belgeleri parola ile koruma veya dış ortaklarla çalışırken güvenli işbirliği için tasarlanmış platformları kullanma gibi uygulamalar.

- **Uzaktan çalışma önlemleri:** Güvenilir olmayan ağlarda VPN kullanma, ev Wi-Fi yönlendiricilerini güvenli hale getirme, sanal toplantı alanlarını koruma (bekleme odaları, toplantı şifreleri, ekran paylaşımını sınırlama) ve uzaktan kullanılan iş cihazlarını yönetme dahil olmak üzere ofis dışında çalışmak için en iyi uygulamalar.
- **Güvenlik ve erişilebilirlik arasında denge kurma:** Güvenlik önlemlerinin (şifreleme ve erişim kontrolleri gibi) kullanıcı dostu olmasını sağlayarak personelin bunları tutarlı bir şekilde kullanmasını sağlamak ve güvenlik nedenleriyle tanıtılan yeni iletişim araçları hakkında eğitim vermek.

Örnek Etkinlikler veya Alıştırmalar:

- **Oltalama E-postası Tatbikatı:** Kolaylaştırıcı, grupla örnek e-postaları paylaşır. Katılımcılar, her birinin meşru bir e-posta mı yoksa oltalama girişimi mi olduğuna karar vermeli ve kararlarını etkileyen ipuçlarını vurgulamalıdır.
- **Mesajlaşma Uygulaması Karşılaştırması:** Küçük gruplara ayrılın; her grup farklı bir mesajlaşma uygulamasını (ör. WhatsApp, Signal, Telegram) inceler ve güvenlik özellikleri (şifreleme, iki faktörlü kimlik doğrulama vb.) ve sınırlamaları hakkında rapor verir. Çeşitli CSO iletişim türleri için en uygun uygulamaların hangileri olduğunu tartışın.
- **Güvenli Video Görüşmesi Kurulumu:** Uygun güvenlik önlemleriyle çevrimiçi toplantı kurulumunun canlı gösterimi: bekleme odasını etkinleştirme, toplantı şifresi gerektirme, katılımcıların ekran paylaşımını kısıtlama vb. Gösterimden sonra, katılımcılar bu ayarları yapılandırmayı dener veya kendi toplantılarını güvenli hale getirme deneyimlerini tartışır.
- **Yerel Bağlam Tartışması:** [Ülkenizde popüler olan güvenli bir iletişim aracını veya ilgili şifreleme yasasını ekleyin] – Bu yerel bağlamın CSO'nun iletişim güvenliğini nasıl etkilediğini tartışın. Örneğin, belirli bir şifreli uygulama yerel olarak yaygın olarak kullanılıyorsa, CSO bunu nasıl kullanabilir? Şifreleme veya veri depolama ile ilgili yerel düzenlemeler varsa, bunlar iletişim seçeneklerini nasıl etkiler?

Modül 4 Vaka Çalışması: Uzaktan Çalışma E-posta İhlali

Bağlam: Bir insani kriz sırasında, bir CSO'nun saha görevlisi, genel Wi-Fi kullanarak bir kafeden uzaktan çalışarak durum raporlarını merkeze gönderiyor. Kuruluş, günlük iletişim için e-posta kullanıyor, ancak uzaktaki kullanıcılar için şifreli bağlantıları zorunlu kılmıyor.

Sorun: Aynı halka açık Wi-Fi ağındaki bir siber suçlu, görevlinin şifrelenmemiş e-posta trafiğini ele geçirir. Saldırgan, görevli CSO'nun e-posta hesabına giriş yaptığında giriş bilgilerini ele geçirir. Ertesi gün, saldırgan görevliyi taklit ederek bağışçılara sahte bir proje için acil fon talebinde bulunan sahte e-postalar gönderir. Dolandırıcılık ortaya çıkmadan önce bir bağışçı saldırganın hesabına para havale etti. CSO fonlarını kaybetti ve bağışçılara bu aldatmacayı açıklamak zorunda kaldı.

Sonuç: Buna yanıt olarak, CSO güvenli iletişim uygulamaları hayata geçirdi. Uzaktan çalışan tüm personelin e-posta erişimi için VPN veya HTTPS kullanması zorunlu hale getirildi ve e-posta hesaplarında iki faktörlü kimlik doğrulama etkinleştirildi. CSO ayrıca iç iletişim için şifreli bir mesajlaşma uygulaması benimsedi. Bağışçılarla gelecekteki taleplerin doğrulanması konusunda iletişim kurdular ve personel için e-posta eğitimini iyileştirdiler (sahte e-postaları tespit etme, korumasız halka açık Wi-Fi kullanmama). Bu önlemlerin alınmasından sonra başka bir olay yaşanmadı.

Tartışma Soruları:

- *Bu durumda CSO'nun uzaktan çalışma uygulamalarının hangi güvenlik açıkları vardı?*
- *VPN'ler ve iki faktörlü kimlik doğrulama, saldırganın erişimini nasıl engelleyebilirdi?*
- *CSO, ihlalin ardından iletişimi ve bağışçıların güvenini korumak için hangi adımları attı?*

Modül 4 Değerlendirme

Bu modül, beş kısa soru ve bir küçük görevle değerlendirilecektir. Geçmek için en az %70 puan alınması gerekir.

Modül 4 – Değerlendirme

5 Kısa Soru

1. Bir e-postanın kimlik avı girişimi olabileceğine dair iki yaygın işaret nedir?
   (Kısaca cevaplayın.)
2. İki faktörlü kimlik doğrulama (2FA) CSO'lar tarafından kullanılan e-posta hesapları için neden özellikle önemlidir?
3. Hassas iletişimlerin korunmasına yardımcı olan bir güvenli mesajlaşma özelliği belirtin.
4. Çalışanlar korumasız halka açık Wi-Fi kullanarak uzaktan çalıştığında CSO'lar hangi risklerle karşı karşıya kalır?
5. Çevrimiçi toplantıları güvenli hale getirmek (ör. şifreler, bekleme odaları) güvenlik risklerini nasıl azaltabilir?

Pratik Görev: Güvenli İletişim Kontrolü

Katılımcılar aşağıdaki görevi bireysel olarak veya çiftler halinde tamamlar:

1. CSO'nuzun kullandığı **bir iletişim kanalını seçin**
   (e-posta, mesajlaşma uygulaması, dosya paylaşım platformu veya video toplantı aracı).
2. Kısaca cevaplayın:
   - **Şu anda bir güvenlik önlemi uygulanmaktadır**
     (ör. 2FA etkinleştirilmiş, şifreli mesajlaşma, toplantı şifreleri)
   - Güvenliği güçlendirebilecek **bir iyileştirme**
     (ör. VPN kullanımını etkinleştirme, şifreli bir uygulamaya geçme, erişim haklarını sınırlama)
3. Bu iyileştirmenin riski nasıl azaltacağını **bir veya iki cümle** ile açıklayın.

Değerlendirme Kriterleri:

- Seçilen kanal CSO iletişimi ile ilgilidir,
- Güvenlik önlemleri ve iyileştirmeler gerçekçidir,
- Açıklama, güvenli iletişim uygulamalarına ilişkin anlayışı göstermektedir.

3.5 MODÜL 5: VERİ KORUMA VE GİZLİLİK UYUMU – VERİLERİ KORUMA VE YASAL YÜKÜMLÜLÜKLERİ ANLAMA

Bu modülün sonunda katılımcı şunları yapabilecektir:

- *CSO'nun topladığı hassas verileri tanımlayacak ve bunların neden korunması gerektiğini açıklayabilecek.*
- *Temel veri koruma uygulamalarını (veri minimizasyonu, şifreleme, güvenli depolama, düzenli yedekleme ve güvenli imha) uygulamak.*
- *Veri koruma yasaları (GDPR gibi) kapsamındaki CSO'nun yasal yükümlülüklerini ve uyumluluğun nasıl sağlanacağını anlamak ve özetlemek.*

Öğrenim Hedefleri:

- CSO'ların topladığı hassas veri türlerini (ör. yararlanıcıların kişisel bilgileri, bağışçı kayıtları) ve bu tür verilerin korunmasının neden çok önemli olduğunu tanımak.
- Gizlilik ve güvenliği artırmak için veri minimizasyonu, şifreleme (depolanan ve aktarılan veriler için), güvenli depolama/yedekleme ve verilerin uygun şekilde imha edilmesi gibi temel veri koruma ilkelerini uygulayın.
- AB'nin GDPR'si ve eşdeğer ulusal veri koruma yasaları gibi veri koruma ile ilgili yasal yükümlülükleri ve çerçeveleri ve CSO'nun bu düzenlemelere nasıl uyum sağlayacağını anlamak.

Ana Konular:

- **Hassas verilerin belirlenmesi:** CSO bağlamında kişisel veya hassas veri olarak kabul edilenler (adlar, adresler, sağlık veya yasal dava bilgileri vb.) ve bu tür verilerin sızdırılması durumunda ortaya çıkan riskler.
- **Veri koruma ilkeleri:** Veri minimizasyonu (sadece gerçekten gerekli olanların toplanması), depolanan verilerin (örneğin, sürücülerdeki dosyalar) ve aktarım halindeki verilerin (veri aktarımı için SSL/HTTPS kullanımı) şifrelenmesi, güvenli veri depolama çözümleri (fiziksel ve bulut), düzenli yedeklemelerin yapılması ve artık gerekli olmayan verilerin uygun şekilde silinmesi için pratik adımlar.

- **Yasal çerçeveler:** Önemli veri koruma yasalarına genel bakış – örneğin, Avrupa'da önde gelen bir çerçeve olan GDPR (Genel Veri Koruma Yönetmeliği) ve [ülkenizin veri koruma yönetmeliğini buraya ekleyin]. Temel yükümlülükler arasında veri toplama için bilgilendirilmiş onam alınması, teknik ve organizasyonel önlemler yoluyla kişisel verilerin güvenliğinin sağlanması ve ihlal bildirim gereklilikleri yer alır.
- **Etik veri işleme:** Yasal kuralların ötesinde, bireylerin gizliliğini korumak için etik sorumluluğu vurgulamak. Yararlanıcıların zarar görmesi, güven kaybı, yasal cezalar ve itibar kaybı dahil olmak üzere veri ihlallerinin CSO'lar için sonuçlarının tartışılması.
- **Uyumun uygulamaya geçirilmesi:** STK'ların basit gizlilik politikaları, veri işleme kılavuzları geliştirmeleri ve personeli bu politikalar konusunda eğitmeleri. Ortaklarla çalışırken Veri Koruma Görevlileri (ilgiliyse) veya veri işleme anlaşmaları gibi kavramların tanıtılması.

Örnek Faaliyetler veya Alıştırmalar:

- **Veri Denetim Alıştırması:** Katılımcılar, STK'larının topladığı veya işlediği kişisel veri türlerini sıralar ve bu verilerin nerede depolandığını (veritabanları, elektronik tablolar, e-posta, bulut hizmetleri) haritalandırır. Ardından her bir öğe için kimlerin erişimi olduğunu, şu anda nasıl korunduğunu ve fark ettikleri eksiklikleri tartışırlar.
- **Şifreleme Demosu:** Eğitmen, örnek bir dosya veya klasörü şifrelemeyi (veya e-postalar/metinler için bir şifreleme aracı kullanmayı) gösterir. Katılımcılar, şifrelenmiş verilerin nasıl göründüğünü öğrenir ve bir test verisini şifrelemeyi ve şifresini çözmeyi pratik eder, anahtar/şifre yönetiminin önemini vurgular.
- **Politika İncelemesi:** Basit bir Veri Koruma Politikası veya Gizlilik Bildirimi şablonu veya örneği sağlayın. Küçük gruplar halinde, katılımcılar bu belgenin GDPR gerekliliklerini nasıl karşıladığını belirler ve [Buraya ülkenizin veri koruma düzenlemesini ekleyin] ile uyum sağlamak için hangi değişikliklerin gerekli olacağını değerlendirir. Her grup, kendi CSO politikasına dahil edecekleri bir anahtar noktayı sunabilir.
- **Yasal Uyumluluk Tartışması:** GDPR uyumluluğu için eylemlerin kontrol listesini gözden geçirin (ör. sorumlu bir kişi atama, onay formları hazırlama, veri ihlali planı). Katılımcılar, listedeki hangi maddeleri uyguladıklarını ve hangilerini uygulamaları gerektiğini

tartışırlar. Ulusal yasaların gerektirdiği ek adımları vurgulayın (ör. [Ülkenizin veri koruma yönetmeliğini buraya ekleyin] gerektiriyorsa, veri koruma otoritesine kayıt olma).

Modül 5 Vaka Çalışması: Bağışçı Veritabanı İhlali

Bağlam: Uluslararası bir yardım STK'sı, bağışçı bilgileri (adlar, iletişim bilgileri, bağış geçmişi) ve yararlanıcı verileri (hassas sağlık bilgileri) içeren bir veritabanı tutmaktadır. Veriler, program personelinin erişebileceği bir iç ağ sürücüsünde saklanmaktadır.

Sorun: Sistem yükseltmesi sırasında, bir yönetici yanlışlıkla bağışçı veritabanı klasörünü şifreleme veya erişim denetimi olmaksızın halka açık bir bulut dosya paylaşım bağlantısında ifşa etmiştir. Bir hacker bu bağlantıyı keşfetmiş ve bağışçı listesinin tamamını indirmiştir. Binlerce bağışçının kişisel bilgileri (adlar, e-postalar ve bağış tutarları) çevrimiçi olarak sızdırılmıştır. STK, yasaların gerektirdiği şekilde bağışçılara ihlali bildirmek zorunda kalmıştır. Birkaç bağışçı, güven kaybını gerekçe göstererek desteğini çekmiştir. STK, verileri uygun şekilde korumadığı için de incelemeye tabi tutulmuştur.

Sonuç: İhlalin ardından CSO, veri işleme uygulamalarını revize etti. Depolanan ve aktarılan tüm hassas verileri şifreledi ve güçlü erişim kontrolleri uygulayarak veritabanına erişimi kısıtladı. Ayrıca, genel dosyalardan gereksiz kişisel bilgileri kaldırarak veri minimizasyonu uyguladı. CSO, uyumluluğu denetlemek üzere bir veri koruma görevlisi atadı ve açık bir gizlilik politikası taslağı hazırladı. Personele uygun veri işleme konusunda eğitim verildi ve gelecekte paylaşımlar güvenli bağlantılar ve şifreler kullanılarak yapıldı. CSO, güvenliği hızla sıkılaştırarak ve iyileştirmeleri şeffaf bir şekilde raporlayarak bağışçılarının güvenini yeniden kazandı.

Tartışma Soruları:

- *Bu ihlale hangi veri koruma hataları yol açtı ve bunlar nasıl önlenebilirdi?*
- *CSO, olaydan sonra (bu modülün konularından) hangi veri koruma uygulamalarını benimsedi?*
- *CSO'nun bu ihlali ele almak için hangi yasal yükümlülükleri vardı ve uyum CSO'lar için neden önemlidir?*

Modül 5 Değerlendirme

Bu modül, beş kısa soru ve bir küçük görevle değerlendirilecektir. Geçmek için en az %70 puan alınması gerekir.

Modül 5 Değerlendirme

Kısa Sorular

1. CSO'lar genellikle ne tür kişisel veya hassas veriler toplar ve bu veriler neden korunmalıdır?
2. Veri minimizasyonu ilkesini açıklayın ve bir CSO'nun bunu nasıl uygulayabileceğine dair pratik bir örnek verin.
3. Saklanan verilerin şifrelenmesi ile aktarılan verilerin şifrelenmesi arasındaki fark nedir?
4. GDPR (veya eşdeğer ulusal veri koruma yasaları) kapsamında, kişisel veri ihlali durumunda bir CSO'nun yapması gerekenler nelerdir?
5. Yasal uyumluluğun ötesinde, etik veri işleme CSO'lar için neden önemlidir? Verileri uygun şekilde korumamanın olası sonuçlarından birini belirtin.

Pratik Görev: Mini Veri Koruma İncelemesi

Katılımcılardan aşağıdaki görevi tamamlamaları istenir:

- CSO tarafından toplanan **kişisel veya hassas verilerin bir türünü** belirleyin (örneğin, yararlanıcı kayıtları, bağışçı iletişim bilgileri, personel bilgileri).
- Kısaca açıklayın:
    - Bu verilerin nerede saklandığı (ör. bilgisayar, bulut hizmeti, e-posta, kağıt dosyalar),
    - Bu verilere kimlerin erişimi var,
    - Bu verileri daha iyi korumak için yapılabilecek bir iyileştirme (ör. şifreleme, sınırlı erişim, veri minimizasyonu).

Katılımcılar cevaplarını **üç ila beş kısa madde halinde** sunmalı veya küçük gruplar halinde kısaca tartışmalıdır.

3.6 **MODÜL 6: SOSYAL MEDYA VE ÇEVRİMİÇİ VARLIK GÜVENLİĞİ – KURUMSAL İTİBAR VE HESAPLARIN KORUNMASI**

Bu modülün sonunda katılımcılar şunları yapabileceklerdir:

- *CSO'nun sosyal medya hesaplarını korumak için güvenlik önlemleri uygulamak (güçlü, benzersiz şifreler, iki faktörlü kimlik doğrulama, sınırlı yönetici rolleri).*
- *Raporlama ve iletişim prosedürlerini izleyerek sosyal medya olaylarına (hesap ele geçirme veya kimlik sahtekarlığı) etkili bir şekilde yanıt vermek.*
- *Güvenli bir çevrimiçi varlığı sürdürmek için en iyi uygulamaları uygulamak (web sitesi/CMS'nin düzenli güncellemeleri, yanlış bilgilere yanıt verme ve bunları yayınlama konusunda personel kılavuzları).*

Öğrenim Hedefleri:

- CSO'nun sosyal medya hesaplarını korumak için güvenlik önlemleri uygulamak (güçlü kimlik doğrulama, izlenen erişim, hesap ayarlarının düzenli denetimleri).
- Hesap ele geçirme, kimlik sahtekarlığı veya yanlış bilgi saldırılarına nasıl yanıt verileceği dahil olmak üzere, kuruluşun çevrimiçi varlığını ve itibarını korumak için stratejiler geliştirin.
- İnternette tutarlı ve güvenli bir kurumsal temsil sağlamak için web sitesi içeriği yönetimi ve personelin çevrimiçi davranışları için en iyi uygulamaları uygulayın.

Ana Konular:

- **Sosyal medya hesabı güvenliği:** Tüm kuruluşun sosyal medya hesaplarının güçlü, benzersiz şifreler kullanmasını ve iki faktörlü kimlik doğrulamanın etkinleştirilmesini sağlamak. Birden fazla yöneticiyi güvenli bir şekilde yönetmek (şifreleri paylaşmak yerine rol tabanlı erişim denetimleri veya ekip işbirliği özelliklerini kullanmak).
- **Hesap izleme ve kurtarma:** Hesap etkinliklerini takip etmek (böylece yetkisiz erişimler erken tespit edilir) ve hesaplar ele geçirildiğinde nasıl kurtarılacağını bilmek (hacklenen hesaplar için platform destek süreçlerini anlamak).
- **Hesap ele geçirme ve kimlik sahtekarlığı ile başa çıkma:** CSO'nun hesabı ele geçirilirse veya sahte hesaplar CSO'nun kimliğine bürünürse atılması gereken adımlar – sosyal

platformlarında bildirim mekanizmaları, yanlış bilgileri açıklığa kavuşturmak için destekçilerle iletişim kurma ve hesapların kontrolünü geri kazanma dahil.

- **Çevrimiçi taciz ve yanlış bilgilerle başa çıkma:** Trollere veya koordineli taciz kampanyalarına yanıt verme taktikleri (ör. tacizi belgeleme, engelleme/bildirme işlevlerini kullanma, yorumlar için moderasyon politikası oluşturma). Yanlış iddiaları abartmadan, gerçeklere dayalı mesajlarla çevrimiçi yanlış bilgilere veya iftiraya nasıl karşı koyulacağı.
- **Web sitesi ve içerik yönetimi güvenliği:** STK'nın web sitesini güvenli ve saygın tutmak – web sitesi CMS/eklentilerini düzenli olarak güncellemek, site yöneticileri için güvenli şifreler kullanmak, içerik yayınlayabilecek kişileri sınırlamak ve yanlış veya yetkisiz içeriği hızlı bir şekilde düzeltmek veya kaldırmak için bir süreç oluşturmak.
- **İtibar yönetimi:** CSO'nun olumlu ve güvenli bir çevrimiçi varlığını sürdürmek için, personeli ve gönüllüleri kuruluşu çevrimiçi olarak temsil etme kuralları konusunda eğitmek (kişisel sosyal medya kullanım politikaları, iş hakkında ne yayınlamamaları gerektiği, yanlış bilgi gördüklerinde nasıl tepki vermeleri gerektiği).

Örnek Faaliyetler veya Alıştırmalar:

- **Hesap Güvenliği Kontrolü:** Katılımcılar, STK'nın sosyal medya hesaplarından birini hızlı bir şekilde denetler. 2FA'nın etkinleştirilip etkinleştirilmediğini, şifrelerin güçlü/yakın zamanda güncellenmiş olup olmadığını, kurtarma iletişim bilgilerinin doğru olup olmadığını ve yalnızca yetkili kişilerin erişimi olup olmadığını doğrularlar. Ardından, gerekli iyileştirmeler için bir yapılacaklar listesi oluştururlar.
- **Olay Rol Oyunu:** CSO'nun resmi sosyal medya hesabının ele geçirildiği veya sahte bir hesabın kuruluş hakkında yanlış bilgiler yaydığı bir senaryo simüle edilir. Ekip, acil bir eylem planı belirlemelidir: kamuoyuna kim bilgi verecek, platform ve takipçileri nasıl uyaracak ve hesabı güvence altına almak veya kurtarmak için hangi adımlar atılacak. Rol oyununun ardından, yanıtlarında nelerin iyi gittiği ve nelerin iyileştirilebileceği tartışılır.
- **Taciz Müdahale Planı:** Katılımcılar gruplar halinde, çevrimiçi taciz veya nefret kampanyalarıyla başa çıkmak için basit bir protokol hazırlar. Bu protokol, öfkeyle kamuoyuna açıklama yapmamak, rahatsız edici gönderileri belgelemek, bunları

platforma bildirmek, CSO yönetimini uyarmak ve hedef alınan personeli desteklemek gibi adımları içerebilir. Gruplar planlarını paylaşır ve ortak unsurları tartışır.

- **Yerel Örnek Tartışma:** [CSO'nun dahil olduğu, sosyal medya ile ilgili yakın zamanda meydana gelen bir olayı anlatın] – Olanları analiz edin ve sağlam sosyal medya güvenlik uygulamaları ve olay müdahale planının bu tür bir durumu yönetmeye veya önlemeye nasıl yardımcı olabileceğini tartışın.

Modül 6 Vaka Çalışması: Sosyal Medya Hesabı Ele Geçirme

Bağlam: Bir çevre STK'sı, bağışçıları çekmek ve kampanya haberlerini paylaşmak için sosyal medyayı (Twitter ve Facebook) kullanıyor. Birden fazla personel, paylaşılan şifrelerle hesaplara erişebiliyor ve kimse oturum açma faaliyetlerini yakından izlemiyor.

Sorun: Bir sabah, STK'nın Twitter hesabı, STK'nın misyonuyla ilgisi olmayan kışkırtıcı siyasi mesajlar yayınlamaya başladı. Takipçiler kafası karışmış ve bazıları STK'yı siyasi bir tavır almamakla suçlamıştır. Bu mesajlar, bir personel ortak bir şifreyi tekrar kullandığında erişim sağlayan bir hacker tarafından yazılmıştır. Personel ihlali fark ettiğinde, mesajlar destekçiler tarafından retweetlenmiş ve itibar kaybına neden olmuştur. Platformun destek süreciyle erişimi geri kazanmak saatler sürmüş ve bu süre zarfında olumsuz izlenimler çevrimiçi olarak yayılmıştır.

Sonuç: CSO, tüm kanallarda derhal bir açıklama yayınlayarak ve ihlal için özür dileyerek bir olay müdahalesi gerçekleştirdi. Tüm sosyal medya şifrelerini sıfırladılar ve tüm hesaplarda iki faktörlü kimlik doğrulamayı etkinleştirdiler. Ayrıca rol tabanlı erişim kurdular (şifreleri paylaşmak yerine belirli yönetici hesapları atadılar). Personel, web sitesi içeriğini gözden geçirip güncelledi ve eski bilgilerin kalmadığından emin oldu. CSO, hesap faaliyetlerini günlük olarak izlemek için bir politika oluşturdu. Sonuç olarak, normal iletişimi yeniden sağlayabildiler ve daha sonra şeffaf olmaları nedeniyle destek bile kazandılar. Yeni güvenlik önlemleri, başka ele geçirme girişimlerini önledi.

Tartışma Soruları:

- *Hesap ele geçirilmesine neden olan temel hatalar nelerdi?*
- *CSO, hem teknolojik hem de iletişim açısından hasarı azaltmak için nasıl bir yanıt verdi?*

- *CSO, sosyal medyadaki varlığını korumak için hangi güvenlik iyileştirmelerini uyguladı?*

Modül 6 Değerlendirme

Bu modül, beş kısa soru ve bir küçük görevle değerlendirilecektir. Geçmek için en az %70 puan alınması gerekir.

Modül 6 Değerlendirmesi

Kısa Sorular

1. CSO'ların sosyal medya hesaplarında güçlü, benzersiz şifreler ve iki faktörlü kimlik doğrulama kullanması neden önemlidir?
2. Sosyal medya hesap şifrelerinin birden fazla personel arasında paylaşılması ne gibi riskler doğurabilir?
3. CSO'nun sosyal medya hesabı ele geçirilirse veya güvenliği ihlal edilirse, CSO'nun hemen alması gereken önlemler nelerdir?
4. Çevrimiçi yanlış bilgiler veya kimlik hırsızlığı, CSO'nun itibarını ve kamuoyunun güvenini nasıl etkileyebilir?
5. Çevrimiçi davranışlar ve kuruluşun temsiline ilişkin net personel yönergelerine sahip olmak neden önemlidir?

Pratik Görev: Sosyal Medya Güvenliği İncelemesi

Katılımcılardan aşağıdaki görevi tamamlamaları istenir:

- CSO'larının (veya varsayımsal bir CSO'nun) resmi sosyal medya hesaplarından birini seçin.
- Kısaca açıklayın:
    - İki faktörlü kimlik doğrulamanın etkinleştirilip etkinleştirilmediği
    - Erişimin şu anda nasıl yönetildiğini (paylaşılan şifreler mi, rol tabanlı erişim mi),
    - Bu hesabın güvenliğini veya izlenmesini iyileştirebilecek somut bir eylem.

Katılımcılar cevaplarını üç ila beş kısa madde halinde özetlemeli veya küçük gruplar halinde kısaca tartışmalıdır.

3.7 MODÜL 7: GÜVENLİK KÜLTÜRÜ GELİŞTİRME – PERSONEL EĞİTİMİ, POLİTİKALAR VE OLAYLARA MÜDAHALE

Bu modülün sonunda katılımcılar şunları yapabileceklerdir:

- *Liderlik ve personeli dahil ederek kuruluşta güvenlik bilincine sahip bir kültür oluşturmak.*
- *Temel BT güvenlik politikaları (ör. kabul edilebilir kullanım, BYOD, şifre kuralları) geliştirmek ve tüm personel için düzenli güvenlik eğitimi planlamak.*
- *Siber olayları verimli bir şekilde ele almak için basit bir olay müdahale planı (roller, adımlar ve iletişim tanımları) oluşturmak ve prova yapmak.*

Öğrenim Hedefleri:

- CSO içinde, her personelin siber güvenliği sağlamadaki kişisel rolünü anladığı, güvenlik bilincine sahip bir kültür oluşturmak.
- Temel BT güvenlik politikaları (ör. teknolojinin kabul edilebilir kullanımı, kendi cihazını getir kuralları) geliştirin ve iyi güvenlik uygulamalarını pekiştirmek için düzenli personel eğitim programları uygulayın.
- Kuruluşun siber güvenlik olaylarına etkili bir şekilde yanıt verebilmesi için bir olay müdahale planı oluşturun ve prova yapın (adımları, rolleri ve iletişim kanallarını açıkça tanımlayın).

Ana Konular:

- **Siber güvenlik kültürü oluşturmak:** Güvenlik girişimleri için liderlerin desteğini ve personelin katılımını nasıl sağlayabilirsiniz? Çalışanların güvenliği yalnızca BT personelinin görevi olarak görmek yerine, veri ve sistemleri korumaktan sorumlu olduklarını hissettikleri bir ortam yaratmak.
- **Temel güvenlik politikaları:** Teknolojinin güvenli kullanımı için beklentileri belirleyen basit ve açık politikalar hazırlamak. Örnekler arasında Kabul Edilebilir Kullanım Politikası (iş cihazlarında ve hesaplarında izin verilen/yasaklananlar), personel iş için kişisel cihazlarını kullanıyorsa BYOD (kendi cihazını getir) yönergeleri ve şifre oluşturma ve yönetme kuralları sayılabilir.

- **Sürekli personel farkındalığı ve eğitimi:** Güvenlik bilgilerini güncel tutmak için eğitimlerin (atölye çalışmaları, haber bültenleri, kimlik avı simülasyon testleri) önemini vurgulamak. Eğitimsiz personel, güvenlik konusunda en zayıf halka haline gelebileceğinden, düzenli eğitimin hayati önem taşıdığını belirtmek.
- **Olay müdahale planlaması:** Olay müdahale planının temel bileşenleri – bir olayı nasıl tespit edip raporlayacağınız, sorunu kontrol altına almak için acil adımlar (ör. etkilenen bilgisayarların bağlantısını kesmek), roller ve sorumluluklar (müdahaleyi kim yönetir, paydaşlarla kim iletişim kurar) ve kesintiler sırasında operasyonları nasıl sürdüreceğiniz.
- **Olayları raporlama ve olaylardan ders çıkarma:** Siber olayları yetkililere veya düzenleyicilere ne zaman ve nasıl raporlayacağınız (özellikle kişisel veriler söz konusuysa) ve gelecekteki dayanıklılığı artırmak için olay sonrası inceleme yapma konusunda kılavuzlar.

Örnek Etkinlikler veya Alıştırmalar:

- **Politika Yazma Atölyesi:** Katılımcılar, CSO'larıyla ilgili kısa bir güvenlik politikası taslağı oluşturur (örneğin, ofis bilgisayarları için Kabul Edilebilir Kullanım Politikası veya Mobil Cihaz Politikası). Her grup birkaç temel kural yazar ve ardından bunları herkesle paylaşarak, politikaların açık ve uygulanabilir olmasını sağlamak için geri bildirim ister.
- **Güvenlik Farkındalığı Tatbikatı:** Sahte kimlik avı tatbikatı veya sürpriz bir "USB bırakma" tatbikatı düzenleyin (bulunmuş gibi bir USB bellek bırakarak, kimsenin takıp takmadığını kontrol edin). Ardından sonuçları tartışın: Personel nasıl tepki verdi? Dikkat çeken noktalar nelerdi? Bunu, güvenli bir ortamda eğitim konularını pekiştirmek için bir öğrenme fırsatı olarak kullanın.
- **Olay Müdahale Masaüstü Simülasyonu:** Varsayımsal bir siber güvenlik olayı sunun (örneğin, CSO verilerini şifreleyen bir fidye yazılımı saldırısı). Ekibin adım adım müdahale sürecini gözden geçirmesini sağlayın: sorunun kapsamını nasıl belirliyorlar, ilk olarak kimi arıyorlar, personele ve muhtemelen kamuoyuna nasıl bilgi veriyorlar ve sistemleri veya verileri nasıl kurtarıyorlar? Alıştırma sonrasında, nelerin iyi gittiğini ve planlarında hangi roller veya adımların açıklığa kavuşturulması gerektiğini değerlendirin.

- **Yerel Raporlama Bilgileri:** [Ülkenizin siber olay raporlama mekanizmasını veya ilgili yetkili makamın iletişim bilgilerini buraya ekleyin] – Katılımcıların, yerel bağlamda ciddi bir siber güvenlik olayını nasıl raporlayacaklarını bildiklerinden emin olun (örneğin, ulusal CERT veya kolluk kuvvetlerine bildirimde bulunmak) ve ülkelerindeki CSO'lar için geçerli olan ihlal raporlamasına ilişkin yasal gereklilikleri tartışın.

Modül 7 Vaka Çalışması: Güvenli Olmayan USB'nin Kötü Amaçlı Yazılım Salgınına Yol Açması

Bağlam: Bir CSO ofisi, çalışanların iş bilgisayarlarında kişisel USB sürücülerini kullanmasına izin verdi. Çıkarılabilir medya kullanımıyla ilgili yazılı bir politika veya eğitim yoktu. Yeni bir gönüllü, sık sık kendi USB belleğini kullanıyordu.

Sorun: Bir gün, bir personel ofis otoparkında bir USB sürücü buldu (muhtemelen biri düşürmüştü). Merak eden çalışan, USB'yi ofis bilgisayarına taktı ve içindeki bir belgeyi açtı. USB, kötü amaçlı yazılımla enfekteydi. Kötü amaçlı yazılım, CSO'nun ağına hızla yayıldı ve birden fazla bilgisayardaki dosyaları şifreledi. CSO'nun verilerine erişilemez hale geldi ve operasyonlar kesintiye uğradı. Olay müdahale planının olmaması kafa karışıklığına neden oldu: kimse müdahaleyi kimin yöneteceğini veya kime haber vereceğini bilmiyordu.

Sonuç: Etkilenen makinelerin bağlantısını keserek salgını kontrol altına aldıktan sonra, CSO bir BT uzmanı ile anlaşarak son yedeklemelerden verileri kurtardı. Yedeklemelerin çoğu verinin geri yüklenmesine yardımcı olduğunu fark ettiler. CSO daha sonra sıkı politikalar uyguladı: resmi bir Kabul Edilebilir Kullanım Politikası yazıldı (onaylanmamış USB sürücülerinin kullanımını yasaklayan ve tüm harici ortamların taranmasını gerektiren) ve tüm personel, şüpheli cihazları ve ekleri tanıma konusunda eğitim aldı. Ayrıca, basit bir olay müdahale planı geliştirdiler, bir müdahale ekibi atadılar ve gelecekteki olaylarda izlenecek açık adımlar belirlediler (ilk olarak kimi arayacakları ve paydaşlarla nasıl iletişim kuracakları dahil). Daha sonra, küçük bir kimlik avı olayı sırasında, CSO yeni planı kullanarak olayı başarıyla kontrol altına aldı ve hasarı en aza indirdi.

Tartışma Soruları:

- *Bu olayın meydana gelmesine neden olan eksik politikalar veya uygulamalar nelerdir?*

- *Son zamanlarda yapılan yedeklemeler ve müdahale ekibinin olması, olayın sonucunu nasıl etkiledi?*
- *CSO olaydan sonra hangi yeni önlemleri ve planları uyguladı ve bunlar gelecekteki olayları önlemek için neden önemlidir?*

Modül 7 Değerlendirme Notu

Bu modül, beş kısa soru ve bir küçük görevle değerlendirilecektir. Geçmek için en az %70 puan alınması gerekir.

Modül 7 Değerlendirme

Kısa Sorular

1. CSO bağlamında "güvenlik kültürü" ne anlama gelir ve bunu oluşturmak için personel katılımı neden önemlidir?
2. Temel BT güvenlik politikaları (Kabul Edilebilir Kullanım veya BYOD politikaları gibi) CSO'lar için neden önemlidir?
3. Düzenli personel eğitimi ve farkındalık faaliyetleri, bir kuruluşun siber güvenlik risklerini nasıl azaltabilir?
4. CSO için basit bir olay müdahale planının temel unsurları nelerdir?
5. Siber güvenlik olayları meydana geldikten sonra bunları gözden geçirmek ve bunlardan ders çıkarmak neden önemlidir?

Pratik Görev: Mini Güvenlik Kültürü Eylem Planı

Katılımcılardan aşağıdaki görevi tamamlamaları istenir:

- CSO'larının güvenlik kültürünü güçlendirmek için alabilecekleri somut bir önlemi belirleyin (örneğin, basit bir Kabul Edilebilir Kullanım Politikası uygulamaya koymak, yıllık güvenlik eğitimi düzenlemek veya olay müdahale irtibat kişisini belirlemek).
- Kısaca açıklayın:
    - Bu eylemden kim sorumlu olacak?
    - Bu eylem personele nasıl iletilecek,
    - Bu eylemin siber güvenlik olaylarını önlemeye veya azaltmaya nasıl yardımcı olacağı.

Katılımcılar cevaplarını üç ila beş kısa madde halinde sunmalı veya küçük gruplar halinde kısaca tartışmalıdır.

3.8 MODÜL 8: İLERİ DÜZEY KONULAR – ORTAYA ÇIKAN TEHDİTLER VE ARAÇLAR

Bu modülün sonunda katılımcılar şunları yapabileceklerdir:

- *Gelişmiş siber tehditleri (hedefli kimlik avı ve sahtekarlık gibi) tanıyacak ve doğrulama yöntemlerini (alternatif kanallar aracılığıyla istekleri onaylama gibi) uygulayabilecek.*
- *Gelişmiş güvenlik araçlarını uygun şekilde kullanmak (ör. kritik hesaplar için donanım güvenlik anahtarları, anormallikler için ağ izleme, tehdit istihbaratı kaynakları).*
- *CSO'nun kapasitesi ve ihtiyaçlarına göre kurumsal güvenlik iyileştirmeleri (kurumsal şifre yöneticileri veya saldırı tespit sistemleri kullanımı gibi) planlayabilecek.*

Öğrenim Hedefleri:

- Gelişmekte olan veya sofistike siber tehditleri (gelişmiş kimlik avı teknikleri veya sahtecilik saldırıları gibi) tanımak ve bunlara karşı koymak için doğrulama yöntemlerini öğrenmek.
- CSO'ların ihtiyaçlarına göre uyarlanmış, donanım tabanlı güvenlik (örneğin güvenlik anahtarları), ağ izleme ve tehdit istihbaratı dahil olmak üzere korumayı daha da artırabilecek gelişmiş güvenlik araçlarını ve uygulamalarını keşfedin.
- Kurumsal şifre yöneticileri veya saldırı tespit sistemleri gibi kuruluş genelinde güvenlik iyileştirmelerini nasıl uygulayacağınızı düşünün ve bu gelişmiş önlemlerin CSO'nun kapasitesi için ne zaman uygun olduğunu anlayın.

Ana Konular:

- **Gelişmiş kimlik avı ve sahtecilik:** Üst düzey sosyal mühendislik saldırılarını (CEO dolandırıcılık e-postaları, klonlanmış web siteleri vb.) anlayın ve iletişimi doğrulama tekniklerini öğrenin (örneğin, şüpheli istekleri ikincil bir kanal üzerinden doğrulama veya dijital imzalar kullanma).
- **Donanım güvenlik anahtarları:** SMS veya uygulama 2FA'ya alternatif olarak fiziksel kimlik doğrulama jetonlarına (U2F/FIDO2 anahtarları gibi) giriş. Hesap ele geçirmelerini

önlemek için nasıl çalıştıkları (kimlik avına dayanıklı 2FA) ve bunları personele dağıtmak için dikkate alınması gerekenler.

- **Ağ izleme ve saldırı tespiti:** Bir CSO'nun ağındaki olağandışı etkinlikleri nasıl izleyebileceğine dair temel kavramlar. Saldırı tespit sistemleri (IDS) veya saldırı önleme sistemleri (IPS) gibi araçların basit terimlerle açıklaması ve bu araçların yöneticileri potansiyel ihlallere nasıl uyardığı.
- Kuruluş **genelinde güvenlik araçları:** Tüm kuruluş için şifre yöneticileri gibi gelişmiş araçları uygulamak (tüm personelin güçlü, benzersiz şifreler kullanmasını sağlamak için) veya sivil toplumla ilgili yeni tehditler hakkında güncel bilgi sahibi olmak için tehdit istihbaratı beslemelerini/topluluk uyarılarını kullanmak.
- **Kendi bağlamınıza uyarlama:** Bu gelişmiş önlemlerin isteğe bağlı olduğunu ve CSO'nun teknik uzmanlığı ve kaynaklarına göre ölçeklendirilmesi gerektiğini vurgulamak. Hangi gelişmiş araçların benimsenmeye değer olduğuna karar verme ve personelin bunları etkili bir şekilde kullanmak için eğitilmesini sağlama konusunda rehberlik.

Örnek Etkinlikler veya Alıştırmalar:

- **Spear-Phishing Senaryosu:** Kolaylaştırıcı, yüksek düzeyde hedeflenmiş bir phishing girişiminin bir örneğini sunar (örneğin, bilinen bir fon sağlayıcıdan transfer talebinde bulunan bir e-posta). Katılımcılar, e-posta ile yanıt vermek yerine bir doğrulama adımı (gönderenin resmi telefon numarasını aramak veya e-posta başlığını kontrol etmek gibi) uygular. Bu yaklaşımın sofistike dolandırıcılıkları nasıl engelleyebileceğini tartışın.
- **Donanım Anahtarı Demosu:** Katılımcılar bir donanım güvenlik anahtarını görür veya dener. Eğitmen, anahtarı bir hesaba kaydettikten sonra anahtarı kullanarak oturum açma işlemini adım adım gösterir. Mümkünse, gönüllülerin bu işlemleri bir demo hesabında denemelerine izin verin, böylece bu cihazların nasıl çalıştığını açıklayın ve güvenlik avantajlarını vurgulayın.
- **Mini Tehdit Avı:** Basitleştirilmiş bir ağ günlüğü veya varsayımsal bir saldırı tespit sistemi (IDS) örneği sunun. Katılımcılardan girişleri inceleyerek şüpheli herhangi bir şey (örneğin, garip saatlerde birden fazla oturum açma denemesi yapan bilinmeyen bir IP adresi)

bulmalarını isteyin. Bu, ağ izleme araçlarının anormallikleri nasıl ortaya çıkarabileceğini gösterir.

- **Yerel Alaka Tartışması:** [Ülkenizde dikkat çeken gelişmiş bir tehdit veya siber güvenlik aracının bir örneğini ekleyin] – Bu tehdit veya aracın CSO'nun ilgilenmesi veya kullanmayı düşünmesi gereken bir şey olup olmadığını tartışın. Yerel kaynaklar (ulusal CSIRT danışma hizmetleri veya siber güvenlik toplulukları gibi) CSO'nun bu tür gelişmiş tehditlerle başa çıkmasına nasıl yardımcı olabilir?

Modül 8 Vaka Çalışması: CEO Dolandırıcılık Girişimi Engellendi

Bağlam: Bir CSO, çok sayıda uluslararası bağışçının yer aldığı büyük bir hibe projesini yönetiyordu. Personel temel güvenlik konusunda deneyimliydi, ancak yüksek düzeyde hedefli saldırılarla daha önce karşılaşmamıştı. Kuruluş, kısa süre önce kilit yöneticileri için donanım güvenlik anahtarları kullanmaya başlamış ve gelişmiş güvenlik araçlarını gözden geçirmişti.

Sorun: CSO'nun finans sorumlusu, sözde icra direktöründen gelen acil bir e-posta aldı ve proje malzemeleri için yeni bir tedarikçiye büyük bir havale yapılmasını talep ediyordu. E-posta, bariz bir kimlik avı belirtisi olmadan meşru görünüyordu. Yetkili, talebi doğrulamayı hatırlayana kadar işlemi gerçekleştirmeye hazırlanıyordu. Ofisteki direktörü aradı. Direktör, şaşkın bir şekilde, böyle bir e-posta göndermediğini söyledi. Hemen bunun sofistike bir e-posta sahtekarlığı girişimi (CEO dolandırıcılığı) olduğunu anladılar. Direktörün hesapları için donanım güvenlik anahtarları kullanıldığı için saldırgan, direktörün giriş bilgilerini ele geçirmemişti; bu tamamen sahte bir e-postaydı.

Sonuç: CSO personeli, saldırganın adresinden gelen tüm e-postaları engelledi ve dolandırıcılık girişimini bildirdi. Gelecekteki girişimleri önlemek için CSO, olağandışı taleplerin doğrulanması (ayrı kanallar kullanılarak) konusunda bir brifing düzenledi ve şüpheli kimlik avı girişimlerine yönelik adımları içerecek şekilde olay müdahale kontrol listesini güncelledi. Ayrıca, yüksek ayrıcalıklı hesaplar için güvenlik anahtarlarını daha yaygın olarak kullanmaya karar verdiler. Bu önlemler sayesinde CSO, herhangi bir mali kayıp yaşamadı ve personel, gelişmiş kimlik avı saldırılarının tespit edilip önlenebileceğine olan güvenini artırdı.

Tartışma Soruları:

- *CSO, fonlar kaybedilmeden dolandırıcılık girişimini nasıl tespit etti ve önledi?*
- *Bu senaryoda donanım güvenlik anahtarları ve doğrulama prosedürü ne gibi bir rol oynadı?*
- *CSO, bu olayın sonucunda (bu modülden) hangi gelişmiş güvenlik iyileştirmelerini uygulamaya karar verdi?*

Modül 8 Değerlendirme

Bu modül, beş kısa soru ve bir küçük görevle değerlendirilecektir. Geçmek için en az %70 puan alınması gerekir.

Modül 8 Değerlendirmesi

Kısa Sorular

1. Gelişmiş kimlik avı veya sahtecilik saldırılarını temel kimlik avı girişimlerinden daha tehlikeli kılan nedir?
2. CEO dolandırıcılığı nedir ve CSO'lar bu tür saldırılara neden özellikle savunmasızdır?
3. Donanım güvenlik anahtarları geleneksel iki faktörlü kimlik doğrulama yöntemlerinden nasıl farklıdır ve neden kimlik avına karşı dirençli olarak kabul edilirler?
4. Bir kuruluşta ağ izleme veya saldırı tespit sistemlerinin amacı nedir?
5. CSO'lar, gelişmiş güvenlik araçlarını uygulamaya koymadan önce kapasitelerini ve ihtiyaçlarını neden dikkatlice değerlendirmelidir?

Pratik Görev: Gelişmiş Tehdit Hazırlık Kontrolü

Katılımcılardan aşağıdaki görevi tamamlamaları istenir:

- CSO'larıyla ilgili **bir gelişmiş tehdit** belirleyin (ör. CEO dolandırıcılığı, hedefli kimlik avı, hesap sahtekarlığı).
- Kısaca açıklayın:
    - Şüpheli taleplere yanıt vermeden önce personelin alması gereken bir doğrulama adımı,
    - Riski azaltmaya yardımcı olabilecek bir gelişmiş güvenlik aracı veya uygulaması (ör. donanım güvenlik anahtarları, şifre yöneticileri, doğrulama prosedürleri),
    - Bu önlemin şu anda CSO'ları için uygulanabilir olup olmadığı ve nedeni.

Katılımcılar cevaplarını üç ila beş kısa madde halinde sunmalı veya küçük gruplar halinde kısaca tartışmalıdır.

4 . ÜLKE BAZLI YASAL VE DÜZENLEYİCİ ÇERÇEVELER

4.1 Türkiye'deki Yasal ve Düzenleyici Çerçeve ve Türkiye'deki STK'lara Öneriler

Kişisel Verilerin Korunması Kanunu'nun (KVKK) Kapsamı ve STK'lar Üzerindeki Etkisi

Kişisel Verilerin Korunması Kanunu (KVKK) No. 6698, Türkiye'de kişisel verilerin işlenmesini düzenleyen birincil mevzuattır. Kanun, kamu kurumları, özel sektör kuruluşları ve sivil toplum kuruluşları (STK'lar) dahil olmak üzere kişisel verileri işleyen tüm gerçek ve tüzel kişilere uygulanır (Kişisel Verilerin Korunması Kurumu [KVKK], 2020).

STK'lar genellikle üyeleri, gönüllüleri, bağışçıları ve çalışanları ile ilgili kişisel verileri toplar ve işler. Bu veriler arasında isimler, iletişim bilgileri, fotoğraflar, bağış tutarları ve etkinlik katılım kayıtları yer alabilir. Bu nedenle, STK'lar da KVKK kapsamında veri sorumlusu olarak yükümlülükler taşımaktadır.

Kanuna göre, kişisel veriler yalnızca belirli, açık ve meşru amaçlar için işlenebilir ve işleme amacı ortadan kalktığında silinmeli veya anonim hale getirilmelidir. STK'lar, üyelik formlarından dijital kampanyalara kadar tüm veri toplama süreçlerinde bu ilkelere uygun hareket etmelidir.

STK'ların KVKK'ya Uyum Sağlamak İçin Atması Gereken Adımlar

Sivil toplum kuruluşlarının KVKK'ya uymak için izlemesi gereken başlıca adımlar şunlardır:

1. **Veri Envanterinin Hazırlanması:** STK'lar, hangi kişisel verileri hangi amaçlarla işlediklerini, verilerin ne kadar süreyle saklandığını ve kimlerle paylaşıldığını belirlemeli ve belgelemelidir.
2. **Açık Rıza Alınması:** Yasal olarak zorunlu olmayan işleme faaliyetleri (örneğin, tanıtım amaçlı e-postalar) için açık rıza alınmalıdır. Rıza, özgürce verilmeli, bilgilendirilmiş olmalı ve herhangi bir zamanda geri alınabilmelidir.
3. **Bilgilendirme Yükümlülüğü:** Kişisel verileri toplanan kişiler, verilerini kimin işlediği, hangi amaçlarla, hangi yasal dayanaklarla ve haklarının neler olduğu konusunda yazılı olarak bilgilendirilmelidir.
4. **Veri Güvenliği Önlemleri:** Fiziksel (kilitli dolaplar), dijital (şifreleme, antivirüs yazılımı, erişim kısıtlamaları) ve organizasyonel (gizlilik anlaşmaları, farkındalık eğitimi) önlemler alınmalıdır.

5. **VERBIS Kaydı:** Faaliyetleri yalnızca kendi üyeleri, gönüllüleri ve bağışçılarıyla sınırlı olan STK'lar VERBIS kaydından muaftır. Ancak, ekonomik faaliyette bulunan STK'ların sisteme kaydolması zorunludur (KVKK, 2020).

KVKK İhlalleri ve Yaptırımlar

KVKK, ihlaller durumunda idari para cezaları ve bazı durumlarda cezai yaptırımlar öngörmektedir (KVKK, 2020). STK'lar veri güvenliği yükümlülüklerini yerine getirmezlerse, veri ihlalleri, yetkisiz veri paylaşımı veya ihlallerin bildirilmemesi durumunda önemli para cezaları ile karşı karşıya kalabilirler.

2024 itibariyle, idari para cezaları ihlalin niteliğine bağlı olarak 25.000 TL (569 $) ile 1.800.000 TL arasında değişmektedir. Örneğin, kayıt yükümlülüğüne tabi bir STK'nın VERBIS'e kaydolmaması ciddi bir ihlal teşkil eder.

KVKK Kurulu, CSO'lara da yaptırımlar uygulamıştır. 2020 yılında, bir dernek, yetkisiz SMS iletişimi ile ilgili bir şikayetin ardından, açık rıza vermemesi ve kişisel verileri silmemesi nedeniyle para cezasına çarptırılmıştır. Bu, CSO'ların kanun kapsamında denetim ve yaptırım tedbirlerine tabi olduğunu göstermektedir.

Siber Güvenlik Kanunu ve Bildirim Yükümlülükleri

Siber Güvenlik Kanunu No. 7545, 2025 yılından itibaren yürürlüğe girmiştir ve kamu ve özel kuruluşlar arasında ayrım yapmaksızın dijital ortamlarda hizmet sunan tüm kurumları kapsamaktadır (Resmi Gazete, 2024). Bu çerçeve içinde, CSO'lar da olay bildirim yükümlülüklerine tabidir.

Bir veri ihlali, kötü amaçlı yazılım bulaşması, siber saldırı veya bir STK'nın sistemlerinde kritik bir güvenlik açığı tespit edilmesi durumunda, olay en geç 48 saat içinde Türkiye Cumhurbaşkanlığı'na bağlı Siber Güvenlik Genel Müdürlüğü'ne bildirilmelidir.

Bu yükümlülüğe uyulmaması, 1.000.000 TL'den başlayan idari para cezaları ve bazı durumlarda sorumlu kişilere hapis cezası gibi cezai yaptırımlarla sonuçlanabilir. Bu düzenleme, tüm STK'lar için güvenlik ve şeffaflık konusunda temel bir yükümlülük getirmektedir.

Ulusal Siber Güvenlik Stratejisi ve CSO'ların Rolü

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028, Türkiye'nin dijital güvenlik vizyonunu tanımlayan temel belgedir. Belge, kamu kurumlarına, özel sektöre ve STK'lara belirli roller atamaktadır (Ulaştırma ve Altyapı Bakanlığı, 2023).

Sivil toplum kuruluşlarından beklenen temel görevler arasında halkın bilinçlendirilmesi, bireysel dijital güvenlik okuryazarlığının teşvik edilmesi ve çocuklar ve yaşlılar gibi savunmasız gruplar için dijital okuryazarlık faaliyetlerinin yürütülmesi yer almaktadır.

Ayrıca strateji, sivil toplum katılımının önemini vurgulamakta ve STK'ları kamu kurumlarıyla işbirliği içinde kampanyalar ve eğitim faaliyetleri yürütmeye teşvik etmektedir.

Dijital Araçların Yasal Durumu

Dijital dönüşümün bir parçası olarak, STK'ların belirli dijital araçları kullanması gerekebilir. 5070 sayılı Elektronik İmza Kanunu uyarınca, elektronik imzalar el yazısı imzalarla aynı hukuki geçerliliğe sahiptir. Bu nedenle, yönetim kurulu kararları, sözleşmeler ve resmi yazışmalar elektronik olarak imzalanabilir (Bilgi ve İletişim Teknolojileri Kurumu, 2023).

Ekonomik faaliyette bulunan veya belirli ciro eşiklerini aşan STK'lar, e-fatura (e-Fatura) ve e-arşiv (e-Arşiv) yükümlülüklerine tabi olabilir. Gelir İdaresi, geçerli eşikleri belirten yıllık bildiriler yayınlamaktadır (Gelir İdaresi, 2024).

Kayıtlı Elektronik Posta (KEP), özellikle yasal geçerliliği sağlamak için resmi bildirimler için tercih edilen bir başka yöntemdir. Tüm bu araçları kullanırken, STK'lar sadece teknik yeterliliği değil, aynı zamanda ilgili yasal çerçeveye tam uyumu da sağlamalıdır.

Türkiye'deki Küçük ve Orta Ölçekli STK'lar için Dijital Güvenlik

Giriş

Aşağıdaki beş orijinal vaka, eğitim amaçlı hazırlanmış olup, Türkiye'de faaliyet gösteren küçük ve orta ölçekli sivil toplum kuruluşlarının (STK'lar) gerçekçi dijital güvenlik risklerine ve deneyimlerine dayanmaktadır. Her vaka, STK'nın yapısını, yaşanan olayı, ilgili teknik veya insani zafiyetleri, sonuçları ve diğer STK'lar için çıkarılabilecek dersleri açıkça sunmaktadır. Bu çalışmada tüm STK'lar anonim olarak sunulmuştur.

TÜRKİYE'DEN YEREL VAKA ÇALIŞMALARI

Vaka 1: Sahte E-posta Tuzağının Neden Olduğu Baş Ağrısı

Bu STK, yerel öğrencilere burs ve eğitim desteği sağlamayı amaçlayan, sadece dört çalışan ve birkaç gönüllü ile faaliyet gösteren küçük bir eğitim derneğidir. Dijital faaliyetleri ağırlıklı olarak e-posta iletişimi, ofis yazılımları ve gönüllülerle WhatsApp üzerinden koordinasyona dayanmaktadır. Kuruluşun özel bir BT personeli yoktur ve çalışanlar genellikle iş için kişisel dizüstü bilgisayarlarını kullanmaktadır.

"Bir gün, derneğin genel info@... posta kutusuna "Bakanlık Eğitim Hibesi" konulu bir e-posta gelir. Mesajda, kuruluşun başvurduğu hibeye hak kazandığı iddia edilir ve ayrıntılar için ekli PDF dosyasının açılması istenir. Bu haberden heyecanlanan proje sorumlusu, dosyanın gerçekliğini doğrulamadan eki indirir ve açar. Dosya düzgün açılmaz, ancak bilgisayara sessizce kötü amaçlı bir yazılım yüklenir."

Bu durumda ana güvenlik açığı, insan hatası ve farkındalık eksikliğidir. Çalışan, siber güvenlik eğitimi almamış ve gönderen adresini, dil hatalarını ve şüpheli eki dikkatlice incelememiştir. Bunlar, resmi bir kurumu taklit etmek için tasarlanmış bir kimlik avı e-postasının açık göstergeleridir.

Bir gün içinde, proje sorumlusu ve yönetim kurulu tarafından kullanılan paylaşımlı e-posta hesapları ele geçirildi. Saldırganlar, bağışçılara ve ortaklara para talep eden sahte mesajlar gönderdi. İletişim kesintiye uğradı, güven sarsıldı ve bazı destekçiler geçici olarak katılımlarını askıya aldı. Orta vadede, kuruluş güvenilirliğini ve iç morali geri kazanmak için zaman ve çaba harcamak zorunda kaldı.

Çıkarılan Dersler ve Öneriler

Kimlik avı saldırıları, STK'lar için en yaygın siber tehditlerden biridir. Tüm personel ve gönüllüler, şüpheli e-postaları tanımlamak için eğitilmelidir. Gönderen adresleri, ekler ve acil talepler her zaman doğrulanmalıdır. Temel siber hijyen uygulamaları ve kritik hesaplar için iki faktörlü kimlik doğrulama uygulanmalıdır.

Vaka 1: Sahte E-posta Tuzağının Neden Olduğu Baş Ağrısı

İlgili Modüller

- Modül 4: Yaygın siber tehditler (Kimlik Avı ve Kötü Amaçlı Yazılım)
- Modül 5: Veri Koruma ve Gizlilik Uyumluluğu
- Modül 7: Güvenlik Kültürü Geliştirme

Bu Vaka Eğitimde Nasıl Kullanılabilir

- **Farkındalık Artırma Örneği (Modül 4):**
  Bu vaka, modülün başında küçük CSO'ları hedef alan **gerçekçi** bir **kimlik avı senaryosu** olarak sunulabilir. Eğitmenler, sonucu açıklamadan önce katılımcılardan e-postadaki uyarı işaretlerini (gönderen adresi, ek, aciliyet, dil hataları) belirlemelerini isteyebilir.
- **İnsan Hatası Tartışması (Modül 7):**
  Bu vakayı, siber güvenliğin sadece teknik bir sorun değil, aynı zamanda **insan davranışı ile ilgili** bir **sorun** olduğunu vurgulamak için kullanın. Özellikle BT personeli olmayan küçük STK'larda personel ve gönüllüleri eğitmenin neden kritik öneme sahip olduğu konusunda tartışma başlatmak için çok uygundur.
- **Hesap Güvenliği Yansıtma (Modül 5):**
  Bu vaka, kimlik avı saldırılarını daha geniş veri koruma riskleriyle ilişkilendirerek, iki faktörlü kimlik doğrulama ve erişim yönetimi dahil olmak üzere **e-posta hesabı koruması** konusundaki tartışmayı destekleyebilir.

Önerilen Yöntem:

Grup tartışması + "Siz olsanız neyi farklı yapardınız?" alıştırması.

Vaka 2: Sosyal Medya Hesabı Ele Geçirme

Bu vaka, yaklaşık 20 personel ve gönüllüden oluşan orta ölçekli bir kadın hakları STK'sını içermektedir. Kuruluş, savunuculuk ve halkın katılımı için Instagram, X (eski adıyla Twitter) ve Facebook gibi sosyal medya platformlarını aktif olarak kullanmaktadır. Hesaplar çoğunlukla bir iletişim görevlisi tarafından yönetilmektedir, ancak gönüllüler de zaman zaman katkıda bulunmaktadır. İki faktörlü kimlik doğrulama etkinleştirilmemiştir.

Bir sabah, kuruluşun resmi Instagram hesabında olağandışı gönderiler görünür. Profil resmi ve biyografi değiştirilir ve takipçilerle sahte yatırımla ilgili içerikler paylaşılır. Üyeler ve takipçiler, hesabın hacklendiğini kuruluşa bildirir.

İletişim sorumlusu, aynı şifreyi birden fazla platformda kullanmıştır. Başka bir hizmetteki veri ihlali, şifrenin açığa çıkmasına neden olmuş ve saldırganların sosyal medya hesabına erişmesine olanak sağlamıştır. İki faktörlü kimlik doğrulamanın olmaması, hesabın ele geçirilmesini daha da kolaylaştırmıştır. Ayrıca, kuruluşun önceden tanımlanmış bir kriz müdahale planı da yoktur.

Kurtarma prosedürleri başlatılırken hesap geçici olarak askıya alınır. Takipçiler alternatif kanallar aracılığıyla uyarılır. Erişime sonunda yeniden izin verilir, ancak itibar kaybı yaşanır ve bazı takipçiler güvenlerini yitirir. Buna karşılık, kuruluş şifre politikalarını güçlendirir ve iki faktörlü kimlik doğrulamayı etkinleştirir.

Öğrenilen Dersler ve Öneriler

Sosyal medya hesapları siber saldırıların sık hedefidir. Güçlü, benzersiz şifreler ve iki faktörlü kimlik doğrulama çok önemlidir. Şifrelerin tekrar kullanılması önlenmeli ve sosyal medyayı yöneten personel, hedefli güvenlik farkındalık eğitimi almalıdır.

Vaka 2: Sosyal Medya Hesabının Ele Geçirilmesi

İlgili Modüller

- **Modül 6: Sosyal Medya ve Çevrimiçi Varlık Güvenliği**
- **Modül 7: Güvenlik Kültürü Geliştirme**

Bu Vaka Eğitiminde Nasıl Kullanılabilir

- **Temel Vaka Çalışması (Modül 6):**
  Bu vaka, sosyal medya güvenliği öğretilirken **birincil vaka çalışması** olarak idealdir. Eğitmenler, katılımcılara olayı adım adım anlatabilir ve başarısızlıkları eksik kontrollere (şifrelerin tekrar kullanılması, 2FA olmaması, müdahale planının olmaması) bağlayabilir.
- **Olay Müdahale Alıştırması (Modül 7):**
  Vaka, katılımcıların takipçileriyle nasıl iletişim kuracaklarına, ihlali platforma nasıl bildireceklerine ve hesabı nasıl kurtaracaklarına karar verdikleri bir rol yapma senaryosuna dönüştürülebilir.
- **Hedefli Eğitim Tartışması:**
  İletişim ve savunuculuktan sorumlu personelin genel eğitimden ziyade özel güvenlik bilincine ihtiyaç duyduğunu vurgulayın.

Önerilen Yöntem:
Vaka analizi + olay müdahale rol oyunu.

Vaka 3: Veri Kaybının ve Yedekleme Eksikliğinin Maliyeti

CSO'nun Türü, Ölçeği ve Dijital Çalışma Uygulamaları

Bu vaka, üç tam zamanlı çalışan ve birkaç gönüllüden oluşan küçük bir çevre CSO'su ile ilgilidir. Proje belgeleri kişisel dizüstü bilgisayarlarda hazırlanır ve bulut hizmetleri aracılığıyla paylaşılır. Ancak, bağışçı listeleri ve mali kayıtlar gibi kritik veriler, düzenli yedeklemeler yapılmadan yalnızca müdürün masaüstü bilgisayarında saklanır.

Bir elektrik kesintisinden sonra, direktörün bilgisayarı sabit disk hasarı nedeniyle yeniden başlatılamamıştır. Verileri yerel olarak kurtarma girişimleri başarısız olmuş ve başarı garantisi olmayan yüksek maliyetli profesyonel veri kurtarma hizmetleri önerilmiştir.

Siber saldırı söz konusu değildir; olay, yetersiz veri yönetimi ve yedekleme stratejisinin olmaması nedeniyle meydana gelmiştir. Önemli verilerin tek bir cihazda saklanması ve eski donanımların kullanılması, veri kaybı riskini önemli ölçüde artırmıştır.

OCSOing projeleri kesintiye uğradı ve önemli raporlar, mali belgeler ve kişi listeleri kayboldu. Personel, kaybolan verileri yeniden oluşturmak için haftalarca uğraştı. Bağışçılar ve ortakların güveni sarsıldı ve kurtarma çalışmaları ve kesintiye uğrayan projeler nedeniyle mali kayıplar meydana geldi.

Çıkarılan Dersler ve Öneriler

Düzenli veri yedeklemeleri, organizasyonun sürekliliği için çok önemlidir. Yedeklemeler birden fazla platformda saklanmalı ve periyodik olarak test edilmelidir. Donanım güncel tutulmalı ve güç koruma sistemleri kullanılmalıdır.

Vaka 3: Veri Kaybının ve Yedekleme Eksikliğinin Maliyeti

İlgili Modüller

- **Modül 5: Veri Koruma ve Gizlilik Uyumluluğu**
- **Modül 7: Güvenlik Kültürü Geliştirme**

Bu Vaka Eğitiminde Nasıl Kullanılabilir

- **Veri Yönetimi Örneği (Modül 5):**
  Bu vaka, tüm güvenlik olaylarının hackerlarla ilgili olmadığını açıklamak için etkilidir. Eğitmenler bu vakayı yedekleme stratejileri, veri kullanılabilirliği ve organizasyonel sürekliliği tanıtmak için kullanabilirler.
- **Risk Değerlendirme Alıştırması:**
  Katılımcılardan kendi CSO'larında kritik verileri listelemeleri ve benzer tekil hata noktaları olup olmadığını belirlemeleri istenebilir.
- **Liderlik Sorumluluğu Tartışması (Modül 7):**
  Bu vaka, veri koruma ve yedeklemenin neden sadece teknik görevler değil, yönetim düzeyinde sorumluluklar olduğunu göstermektedir.

Önerilen Yöntem:
Rehberli yansıtma + mini veri denetim etkinliği.

Vaka 4: Zayıf Şifrelerin ve Paylaşılan Hesapların Tehlikesi

Bu senaryo, engelli kişilere destek veren orta ölçekli bir vakfı konu almaktadır. Yaklaşık 15 personel ve gönüllü, günlük işlemler için paylaşılan e-posta ve sistem hesaplarını kullanmakta ve birden fazla platformda tek bir kullanıcı adı ve şifre kullanmaktadır.

Bağışçı, para talep eden şüpheli mesajlar aldığını bildirmiştir. Soruşturma, eski bir gönüllünün ayrılmasından sonra şifrelerin hiç değiştirilmediği için paylaşılan hesaplara hala erişimi olduğunu ortaya çıkarmıştır. Bu kimlik bilgileri daha sonra yetkisiz kişiler tarafından kötüye kullanılmıştır.

Zayıf ve paylaşılan şifreler, şifrelerin tekrar kullanılması ve erişim iptal prosedürlerinin olmaması ciddi bir güvenlik açığı yaratmıştır. Kuruluş, personel veya gönüllüler ayrıldığında dijital erişimi yönetmek için net politikalarından yoksundu.

Şifreler derhal değiştirilmiş ve bağışçılar bilgilendirilmiştir. Anlık zarar sınırlı olsa da, itibar kaybı yaşanmıştır. Orta vadede, kuruluş daha güçlü şifre politikaları, bireysel kullanıcı hesapları ve personel farkındalık oturumları uygulamaya koymuştur.

Her hesabın güçlü ve benzersiz bir şifresi olmalıdır. Mümkün olduğunca paylaşılan hesaplardan kaçınılmalı ve personel ayrıldığında erişim hakları derhal gözden geçirilmeli ve iptal edilmelidir. Net iç politikalar çok önemlidir.

Vaka 4: Zayıf Şifrelerin ve Paylaşılan Hesapların Tehlikesi

İlgili Modül(ler)

- **Modül 6: Sosyal Medya ve Çevrimiçi Varlık Güvenliği**
- **Modül 7: Güvenlik Kültürü Geliştirme**
- **Modül 8: İleri Düzey Konular (Hesap Erişimi ve Denetimleri)**

Bu Vaka Eğitiminde Nasıl Kullanılabilir

- **Politika Boşluğu Örneği (Modül 7):**
  Bu vaka, personel veya gönüllüler ayrıldığında **erişim yönetimi politikalarının**, özellikle de işten ayrılma prosedürlerinin eksikliğinin risklerini açıkça göstermektedir.
- **Hesap Güvenliği Tartışması (Modül 6):**
  Eğitmenler bu örneği, özellikle e-posta ve bağışçı iletişimi için bireysel hesapların, güçlü şifrelerin ve rol tabanlı erişimin önemi ile ilişkilendirebilirler.

- **Gelişmiş Erişim Kontrolü Giriş (Modül 8):**
  Bu vaka, hesap denetimleri, şifre yöneticileri ve ayrıcalık yönetimi gibi daha gelişmiş uygulamalara geçiş için bir köprü görevi görebilir.

Önerilen Yöntem:
Vaka temelli politika taslak hazırlama alıştırması (ör. "İşten ayrılma kontrol listesi neleri içermelidir?").

Eğitmenin Notu (Bölümün Sonuna Eklenebilir)

Bu yerel vaka çalışmaları aşağıdaki amaçlarla tasarlanmıştır:

- Türkiye'deki CSO'ların karşılaştığı gerçekçi riskleri yansıtmak,
- Akran öğrenimini ve tartışmayı teşvik etmek,
- Siber güvenlik olaylarının genellikle basit, önlenebilir sorunlardan kaynaklandığını göstermek,
- Sadece teknolojinin değil, politikaların, eğitimin ve hazırlıklı olmanın da önemini vurgulamak.

Eğitmenlerin, katılımcıların kuruluşlarının büyüklüğü, dijital olgunluk düzeyleri ve rollerine göre tartışmanın derinliğini uyarlamaları teşvik edilir.

CSO'lar için Pratik Dijital Güvenlik Politikaları ve Şablonları

Giriş

Bu belge, Türkiye'deki küçük ve orta ölçekli sivil toplum kuruluşlarının (STK'lar) dijital güvenlik kapasitesini güçlendirmek için kullanılabilecek pratik politika şablonlarını sunmaktadır. Şablonlar, basit, uygulanabilir ve hem ulusal mevzuat (Kişisel Verilerin Korunması Kanunu – KVKK, Siber Güvenlik Kanunu) hem de uluslararası iyi uygulamalar (NIST, ENISA, Tactical Tech) ile uyumlu olacak şekilde tasarlanmıştır.

1. Kabul Edilebilir Kullanım Politikası (AUP)

Amaç

Kurumsal dijital araçların, internet erişiminin ve bilgi sistemlerinin sorumlu kullanımını teşvik etmek.

Politika Hükümleri:

- Tüm personel, kuruluşun dijital kaynaklarını yalnızca işle ilgili amaçlar için kullanmalıdır.
- Şifreler kişisel olmalı ve başkalarıyla paylaşılmamalıdır.
- Yasadışı içerik, organizasyonel sistemler aracılığıyla depolanamaz, erişilemez veya dağıtılamaz.
- Sosyal medya kullanımı, kuruluşun itibarına zarar vermemelidir.
- Yönetimin önceden onayı olmadan hiçbir veri kuruluş dışına aktarılamaz.

Not

Bu politika, personel tarafından işe başlarken imzalandıktan sonra yürürlüğe girer ve her yıl gözden geçirilmelidir. (ENISA, 2021)

2. Olay Müdahale Planı (IRP)

Amaç

Olası dijital güvenlik olaylarına hızlı ve etkili bir şekilde müdahale edilmesini sağlamak.

Adımlar:

1. Olayı tespit eden kişi, derhal kuruluş içindeki yetkili makama bilgi verir.
2. Yetkili makam, olayın türünü (kimlik avı, kötü amaçlı yazılım, veri ihlali) belirler.
3. Etkilenen sistemler izole edilir (gerekirse ağdan çıkarılır).
4. Olayla ilgili tüm dijital günlükler ve kayıtlar saklanır.
5. Olay, en geç 48 saat içinde Siber Güvenlik Direktörlüğüne bildirilir (Resmi Gazete, 2024).
6. Olay sonrası değerlendirme yapılır ve prosedürler buna göre güncellenir.

Not

Bu plan, Siber Güvenlik Kanunu No. 7545 ve NIST SP 800-61 Rev. 2'ye dayanmaktadır.

3. Temel Veri Koruma Prosedürü

Amaç

CSO içinde işlenen kişisel verilerin KVKK'ya uygun olarak yönetilmesini sağlamak.

Uygulama:

- Her veri işleme faaliyetinin açık bir amacı olmalı ve veri minimizasyonu ilkesine uygun olmalıdır.
- Kişisel veriler, kanunlarca izin verilmedikçe (KVKK, 2020), açık rıza olmadan işlenemez.
- Her veri paylaşım faaliyeti için paylaşım nedeni, alıcı ve süre belgelendirilmelidir.
- Veri saklama ve imha politikası oluşturulmalıdır; kişisel veriler artık gerekli olmadığında silinmeli veya anonim hale getirilmelidir.
- Kağıt tabanlı kayıtlar kilitli dolaplarda saklanmalı ve dijital veriler şifreli klasörlerde korunmalıdır.

Not:

Kuruluşun bir iç veri denetleyicisi veya sorumlu kişi ataması önerilir.

4. Kimlik Bilgileri ve Cihaz Paylaşımı Protokolü

Amaç

Kuruluş içinde şifrelerin, kullanıcı hesaplarının ve dijital cihazların güvenli kullanımını ve paylaşımını düzenlemek.

Kurallar:

- Şifreler bireysel olarak atanmalı ve yazılmamalıdır.
- Paylaşılan cihazlarda, her kullanıcı ayrı bir hesapla oturum açmalı ve şifreleri paylaşmamalıdır.
- Verilerin harici cihazlara (örneğin kişisel dizüstü bilgisayarlara) aktarılması yasaktır.
- USB sürücüler veya harici depolama cihazlarının kullanımı yalnızca yönetimin onayı ile izin verilir.

Not:

Kuruluşlar ayrıca bir kimlik doğrulama politikası (örneğin, çok faktörlü kimlik doğrulama) tanımlayabilir.

5. Dijital Güvenlik Taahhüdü (Personel / Gönüllüler)

Taahhüt Metni (Örnek):

"Bu belge ile, [Kurum Adı] tarafından sağlanan dijital sistemleri ve araçları yalnızca görevim kapsamında ve gerekli özeni göstererek kullanmayı taahhüt ederim. Kurumsal verilerin güvenliği ile ilgili tüm yükümlülükleri yerine getirme sorumluluğumu kabul ediyorum."

"Bu belgeyle, [Kurum Adı] tarafından tahsis edilen dijital sistem ve araçları yalnızca görev kapsamımda ve dikkatli biçimde kullanacağımı taahhüt ederim. Kurum içi verilerin güvenliği için üzerime düşen yükümlülükleri yerine getireceğimi kabul ederim."

Not:

Bu taahhütname tüm personel ve gönüllüler tarafından imzalanmalı ve personel dosyalarında saklanmalıdır.

Sivil Toplum Kuruluşları için Dijital Güvenlik Kontrol Listeleri

Türkiye'de faaliyet gösteren küçük ve orta ölçekli sivil toplum kuruluşlarının (STK) dijital güvenliğini güçlendirmek için aşağıda dört ayrı kontrol listesi sunulmaktadır. Bu listeler, teknik bilgisi sınırlı kullanıcılar tarafından bile kolayca uygulanabilecek basit ve pratik maddelerden oluşmaktadır. Her kontrol listesi, mevcut yasal düzenlemelere uygun olarak temel güvenlik adımlarını özetlemektedir. Amaç, günlük dijital işlemlerde güvenlik bilincini artırmak ve olası acil durumlara hazırlıklı olmaktır.

1. Temel Dijital Güvenlik Kontrol Listesi

☐ Tüm kullanıcılar güçlü ve benzersiz şifreler kullanıyor mu?

☐ Bilgisayarlarda ve cep telefonlarında otomatik ekran kilidi etkinleştirilmiş mi?

☐ Tüm cihazlarda güncel antivirüs yazılımı yüklü mü?

☐ Tüm yazılım ve uygulamalar düzenli olarak güncelleniyor mu?

☐ Önemli belgeler düzenli olarak yedekleniyor mu (harici sürücü veya bulut depolama)?

☐ Tüm kullanıcılar e-posta eklerini açarken dikkatli davranıyor mu?

☐ Harici veya kişisel cihazların kullanımı izleniyor mu?

2. Olaylara Müdahale Hazırlık Kontrol Listesi

☐ Dijital güvenlikten sorumlu bir kişi atanmış mı?

☐ Olayların kime ve nasıl bildirilmesi gerektiği açıkça tanımlanmış mı?

☐ Tüm personel, olayları (kimlik avı, kötü amaçlı yazılım vb.) tanımak için temel bilgiye sahip mi?

☐ Kritik belgeler ve sistemler yedekleniyor mu?

☐ Olay sonrası prosedür yazılı olarak belirlenmiş mi?

☐ Personel 48 saatlik bildirim kuralından haberdar mı? (7545 sayılı Kanun)

3. Sosyal Medya Güvenliği Kontrol Listesi

☐ Sosyal medya hesaplarına yalnızca yetkili kişiler erişebiliyor mu?

☐ Tüm hesaplarda iki faktörlü kimlik doğrulama (2FA) etkinleştirilmiş mi?

☐ Şifreler güçlü mü ve diğer platformlarda tekrar kullanılmıyor mu?

☐ Hesapları kimin ve hangi amaçla yönettiği açık mı?

☐ İçerik paylaşılmadan önce önceden onaylanıyor mu?

☐ Şüpheli oturum açma işlemleri veya olağandışı takipçi artışları izleniyor mu?

4. Yeni Personel / Gönüllü Bilgi Güvenliği Kontrol Listesi

☐ Yeni personel veya gönüllüler dijital güvenlik oryantasyonu alıyor mu?

☐ Kabul Edilebilir Kullanım Politikası imzalanıyor mu?

☐ Kişisel verilerin işlenmesine ilişkin taahhütler alınmaktadır mı?

☐ Erişim hakları iş sorumluluklarıyla sınırlı mıdır?

☐ Kişisel hesaplar yerine kurumsal hesaplar kullanılıyor mu?

☐ Kurumsal şifre ve cihaz politikalarına uyum sağlanıyor mu?

4.2 Bosna Hersek'teki Yasal ve Düzenleyici Çerçeve ve Bosna Hersek'teki Sivil Toplum Örgütlerine Öneriler

Bosna Hersek'teki Yasal ve Düzenleyici Bağlam

Bosna Hersek'te kişisel verilerin korunması, **Kişisel Verilerin Korunması Kanunu (Zakon o zaštiti ličnih podataka)** ile düzenlenmektedir. Yetkili denetim makamı **Bosna Hersek Kişisel Verilerin Korunması Ajansı'dır (AZLP)**. AB Genel Veri Koruma Yönetmeliği (GDPR) BiH'de doğrudan uygulanmasa da, AB tarafından finanse edilen birçok program ve uluslararası bağışçılar GDPR ile uyumlu standartlar talep etmektedir. Sonuç olarak, BiH'deki kurumsal uygulamalar ve kılavuzlar, yasallık, veri minimizasyonu, hesap verebilirlik ve işleme güvenliği gibi GDPR'nin temel ilkelerini giderek daha fazla yansıtmaktadır.

Bosna Hersek'te henüz tek ve kapsamlı bir ulusal siber güvenlik yasası bulunmamaktadır. Bu bağlamda, Sivil Toplum Kuruluşlarının (STK'lar) öncelikle, açıkça tanımlanmış roller ve sorumluluklar, iç bilgi güvenliği politikaları ve günlük faaliyetlerde tutarlı bir şekilde uygulanan belgelenmiş prosedürler dahil olmak üzere iç yönetişim mekanizmaları aracılığıyla dijital güvenliği sağlamaları beklenmektedir.

Siber olaylar için ulusal kurumlar ve destek mekanizmaları

Bosna Hersek'te siber güvenlik olayları durumunda birkaç kamu kurumu destek, koordinasyon veya soruşturma işlevleri sağlamaktadır. Bunlar arasında olaylara müdahale desteği, erken uyarılar ve tehdit izleme sorumluluğunu üstlenen CERT **BiH** ile politika düzeyinde koordinasyon ve rehberlik sağlayan **Bosna Hersek Güvenlik Bakanlığı - Siber Güvenlik Sektörü** bulunmaktadır. Siber suçların bildirilmesi ve soruşturulması, yerel düzeyde operasyonel soruşturmalardan sorumlu olan varlık ve kanton polis siber suç birimlerinin yanı sıra, **Devlet Soruşturma ve Koruma Ajansı (SIPA)** tarafından uzman birimler aracılığıyla yürütülmektedir.

Bosna Hersek'teki Sivil Toplum Kuruluşları için Siber Tehdit Ortamı

Bosna Hersek'teki sivil toplum kuruluşları en çok, kuruluşların finansmanı, hibeleri ve bağışçılarla iletişimi hedef alan kimlik avı saldırıları ile ilgili siber tehditlerle karşı karşıyadır. Fidye yazılımı olayları ve kalıcı veri kaybı da, genellikle eksik veya yetersiz yedekleme uygulamaları nedeniyle sık sık görülmektedir. WhatsApp ve Viber gibi mesajlaşma platformları

üzerinden kimlik sahtekarlığı ve sosyal mühendislik saldırıları giderek daha fazla gözlemlenirken, web sitelerinin tahrif edilmesi siyasi veya sosyal açıdan hassas konularda çalışan kuruluşlar için özel bir risk oluşturmaktadır. Ayrıca, güvenli olmayan halka açık Wi-Fi ağlarının kullanımıyla bağlantılı kimlik bilgisi hırsızlığı da tekrarlayan bir sorun olmaya devam etmektedir.

Bosna Hersek'teki STK'ların Operasyonel Gerçekliği ve Basitleştirilmiş Bir Yaklaşımın Gerekçesi

Uygulamada, Bosna Hersek'teki birçok STK, örgütsel çalışmalarında büyük ölçüde kişisel dizüstü bilgisayar ve cep telefonlarına güvenmekte ve Gmail, Google Workspace ve sosyal medya gibi platformları birincil operasyonel araçları olarak kullanmaktadır. Özel BT veya siber güvenlik personeli nadirdir ve ekipler içinde şifre paylaşımı gibi gayri resmi uygulamalar hala yaygındır.

Bu gerçeklik göz önüne alındığında, müfredat kasıtlı olarak basitleştirilmiş ve pragmatik bir yaklaşım benimsemektedir. Düşük maliyetli ve kolay uygulanabilir güvenlik önlemlerine öncelik vermekte, pratik şablonlar ve kullanıma hazır belgeler sunmakta ve karmaşık teknik çözümlerden ziyade teknik bilgiye sahip olmayan personel için tasarlanmış açık ve adım adım kontrol listelerine odaklanmaktadır.

Avrupa Politika Çerçeveleriyle Uyum

Bosna Hersek, Avrupa Birliği üyesi olmasa da, birçok STK AB tarafından finanse edilen programlar ve Avrupa politika çerçeveleri kapsamında faaliyet göstermektedir. Bu nedenle, bu müfredat GDPR'nin temel ilkeleriyle, özellikle risk temelli yaklaşımla ve daha geniş kapsamlı Avrupa siber güvenlik farkındalık ve kapasite geliştirme stratejileriyle uyumludur. Uyum, yasal olmaktan çok pratiktir ve resmi uyum gereklilikleri yerine günlük uygulama ve örgütsel davranışlara odaklanır.

Risk Temelli Yaklaşım ve Politika Mantığı

Avrupa politika çerçeveleri orantılılık, bağlamsal farkındalık ve etki değerlendirmesini vurgular. Müfredat, yüksek riskli varlıkları ve faaliyetleri önceliklendirerek, aşırı karmaşık veya

kaynak yoğun kontrolleri önleyerek ve STK ortamlarında sürdürülebilir, insan merkezli ve gerçekçi güvenlik uygulamalarına odaklanarak bu mantığı uygular.

ISO'dan Esinlenen Mantık (Basitleştirilmiş)

Resmi sertifikasyon olmasa bile, CSO'lar ISO bilgi güvenliği standartlarından esinlenen basitleştirilmiş ilkelerden yararlanabilir. Bunlar arasında temel kurumsal varlıkların belirlenmesi, temel erişim kontrol ilkelerinin uygulanması, yapılandırılmış olay yönetimi süreçlerinin oluşturulması ve inceleme ve öğrenme yoluyla sürekli iyileştirmenin teşvik edilmesi yer alır. Bu yaklaşım, zaman içinde kurumsal olgunluğun ve dayanıklılığın kademeli olarak güçlendirilmesini destekler.

Bosna Hersek'ten Yerel Vaka Çalışmaları

Vaka 1: Hesabın Tamamen Ele Geçirilmesine Yol Açan Kimlik Avı Bağlantısı

Bu vaka, Saraybosna merkezli bir gençlik sivil toplum kuruluşunu ilgilendirir. Kuruluş, küçük bir ekiple çalışır ve iletişim, koordinasyon ve halkla ilişkiler için büyük ölçüde paylaşılan e-posta gelen kutularına ve Facebook ve Instagram gibi sosyal medya platformlarına güvenir. Şifreler kurum içinde paylaşılır ve iki faktörlü kimlik doğrulama etkinleştirilmez. Bir personel, güvenilir bir proje ortağından gelmiş gibi görünen bir Facebook Messenger mesajı aldı. Mesaj, ortak bir faaliyetin ayrıntılarının onaylanmasını istiyordu ve bir bağlantı içeriyordu. Çalışan bağlantıya tıklamış ve kuruluşun e-posta kimlik bilgilerini girmiştir. Birkaç dakika içinde saldırgan, paylaşılan e-posta gelen kutusuna ve bağlı sosyal medya hesaplarına erişim sağlamıştır. Kurtarma iletişim bilgileri değiştirilmiş ve bağışçılara sahte ödeme talepleri gönderilmiştir.

Bu olay, paylaşılan şifreler, platformlar arasında şifrelerin tekrar kullanılması, iki faktörlü kimlik doğrulamanın olmaması ve tüm kullanıcılar için aşırı yönetici ayrıcalıkları gibi birçok zayıflık nedeniyle meydana geldi. Mesaj, bağımsız bir doğrulama yapılmadan güvenilir kabul edildi. Kısa vadede, kuruluş e-posta ve sosyal medya hesaplarına erişimini kaybetti, bu da iletişim ve bağış toplama faaliyetlerini aksattı. Sahte mesajlar bağışçıların güvenini zedeledi. Orta vadede, CSO

hesapların kurtarılması ve güvenilirliğin yeniden tesis edilmesi için önemli miktarda zaman harcamak zorunda kaldı.

Çıkarılan Dersler ve Öneriler

Tüm kuruluş hesapları, şifre yöneticisi aracılığıyla yönetilen benzersiz şifreler kullanmalı ve iki faktörlü kimlik doğrulama özelliği etkinleştirilmelidir. Yönetimsel ayrıcalıklar sınırlandırılmalı ve hassas talepler her zaman ikincil bir iletişim kanalı aracılığıyla doğrulanmalıdır.

İlgili Modüller ve Müfredatta Kullanımı

- **Modül 1 – Siber Güvenliğin Temelleri:**
  Kimlik avı saldırıları, kimlik bilgisi hırsızlığı ve hızlı hesap ele geçirmeyi açıklamak için temel örnek olarak kullanılır.
- **Modül 4 – Yaygın siber tehditler (Kimlik Avı ve Kötü Amaçlı Yazılım):**
  Sosyal mühendisliğin güveni ve doğrulama eksikliğini nasıl istismar ettiğini gösterir.
- **Modül 7 – Güvenlik Kültürü Geliştirme:**
  Personel farkındalığı, şifre hijyeni ve iki faktörlü kimlik doğrulamanın önemi hakkında tartışmayı destekler.

Önerilen Kullanım:
Vaka analizi, ardından tehlike işaretlerinin belirlenmesi ve önleyici kontrollerin haritalandırılması.

Vaka 2: WhatsApp/Viber Kimlik Sahtekarlığı Sonucu Mali Kayıp

Bu vaka, iç koordinasyon ve finansal iletişim için sık sık WhatsApp ve Viber kullanan orta ölçekli bir CSO ile ilgilidir. Hassas kararlar genellikle mesajlaşma uygulamaları aracılığıyla gayri resmi olarak ele alınır.

Bir saldırgan, gerçek bir proje koordinatörünün adını ve profil fotoğrafını kullanarak bir WhatsApp veya Viber hesabı oluşturdu. Saldırgan, banka bilgilerinin değiştiğini belirten acil bir

mesajla finans personeli ile iletişime geçti ve yeni IBAN'ın derhal kullanılmasını talep etti. Talep, doğrulama yapılmadan işleme alındı.

Kuruluş, hassas finansal kararlar için gayri resmi mesajlaşma platformlarına güveniyordu ve ikincil doğrulama mekanizmaları yoktu. Finansal işlemler için çok kişili onay gerekliliği yoktu.

Fonlar saldırgana aktarıldı ve geri alınamadı. Olay, mali kayıplara ve iç sıkıntılara yol açtığı gibi, bağışçılar ve ortaklar nezdinde itibar sorunlarına da neden oldu.

Finansal işlemler asla mesajlaşma platformları üzerinden onaylanmamalıdır. Ödemeyle ilgili tüm talepler, kuruluşun alan adından gönderilen imzalı e-postalar veya bilinen numaralara yapılan telefon görüşmeleri gibi resmi kanallar aracılığıyla doğrulanmalıdır. Önemli finansal işlemler için iki kişilik onay kuralı uygulanmalıdır.

İlgili Modüller ve Müfredatta Kullanımı

- **Modül 2 – İletişim ve Sosyal Mühendislik:**
  Mesajlaşma platformları aracılığıyla kimlik sahtekarlığı ve aciliyet temelli manipülasyonu gösteren birincil vaka.
- **Modül 7 – Güvenlik Kültürü Geliştirme:**
  Finansal kararlar için iç kuralların, doğrulama prosedürlerinin ve ortak sorumluluğun gerekliliğini vurgular.

Önerilen Kullanım:
Acil finansal taleplerin doğrulanması ve iki kişilik onay kuralının uygulanmasına ilişkin rol yapma alıştırması.

Vaka 3: Halka Açık Wi-Fi Aracılığıyla Kimlik Bilgilerinin Çalınması

Bu vaka, gönüllülerin kişisel cihazlarını kullanarak uzaktan çalışmasına izin veren bir CSO ile ilgilidir. Gmail ve Google Drive gibi bulut hizmetleri günlük operasyonların merkezinde yer

almaktadır ve uzaktan erişim veya cihaz güvenliğini düzenleyen resmi bir politika bulunmamaktadır.

Bir gönüllü, ücretsiz halka açık Wi-Fi kullanarak bir kafede çalışmış ve kuruluşun e-postasına ve bulut depolama alanına giriş yapmıştır. Cihazda son güvenlik güncellemeleri yapılmamıştı ve şifreler tarayıcıya kaydedilmişti. Kısa bir süre sonra, bilinmeyen girişler tespit edilmiş ve bağışçıların iletişim listeleri indirilmiştir. Raporlama prosedürlerinin belirsiz olması nedeniyle müdahale gecikmiştir.

Kuruluş, güvenli olmayan halka açık Wi-Fi üzerinden hassas hesaplara erişime izin verdi, eski cihazlar kullandı ve tarayıcıya kaydedilmiş şifrelere izin verdi. Ayrıca, net bir iç olay raporlama mekanizması da yoktu.

Hassas veriler açığa çıktı ve bağışçıların güveni tehlikeye girdi. Geciken müdahale, ihlalin potansiyel etkisini artırdı.

Hassas hesaplara VPN olmadan halka açık Wi-Fi üzerinden erişilmemelidir. Cihazlar güncel tutulmalı, otomatik bağlanma özellikleri devre dışı bırakılmalı ve olay raporlama prosedürleri tüm personel ve gönüllülere açıkça iletilmelidir.

İlgili Modüller ve Müfredatta Kullanımı

- **Modül 3 – Cihazlar ve Altyapı Güvenliği:**
  Halka açık Wi-Fi, yamalanmamış cihazlar ve güvenli olmayan kimlik bilgisi depolama ile ilgili risklerin temel örneği.
- **Modül 7 – Güvenlik Kültürü Geliştirme:**
  Net olay raporlama prosedürlerinin ve personel farkındalığının önemini vurgular.

Önerilen Kullanım:
Grup tartışmasının ardından güvenli uzaktan çalışma uygulamaları hakkında bir kontrol listesi alıştırması yapılır.

Vaka 4: E-posta Ekinde Ransomware

Bu vaka, paylaşılan ofis dizüstü bilgisayarları ve e-posta tabanlı belge alışverişi kullanan bölgesel bir CSO ile ilgilidir. Yedekleme uygulamaları gayri resmiydi ve çevrimdışı yedeklemeler yapılmıyordu. Bağışçı raporuna benzeyen bir e-posta alındı ve bir personel, adresinde paylaşılan bir dizüstü bilgisayarda eki açtı. Kısa bir süre sonra dosyalara erişilemez hale geldi ve ekranda bir fidye notu belirdi. Kuruluş, gönderenin görünüşüne güvendi, ek filtreleme kuralları yoktu ve çevrimdışı veya izole yedeklemeler yapmıyordu. Mali kayıtlar ve proje belgeleri kalıcı olarak kaybedildi. OCSOing projeleri kesintiye uğradı ve kurtarma maliyetleri ortaya çıktı. STK'lar en az bir çevrimdışı yedekleme tutmalı ve sürüm geçmişi etkinleştirilmiş bulut hizmetlerini kullanmalıdır. Makro etkin ve yürütülebilir ekler kısıtlanmalı ve personel istenmeyen dosyaları açmamaları konusunda eğitilmelidir.

İlgili Modüller ve Müfredatta Kullanımı

- **Modül 4 – Yaygın siber tehditler (Kötü Amaçlı Yazılım ve Fidye Yazılımı):**
  Fidye yazılımının e-posta ekleri yoluyla nasıl yayıldığını ve yedeklemelerin eksikliğinin etkisini gösterir.
- **Modül 5 – Veri Koruma ve Gizlilik Uyumluluğu:**
  Veri kullanılabilirliği, yedekleme yükümlülükleri ve organizasyonel süreklilik risklerini vurgular.

Önerilen Kullanım:
Yedekleme stratejileri ve "ilk olarak ne yapardınız?" yanıt adımları üzerine senaryo temelli tartışma.

Vaka 5: Paylaşılan Giriş Bilgileri Nedeniyle Ele Geçirilen Facebook Sayfası

Birkaç genç sivil toplum örgütü, kamuya açık sayfaları yönetmek için personel ve gönüllüler arasında tek bir Facebook giriş bilgisini paylaşıyordu. Gönüllüler kuruluştan ayrıldığında erişim gözden geçirilmedi. Eski bir gönüllü, paylaşılan hesaba erişimini korudu ve daha sonra bunu kötüye kullandı. Facebook sayfası ele geçirildi ve dolandırıcılık mesajları ve siyasi içerik yayınlamak için kullanıldı. Paylaşılan kimlik bilgileri, rol tabanlı erişimin olmaması ve personel ayrıldığında erişimin iptal edilmemesi, büyük bir güvenlik açığı yarattı. Kuruluşun itibarı zedelendi ve bağışçılar, yayınlanan içeriğin meşruiyetini doğrulamak için STK ile iletişime geçti. Kurtarma işlemi zaman ve kamuoyuna açıklama gerektirdi.

Çıkarılan Dersler ve Öneriler

Paylaşılan oturum açma bilgileri kullanılmamalıdır. Erişim, platform rol özellikleri aracılığıyla sağlanmalı, yöneticiler için iki faktörlü kimlik doğrulama zorunlu olmalı ve erişim hakları düzenli olarak gözden geçirilmelidir.

İlgili Modüller ve Müfredatta Kullanımı

- **Modül 6 – Sosyal Medya ve Çevrimiçi Varlık Güvenliği:**
  Paylaşılan kimlik bilgileri, rol tabanlı erişim ve hesap kurtarma prosedürleri için birincil vaka.
- **Modül 7 – Güvenlik Kültürü Geliştirme:**
  Erişim iptali ve işten ayrılma prosedürleri ile ilgili politika tartışmalarını destekler.
- **Modül 8 – İleri Düzey Konular (Erişim Kontrol Uygulamaları):**
  Daha güçlü hesap yönetimi ve idari kontroller getirilirken başvurulabilir.

Önerilen Kullanım:
Sosyal medya erişim yönetimine odaklanan vaka temelli politika taslak hazırlama alıştırması.

PRATİK ŞABLONLAR VE KONTROL LİSTELERİ Bosna Hersek'teki Sivil Toplum Kuruluşları (STK'lar) için

EK 1 – KABUL EDİLEBİLİR KULLANIM POLİTİKASI (AUP)

Bosna Hersek'teki Küçük ve Orta Ölçekli STK'lar için Şablon

Belge Başlığı: Kabul Edilebilir Kullanım Politikası (AUP)

Uygulanır: Tüm personel, gönüllüler, stajyerler, dış danışmanlar

1. Amaç

   Bu politika, STK cihazlarının, kullanıcı hesaplarının ve verilerinin güvenli ve sorumlu kullanımına ilişkin kuralları tanımlar.

2. Hesaplar ve Şifreler

- Her hesap için benzersiz şifreler kullanın.
- Şifreleri sohbet grupları, mesajlaşma uygulamaları veya e-posta yoluyla paylaşmayın.
- E-posta, bulut depolama ve sosyal medya yönetici hesapları için iki faktörlü kimlik doğrulamayı (2FA) etkinleştirin.
- Mümkün olduğunda bir şifre yöneticisi kullanın.

3. Cihazlar (Dizüstü Bilgisayarlar ve Cep Telefonları)

- Tüm cihazları PIN, şifre veya biyometrik koruma ile kilitleyin.
- Otomatik sistem ve güvenlik güncellemelerini etkinleştirin.
- Kayıp veya çalınan cihazları 1 saat içinde Olay Sorumlusuna bildirin.

4. E-posta ve Bağlantılar

- Beklenmedik ekleri veya bağlantıları açmayın.
- Banka veya ödeme değişikliklerini her zaman bilinen bir numarayı arayarak doğrulayın.
- Acil veya baskı içeren mesajları yüksek riskli olarak değerlendirin.

5. Wi-Fi ve Uzaktan Çalışma

- Yönetici veya hassas hesaplar için halka açık Wi-Fi kullanmaktan kaçının.
- Mümkünse mobil hotspot veya VPN kullanın.

- Wi-Fi ağlarına otomatik bağlanma özelliğini devre dışı bırakın.

6. Sosyal Medya

- Paylaşılan oturum açma bilgileri yerine sayfa rolleri kullanın.
- Yönetici sayısını minimumda tutun.
- Bir personel veya gönüllü ayrıldığında erişimini hemen kaldırın.

7. Veri İşleme

- Yalnızca gerekli kişisel verileri toplayın.
- Kişisel verileri yalnızca onaylanmış konumlarda (ör. CSO bulut sürücüsü) saklayın.
- Yararlanıcı verilerini şifreleme olmadan kişisel cihazlarda saklamayın.

8. Olay Bildirimi

   Şüpheli herhangi bir güvenlik veya veri olayı, CSO Olay Müdahale Planı kullanılarak derhal raporlanmalıdır.

Onaylayan: _____

Tarih: _____

Sonraki Gözden Geçirme Tarihi: _____

EK 2 – OLAY MÜDAHALE PLANI (IRP)

Basitleştirilmiş – Küçük CSO'lar için

Belge Başlığı: Olay Müdahale Planı (Basitleştirilmiş)

1. Olay Nedir

   Olay, kimlik avı, hesap ele geçirme, kötü amaçlı yazılım, fidye yazılımı veya veri sızıntısı dahil olmak üzere CSO hesaplarını, cihazlarını, verilerini veya itibarını tehdit eden herhangi bir olaydır.
2. Görev ve Sorumluluklar (İsimleri doldurun)

   Olay Sorumlusu: _____

   İletişim Sorumlusu: _____

   BT Desteği (iç/dış): _____

   Yönetim Onayı: _____
3. İlk 15 Dakika – Acil Eylemler

- Etkilenen cihazı Wi-Fi veya internet bağlantısından ayırın.
- Ekran görüntüsü alın ve saati ve etkilenen hesapları not edin.
- Dahili ekibi bilgilendirin: "Bağlantılara tıklamayın. Olay inceleniyor."
- Önce e-posta hesabını güvenli hale getirin (şifreyi değiştirin ve 2FA'yı etkinleştirin).

4. İlk 60 Dakika – Kontrol Altına Alma

- Şifreleri şu sırayla sıfırlayın: e-posta, bulut depolama, sosyal medya, bankacılık veya finans araçları.
- Bilinmeyen veya şüpheli oturumların tümünden çıkış yapın.
- Bilinmeyen yöneticileri, uygulamaları ve entegrasyonları kaldırın.
- E-posta yönlendirme kurallarını kontrol edin.

5. Değerlendirme (Aynı Gün)

- Ne oldu?

- Hangi veriler etkilenebilir (bağışçılar, yararlanıcılar, reşit olmayanlar)?
- Hangi sistemler ve hesaplar etkilendi?

6. Dış Raporlama (Gerekli Olduğunda)

- Olay desteği ve uyarılar için CERT BiH.
- Siber suç şüphesi varsa SIPA veya polis siber suç birimleri.
- Kişisel veri ihlali olasılığı varsa AZLP gerekliliklerine başvurun ve alınan önlemleri belgelendirin.

7. İletişim Kuralları

- Yalnızca İletişim Sorumlusu harici açıklamalar yapar.
- Yalnızca gerçekleri paylaşın.
- Gerekirse bağışçıları veya ortakları bilgilendirin.

8. Kurtarma

- Sistemleri yedeklerden geri yükleyin.
- Tüm cihazları güncelleyin.
- Personeli olay türüne ilişkin yeniden eğitin.

9. Sonrası İnceleme (7 Gün İçinde)

- Hangi kontrol başarısız oldu?
- Neler değişmelidir (2FA, erişim rolleri, yedeklemeler, eğitim)?
- Politikaları ve kontrol listelerini güncelleyin.

EK 3 – VERİ KORUMA KURALLARI (İÇ)

CSO'lar için Basit İç Kurallar Kitabı

Belge Başlığı: Veri Koruma Kuralları (Dahili)

1. Kapsam

   Bu kural kitabı, STK tarafından işlenen tüm kişisel veriler için geçerlidir.

2. Temel Veri Koruma Kuralları

- Verileri yasal ve adil bir şekilde işleyin.
- Sadece gerekli olanları toplayın (veri minimizasyonu).
- Verileri yalnızca gerekli olduğu sürece saklayın.
- Erişim kontrolü, yedekleme ve 2FA gibi koruma önlemleri uygulayın.

3. Onaylanmış Veri Depolama Konumları

   CSO bulut sürücüsü: _____

   CSO e-posta sistemi: _____

   Yerel şifreli klasör (gerekirse): _____

4. Erişim Kontrolü

- Verilere yalnızca ihtiyaç duyan personel erişebilir.
- Birisi ayrıldığında 24 saat içinde erişimini kaldırın.

5. Hassas Veriler ve Küçükler

   Küçüklerin verilerini işlerken, daha sıkı kontroller uygulayın ve erişimi sınırlayın.

6. Veri Paylaşımı

- Verileri yalnızca onaylanmış kanallar aracılığıyla paylaşın.
- WhatsApp veya Viber üzerinden yararlanıcı listelerini paylaşmayın.
- Hassas veriler için şifre korumalı dosyalar kullanın.

7. Olay Yönetimi

   Herhangi bir veri ihlali şüphesi, Olay Müdahale Planını derhal devreye sokar.

Onaylayan: _____

Tarih: _____

Sonraki Gözden Geçirme Tarihi: _____

EK 4 – PRATİK KONTROL LİSTELERİ

Düşük BT Kapasitesine Sahip Bosna Hersek Sivil Toplum Kuruluşları için

Kontrol Listesi A – Temel Dijital Güvenlik Kontrol Listesi (Başlangıç Paketi)

Hesaplar

- E-posta, bulut ve sosyal medya yöneticileri için 2FA etkinleştirilmiş.
- Benzersiz şifreler kullanılır.
- Şifreler sohbet gruplarında paylaşılmamaktadır.

Cihaz

- Ekran kilidi etkinleştirildi.
- Otomatik güncellemeler etkinleştirildi.
- Antivirüs veya sistem savunma sistemi etkin.

Wi-Fi ve Uzaktan Çalışma

- Misafir Wi-Fi, personel Wi-Fi'sinden ayrıdır.
- Hot spot veya VPN olmadan halka açık Wi-Fi'da yönetici girişi yapılamaz.

Veri ve Yedeklemeler

- Bulut sürüm geçmişi etkinleştirilmiştir.
- Haftalık yedekleme mevcuttur (mümkünse bir çevrimdışı kopya).
- Birisi ayrıldığında erişim hemen kaldırılır.

Sosyal Medya

- Sayfa rolleri kullanılır.
- Yalnızca 1-2 yönetici.
- Kurtarma e-postası ve telefonu CSO'ya aittir.

Kontrol Listesi B – Olay Raporlama Kontrol Listesi (Dahili)

Bir olaydan şüphelendiğinizde

- Etkilenen cihazı internet bağlantısından ayırın.
- Ekran görüntüsü alın ve saati not edin.
- Olay Sorumlusunu derhal bilgilendirin.
- E-posta şifresini değiştirin ve 2FA'yı etkinleştirin.
- Bilinmeyen oturum açma işlemlerini ve e-posta yönlendirme kurallarını kontrol edin.
- Etkilenen verileri (bağışçılar, yararlanıcılar, reşit olmayanlar) belirleyin.
- Dışarıya bildirimde bulunulması gerekip gerekmediğine karar verin (CERT BiH, SIPA, polis, AZLP).

Asgari Olay Kaydı

Tespit tarihi ve saati: _____

Tespit eden: _____

Ne oldu (kısa açıklama): _____

Etkilenen hesaplar veya sistemler: _____

Alınan önlemler: _____

Kanıtların saklandığı yer: _____

Dış raporlama tamamlandı (evet/hayır): _____

4 .3 Kuzey Makedonya'daki Sivil Toplum Örgütleri için Yasal, Düzenleyici ve Operasyonel Çerçeve

Kuzey Makedonya'daki Yasal ve Düzenleyici Çerçeve

27 Nisan 2016 tarihinde, Avrupa Parlamentosu ve Avrupa Birliği Konseyi, kişisel verilerin işlenmesi ve bu verilerin serbest dolaşımı konusunda gerçek kişilerin korunmasına ilişkin 2016/679 sayılı Tüzüğü kabul ederek 95/46/EC sayılı Direktifi yürürlükten kaldırmıştır. Bu, kişisel verilerin korunması alanında kapsamlı bir reform sürecinin başlangıcını işaret etmiştir. İki yıllık bir geçiş döneminin ardından, Tüzük 25 Mayıs 2018 tarihinde Avrupa Birliği genelinde uygulanmaya başlanmıştır.

Genel olarak GDPR olarak anılan bu Tüzük, 24 Şubat 2020 tarihinde yürürlüğe giren Kişisel Verilerin Korunması Kanunu'nun kabulüyle Kuzey Makedonya Cumhuriyeti'nde tam olarak uygulanmaya başlanmıştır.

Kişisel Verilerin Korunması Kanunu, kişisel verilerin işlenmesine ilişkin yedi temel ilkeyi düzenlemektedir:

- yasallık, adalet ve şeffaflık,
- amaç sınırlaması,
- veri minimizasyonu,
- doğruluk,
- saklama sınırlaması,
- bütünlük ve gizlilik,
- hesap verebilirlik.

Sivil toplum kuruluşları, veri sorumluları olarak, kişisel verilerin işlendiği her durumda ve veri yaşam döngüsünün tamamında tüm ilkeleri birikimli olarak uygulamakla yükümlüdür . Bu ilkelerden herhangi birinin uygulanmaması, Kişisel Verilerin Korunması Kanunu'nun ihlali anlamına gelir. Kişisel Verilerin Korunması Kanunu'nun uygulanmasından ve denetlenmesinden sorumlu ana otorite, Kişisel Verilerin Korunması Kurumu'dur.

Ayrıca, siber güvenlik alanında, Temmuz 2025'te kabul edilen Ağ ve Bilgi Sistemleri Güvenliği Kanunu, Kuzey Makedonya'da siber güvenliği düzenleyen ilk kapsamlı yasal çerçeveyi

oluşturmaktadır. Kanun, Avrupa NIS2 Direktifi ile uyumludur ve hem kamu hem de özel sektörde ağ ve bilgi sistemlerinin yüksek ve ortak bir koruma seviyesinin oluşturulmasını amaçlamaktadır.

Dijital Dönüşüm Bakanlığı ve Elektronik İletişim Ajansı bünyesinde faaliyet gösteren Ulusal Bilgisayar Olaylarına Müdahale Ekibi (MKD-CIRT), siber güvenlik olaylarını izlemek, koordine etmek ve bunlara müdahale etmekten sorumludur. Sivil toplum kuruluşları da dahil olmak üzere özel sektör için önemli olan, 2027 yılına kadar sürecek geçiş dönemi uygulamasıdır. Bu süre zarfında tüm kuruluşların kanunla getirilen yükümlülükleri aşamalı olarak yerine getirmeleri beklenmektedir.

Sivil Toplum Kuruluşlarını Etkileyen Ortak Tehditler ve Son Dönemdeki Olaylar

Kuzey Makedonya'daki sivil toplum kuruluşları, diğer sektörlere benzer şekilde, siber güvenlik tehditlerine karşı oldukça savunmasızdır. Önemli bir sorun, birçok siber olayın fark edilmeden veya rapor edilmeden kalması ve bunun sonucunda kapsamlı ve güvenilir olay verilerinin eksikliğidir. Önemli sayıda sivil toplum kuruluşu, yasal değişikliklerden haberdar olduğunu ve operasyonel uygulamalarını buna göre uyarladığını bildirirken, mevcut veriler birçok kuruluşun iç kişisel veri koruma kanunlarını benimsemediğini ve kişisel veri koruma görevlisi atamadığını göstermektedir.

Ayrıca, kişisel veri koruması konusunda resmi eğitim almış STK personelinin oranı çok düşük kalmaktadır. STK'ların genellikle sınırlı mali kaynaklarla çalıştığı ve personel eğitimi için fon ayırmakta zorluk yaşadığı göz önüne alındığında, eğitim fırsatlarına erişimi kolaylaştırmak için Kişisel Verilerin Korunması Kurumu ile sivil toplum sektörü arasında yapılandırılmış işbirliği mekanizmaları kurulması önerilmektedir.

Sivil toplum kuruluşları için önemli bir risk faktörü, veri koruma ve siber güvenliğe yatırım yapmak için sınırlı bütçelerine sahip olmalarıdır. Birçok küçük kuruluş, lisanssız veya eski yazılımları kullanmaya devam etmekte ve bu da siber tehditlere maruz kalma risklerini önemli

ölçüde artırmaktadır. Aynı zamanda, Makedonca dilinde sivil toplum kuruluşlarının dijital güvenliğini güçlendirmelerine destek olabilecek çeşitli kılavuzlar ve rehber belgeler mevcuttur.

En çok tespit edilen tehditler şunlardır:

• bağlantılara tıklamadan veya mesajları açmadan önce gönderenleri doğrulamamak,
• Şifre yöneticilerinin sınırlı kullanımı ve benzer şifrelerin sık sık yeniden kullanılması,
• düzensiz veya eksik veri yedekleme uygulamaları,
• lisanssız ve güncel olmayan yazılımların kullanılması,
• mobil cihazlar için yetersiz güvenlik önlemleri,
• iki faktörlü kimlik doğrulamanın çok az kullanılması.

Ulusal Destek ve Kaynaklar

Kişisel Verilerin Korunması Kurumu, Dijital Dönüşüm Bakanlığı ve Elektronik Haberleşme Kurumu dahil olmak üzere birçok ulusal kurum, dijital güvenlik ve veri korumasını iyileştirmeyi amaçlayan STK'lara destek ve rehberlik sağlamaktadır. Bununla birlikte, sistematik planlama ve devlet tarafından finanse edilen girişimler dahil olmak üzere daha fazla kurumsal çaba gerekmektedir.

Sivil toplum kuruluşları ve genel nüfus arasında dijital okuryazarlığı artırmak için, esas olarak yabancı bağışçılar tarafından finanse edilen sivil toplum projeleri aracılığıyla da destek sağlanmaktadır. Önemli bir örnek, 2025 yılında marjinal gruplarla çalışan kuruluşlar için üç siber güvenlik eğitim oturumu düzenlenen "CyberShield: Siber Dayanıklılık için Güçlendirilmiş Vatandaşlar" projesidir. Bunun devamı olarak, altı sivil toplum kuruluşu için dijital güvenlik planları geliştirilmiştir. Bu özel planlar, siber güvenlik uygulamalarının sistematik bir şekilde uygulanmasını sağlamak, kurumsal dayanıklılığı artırmak ve dolaylı olarak son kullanıcılara sunulan hizmetleri iyileştirmek amacıyla hazırlanmıştır.

Bu olumlu örneklere rağmen, sınırlı finansman nedeniyle sadece az sayıda STK bu tür girişimlerden yararlanabilmektedir. Makedonca dilinde çeşitli kılavuzlar ve farkındalık artırıcı materyaller mevcut olmakla birlikte, eğitim ve kapasite geliştirme faaliyetlerine erişimi

genişletmek için kamu kurumları ve STK'lar arasında daha geniş ve sürdürülebilir bir işbirliği gereklidir. STK personelinin doğrudan eğitim ve öğretimini desteklemek için özellikle daha fazla finansman ve hedefli programlara ihtiyaç vardır.

Kuzey Makedonya'daki STK'ların Kültürel ve Operasyonel Bağlamı

Kuzey Makedonya'daki çoğu STK, bağışçı ve proje temelli bir model ile çalışmaktadır ve genellikle küçük idari ve operasyonel ekiplere sahiptir veya büyük ölçüde gönüllülere dayanmaktadır. Örgütsel çalışmalar genellikle kişisel cihazlar ve Google Workspace, Dropbox veya Microsoft 365 gibi yaygın olarak kullanılan dijital hizmetler kullanılarak, çoğu zaman uygun lisanslar olmadan yürütülmektedir.

Bu nedenle, eğitim ve kapasite geliştirme girişimleri aşağıdakiler dahil olmak üzere pratik ve gerçekçi önlemlere odaklanmalıdır:

- Lisanslı ürün ve hizmetleri kullanmanın avantajları
- "Tıklamadan Önce Düşün" farkındalık kampanyaları,
- düzenli veri ve bilgi yedeklemeleri,
- iki faktörlü kimlik doğrulamanın aktif ve tutarlı kullanımı,
- mobil cihazların güvenliğini sağlama ve kullanımını yönetme,
- sorumlu şifre uygulamaları,
- bulut tabanlı çözümlerin etkili kullanımı,
- veri paylaşım uygulamalarına ilişkin farkındalığın artırılması.

Kuzey Makedonya'da dijital okuryazarlık düzeyleri, STK sektörü dahil olmak üzere, hala yetersizdir. Daha yüksek bir dijital güvenlik düzeyine ulaşmak için ek finansman, kaynaklar ve koordineli çabalar gerekmektedir. Bu çabalar, sivil toplum kuruluşlarının gerçek ihtiyaçlarına ve kapasitelerine uygun somut programlara ve pratik eylem planlarına dönüştürülmelidir.

Ekler ve Kullanıma Hazır Şablonlar (Kuzey Makedonya)

EK 1 – Kuzey Makedonya'daki STK'lar için Dijital Güvenlik Ortamı

Bu ek, Kuzey Makedonya'daki sivil toplum kuruluşlarını etkileyen yasal, kurumsal ve operasyonel gerçekleri yansıtmakta ve müfredatın yerelleştirilmesini desteklemektedir.

Tehdit Ortamı

• E-posta ve sahte kurumsal mesajlar yoluyla kimlik avı saldırıları,
• Fidye yazılımı olayları ve yedeklemelerin eksikliği nedeniyle veri kaybı,
• Güvenli olmayan kişisel verilerin kötüye kullanılması,
• Kişisel dizüstü bilgisayarların ve mobil cihazların kullanımına ilişkin riskler.

Operasyonel Zorluklar

• Şifre yöneticilerinin az kullanılması ve şifrelerin sık sık tekrar kullanılması,
• Düzensiz veya eksik veri yedekleme rutinleri,
• Lisanssız veya güncel olmayan yazılımların kullanımı,
• Mobil cihazların yetersiz güvenliği,
• İki faktörlü kimlik doğrulamanın sınırlı kullanımı,
• Dijital güvenlik önlemleri için özel fon eksikliği.

Şablon: Dijital Korumayı Artırmak için 10 Temel Adım

Kuzey Makedonya'daki CSO'lar için aşağıdaki temel adımlar önerilir:

• Antivirüs ve kötü amaçlı yazılımdan koruma yazılımı yükleyin ve düzenli olarak güncelleyin,
• Sistem ve yazılım güncellemelerini hemen uygulayın,
• Her hesap için güçlü ve benzersiz şifreler kullanın,
• Bilinmeyen veya şüpheli kaynaklardan gelen ekleri açmaktan kaçının,
• Hassas verileri yalnızca şifrelenmiş web sitelerine girin,
• Kurumsal verilerin düzenli yedeklemelerini yapın,
• Farklı amaçlar için ayrı e-posta adresleri kullanın,
• Web sitesi adreslerini manuel olarak yazarak kimlik avını önleyin,

• Güncel olmayan veya desteklenmeyen uygulamaları kaldırın,
• Kişisel ve kurumsal verileri dikkatli bir şekilde kullanın.

Şablon – Dijital Güvenlik için İç İşletim Kuralları

Her CSO, personel, gönüllüler ve ziyaretçiler için dijital güvenlik kurallarını tanımlayan basit bir iç belge benimsemelidir. Belge şunları içermelidir:

• Her hesap için benzersiz şifreler kullanın,
• Şifreleri sohbet uygulamaları veya e-posta yoluyla paylaşmayın,
• E-posta, bulut depolama ve sosyal medya yönetici hesapları için iki faktörlü kimlik doğrulamayı etkinleştirin,
• Mümkün olduğunda şifre yöneticisi kullanın,
• Tüm cihazları PIN veya şifrelerle kilitleyin,
• Otomatik güncellemeleri etkinleştirin,
• Kayıp veya çalınan cihazları derhal bildirin,
• Tüm banka ve ödeme değişiklik taleplerini doğrulayın,
• CSO tesisleri dışında çalışırken mobil erişim noktalarını kullanın,
• Sosyal medya erişimini yalnızca platform rolleri aracılığıyla atayın,
• Yönetici sayısını minimumda tutun,
• Yalnızca gerekli kişisel verileri toplayın ve saklayın,
• Herhangi bir güvenlik olayını derhal sorumlu kişiye bildirin.

Şablon – Olay Müdahale Planı (Basitleştirilmiş)

Bir dijital güvenlik olayı meydana geldiğinde veya şüphelenildiğinde, aşağıdaki adımlar atılmalıdır:

- Etkilenen cihazı ağdan ayırın,
- Olayla ilgili kanıtları saklayın,
- İç ekibi bilgilendirin,

- Öncelikle şifreleri değiştirerek ve 2FA'yı etkinleştirerek e-posta hesabını güvenli hale getirin,
- Etkilenen tüm hesapların şifrelerini sıfırlayın,
- Bilinmeyen veya şüpheli oturumlardan çıkış yapın,
- Bilinmeyen yöneticileri ve bağlı uygulamaları kaldırın, olayları MKD-CIRT'e bildirin,
- Şüpheli siber suçları polis siber suç birimlerine bildirin,
- Veri ihlali şüphesi varsa Kişisel Verilerin Korunması Kurumu'na danışın,
- Olayın etkisini değerlendirin ve sistemleri yedeklerden geri yükleyin,
- Cihazları ve yazılımları güncelleyin,
- Personeli yeniden eğitin,
- Gerekirse iç politikaları ve kontrol listelerini güncelleyin.

Kuzey Makedonya'daki CSO'lar için Pratik Kontrol Listeleri

EK 1 – Kuzey Makedonya'daki STK'lar için Dijital Güvenlik Ortamı

Bu ek, Kuzey Makedonya'daki Sivil Toplum Örgütlerini (STÖ'ler) etkileyen yasal, kurumsal ve operasyonel bağlamı özetlemektedir. Ülkede faaliyet gösteren STÖ'lerin ortak risklerini, kapasitelerini ve pratik ihtiyaçlarını yansıtarak dijital güvenlik müfredatının yerelleştirilmesini desteklemektedir.

Tehdit Ortamı

Kuzey Makedonya'daki sivil toplum kuruluşları genellikle aşağıdaki dijital güvenlik tehditleriyle karşı karşıyadır:

- e-posta ve sahte kurumsal mesajlar yoluyla kimlik avı saldırıları
- fidye yazılımı olayları ve eksik veya yetersiz yedeklemeler nedeniyle veri kaybı
- güvenli olmayan kişisel verilerin kötüye kullanılması veya ifşa edilmesi
- kurumsal çalışmalar için kişisel dizüstü bilgisayarların ve mobil cihazların kullanımına ilişkin riskler

Operasyonel Zorluklar

Uygulamada, Kuzey Makedonya'daki birçok CSO aşağıdaki zorluklarla karşılaşmaktadır:

- Şifre yöneticilerinin az kullanılması ve şifrelerin sık sık yeniden kullanılması
- Düzensiz veya eksik veri yedekleme rutinleri,
- Lisanssız veya güncel olmayan yazılımların kullanımı,
- Mobil cihazların yetersiz güvenliği,
- İki faktörlü kimlik doğrulamanın sınırlı kullanımı,
- Dijital güvenlik önlemleri için özel fon eksikliği.

Dijital Korumayı Artırmak için On Temel Adım

Kuzey Makedonya'daki CSO'ların dijital güvenlik durumlarını iyileştirmeleri için aşağıdaki temel adımlar önerilmektedir:

1. Antivirüs ve kötü amaçlı yazılımdan koruma yazılımlarını yükleyin ve düzenli olarak güncelleyin.
2. Sistem ve yazılım güncellemelerini mevcut olduğunda hemen uygulayın.
3. Her hesap için güçlü ve benzersiz şifreler kullanın.
4. Bilinmeyen veya şüpheli kaynaklardan gelen ekleri açmaktan kaçının.
5. Hassas verileri yalnızca şifreli web sitelerinde (HTTPS) girin.
6. Kurumsal verilerin düzenli yedeklemelerini yapın.
7. Farklı amaçlar için ayrı e-posta adresleri kullanın (ör. yönetim, projeler, kamu iletişimi).
8. Bağlantılara tıklamak yerine web sitesi adreslerini manuel olarak yazarak kimlik avını önleyin.
9. Cihazlardan eski veya desteklenmeyen uygulamaları kaldırın.
10. Kişisel ve kurumsal verileri her zaman dikkatli bir şekilde kullanın.

Dijital Güvenlik için İç İşletim Kuralları

Her CSO, personel, gönüllüler ve ziyaretçiler için dijital güvenlik kurallarını tanımlayan basit bir iç belge benimsemelidir. Bu belge en azından aşağıdaki kuralları içermelidir:

- ☐ Her hesap için benzersiz şifreler kullanın.
- ☐ Şifreleri sohbet uygulamaları veya e-posta yoluyla paylaşmayın.
- ☐ E-posta, bulut depolama ve sosyal medya yönetici hesapları için iki faktörlü kimlik doğrulamayı etkinleştirin.
- ☐ Mümkün olduğunda şifre yöneticisi kullanın.
- ☐ Tüm cihazları PIN, şifre veya biyometrik koruma ile kilitleyin.
- ☐ Otomatik sistem ve uygulama güncellemelerini etkinleştirin.
- ☐ Kayıp veya çalınan cihazları derhal bildirin.
- ☐ Tüm banka ve ödeme değişiklik taleplerini ikincil bir kanal üzerinden doğrulayın.
- ☐ CSO tesisleri dışında çalışırken mobil erişim noktalarını kullanın.
- ☐ Sosyal medya erişimini yalnızca platform rol özellikleri aracılığıyla atayın.
- ☐ Yönetici sayısını minimumda tutun.
- ☐ Yalnızca gerekli kişisel verileri toplayın ve saklayın.
- ☐ Herhangi bir güvenlik olayını derhal sorumlu kişiye bildirin.

Kuzey Makedonya'daki CSO'lar için Olay Müdahale Planı

Bir dijital güvenlik olayı meydana geldiğinde veya şüphelenildiğinde, aşağıdaki adımlar sırayla uygulanmalıdır:

1. Etkilenen cihazı ağdan ayırın.
2. Olayla ilgili kanıtları (ekran görüntüleri, günlükler, mesajlar) saklayın.
3. İç ekibi ve sorumlu kişiyi bilgilendirin.
4. Öncelikle şifreleri değiştirerek ve iki faktörlü kimlik doğrulamayı etkinleştirerek e-posta hesabını güvenli hale getirin.
5. Etkilenen tüm hesapların şifrelerini sıfırlayın.
6. Bilinmeyen veya şüpheli aktif oturumlardan çıkış yapın.
7. Bilinmeyen yöneticileri ve bağlı uygulamaları kaldırın.

8. Olayları **MKD-CIRT**'e bildirin.
9. Şüpheli siber suçları polis siber suç birimlerine bildirin.
10. Kişisel veri ihlali şüphesi varsa **Kişisel Verilerin Korunması Kurumu'na** danışın.
11. Olayın etkisini değerlendirin.
12. Mümkünse sistemleri ve verileri yedeklerden geri yükleyin.
13. Cihazları ve yazılımları güncelleyin.
14. Gerekirse personel ve gönüllüleri yeniden eğitin.
15. Öğrenilen derslere dayanarak iç politikaları ve kontrol listelerini güncelleyin.

EK 2: Temel Dijital Güvenlik Kontrol Listesi

Faaliyet/Öneri	Kontrol edildi (E/H)
Tüm çevrimiçi satış noktalarında 2FA etkinleştirildi	
Farklı hesaplar için kullanılan benzersiz şifreler	
Şifreler dijital ortamda paylaşılmaz	
Tüm cihazlarda ekran kilidi etkinleştirilir	
Otomatik güncellemeler etkinleştirilmiştir	
Antivirüs etkinleştirilmiş ve güncellenmiştir	
Personel Wi-Fi'si Misafir Wi-Fi'sinden ayrılmıştır	
Yedekleme verileri etkinleştirilmiştir	
Sosyal medyada farklı sayfa rolleri	
Kurtarma e-postası/telefonu CSO'ya ait	
Kamuya açık alanlarda yönetici cihazlarının Wi-Fi'sinin hot spot kullanımı	
İş bitiminde tüm cihazlar kapatılır ve bağlantıları kesilir	

EK 3: Olay Raporlama Kontrol Listesi

Faaliyet/Öneri	**Kontrol edildi (E/H)**
Etkilenen cihazların internet bağlantısı kesildi	
Saldırıya ilişkin kanıtlar toplandı	
E-posta ve diğer sosyal medya şifreleri değiştirildi	
Etkilenen veriler tespit edildi	
Bilinmeyen yöneticiler/uygulamalar kaldırıldı	
2FA etkinleştirildi	
İç ekip olanlar hakkında bilgilendirildi	
Cihazdan bankacılık ve ödeme bilgileri devre dışı bırakıldı	
Sorumlu makam/kurum saldırı hakkında bilgilendirildi	

Norveç'teki Yasal ve Düzenleyici Çerçeve ve Norveç'teki CSO'lar için Öneriler

Norveç'teki Yasal ve Düzenleyici Çerçeve

Norveç'te faaliyet gösteren sivil toplum kuruluşları (STK'lar), AB Genel Veri Koruma Yönetmeliği (GDPR) ve GDPR'yi Norveç hukukuna dahil eden ve tamamlayan Norveç Kişisel Veriler Kanunu'na (Personopplysningsloven) tabidir. Bu yasal çerçeveler, büyüklüklerine bakılmaksızın, kar amacı gütmeyen ve gönüllü kuruluşlar da dahil olmak üzere kişisel verileri işleyen tüm kuruluşlar için geçerlidir. Yetkili denetim makamı, Norveç Veri Koruma Kurumu olan Datatilsynet'tir.

Norveç'teki STK'lar genellikle yararlanıcılar, üyeler, gönüllüler, bağışçılar, çalışanlar ve çoğu durumda savunmasız gruplarla ilgili kişisel verileri işler. Bu veriler arasında isimler, iletişim bilgileri, finansal bilgiler, sağlıkla ilgili veriler, vaka kayıtları veya hassas arka plan bilgileri yer alabilir. Veri denetleyicileri olarak STK'lar, veri koruma yasasının temel ilkelerine uymakla yükümlüdür.

Temel yasal yükümlülükler şunlardır:

İşleme için yasal dayanak: Tüm kişisel veriler, rıza, meşru menfaat, sözleşme gerekliliği veya yasal yükümlülük gibi geçerli bir yasal dayanakla işlenmelidir.

Bilgilendirilmiş rıza (uygulanabilir olduğu durumlarda): Rıza, özgürce verilmiş, spesifik, bilgilendirilmiş ve geri alınabilir olmalıdır.

Şeffaflık: Bireyler, verilerinin nasıl toplandığı, kullanıldığı, saklandığı, paylaşıldığı ve muhafaza edildiği konusunda açık gizlilik bildirimleri yoluyla bilgilendirilmelidir.

Veri minimizasyonu ve amaç sınırlaması: Yalnızca tanımlanmış amaçlar için kesinlikle gerekli olan veriler toplanabilir ve saklanabilir.

İşleme güvenliği: STK'lar, kişisel verileri yetkisiz erişim, kayıp veya kötüye kullanıma karşı korumak için uygun teknik ve organizasyonel önlemleri almalıdır.

Veri saklama ve silme: Kişisel veriler gereğinden fazla süreyle saklanmamalıdır; saklama süreleri ve silme rutinleri tanımlanmalıdır.

İşleyici yönetimi: Kişisel verileri işleyen tüm harici hizmet sağlayıcılarla yazılı veri işleme anlaşmaları yapılmalıdır.

Uluslararası veri aktarımları: Kişisel veriler tercihen AB/AEA içinde saklanmalıdır. Üçüncü ülkelere yapılan aktarımlar için Standart Sözleşme Maddeleri (SCC) ve ek önlemler gibi geçerli koruma tedbirleri gereklidir.

İhlal bildirimi: Kişisel veri ihlalleri derhal değerlendirilmeli ve gerektiğinde 72 saat içinde Datatilsynet'e bildirilmelidir.

Datatilsynet, Norveçli STK'lar arasında belirsiz onay rutinleri, AB/AEA dışındaki güvenli olmayan bulut depolama, belgelenmiş iç prosedürlerin eksikliği ve aşırı veri saklama gibi yaygın zorlukları defalarca tespit etmiştir.

Veri Korumada Etik Sorumluluklar

Yasal yükümlülüklerin ötesinde, Norveçli STK'lar, işledikleri verilerin sahiplerinin mahremiyetini, onurunu ve güvenliğini korumakla etik bir yükümlülüğe sahiptir. Birçok STK, verilerin ifşa edilmesinin ciddi kişisel zarara yol açabileceği, mülteciler, çocuklar, şiddet mağdurları veya siyasi açıdan risk altında olan kişiler gibi savunmasız durumdaki kişilerle çalışmaktadır.

Veri ihlalleri şu sonuçlara yol açabilir:

- Yararlanıcılar ve gönüllülere zarar verme,
- Bağışçıların, ortakların ve halkın güveninin kaybı,
- Yasal sonuçlar ve mali cezalar,
- İtibar kaybı ve operasyonel aksaklıklar.

Bu nedenle, etik veri işleme, ihtiyati bir yaklaşım gerektirir: gerekli minimum veriyi toplamak, veriyi etkili bir şekilde korumak ve yalnızca kesinlikle gerekli olduğunda paylaşmak.

Günlük Uygulamalarda Uyumluluk Sağlamak

Birçok Norveçli STK için, özellikle gönüllülere ve sınırlı BT kapasitesine dayananlar için, uyumun pratik ve sürdürülebilir olması gerekir.

Etkili uygulama şunları içerir:

- Veri koruma ve dijital güvenlikten sorumlu bir kişi belirlemek, bu kişi yarı zamanlı çalışıyor veya başka bir görevle birleştirilmiş olsa bile.
- Veri Koruma Politikası ve veri işleme kılavuzları gibi kısa ve erişilebilir iç belgeler geliştirmek.

- Bireysel kullanıcı hesapları, rol tabanlı erişim ve aktif olmayan kullanıcıların zamanında kaldırılması dahil olmak üzere erişim kontrol rutinleri uygulamak.
- Kişisel veriler için güvenli depolama çözümleri, tercihen AB/AEA tabanlı bulut hizmetleri seçmek.
- Tüm harici sağlayıcılarla veri işleme anlaşmalarının yapılmasını sağlamak.
- Personel ve gönüllülere kimlik avı, şifreler ve güvenli veri işleme konusunda düzenli farkındalık eğitimi verilmesi.
- Tanımlama, sınırlama, belgeleme ve eskalasyonu kapsayan basit bir olay müdahale rutini sürdürmek.
- Bu rutinleri günlük operasyonlara dahil etmek, uyumluluğun reaktif değil sürekli olmasını sağlar.

Norveç'ten Vaka Çalışmaları

Vaka Çalışması 1: Bağış Toplama Kampanyası Sırasında Hedefli Kimlik Avı (Oslo, 2023)

2023 yılında, Oslo merkezli küçük bir insani yardım STK'sı, yıllık bağış toplama kampanyası sırasında hedefli bir kimlik avı kampanyasına maruz kaldı. Saldırganlar, STK'nın bağış sayfasının sahte bir versiyonunu oluşturdu ve destekçilere, kuruluşun "ödeme sistemini güncellediğini" iddia eden e-postalar gönderdi. STK dolandırıcılığın farkına varmadan önce birkaç bağışçı kart bilgilerini girdi. Olay, bağışçıların güvenini zedeledi ve bankalarla ve etkilenen destekçilerle sorunları çözmek için önemli miktarda zaman ve çaba gerektirdi.

E-posta hesaplarında iki faktörlü kimlik doğrulama, etki alanı izleme ve kimlik avı uyarı işaretleri konusunda personel eğitimi gibi temel güvenlik önlemlerinin bir kombinasyonu, olayın etkisini azaltabilir veya saldırıyı tamamen önleyebilirdi.

Tartışma Soruları:

- Bu olayda istismar edilen başlıca güvenlik açıkları nelerdi?
- E-postaların ve bağış sayfasının sahte olduğunu gösteren uyarı işaretleri nelerdi?
- Hangi temel dijital güvenlik önlemleri zararı önleyebilir veya sınırlayabilirdi?

İlgili Modüller ve Müfredatta Kullanımı

- **Modül 1 – Siber Güvenliğin Temelleri:**
  Bağışçıları ve destekçileri hedef alan kimlik avı ve güven istismarının temel bir örneği olarak kullanılır.
- **Modül 4 – Yaygın siber tehditler (Kimlik Avı ve Sosyal Mühendislik):**
  Sahte web siteleri ve kimlik sahtekarlığı dahil olmak üzere gelişmiş kimlik avı tekniklerini gösterir.
- **Modül 6 – Sosyal Medya ve Çevrimiçi Varlık Güvenliği:**
  Kurumsal itibar, kamu güveni ve güvenli çevrimiçi bağış toplama uygulamaları tartışılırken referans alınabilir.
- **Modül 7 – Güvenlik Kültürü Geliştirme:**
  Personel farkındalığı, bağışçı iletişim protokolleri ve önleyici eğitim konularındaki tartışmaları destekler.

Önerilen Kullanım:

Vaka analizi, ardından bağış toplama iletişimlerinde kimlik avı uyarı işaretlerini belirleme ve güvenli bağışçı iletişim kontrol listesi tasarlama konusunda grup çalışması.

Vaka Çalışması 2: Güncel Olmayan Eklenti Nedeniyle Web Sitesi Tahribatı (Bergen, 2022)

2022 yılında, Bergen merkezli küçük bir insan hakları STK'sının WordPress web sitesi, saldırganların eski bir eklentiyi istismar etmesiyle tahrip edildi. Ana sayfa siyasi propaganda ile değiştirildi ve kuruluş, yönetici paneline erişimini kaybetti. STK'nın web sitesinin güncel yedeklemesi olmadığı için, sitenin geri yüklenmesi iki haftadan fazla sürdü ve dışardan teknik yardım gerektirdi. Olay, gönüllüler ve bağışçılarla iletişimi kesintiye uğrattı ve itibar sorunlarına yol açtı.

Rutin yazılım güncellemeleri, güçlü yönetici şifreleri, iki faktörlü kimlik doğrulama ve otomatik yedeklemeler, saldırının etkisini önemli ölçüde azaltabilirdi**.**

Tartışma Soruları:

- Bu olaya hangi teknik ve organizasyonel zayıflıklar katkıda bulundu?
- Yedeklemelerin olmaması, kuruluşun kurtarma yeteneğini nasıl etkiledi?
    - Modülün ana konularında tartışılan önleyici tedbirlerden hangileri gelecekte benzer olayların önlenmesine yardımcı olabilir?

Norveç'teki CSO'lar için Pratik Dijital Güvenlik ve Veri Koruma Kontrol Listeleri

İlgili Modüller ve Müfredatta Kullanımı

- **Modül 3 – Cihazlar ve Altyapı Güvenliği:**
  Eski yazılım ve güvenli olmayan web sitesi altyapısı ile ilgili riskleri gösteren temel vaka.
- **Modül 5 – Veri Koruma ve Gizlilik Uyumluluğu:**
  Kurumsal süreklilik için veri kullanılabilirliği, bütünlüğü ve yedeklemelerin önemini vurgular.
- **Modül 6 – Sosyal Medya ve Çevrimiçi Varlık Güvenliği:**
  Web sitesi bütünlüğü, itibar yönetimi ve içerik kontrolü ile ilgili tartışmalar için önemlidir.

- **Modül 7 – Güvenlik Kültürü Geliştirme:**
  Yalnızca "BT görevleri" değil, güncellemeler ve bakım için ortak sorumluluk bilincini destekler.

Önerilen Kullanım:

Senaryo temelli tartışmanın ardından web sitesi bakımı, güncelleme rutinleri ve yedekleme planlaması ile ilgili pratik bir kontrol listesi alıştırması yapılır.

EK-1: Norveç'teki CSO'lar için Yasal ve GDPR Uyumluluk Kontrol Listesi

☐ Kuruluş tarafından işlenen tüm kişisel veriler tanımlanır ve belgelenir.

☐ Her bir işleme faaliyeti için yasal dayanak tanımlanmış ve kaydedilmiştir.

☐ Gizlilik Bildirimi/Veri Koruma Politikası mevcuttur ve iletilmiştir.

☐ Onay mekanizmaları açıktır ve gerektiğinde geri alınabilir.

☐ Veri saklama süreleri tanımlanmış ve uygulanmaktadır.

☐ Tüm harici hizmet sağlayıcılarla veri işleme anlaşmaları mevcuttur.

☐ Kişisel veriler AB/AEA içinde saklanır veya geçerli güvenlik önlemleriyle korunur.

☐ Veri ihlali bildirim prosedürü mevcuttur ve 72 saat kuralı bilinmektedir.

EK-2. Temel Dijital Güvenlik Kontrol Listesi

☐ Tüm kurumsal hesaplar için güçlü, benzersiz şifreler kullanılmaktadır.

☐ Bir şifre yöneticisi kullanılmaktadır.

☐ E-posta, bulut ve sosyal medya hesaplarında iki faktörlü kimlik doğrulama etkinleştirilmiştir.

☐ Cihazlar ekran kilitleri ve güçlü PIN'ler/parolalarla korunmaktadır.

☐ İşletim sistemleri ve uygulamalar otomatik olarak güncellenmektedir.

☐ Antivirüs/kötü amaçlı yazılımdan koruma yazılımı yüklenmiştir ve günceldir.

☐ Önemli veriler düzenli ve güvenli bir şekilde yedekleniyor.

EK -3. Bulut ve Hesap Yönetimi Kontrol Listesi

☐ Bireysel kullanıcı hesapları kullanılır; paylaşılan oturum açma işlemlerinden kaçınılır.

☐ Erişim hakları role dayalıdır ve gereklilikle sınırlıdır.

☐ Etkin olmayan hesaplar derhal kaldırılır.

☐ Bulut erişim izinleri periyodik olarak gözden geçirilir.

☐ Hassas dosyalar kısıtlamalar ve süre sınırlamaları ile paylaşılır.

☐ Mümkün olduğunda etkinlik günlükleri etkinleştirilir.

EK-4. Sosyal Medya ve Çevrimiçi Varlık Kontrol Listesi

☐ Tüm sosyal medya hesaplarında iki faktörlü kimlik doğrulama etkinleştirilir.

☐ Yönetici rolleri bireysel olarak atanır.

☐ Kurtarma e-posta adresleri ve telefon numaraları günceldir.

☐ Yönetici listeleri düzenli olarak gözden geçirilir.

☐ Hesap ele geçirme veya kimlik sahtekarlığı için bir müdahale planı mevcuttur.

☐ Web sitesi CMS ve eklentileri düzenli olarak güncellenir.

EK-5. Olaylara Müdahale ve Raporlama Kontrol Listesi

☐ Güvenlikten sorumlu bir kişi belirlenmiştir.

☐ Personel, şüpheli olayları kurum içinde nasıl bildireceğini bilmektedir.

☐ Yazılı bir olay müdahale prosedürü mevcuttur.

☐ Olaylardan sonra kanıtlar ve günlükler saklanır.

☐ Ciddi siber olaylar uygun olduğunda NorCERT'e bildirilir.

☐ Kişisel veri ihlalleri gerektiğinde Datatilsynet'e bildirilir.

☐ Alınan dersler belgelenir ve prosedürler güncellenir.

EK-6. Personel ve Gönüllü Farkındalık Kontrol Listesi

☐ Yeni personel ve gönüllüler güvenlik ve gizlilik konusunda oryantasyon eğitimi alır.

☐ Kabul Edilebilir Kullanım ve Veri Koruma politikaları kabul edilir.

☐ Düzenli olarak yenileme eğitimi verilir.

☐ CSO çalışmaları için kişisel cihazların kullanımına ilişkin açık kurallar mevcuttur.

☐ Hassas veriler güvenli olmayan kanallar üzerinden paylaşılmaz.

Öneriler ve Pratik Tavsiyeler

Norveçli STK'lar, karmaşık teknik çözümler yerine basit, iyi belgelenmiş rutinlere öncelik vermelidir. Net iç politikalar, temel teknik güvenlik önlemleri, düzenli eğitim ve etik farkındalığı bir araya getirerek, kuruluşlar GDPR ve Norveç yasalarına uyumu sürdürürken dijital risklerini önemli ölçüde azaltabilirler.

CSO'ların Dikkat Etmesi Gereken Norveç'e Özgü Ek Noktalar

1. Gönüllülerin İşten Ayrılması ve Erişim Yaşam Döngüsü Yönetimi

Norveçli STK'lar büyük ölçüde kısa süreli gönüllülere, stajyerlere ve yarı zamanlı personele güvenmektedir. Datatilsynet ve NSM tarafından bildirilen en yaygın risklerden biri, bireyler kuruluştan ayrıldığında erişim haklarının iptal edilmemesidir.

CSO'ların bilmesi gerekenler:

- Her işe alım için karşılık gelen bir işten ayrılma kontrol listesi olmalıdır.
- Hesaplar, e-posta erişimi, bulut klasörleri ve sosyal medya rolleri derhal kaldırılmalıdır.
- Paylaşılan hesaplar, gönüllü temelli kuruluşlarda riski önemli ölçüde artırır.
- Bu nokta, Modül 7'yi (Güvenlik Kültürü ve Politikaları) güçlendirir.

2. Ulusal Kimlik Numaraları ve Hassas Tanımlayıcılar

Bazı Norveçli STK'lar fødselsnummer (ulusal kimlik numaraları), sağlık verileri, sığınma ile ilgili bilgiler veya yasal dava ayrıntılarını işler.

Bunun önemi:

- Bu veri türleri, GDPR kapsamında daha yüksek koruma standartları gerektirir.
- Güvenli olmayan elektronik tablolarda veya genel bulut klasörlerinde saklamak yüksek riskli bir uygulamadır.
- Şifreleme ve sıkı erişim kontrolü şarttır.
- Bu konu doğal olarak Modül 5 (Veri Koruma ve Gizlilik) kapsamına girer, ancak Modül 7 eğitiminde çapraz referans olarak kullanılabilir.

3. Bulut Hizmetleri ve Schrems II Farkındalığı

Birçok Norveçli CSO, veri aktarımının sonuçlarını anlamadan küresel bulut hizmetlerini (Google, Microsoft, Dropbox) kullanmaktadır.

Norveç'e özgü gerçeklik:

- Datatilsynet, CSO'ların AB/AEA veri yerleşim yeri konusunda farkında olmasını beklemektedir.
- AB/AEA dışına yapılan transferler için güvenlik önlemleri (SCC'ler + risk değerlendirmesi) gereklidir.
- "Büyük bir sağlayıcı kullanıyoruz" yeterli bir gerekçe değildir.
- Bu, Modül 8'i (İleri Düzey Konular) hukuki-teknik açıdan güçlendirmektedir.

4. NorCERT ve Datatilsynet Arasındaki Koordinasyon

CSO'lar genellikle kime neyi bildirecekleri konusunda kafaları karışır.

CSO'ların bilmesi gereken net ayrım:

- NorCERT (NSM): ciddi siber güvenlik olayları (fidye yazılımı, hesap ele geçirme, hizmet kesintisi),
- Datatilsynet: kişisel veri ihlalleri (GDPR – 72 saat içinde),
- Bazı olaylar her iki kuruma da bildirim gerektirir,
- Bu, Modül 7'ye (Olaylara Müdahale ve Raporlama) önemli bir eklemedir.

5. Psikolojik Güvenlik ve "Suçlamayan" Raporlama Kültürü

Norveç organizasyon kültürü güvene ve düz hiyerarşilere büyük önem verir, ancak personel utançtan korkarsa bu durum ters tepebilir.

En iyi uygulama:

- Personel, hataları (tıklanan kimlik avı bağlantısı, kaybolan cihaz) derhal bildirmeleri için teşvik edilmelidir.
- Suçlamama kültürü, hasarı azaltır ve müdahale süresini iyileştirir.
- Bu, teknik kontrollerin ötesine geçen Modül 7 için önemli bir kültürel katmandır.

6. Yönetim Kurulu Sorumluluğu ve Yönetişim Denetimi

Norveç'te, CSO'ların yönetim kurullarından iyi yönetişimin bir parçası olarak dijital riskleri anlamaları giderek daha fazla beklenmektedir.

Yönetim kurullarının bilmesi gerekenler:

- Siber güvenlik ve veri koruma, sadece BT meseleleri değil, yönetişim meseleleridir.
- Yönetim kurulları temel güvenlik politikalarını ve olay müdahale planlarını onaylamalıdır.
- Ciddi olaylar, liderlik için yasal ve itibar açısından sonuçlar doğurabilir.

- Bu, Modül 7 veya Modül 8 altında bir yönetişim notu olarak eklenebilir.

7. Stratejik Hedef Olarak Sivil Toplum

Demokrasi, insan hakları, dış politika veya uluslararası yardım alanlarında çalışan Norveçli STK'lar rastgele kurbanlar değil, stratejik hedefler olarak kabul edilmektedir.

Sonuçlar:

- Saldırılar ısrarcı, kurnaz ve istihbarat odaklı olabilir
- Tüm tehditler para amaçlı değildir; bazıları gözetim veya aksaklık amaçlıdır
- NSM tehdit brifinglerinin farkında olmak çok önemlidir
- Bu, Modül 1 ve Modül 8'i Norveç'e özgü bir tehdit modeliyle pekiştirir.

EK

Ek 1: Anahtar Terimler Sözlüğü

- ***Antivirüs (AV):*** *Bilgisayarlardaki kötü amaçlı yazılımları (virüsler, truva atları vb.) algılayan ve kaldıran yazılım. Örnek: Windows Defender veya Avast.*
- ***Yedekleme:*** *Kurtarma amacıyla ayrı olarak saklanan verilerin ekstra kopyası, örneğin, orijinalleri kaybolduğunda geri yüklenebilmeleri için dosyaları harici bir sabit sürücüye veya bulut hizmetine kaydetmek.*
- ***Kaba kuvvet saldırısı:*** *Saldırganların doğru şifreyi bulana kadar birçok şifre veya anahtar denediği bir yöntem. Güçlü şifreler ve kilitleme politikaları buna karşı savunma sağlar.*
- ***Veri İhlali:*** *Hassas bilgilere yetkisiz olarak erişilen veya bu bilgilerin yetkisiz olarak ifşa edildiği bir olay. Hackleme, kayıp cihazlar vb. yoluyla meydana gelebilir.*
- ***Şifreleme:*** *Verileri, anahtar olmadan okunamayan şifreli bir biçime dönüştürme işlemi. Bilgilerin gizliliğini korur (örneğin, HTTPS web trafiğini şifreler).*
- ***Güvenlik Duvarı:*** *Güvenlik kurallarına göre gelen ve giden ağ trafiğini izleyen ve filtreleyen bir ağ güvenlik cihazı veya yazılımıdır. Yetkisiz erişimi engellerken, meşru iletişime izin verir.*
- ***Kötü amaçlı yazılım:*** *Sistemlere zarar vermek veya bunları istismar etmek için tasarlanmış kötü amaçlı yazılım. Virüsler, fidye yazılımları, casus yazılımlar vb. içerir. Genellikle e-posta ekleri veya kötü amaçlı web siteleri aracılığıyla yayılır.*
- ***Çok Faktörlü Kimlik Doğrulama (MFA / 2FA):*** *Oturum açmak için birden fazla doğrulama yöntemi kullanma (ör. şifre + telefonda tek kullanımlık kod). Hesap güvenliğini önemli ölçüde artırır.*
- ***Oltalama:*** *Güvenilir bir kuruluş gibi davranarak kişileri hassas bilgileri ifşa etmeye veya kötü amaçlı yazılım yüklemeye ikna etmek için yapılan dolandırıcılık girişimi (genellikle e-posta yoluyla). Hedefli oltalama, belirli kişileri veya kuruluşları hedef alan girişimleri ifade eder.*

- ***Fidye Yazılımı:*** *Kurbanın verilerini şifreleyen ve şifre çözme anahtarı için ödeme talep eden kötü amaçlı yazılım. Yedekleme yoksa, kurbanlar erişimi geri kazanmak için hackerlara ödeme yapma baskısıyla karşı karşıya kalır.*
- ***Sosyal Mühendislik:*** *İnsanları gizli bilgileri ifşa etmeye veya güvenliği tehlikeye atan eylemler gerçekleştirmeye yönlendiren taktikler. Kimlik avı bunun bir türüdür; diğerleri arasında bahane uydurma veya yemleme sayılabilir. İnsanların güvenini ve merakını kullanır.*
- ***VPN (Sanal Özel Ağ):*** *Cihazınızdan bir sunucuya internet üzerinden şifreli bir tünel oluşturarak aktarımdaki verileri koruyan ve IP adresinizi gizleyen bir araçtır. Güvenli bağlantı için halka açık Wi-Fi ağlarında kullanışlıdır.*
- ***Güvenlik Açığı:*** *Saldırganların yetkisiz erişim elde etmek veya yetkisiz eylemler gerçekleştirmek için yararlanabilecekleri yazılım, donanım veya prosedürdeki zayıflık. Yama, bilinen güvenlik açıklarını giderir.*
- ***Wi-Fi Şifreleme (WPA2/WPA3):*** *Cihazlar ve yönlendirici arasındaki trafiği şifreleyen kablosuz ağlar için güvenlik protokolleri. Dinlenmeyi önlemek için Wi-Fi'nizin en az WPA2 ve güçlü bir parolayı kullandığından emin olun.*

Ek II: Parola Politikası Şablonu (Örnek)

Amaç: Kuruluşun bilgi sistemlerini korumak için şifre oluşturma, kullanma ve yönetme gerekliliklerini belirlemek.

Kapsam: Bu politika, organizasyonel çalışmalar için BT sistemlerini (bilgisayarlar, e-posta, uygulamalar ve web siteleri dahil) kullanan [Organizasyon Adı]'nın tüm personeli, gönüllüleri ve yüklenicileri için geçerlidir.

Politika Beyanları:

- *Tüm kullanıcı şifreleri en az 12 karakter uzunluğunda olmalı, büyük ve küçük harfler, rakamlar ve özel semboller içermelidir.*
- *Varsayılan şifreler, ilk kullanımdan hemen sonra değiştirilmelidir.*

- *Şifreler kişiler arasında paylaşılmamalı veya güvenli olmayan yerlere yazılmamalıdır.*
- *Organizasyon sistemlerine ve e-posta hesaplarına tüm uzaktan erişimler için iki faktörlü kimlik doğrulama (2FA) gereklidir.*
- *Kritik sistemlerin (finansal, bağışçı veritabanları) şifreleri 90 günde bir değiştirilmelidir.*
- *Kullanıcılar, diğer (kamuya açık) hesaplarda kullanılmış veya ihlallerde sızdırılmış şifreleri tekrar kullanmamalıdır.*
- *Bir şifrenin güvenliğinin ihlal edildiğinden şüpheleniliyorsa, derhal değiştirilmeli ve BT/güvenlik görevlisine bildirilmelidir.*

Rolleri ve Sorumlulukları:

- *Kullanıcılar bu kurallara uymalı ve şüpheli durumları bildirmelidir.*
- *BT personeli, teknik kontroller (ör. şifre yöneticileri, başarısız denemelerden sonra hesap kilitlemeleri) yoluyla şifre kurallarını uygulayacaktır.*
- *Güvenlik görevlisi, uyumluluğu gözden geçirecek ve politikayı yıllık olarak güncelleyecektir.*

Uygulama: Bu politikanın ihlali, erişim ayrıcalıklarının iptal edilmesine veya diğer disiplin cezalarına neden olabilir.

Ek III: Yedekleme Politikası Şablonu (Örnek)

Amaç: Kritik verilerin düzenli olarak yedeklenmesini ve kayıp, bozulma veya felaket durumunda geri yüklenebilmesini sağlamak.

Kapsam: [Kuruluş Adı]'nın kurumsal sunucularında, iş istasyonlarında ve ağ depolama cihazlarında depolanan tüm veriler için geçerlidir.

Politika Beyanları:

- *Önemli veriler (bağışçı kayıtları, finansal dosyalar, proje veritabanları vb.) en az günde bir kez yedeklenmelidir.*
- *Yedeklemeler, işlemleri geri yüklemek için gerekli sistem yapılandırmalarını ve uygulamaları içermelidir.*
- *Yedek kopyalar, yerel olaylardan kaynaklanan kayıpları önlemek için tesis dışında veya ayrı bir bulut depolama alanında güvenli bir şekilde saklanmalıdır.*
- *Tam yedeklemeler haftalık olarak, artımlı yedeklemeler ise günlük olarak (veya çok hassas veriler için daha sık) gerçekleştirilir.*
- *Verilerin kurtarılabilmesini sağlamak için aylık olarak yedekleme bütünlüğü kontrolleri ve test geri yüklemeleri yapılmalıdır.*
- *Saklama: En az bir haftalık günlük yedeklemeleri tesis içinde saklayın ve aylık tam yedeklemeleri en az bir yıl boyunca tesis dışında arşivleyin.*
- *Yedekleme verilerine erişim, yalnızca yetkili BT veya yönetim personeli ile sınırlıdır.*

Rolleri ve Sorumlulukları:

- *BT personeli, bu programa göre otomatik yedeklemeleri yapılandırmalı ve izlemelidir.*
- *Atanan Yedekleme Yöneticisi, yedekleme prosedürlerini belgelendirecek ve yedeklemenin tamamlandığını ve bütünlüğünü doğrulayacaktır.*
- *Tüm personel, yedekleme programında belirtilen belirlenen konumlara kritik iş dosyalarını kaydetmekten sorumludur.*

Uygulama: Uyulmaması veri kaybına neden olabilir ve [Kuruluş Adı] yönetimi tarafından uygun şekilde ele alınacaktır.

Ek IV: Varlık Envanteri Şablonu (Örnek)

Varlık Kimliği	Varlık Adı	Kategori	Sahibi/Departman	Konum	Hassasiyet Düzeyi	Gerekli Koruma	Not
A001	Bağışçı Veritabanı	Yazılım/Veri	Program Direktörü	Yerinde	Yüksek	Şifreli, parola korumalı	Bağışçıların kişisel bilgilerini içerir
A002	Finansal Sunucu	Donanım/Sunucu	BT Departmanı	Veri Merkezi	Yüksek	Düzenli yedeklemeler, erişim için 2FA	Muhasebe yazılımını destekler
A003	Dizüstü	Donanım/Cihaz	Çeşitli personel	Ofis/Saha	Orta	Zorunlu disk şifreleme, şifre	Her cihazın bir kimlik etiketi vardır
A004	Web	Yazılım	İletişim	Bulut tabanlı	Orta	HTTPS etkin, güncellenmiş CMS	Halka açık web sitesi
A005	CRM Yazılımı	Yazılım	Veri Yöneticisi	Bulut	Yüksek	Rol tabanlı erişim, günlük yedeklemeler	Yararlanıcı bilgilerini izler

(Not: 'Hassasiyet Seviyesi' Düşük/Orta/Yüksek olabilir. 'Gerekli Koruma' her bir varlık için güvenlik önlemlerini özetler.)

Ek V: Basit Risk Matrisi Şablonu (Örnek)

	Etki: Düşük (1)	**Etki: Orta (2)**	**Etki: Yüksek (3)**
Olasılık: Yüksek (3)	Yüksek Risk (3×1)	Kritik Risk (3×2)	Kritik Risk (3×3)
Olasılık: Orta (2)	Orta Risk (2×1)	Yüksek Risk (2×2)	Kritik Risk (2×3)
Olasılık: Düşük (1)	Düşük Risk (1×1)	Orta Risk (1×2)	Yüksek Risk (1×3)

- **Risk Seviyeleri:** Olasılık ve etki puanlarını çarparak riski hesaplayın. Örneğin, Olasılık=3 (Yüksek) ve Etki=2 (Orta) olarak derecelendirilen bir senaryo, 6 (Kritik Risk) risk puanı verir.
- Bu matrisi kullanarak, önce yüksek riskli senaryolara öncelik verin (Kritik > Yüksek > Orta > Düşük).

SONUÇ

Dijital güvenlik, tek seferlik bir proje veya kontrol edilmesi gereken bir kutu değildir – bu, sürekli bir taahhüttür. Bu e-kitabı sonlandırırken, her bölümde yankı bulan temel bir dersi yeniden vurgulamak istiyoruz: sivil toplum kuruluşlarımızın çevrimiçi güvenliğini sağlamak, sürekli dikkat, uyum ve özen gerektirir. Başlangıçta ele aldığımız siber tehdit ortamı sürekli olarak gelişmekte ve saldırganlar her gün savunmayı aşmak için yeni yollar aramaktadır. Bugün güvence altına aldığımız şeyler, yarın yeni taktiklerle sınanabilir.

Bu gerçeklik, dijital güvenliğin uzun vadede radarımızda kalması gerektiği anlamına gelir; bütçeleme veya program yönetimi gibi planlama ve operasyonlarımızın ayrılmaz bir parçası olmalıdır. Siber güvenliği ikinci planda tutmayı göze alamayız; aksine, bu konu çalışma şeklimizin alışılmış bir parçası haline gelmelidir. Riskler çok yüksektir – tek bir başarılı saldırı, hassas yararlanıcı verilerini açığa çıkarabilir veya bir savunuculuk kampanyasını rayından çıkarabilir; bu nedenle dijital güvenlik konusunda uyanık olmak, misyonlarımızı yerine getirmenin ayrılmaz bir parçasıdır. Bu e-kitaptan edindiğiniz bilgiler ve stratejiler, üzerine inşa edebileceğiniz bir temeldir. İleride, güvenliği sağlamak, bu konuları düzenli olarak gözden geçirmek, yeni tehditler (ve çözümler) ortaya çıktıkça uygulamalarınızı güncellemek ve güvenlik hakkında öğrenmenin sürekli bir süreç olduğu bir ortam yaratmak anlamına gelecektir. Kısacası, dijital güvenlik çalışmaları asla "bitmez", ancak aşılamaz da değildir. Kuruluşunuzun siber savunmasını güçlendirmek için attığınız her adımla, daha dirençli bir sivil topluma katkıda bulunuyorsunuz.

Güvenliği Korumak Artık Kolay: Önemli bir çıkarım, güvenliğin aşırı derecede karmaşık olması gerekmediğidir. Genellikle, basit şeyleri tutarlı bir şekilde yapmakla ilgilidir. Güçlü, benzersiz parolalar (ve bir parola yöneticisi) kullanın. Yazılımlarınızı güncel tutun. Beklenmedik bağlantılara tıklamadan önce iki kez düşünün. Verilerinizi düzenli olarak yedekleyin. Bu temel uygulamalar, alışkanlık haline getirildiğinde tehditlerin büyük bir kısmını ortadan kaldırır. Gördüğümüz gibi, birçok saldırı gözden kaçan temel unsurlar nedeniyle başarılı olmaktadır. Bu nedenle, bu unsurlara dikkat ederek saldırganların kullandığı yaygın kapıları kapatabilirsiniz.

Yeni Zorluklara Uyum Sağlama: Dijital dünya değişmeye devam edecek. Beş yıl önce, fidye yazılımları bu kadar yaygın değildi; bugün ise en büyük tehditlerden biri. Gelecekte, yapay zeka araçlarına yönelik saldırılar veya daha sofistike deepfake kimlik avı saldırıları ile mücadele

etmek zorunda kalabiliriz. CSO'nuz uyum sağlayabilmeli ve öğrenmeye devam etmelidir. İlgili bir güvenlik beslemesine abone olun veya yeni tehditlerin tartışıldığı bir topluluğa katılın . Böylece, ortaya çıkan sorunlar hakkında erken uyarı alırsınız. Önemli bir değişiklik olduğunda (örneğin, mobil kötü amaçlı yazılımlar artarsa, bu konuda özel bir oturum düzenleyin) personel için periyodik yenileme eğitimi veya yeni modüller düşünün. Sürekli iyileştirme zihniyetini benimseyin, her yakın kaçırma veya olayı savunmayı daha da güçlendirmek için bir öğrenme fırsatı olarak değerlendirin.

Kaynakları Akıllıca Tahsis Etme: Güvenlik, kuruluşunuzun sürdürülebilirliğine yapılan bir yatırımdır. Biraz bütçe (daha iyi ekipman, yazılım veya eğitim süresi için) ve yönetimin ilgisi gerekebilir. Ancak gösterildiği gibi, güvenliği sağlamamanın maliyeti (ihlaller, kesinti süreleri, güven kaybı) çok daha yüksektir. Uzun vadeli stratejinizde güvenliği planlayın; örneğin, teknoloji güncellemeleri veya eğitim için hibe bütçesine bir kalem ekleyin. 6. Bölümde tartışıldığı gibi, CSO'lar için ücretsiz veya indirimli hizmetlerden (ücretsiz Google Workspace'ten bağışlanan güvenlik duvarlarına kadar pek çok seçenek vardır) yararlanın. Ayrıca, güvenlik görevlerini ve gelişmeleri takip eden bir güvenlik sorumlusu (tam zamanlı olmasa bile) atamayı düşünün; sorumlu bir kişinin olması, bu konunun gözden kaçmamasını sağlar.

Liderlikten destek: Sürdürülebilir güvenlik, liderliğin desteğine ihtiyaç duyar. Liderler, iyi uygulamaları örnek alarak ve kaynakları tahsis ederek güvenliğe öncelik verdiklerinde, bunun herkes için önemli olduğu mesajını açıkça vermiş olurlar. Bu, herhangi bir direnişi (örneğin "bununla gerçekten uğraşmamız gerekiyor mu?") de önler: yönetici 2FA ile oturum açıyor ve aynı eğitimlere katılıyorsa, bu çabayı meşrulaştırır. Bu nedenle, yönetim ekibinizin tamamen desteklediğinden ve hatta güvenlik girişimlerini savunduğundan emin olun.

Tüm Ekibinizi Dahil Edin**:** Güvenli bir gelecek, herkesin rol oynamasına bağlıdır. En yeni stajyerden yönetim kurulu üyelerine kadar, her kişi zincirin bir parçasıdır. Güvenliği kapsayıcı tutun: Soruları teşvik edin, hataları utandırmayın, uyanıklığı ödüllendirin. Bazı kuruluşlar, performans değerlendirmelerine veya iş tanımlarına güvenlik yetkinliğini dahil ederek, bunun tüm roller için bir beklenti olduğunu vurgular. Personeli güçlendirerek (onlara bilgi ve araçlar sağlayarak), esasen CSO'nuzun etrafında bir insan güvenlik duvarı oluşturmuş olursunuz. Bir

deyişle, "kullanıcıların güvenlik bilinci, sahip olabileceğiniz en ucuz ve en etkili güvenlik duvarıdır."

İyimserlikle Geleceğe Bakmak: Siber tehditlerden korkmak kolay olabilir, ancak bilgi ve hazırlık dengesini sizin lehinize çevirebileceğini unutmayın. Dünyanın dört bir yanındaki birçok CSO , kaynakları yetersiz olanlar bile, proaktif ve birleşik bir şekilde hareket ederek kendilerini başarıyla savunmuştur. Bu e-kitabı okuyarak ve içindeki kılavuzları uygulayarak, kuruluşunuzun dijital geleceğini güvence altına almak için önemli bir adım attınız. Bu bir yolculuktur – engeller ve muhtemelen olaylar olacaktır – ancak şu anda attığınız her adım bunların etkisini azaltır ve iyileşmenizi hızlandırır.

Sivil toplumun bazen siber saldırıların özel hedefi olduğu bir dünyada, dijital güvenliğe olan bağlılığınız, davanıza ve hizmet ettiğiniz insanlara olan bağlılığınız anlamına da gelir. Bu, önemli çalışmalarınızın önlenebilir aksaklıklar nedeniyle sekteye uğramadan devam edebileceği anlamına gelir. Bu, insanların verilerini işlemek veya seslerini duyurmak için size duydukları güvenin sağlam temellere dayandığı anlamına gelir.

Sonuç olarak, geliştirilmesi gereken birkaç uzun vadeli güvenlik alışkanlığını özetleyelim:

- *Risk değerlendirmenizi düzenli olarak gözden geçirin ve güvenlik planınızı güncelleyin (en azından yılda bir kez veya önemli değişiklikler olduğunda).*
- *Öğrenmeye devam edin – web seminerlerine katılın, kılavuzları okuyun, meslektaşlarınızla görüşlerinizi paylaşın.*
- *Bağlantıda kalın – güvenlik çabalarınızı izole etmeyin; birlikte öğrenen ve savunma yapan topluluğun bir parçası olun.*
- *Hazırlıklı olun – olay müdahale planınızı sürdürün ve gerektiğinde hazır olması için ara sıra test edin.*
- *Tetikte olun, ancak korkmayın. İyi uygulamalarla, dijital tehditler konusunda endişeli değil, kendinden emin ve sakin olabilirsiniz.*

Güvenli bir geleceğe doğru: Dijital güvenliği CSO'nuzun günlük operasyonlarının ve kültürünün ayrılmaz bir parçası haline getirerek, geleceğe karşı iyi bir konumda olursunuz. Şüphesiz zorluklar ortaya çıkacaktır, ancak bunları aşmak için gerekli araçlara, bilgiye ve desteğe

sahipsiniz. Bunu yaparak, sadece kuruluşunuzu korumakla kalmaz, aynı zamanda daha geniş sivil toplum için daha güvenli bir dijital ortama da katkıda bulunursunuz.
İleride, sürekli iyileştirmeye kararlı olun. Güvenlik alanındaki başarılarınızı kutlayın ("bu çeyrekte kimse phishing tuzağına düşmedi!" veya "küçük bir sunucu çökmesinden sonra yedeklemeden verileri başarıyla geri yükledik" gibi küçük başarılar bile). Her türlü aksilikten ders alın. Ve nedenini daima hatırlayın: Güvenli bir CSO, misyonunu daha iyi yerine getirebilir ve kesintisiz olarak olumlu bir etki yaratabilir.

Dayanıklılık oluşturmak, vurguladığımız bir diğer konudur ve burada, sonuç bölümünde tekrar vurgulanması gereken bir konudur. Dayanıklılık, yalnızca saldırıları önlemeye çalışmak değil, aynı zamanda bir sorun meydana geldiğinde kuruluşunuzun yeniden ayağa kalkabilmesini sağlamak anlamına da gelir. Bu, fidye yazılımı saldırısının faaliyetlerinizi felce uğratmaması için yedeklemelerinizin olması, kimlik avı olaylarının kontrol altına alınabilmesi ve bunlardan ders çıkarılabilmesi için müdahale planlarınızın olması ve aksilikleri iyileştirme fırsatları olarak gören bir kuruluş zihniyetinin geliştirilmesi ile ilgilidir. Çalışmalarınıza devam ederken, her zorluğun hazırlık ve düşünmeyle karşılaşıldığında sizi daha güçlü hale getirebileceğini unutmayın. Bir güvenlik olayı meydana gelirse, bunu politikalarınızı ve eğitimlerinizi iyileştirmek için bir öğrenme deneyimi olarak kullanın. Kaydettiğiniz ilerlemeyi kutlayın; örneğin, sağlam bir plan uygulayarak kendi bağlamınızda "güvenlik planı olmayan kuruluşların %80'i" istatistiğini tersine çevirin. Kendinizi ve ekibinizi eğitmeye devam edin. Dijital güvenlik alanı hızla gelişmektedir, ancak sizi güncel tutacak her zamankinden daha fazla kaynak bulunmaktadır (bunların çoğunu 7. Bölüm ve eklerde listeledik). Periyodik olarak yenileme atölyelerine katılmayı düşünün, kar amacı gütmeyen kuruluşlar için siber güvenlikle ilgili uyarıları veya haber bültenlerini takip edin ve BT ile ilgilenen genç çalışanları veya gönüllüleri kuruluşunuzda "dijital güvenlik şampiyonları" olarak görev almaya teşvik edin. Sürekli öğrenme, dayanıklılığın temel taşıdır. Sizi çevik tutar ve dijital dünyanın önünüze çıkardığı her şeye hazırlıklı olmanızı sağlar.

Geleceğe bakarken, dijital çağda sivil toplumun geleceği konusunda iyimser ve ileriye dönük olmaya devam ediyoruz. Evet, zorluklar önemli – siber saldırılar giderek daha sofistike hale geliyor ve bizler tetikte olmalıyız. Ancak son birkaç yılda kaydedilen ilerleme cesaret verici. Daha fazla kuruluş dijital güvenliğin öneminin farkına varıyor ve destek yapıları yavaş ama emin

adımlarla güçleniyor. Kâr amacı gütmeyen kuruluşlar için özel olarak tasarlanmış araç ve hizmetlerin geliştirildiğini, bağışçılar ve kurumlar arasında siber güvenlik ihtiyaçlarının finansmanı konusunda farkındalığın arttığını ve topluluklar için "dijital dayanıklılık" kavramına küresel olarak daha fazla ilgi gösterildiğini görüyoruz. Bu e-kitabın her bölümü sadece uyarıcı rehberlik sunmakla kalmamış, aynı zamanda fırsatları da vurgulamıştır – teknolojiyi avantajımıza çevirme, kendimizi koruma yöntemlerinde yenilik yapma ve değerlerimizi destekleyen bir dijital ortam oluşturma fırsatlarını. Belirttiğimiz gibi, siber tehditler gelişmeye devam edecek, ancak savunmamız da gelişebilir. Bilgi ve kapasite alanındaki eksiklikleri gidererek, ortaklıkları güçlendirerek ve siber güvenliği en çok ihtiyaç duyanlar için bir öncelik olarak tutarak, sivil toplumun korkmadan kritik çalışmalarını sürdürebileceği daha güvenli bir dijital ekosistem oluşturabiliriz.

Son olarak, size güç veren bir düşünceyle veda etmek istiyoruz: Dijital güvenliğe yatırdığınız her çaba, işinizin ve hizmet ettiğiniz insanların özgürlüğüne ve bütünlüğüne yapılan bir yatırımdır. Her yeni şifre politikası, her şifrelenmiş veritabanı, her personel eğitimi oturumu, dünya çapında insan haklarını, sosyal adaleti ve toplum refahı girişimlerini koruyan daha güçlü bir kalkan oluşturur. Bu e-kitabı okuduğunuz ve bu konularla ilgilendiğiniz gerçeği, daha güvenli bir geleceğe doğru atılmış olumlu bir adımdır. Bu taahhüdünüzü sürdürmenizi öneririz. Öğrendiklerinizi meslektaşlarınız ve ortak kuruluşlarla paylaşın. Strateji toplantılarınızda ve planlama oturumlarınızda dijital güvenlik konusunu gündemde tutun. İhtiyacınız olan kaynakları ve desteği talep edin – ister daha iyi altyapı için finansman olsun, ister personelin güvenlik önlemlerini öğrenmesi ve uygulaması için ayrılan zaman olsun – çünkü dijital güvenlik buna değer. İleriye dönük bakış açısı, güvenliği günlük çalışmalarımıza dahil ederek, kuruluşlarımızı korumaktan daha fazlasını yaptığımızdır; onların gelişmesini sağlıyoruz. Güvenli bir sivil toplum kuruluşu, sesinin dijital tehditler tarafından kolayca susturulamayacağını bilerek, daha yüksek sesle konuşabilir, daha cesurca hareket edebilir ve daha uzağa ulaşabilir.

KA220 projesi ve bu e-kitaptan elde edilen en cesaret verici içgörülerden biri, bu zorluklarla tek başımıza karşı karşıya olmadığımızdır. Aslında, işbirliği en güçlü varlıklarımızdan biridir. İletilmesi gereken bir mesaj varsa, o da birlikte daha güvende olduğumuzdur. Siber tehditler genellikle izolasyon hissi yaratabilir – küçük bir kar amacı gütmeyen kuruluş, sofistike

bir hacker karşısında kendini güçsüz hissedebilir – ancak sivil toplumun ortak çabalarıyla ortaya çıkan kolektif güç, dengeyi değiştirebilir. Bu proje boyunca, uzmanlıklarını paylaşmak için bir araya gelen kuruluşların örneklerinden, yardım eli uzatan dijital gönüllü ağlarından ve ortak güvenlik sorunlarını ele almak için sınırların ötesinde kurulan ortaklıklardan ilham aldık. Dijital güvenliğe giden yol tek başına yürünmesi gereken bir yol değildir; bu, paylaşılan bir yolculuktur. Sivil toplum kuruluşları, tehditler ve olaylar hakkında açık bir şekilde iletişim kurarak, araçları ve başarı hikayelerini paylaşarak ve acil durumlarda birbirlerini destekleyerek savunma kapasitelerini artırmaktadır. Dahası, kar amacı gütmeyen sektörün ötesinde geniş bir işbirliği de gereklidir. Sivil toplumun dayandığı açık ve güvenli interneti korumaya kararlı olan hükümet, akademi ve teknoloji endüstrisindeki müttefiklerle ortaklıklar kurmaya devam etmeliyiz. Uzmanlar ve küresel siber liderlerin de belirttiği gibi, risk altındaki grupları etkili bir şekilde savunmak "siber güvenlik çözümlerine yatırım, paydaşlar arasında işbirliği ve uzun vadeli dayanıklılık için yenilikçi finansman modelleri" gerektirir. Hiçbir kuruluş, ne kadar iyi kaynaklara sahip olursa olsun, dijital güvenliğin tüm yönlerini tek başına ele alamaz. Koruyucu önlemlerin mevcut, etkili ve uzun vadede sürdürülebilir olmasını sağlamak için farklı sektörleri ve uzmanlıkları kapsayan bir uygulama topluluğu gereklidir. Bu tür işbirliklerini aramaya teşvik ediyorum: güvenlik forumlarına ve koalisyonlarına katılın, STK'lara siber güvenlik yardımı sunan girişimlere katılın ve yardım istemek veya kendi yardımınızı sunmak için meslektaşlarınıza ulaşmaktan çekinmeyin. Bu bağları güçlendirerek, tehditlere hızlı bir şekilde yanıt verebilen ve küçük sorunların büyük krizlere dönüşmesini önleyebilen birleşik bir cephe oluşturuyoruz. Sivil toplum aracılığıyla dijital güvenlik altyapısını geliştirmek için bu yolculuğun bir parçası olduğunuz için teşekkür ederiz. Bu ders kitabının sonu bir son değil, bir başlangıçtır – bu sayfaların ötesinde devam edecek yeni girişimlerin, konuşmaların ve işbirliklerinin başlangıç noktasıdır. Meraklı, uyanık ve birleşik kalın. Birlikte, sivil toplumun sadece güvenli olduğu değil, aynı zamanda bizim için değerli olan davaları savunmak için teknolojiden yararlanma gücüne sahip olduğu bir dijital ortam inşa edeceğiz. Dayanıklılık, işbirliği ve sürekli öğrenmeyi rehberimiz olarak, sizin gibi kuruluşların dijital güvenliğin sağlam temelleriyle desteklenerek inovasyonu güvenle benimseyip sosyal değişimi yönlendirebileceği bir geleceğe doğru ilerliyoruz. Bu önemli çalışmaya devam edelim – topluluklarımız buna güveniyor ve ihtiyacımız

olan araçlar ve müttefikler elimizin altında. Dijital çağda daha güvenli, daha güçlü ve daha fazla yetkiye sahip bir sivil toplum için.

Sivil Toplumda Dijital Güvenliği Güçlendirmeye Yönelik Pratik Dijital Dönüşüm Kılavuzu ve Müfredatı, tek bir açık amaçla oluşturuldu: Dijital güvenliği, büyüklüğü veya teknik kapasitesi ne olursa olsun her kuruluş için ulaşılabilir, anlaşılır, ve uygulanabilir hale getirmek. İlerlerken, bu kılavuzun sadece bir kaynak olarak değil, daha güçlü ve daha güvenli dijital uygulamalara doğru yolculuğunuzda bir yol arkadaşı olarak da hizmet etmesini umuyoruz.

Dijital dayanıklılık, farkındalık, işbirliği ve tutarlılık sayesinde adım adım artar. Bu uygulamaları günlük işlerinize entegre ederek, yalnızca verileri ve iletişimi korumakla kalmaz, aynı zamanda dijital çağda insan haklarını, güveni ve demokratik değerleri de savunursunuz.

Farkında olun. Dayanıklı olun. Güvende olun.