Co-funded by the
Erasmus+ Programme
of the European Union

InCyT Eğitim Modülleri için Şablon

Yöneticiler için Bilgi Güvenliği Ünite 3 – 5. Hafta Birim (Modül) adı: Bilgi Güvenliği Yönetimi 3	
Öğrenme Aktiviteleri	❑ **Web Semineri**❑ **Alıştırmaları**❑ **Atölye Sunumu**❑❑ **Diğer**
Öğrenme Sorumlusu	• George Matache ve ark.
Öğrenme Etkinliği Hedefleri	1 Genel terminoloji 2. Gizlilik, Bütünlük ve Kullanılabilirlik (CIA) 3. Kurallar ve standartlar 4. Bilgi güvenliği yönetimi 5. Kötü amaçlı yazılım nasıl çalışır? 6. En önemli siber tehditler 7. Saldırı türleri 8. Güvenli Web Sunucusu - SSL 9. E-posta gönderme ve alma 10. Varlık yönetimi
Kazanılacak Beceriler	•TS3 Ağ Güvenliği •TS4 Penetrasyon (istismar edilebilir güvenlik açıkları) testi • SS3 Bilişsel ve davranış analizi
Öğrenme aktivitesinin süresi	2 hafta
Öğrenme rdonatımları	***Neye ihtiyaç var?*** • İnternet erişimi • İnternet Tarayıcısı • MS Office365

Modül hakkında kısa bilgi

Giriş

Siber güvenlik, bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve verileri kötü amaçlı saldırılardan koruma uygulamasıdır. Bilgi teknolojisi güvenliği veya elektronik bilgi güvenliği olarak da bilinir. Bu terim, işletmeden mobil bilgi işleme kadar çeşitli bağlamlarda geçerlidir ve birkaç ortak kategoriye ayrılabilir.

İşletmeler genellikle günlük operasyonlarıyla o kadar ilgilenirler ki, ağ güvenliğine büyük yatırım yapmayı unuturlar. Diğerleri kapsamlı ağ güvenliğine duyulan ihtiyacı anlıyor, ancak BT'leri ile ilgili olarak veri sızıntısı durumunda da aynı derecede zararlı olabilecek yumuşak bir stratejiye sahipler. Ağ güvenliğinin ne anlama geldiğini ve şirketinizin ağının ağınıza sızmak isteyen sayısız dış tehdide karşı güvende olmasını sağlayacak en iyi uygulamaları anlamak, verilerinizi ve nihayetinde işinizi güvende tutmak için çok önemlidir.

KOBİ'ler için siber güvenlik eğitiminin – yöneticiler ve çalışanlar – somut ve etkileşimli olması son derece önemlidir – aynı zamanda uygulamalı olması da son derece önemlidir, çünkü küçük KOBİ'lerin bu konuda harcayacak zamanları, motivasyonları veya kaynakları yoktur, bu nedenle eğitimin katılan yöneticiler için alakalı ve yönetilebilir olması çok önemlidir. Bu nedenle, bu modül buna dayanarak planlanmaktadır.

Bilgi güvenliği yönetimi (ISM), bir kuruluşun varlıkların gizliliğini, kullanılabilirliğini ve bütünlüğünü tehditlere ve güvenlik açıklarına karşı makul bir şekilde koruduğundan emin olmak için uygulaması gereken denetimleri tanımlar ve yönetir. Kötü amaçlı yazılım veya "kötü amaçlı yazılım", sistemlere zararlı herhangi bir kötü amaçlı programı veya kodu tanımlayan bir şemsiye terimdir.

Düşmanca, müdahaleci ve kasıtlı olarak kötü amaçlı kötü amaçlı yazılımlar, genellikle bir cihazın işlemleri üzerinde kısmi kontrol sahibi olarak bilgisayarları, bilgisayar sistemlerini, ağları, tabletleri ve mobil cihazları istila etmeyi, zarar vermeyi veya devre dışı bırakmayı amaçlar. İnsan gribi gibi, normal işleyişe müdahale eder. Kötü amaçlı yazılımların arkasındaki nedenler farklılık gösterir. Kötü amaçlı yazılımlar sizden para kazanmak, işinizi yapma yeteneğinizi sabote etmek, politik bir açıklama yapmak veya sadece haklarıyla övünmekle ilgili olabilir. Kötü amaçlı yazılımlar sistemlerin veya ağ ekipmanlarının fiziksel donanımına zarar veremese de, bilginiz veya izniniz olmadan verilerinizi çalabilir, şifreleyebilir veya silebilir, çekirdek bilgisayar işlevlerini değiştirebilir veya ele geçirebilir ve bilgisayar etkinliğinizi gözetleyebilir.

Kötü amaçlı yazılımlar tanımlanır ve tanımlanır, birçok farklı türünü tanıtır ve nasıl çalıştığını açıklar. Ayrıca, virüslü bir cihazın uyarı işaretlerini açıklar ve nasıl önleneceğini açıklarız. Öğrenciler, ilgili metni okuyarak, akış web seminerlerini izleyerek ve alıştırmaları kendi hızlarında çözerek ve sürekli geri bildirim ve oyunlaştırma bilgi kontrolü ile canlı izleyici etkileşimi yoluyla bu yönler hakkında bilgilendirilebilirler.

Öğrenme Materyalinin İçeriği

Özellikle BT sistemlerinizin çalışmasına ve güvenli olmasına çok bağımlı bir şirketiniz varsa maalesef siber güvenlik tehditleri artmaktadır.

AB'de siber saldırılar 2020 ve 2021 yıllarında ve özellikle 2022 yıllarında hem karmaşıklıkları ve sayıları hem de etkileri açısından artmaya devam etti. AB, vatandaşları ve işletmeleri siber suçlardan korumak ve güvenli, açık ve emniyetli bir siber alan sağlamak için çeşitli cephelerde çalışıyor.

2022'de, kripto para birimi endüstrisini hedef alan devlet destekli grupları göreceğiz, siber suçlular ise yerleşik arka kapılara sahip dijital cüzdanlar oluşturarak yatırımcılardan yararlanacak. Ödeme sistemlerine yönelik saldırılarda ve daha gelişmiş mobil tehditlerde bir artış görmemiz muhtemeldir.

Danimarka'da 16-89 yaş arasındaki nüfusun yaklaşık yarısı (yüzde 47) sahte e-postalar, dolandırıcılık, bilgisayar korsanlığı veya kimlik hırsızlığı şeklinde hayatlarına yakın siber suçlar işlemiştir. Aynı şey yüzde 11 için de geçerli. Danimarkalı özel şirketlerin. Şirketlerin yüzde 8'i dijital hizmetlere erişimin engellendiğini ve yüzde 3'ünün yaşadığını deneyimledi. verilerin silinmesini veya imha edilmesini sağlamış olmak. Kimlik avı en yaygın sorundur, ancak ne yazık ki giderek daha fazla insan alışveriş yapıp evden çalıştıkça sahte web sitelerinin sayısında radikal bir artış görüyoruz.

ISM'nin özü, bir kuruluşun varlıkların yönetimi ve korunmasında ele alması gereken risklerin değerlendirilmesini ve risklerin tüm uygun paydaşlara yayılmasını içeren bir süreç olan bilgi riski yönetimini içerir. Bu, gizlilik, bütünlük, kullanılabilirlik ve varlıkların değiştirilmesinin değerini değerlendirmek de dahil olmak üzere uygun varlık tanımlama ve değerleme adımlarını gerektirir. Bilgi güvenliği yönetiminin bir parçası olarak, bir kuruluş bir bilgi güvenliği yönetim sistemini ve bilgi güvenliğine ilişkin ISO/IEC 27001, ISO/IEC 27002 ve ISO/IEC 27035 standartlarında bulunan diğer en iyi uygulamaları uygulayabilir. Bununla birlikte, bu tür bir sertifikasyon genellikle KOBİ'ler için neden çevik bir siber güvenlik uygulamasına hazırlandığımızı talep eden çok fazla kaynaktır:

Bilgi Güvenliği ve İç Kontrol Sistemleri

- Genel terminoloji
- CIA üçlüsü
- Bir Saldırının Anatomisi (Saldırı Yüzeyi Azaltma)
- Siber Güvenlik Çerçeveleri

Bilgi Güvenliği Yönetimi
E-posta ve Ofis
Aygıtları
KOBİ'ler için önemli bir zorluk, bilginiz olmadan cihazınıza sızmak için tasarlanmış her türlü "kötü amaçlı yazılım" için bir şemsiye terim olan kötü amaçlı yazılımdır. Birçok kötü amaçlı yazılım türü

vardır ve her biri hedeflerine ulaşmak için farklı şekilde çalışır. Ancak, tüm kötü amaçlı yazılım varyantları iki tanımlayıcı özelliği paylaşır: sinsidirler ve aktif olarak en iyi çıkarlarınıza karşı çalışırlar.

Kötü amaçlı yazılım virüs müdür? Evet ve hayır. Tüm bilgisayar virüsleri kötü amaçlı yazılım olsa da, tüm kötü amaçlı yazılımlar virüs değildir. Virüsler yalnızca bir tür kötü amaçlı yazılımdır. İki terimi birbirinin yerine kullanan birçok insan duyacaksınız, ancak teknik açıdan virüsler ve kötü amaçlı yazılımlar aynı şey değildir.
Bunu şu şekilde düşünün: Kötü amaçlı yazılım kötü amaçlı koddur. Bilgisayar virüsleri, bilgisayarlara ve ağlara yayılan kötü amaçlı kodlardır.

Kötü amaçlı yazılım nasıl çalışır?

Tüm kötü amaçlı yazılımlar aynı temel kalıbı izler: Kullanıcı farkında olmadan cihaza bulaşan kötü amaçlı yazılımı indirir veya yükler.

Kötü amaçlı yazılım bulaşmalarının çoğu, yanlışlıkla kötü amaçlı yazılımın indirilmesine neden olan bir eylem gerçekleştirdiğinizde oluşur. Bu eylem, bir e-postadaki bağlantıyı tıklamak veya kötü amaçlı bir web sitesini ziyaret etmek olabilir. Diğer durumlarda, bilgisayar korsanları kötü amaçlı yazılımları eşler arası dosya paylaşım hizmetleri ve ücretsiz yazılım indirme paketleri aracılığıyla yayar. Popüler bir torrent veya indirmeye biraz kötü amaçlı yazılım gömmek, onu geniş bir kullanıcı tabanına yaymanın etkili bir yoludur. Mobil cihazlara kısa mesajlar yoluyla da virüs bulaşabilir.

Başka bir teknik, kötü amaçlı yazılımları bir USB çubuğun veya flash sürücünün ürün yazılımına yüklemektir. Kötü amaçlı yazılım, cihazın dahili donanımına (dosya depolama alanı yerine) yüklendiğinden, cihazınızın kötü amaçlı yazılımı algılaması olası değildir. Bu nedenle bilgisayarınıza asla tanımadığınız bir USB sürücüsü takmamalısınız.

Kötü amaçlı yazılım yüklendikten sonra, cihazınıza bulaşır ve bilgisayar korsanlarının hedeflerine doğru çalışmaya başlar. Çeşitli kötü amaçlı yazılım türlerini birbirinden ayıran şey, bunu nasıl yaptıklarıdır. Peki kötü amaçlı yazılımlar nasıl çalışır? Kötü amaçlı yazılım saldırısı nedir?

En önemli siber tehditler

Drive-by açıkları, meşru kullanıcıyla etkileşime girmeden bir PC'ye yüklenen yazılımlardaki mevcut güvenlik açıklarından otomatik olarak yararlanabilir; 2012 yılında kapsamlarını mobil terminallere de genişlettiler. neredeyse tamamen meşru web sitelerini tehlikeye atmaya odaklanır. tarayıcıdaki, eklentilerindeki veya işletim sistemindeki güvenlik açıkları, kullanıcının bilgisi olmadan PC'ye kötü amaçlı yazılım yüklemek için kullanılabilir, enfeksiyon basit internet taraması ile başlatılabilir.

Solucanlar kendi kendini kopyalayan programlardır; kendi kopyalarını diğer düğümlere (ağdaki bilgisayarlar) göndermek için bilgisayar ağını kullanmak, bunu herhangi bir kullanıcının müdahalesi olmadan yapmayı başarmak, bir bilgisayar virüsünün aksine, bir bilgisayar solucanının mevcut bir programa bağlanmasına gerek yoktur, sadece bant genişliğini alarak bile ağa zarar verir.

Truva atı, gerçekte gizli verileri çalmak veya yetkisiz kullanıcıların veya programların virüslü sisteme erişmesine izin vermek amacıyla oluşturulan meşru programlar biçiminde kendini sunar; enfeksiyonların büyük çoğunluğunu (%80) oluşturmaktadır.

Kötü amaçlı yazılım, işlevi bir bilgisayara (ör. virüslere) yazılım veya donanım zarar vermek olan herhangi bir programı temsil eder – yukarıda açıklandığı gibi.

İzleme yazılımı, bir sunucuya veya kişilere erişilen siteler, aranan bilgiler ve kullanıcının tarama alışkanlıkları hakkında bilgi göndermek için bazı web tarayıcısı güvenlik açıklarını kullanan programlardır; Virüsler mümkün olduğunca çok sayıda kişisel bilgisayara bulaşmayı amaçlarken, casus yazılımlar İnternet'e yayılmayı amaçlarken, Virüsler genellikle tehlikeli bir yüke sahiptir, virüslü bilgisayara zarar vermek isterken, casus yazılımlar yalnızca bilgisayar işlemlerini yavaşlatır, açılır pencereler ekler ve tarayıcının dengesini bozar ve diğer "can sıkıcı" etkilere sahiptir.

SQL Enjeksiyonu (Kod Ekleme), bir saldırgan veritabanına gönderilen bir SQL sorgusuna herhangi bir veri ekleyebildiğinde oluşur; sözdizimi eklenerek, ifadenin mantığı farklı bir eylem gerçekleştirecek şekilde değiştirilir, bu en yaygın güvenlik açığıdır. En iyi SQL ekleme savunma stratejisi, saldırganın uygulamanın ihtiyaç duyduğu veriler dışında veri girememesi için güçlü giriş doğrulama yordamları uygulamaya dayanır.

Casus yazılım Genellikle bir sistemin güvenlik açıklarından üçüncü bir tarafın yararına yararlanan bir program olarak tanımlanır, bilgisayarınızı yavaşlatabilir, virüs bulaşmasına karşı savunmasız hale getirebilir ve çeşitli uygulamalar için kullanıcı adları, şifreler ve kredi kartı / banka hesap bilgileri gibi gizli bilgileri toplayabilir.

Bir keylogger, bilgisayar korsanlarının siz fark etmeden bilgisayarınıza yerleştirdiği küçük bir "akıllı" programdır. Burada birkaç ay veya yıl boyunca yalan söyleyebilir ve klavyede yaptığınız her bir tuş vuruşuna göz kulak olabilir. Tüm veriler, verilerinizden en iyi şekilde yararlanmak için farklı algoritmalar ve araçlar kullanabilecekleri bilgisayar korsanlarına gönderilir. Zamanla, davranışınız hakkında farklı şeyler öğrenirler ve en önemlisi, klavyeye girdiğiniz farklı şifreler kullandığınız yerlerde. Daha sonra birkaç dakika içinde tüm dijital kimliğinizi ele geçirmek için kullanılabilir.

Reklam yazılımı, casus yazılımların bir alt kategorisidir ve ürün veya hizmetlerin reklamını yapan bir programdır. Genellikle bu reklamlar, program kaldırıldıktan sonra bile görünür.

Exploitation kitleri, özellikle web tarayıcılarındaki veya web siteleri tarafından erişilebilen uygulamalardaki istemci tarafı güvenlik açıklarından yararlanarak daha az deneyimli saldırganların sistemleri tehlikeye atmalarına yardımcı olan otomatik yazılımlardır; güvenliği ihlal edilmiş web sitelerine kötü amaçlı kodların enjekte edildiği drive-by indirme saldırılarına dayanır; tarayıcıdaki veya eklentilerindeki güvenlik açıklarından yararlanabilir.

Botnet, bir saldırganın kontrolü altındaki bir dizi bilgisayarı temsil eder; Bir botnet birden fazla amaç için kullanılabilir: Dağıtılmış Hizmet Reddi - DDoS saldırıları, spam, kimlik hırsızlığı, kötü amaçlı yazılım dağıtımı, bilgisayar sistemlerine virüs bulaştırma; birden fazla işletim sisteminde çalışabilirler; 2012 yılında "Flashback" botnet'i yaklaşık 600.000 Apple bilgisayarına bulaşmayı başardı.

Hizmet Reddi, bilgisayar sistemlerinin/hizmetlerinin veya elektronik iletişimin kullanılabilirliğini etkileme girişimidir. Hedef sistem, donanım veya yazılım kaynaklarını tüketen ve meşru kullanıcılar tarafından kullanılamaz hale getiren çok sayıda gayri meşru istek göndererek saldırıya uğrar. DDoS saldırılarının ana motivasyonları hacktivizm, vandalizm ve sahtekarlıktır. Gizli bilgilerin tehlikeye atılması; gizli bilgilerin iç veya dış temsilciler tarafından (kasıtlı veya kasıtsız) ifşa edilmesi yoluyla meydana gelen veri güvenliği ihlallerini ifade eder; Bilgi sızıntısı genellikle bilgisayar korsanlığı, kötü amaçlı yazılım dağıtımı, sosyal mühendislik saldırıları, fiziksel saldırılar veya ayrıcalıkların kötüye kullanılması yoluyla elde edilir.

Rogue ware / scareware, sahte yazılım biçimini alan tehdit türüdür; Belirli bir hileli yazılım / korkutma yazılımı durumu, sisteme yüklendikten sonra yanlış güvenlik uyarıları sağlayan ve kullanıcıyı özel bir dezenfeksiyon aracı satın almaya davet eden sahte güvenlik yazılımıdır. Bu tür bir tehdit, sosyal mühendislik teknikleri, truva atları, güvenlik açıklarının sömürülmesi (özellikle java) gibi çeşitli yöntemlerle yayılır.

Fidye yazılımı, siber suçların en tehlikeli ve agresif biçimlerinden biridir. Bilgisayar korsanları, bir bilgisayarın veya bilgisayar kontrollü bir sistemin işlevselliğini kilitlemek için son derece karmaşık bir kod parçası kullanırlar. Daha sonra bilgisayar korsanı tarafından sistemin sahibiyle iletişime geçilir ve sistemi yeniden etkinleştirmek veya sistemdeki bilgilerin "kilidini açmak" için fidye talebinde bulunulur. Hafif vakalarda, aile fotoğrafları veya şirketin hesaplarıyla ilgilidir, ciddi durumlarda, aşağıdakiler gibi hayati sistemlerle ilgili olabilir; fabrikalardaki kontrol sistemleri veya internete bağlı bir kalp pili.

Saldırı türleri

Hedefli saldırılar

- belirli bir kişiyi veya kuruluşu hedefleme
- kişisel/gizli veri toplamayı veya hedef bilgisayar sistemlerini tehlikeye atmayı amaçlar.

•genellikle, saldırganın çeşitli tekniklerle kendini bilgilendirdiği bir aşamaya sahiptir (örn. sosyal mühendislik) hedeflenen BT sistemi hakkında ve ardından saldırıyı tetikler
Genellikle eylemleri meşru görünür, çünkü güvenilir bir kişiden geliyormuş gibi görünürler.

Hırsızlık/Kayıp/Fiziksel İmha
• Dizüstü bilgisayarlar, akıllı telefonlar veya tabletler tarafından sunulan artan hareketlilik nedeniyle, bu tür bir tehdit büyük bir tehdit haline gelmek üzeredir.
•tutarlı veri yedekleme ve içerik şifreleme, gerçek veri kaybını veya gizli verilerin yabancılara açıklanmasını sınırlamak için bir çözüm olabilir

Kimlik hırsızlığı
•giderek daha çevrimiçi bir ortamda gerçek bir tehdittir
•erişim kimlik bilgileri veya kişisel veriler bugün saldırganların hedefidir
•saldırgan eline geçtikten sonra hileli işlemler gerçekleştirebilir (özellikle finansal) veya gizli verileri elde edebilir.

Bilgi sızıntısı
•Bilgilerin kasıtlı veya kasıtsız olarak yetkisiz bir kişiye açıklanması
•coğrafi konum ve telefon rehberi kişileri gibi bilgiler kolayca saldırganların eline geçebilir ve dolandırıcılık amacıyla kullanılabilir

Arama Motoru Manipülasyonu (SEP)
•Kötü amaçlı web sitelerine başvurular içeren arama sonuçlarını görüntülemek için arama motorlarını değiştirir. Böylece, virüslü bir web sayfası kullanıcıları kötü amaçlı sitelere yönlendirir ve kurbanlar ilgili sitelere erişirse, bilgisayarlarını kötü amaçlı yazılımlarla enfekte ederler.
•Sahte dijital sertifikalar
•saldırganlar tarafından, algılanamayan son kullanıcıya iletilmek amacıyla çeşitli siber saldırılarda kullanılan kaynakları (web siteleri, uygulamalar, kaynak kodları vb.) dijital olarak imzalamak için kullanılır.
•genellikle HTTPS protokolünü kullanan e-bankacılık veya e-ticaret gibi kötü amaçlı web uygulamalarını imzalamak için kullanılır
•güvenli web siteleri için dijital sertifikalar veren sertifika yetkililerinin PKI (Ortak Anahtar Altyapısı) sistemlerindeki güvenlik açıklarından yararlanılarak oluşturulabilir veya çalınabilir.

Güvenli Web Sunucusu – SSL

Ortak anahtar şifrelemesini uygulayan protokol, Netscape tarafından geliştirilen SSL (Güvenli Yuva Katmanı) olarak adlandırılır. Bu protokol, verileri güvenli bir şekilde iletmek için tarayıcılar ve web

sunucuları tarafından kullanılır, bu nedenle HTTP protokolü tarafından kullanılmak üzere oluşturulmuştur.

Güvenli bir web sunucusuna bağlanmak, URL'de http yerine https protokolünden bahsederek yapılır - yani, güvenli web sayfasına erişim, sunucunun adıyla değil, protokolle gösterilir.

Güvenli bir web sunucusu şunları sunar: Güvenli bilgi aktarımı: Sunucu ile gezgin arasında iletilen veriler, ele geçirilmeleri durumunda şifreleri çözülemez.
Sunucu kimlik doğrulaması: Web sunucusu bir sertifika yetkilisinden (CA) sertifika aldıysa.

Güvenlik kontrol listesi

Masaüstü ve Mobil Güvenlik Duvarı
Dış çevrelerinizi güvence altına alarak başlayın.
point'in (dijital cihazlar) güvenlik duvarları çalışır. Kulağa basit geliyor, ama aynı zamanda başlamanız gereken en temel bilgilerde. Ağınızda genellikle üç ila dört farklı güvenlik duvarı türü vardır:
• İşletim sisteminizde güvenlik duvarı (Android, iOS, Windows vb.).
• Antivirüs/güvenlik programınızda güvenlik duvarı.
• İnternet yönlendiricinizde güvenlik duvarı.
• ASA kutunuzdaki veya akıllı anahtarınızdaki güvenlik duvarı (Genellikle yalnızca daha büyük şirketler).

Yedek
Yedekleme, haber olmaması gerektiği gibi, listenin en üstünde olmalıdır. Yedekleme, verilerinizin kilidini açmak için fidye ödemek zorunda kalmanızı önleyebilir. Ancak, şirketin büyüklüğü hakkında hata yapmayın, bu tür kötü amaçlı yazılımlarla yapılan saldırıların çoğu küçük işletmelere ve bireylere yöneliktir.

Daha güvenli tarama için kurallar
•en son tarayıcı sürümünü kullanın
• Özellikle güvenli olmayabilecek web sayfalarına erişirken kendinizi diğer tarayıcı türlerine (örneğin Google Chrome, Opera, Firefox, Safari vb.) yönlendirmek;
•çoğu kötü amaçlı yazılım Microsoft Internet Explorer'ı etkiler (kullanıcıların %50'sinden fazlası tarafından kullanılır)
•fare imlecini üzerine getirerek ve tarayıcının sol alt kısmındaki gerçek adresi görüntüleyerek bağlantıların gerçek hedefini kontrol edin
• Hangi eklentileri yüklediğinize dikkat edin, genellikle kötü amaçlı yazılımlarla birlikte gelirler
•açılır pencerelerdeki bağlantılara tıklamayın

•kişisel bilgilerinizi girmeden önce web adresinin başındaki "https://" olup olmadığını kontrol edin
• Çevrimiçi bir satın alma işlemi yapmakla ilgili olarak, bir banka kartıyla çevrimiçi ödeme yapmayı tercih ederse, sayfanın güvenlik seviyesine daha fazla dikkat edilmelidir.

E-posta gönderme ve alma
• hassas bilgileri e-posta ile göndermekten veya almaktan kaçınmak;
•sosyal mühendislik veya kimlik avı girişimlerinden kaçının
•güçlü anti-spam filtreleme sunan bir e-posta sağlayıcısı arayın
•spam'e yanıt vermeyin ve basamaklı veya piramit e-postalardan kaçının
•spam'e yanıt vermeyin ve basamaklı veya piramit e-postalardan kaçının
•kişisel ve iş e-posta hesabınız için aynı adı kullanmayın; Bu hesaplar için farklı adların kullanılması, bir bilgisayar saldırısının hedefi olma riskini azaltır
•kritik bilgileri kişisel e-posta hesaplarında veya çalıştığınız kurum/şirket dışındaki diğer ağlarda depolamaktan kaçının

Gerçek şu ki, e-posta hiçbir zaman geleneksel olarak iletişim için güvenli bir ortam olmamıştır. Sonuçta, sadece suçluların iletişimlerini güvence altına almakla gerçekten ilgilenmeleri gerekir. Bu son derece yaygın, ancak tamamen kusurlu bir düşünce tarzıdır ve Snowden'ın kendisi bu tür bir zihniyeti ünlü bir şekilde gözden düşürmüştür.

Saklayacak hiçbir şeyiniz olmadığı için mahremiyeti umursamadığınızı iddia etmek, söyleyecek hiçbir şeyiniz olmadığı için ifade özgürlüğünü umursamadığınızı iddia etmek gibidir.

Birçok insan, saklayacak hiçbir şeyleri yoksa, endişelenecek hiçbir şeyleri olmadığı zihniyetine hala abone olsa da, gerçek şu ki, endişelenecek çok şey var ve insanların e-posta iletişimlerini şifrelemeleri ve gizliliklerini korumaları için birçok somut neden var. Bu, araştırmacı bir gazeteci, muhalif, muhbir veya sadece sıradan bir ortalama vatandaş olsanız da doğrudur.

Neden herkesin güvenli bir e-posta göndermesi gerekir?

Siber suçluların oluşturduğu tehditlere karşı koruma sağlamak
Hiç bir e-postada hassas kişisel bilgiler gönderdiniz mi ve şöyle düşündünüz mü, 'welp, umarım bu e-posta bir şekilde yanlış ellere geçmez? Bu gerçekten rahatsız edici bir düşüncedir, çünkü hedeflenen alıcı(lar)dan başka biri e-postayı eline geçirirse - özellikle de bu kişi bir siber suçlu olursa - sonuçlar potansiyel olarak felaket olabilir.

Tıbbi bilgileriniz, finansal hesap bilgileriniz, sosyal güvenlik numaranız, adresiniz veya telefon numaranız gibi hassas kişisel verileri içeren bir e-posta göndermek son derece riskli olabilir, çünkü siber suçlular maksimum zararı sağlamak için yalnızca minimum miktarda kişisel veriye ihtiyaç

duyarlar. Bunun gibi hassas kişisel verilere erişim sayesinde siber suçlular çevrimiçi profillerinizi tehlikeye atabilir, banka hesaplarınızı boşaltabilir ve hatta kimliğinizi çalabilir.

E-posta sağlayıcılarının e-postaları izlemesini ve reklamverenlerle veri paylaşmasını önlemek için
E-posta sağlayıcılarının, hedefli reklamcılık çabalarını kolaylaştırmak için kullanıcıların e-posta mesajlarını izlediği ve taradığı bilinmektedir. 2017'de Gmail, reklam amacıyla e-posta tarama uygulamasını görünüşte durdurmuş olsa da, bu, Google'ın e-postaları başka amaçlar için taramayı bıraktığı anlamına gelmez. Örneğin, Gmail'in "Akıllı Yanıt" özelliği, aldığınız bir e-postaya gönderilen hızlı, hazır yanıtlar için iletinin içeriğine göre alakalı öneriler sunar. Bu nedenle, e-posta sağlayıcınızın e-posta iletilerinizi reklam veya başka herhangi bir amaçla taramasını veya izlemesini istemiyorsanız, bu iletilerin içeriğini etkili bir şekilde gizli tutan ve sizden ve e-posta yoluyla iletişim kurduğunuz taraftan başka hiç kimse tarafından erişilemez durumda tutan güvenli e-postalar göndermek istersiniz.

Kitlesel gözetim, sivil özgürlüklerimize ve temel mahremiyet haklarımıza tecavüz ediyor.
Bu tür haksız gözetim haksız yere istilacıdır ve sivil özgürlüklerimize ve temel mahremiyet haklarımıza doğrudan bir hakarettir. Güvenli bir e-posta gönderdiğinizde, yalnızca sizin ve güvenli bir şekilde iletişim kurduğunuz diğer tarafın iletinin içeriğine erişebilmesi için iletişiminizi şifreleyebilirsiniz.

Şifreli bir e-posta göndermek gizliliğinizi korur ve devlet kurumlarının güvenli e-posta iletişimlerinizi gözetlemesini etkili bir şekilde imkansız hale getirir. Bu, özellikle iş sorumlulukları iletişimlerinde tam gizlilik gerektirenler için önemlidir, ancak genellikle hükümetin gizlilik haklarını çiğnemesini istemeyen herkes için de hayati öneme sahiptir.

Devlet gözetim çabalarına karşı korunmak
Daha önce de belirttiğimiz gibi, kitlesel hükümet gözetim uygulamaları kapsamlıdır. Ve bu sadece Çin veya İran gibi otoriter rejimlerde değil, aynı zamanda Amerika Birleşik Devletleri, İngiltere, Avustralya, Kanada, Almanya ve diğer Batı ülkelerinde de geçerlidir.
Kitlesel gözetim bir sapma değildir, normdur ve yasadışı olma noktasına kadar zararlı olabilir.

Bu nedenle, özellikle gönderdiğiniz e-posta hassas kişisel bilgiler içeriyorsa, güvenli e-postalar göndermek çok önemlidir.

Güvenli bir e-posta gönderme
Artık güvenli bir e-posta göndermek istemenizin nedenlerini bildiğinize göre, muhtemelen bunu nasıl yapacağınızı bilmek isteyeceğinizi tahmin ediyoruz. Bunu yapmanın birkaç yolu vardır, her biri belirli doğal avantajlara ve dezavantajlara sahiptir, ancak sonuç olarak, güvenli bir e-posta

göndereceksenız, e-posta mesajınızın şifrelenmesi gerekecektir. Bir e-posta iletisini şifrelediğinizde, aslında bu iletinin içeriğini karıştırırsınız ve şifreleme anahtarı olmayan herhangi birinin iletiyi çözmesini imkansız hale getirirsiniz.

Güvenli bir e-posta göndermek istiyorsanız kullanabileceğiniz seçenekler nelerdir?

Popüler e-posta istemcilerindeki e-postaları şifreleyin
Büyük web tabanlı e-posta sağlayıcılarının çoğu, kullanıcıların iki ana e-posta şifreleme protokolünden biri olan S / MIME veya OpenPGP'yi kullanarak e-postalarını şifrelemelerine izin verecektir. Dezavantajı, bunu doğrudan web tabanlı e-posta sağlayıcınızın arayüzünden yapmak için her zaman basit veya anlaşılır bir süreç olmayabilir ve bunun için ödeme yapmanız gerekebilir.

Örneğin, Gmail'de güvenli bir e-posta göndermek istiyorsanız öncelikle Gmail'de bir GSuite yönetici hesabı kullanarak oturum açarak S/MIME şifrelemesini etkinleştirmeniz gerekir. GSuite hesapları öncelikle ticari amaçlar içindir, ancak teorik olarak kişisel kullanımınız için bir hesap oluşturabilirsiniz. Bununla ilgili diğer bir sorun, e-posta gönderdiğiniz alıcıların da bunun çalışması için S / MIME şifrelemesinin etkinleştirilmesi gerektiğidir.

Benzer şekilde, Outlook da S/MIME şifrelemesini destekler ve el ile etkinleştirmeniz gerekir, ancak bunu yapmadan önce kuruluşunuzun yöneticisinden bir sertifika (veya dijital kimlik) almanız gerekir. Bu, kuşkusuz, en akıcı süreç değildir ve çoğu kişisel e-posta kullanıcısı için çok pratik bir çözüm olması muhtemel değildir. Bu konuda daha fazla bilgi için Outlook e-postalarını nasıl şifreleyeceğimize göz atın.

Bununla birlikte, e-postalarınızı kolaylıkla şifrelemek için Mailvelope gibi ücretsiz bir üçüncü taraf aracı yükleyerek bu sorunları atlayabilirsiniz. Mailvelope, Gmail, Yahoo!, Outlook, Hotmail ve GMX gibi en popüler e-posta hizmetlerinin çoğuyla çalışır. Ancak yine de, şifrelenmiş e-posta mesajınızın alıcılarının da e-postanın şifresini çözmek ve içeriği okumak için benzer PGP / OpenPGP yazılımı kullanıyor olması gerekecektir.

Özel bir güvenli e-posta sağlayıcısı kullanın
Geleneksel web tabanlı e-posta hesabınızda S / MIME veya OpenPGP şifrelemesini manuel olarak etkinleştirme zahmetine girmek istemiyorsanız, güvenli bir e-posta göndermenin çok daha kolay bir yolu, güvenli bir e-posta sağlayıcısıyla bir hesap oluşturmaktır.

ProtonMail gibi güvenli bir e-posta sağlayıcısıyla, kullandığınız aynı güvenli e-posta sağlayıcısını kullanıp kullanmadıklarına bakılmaksızın başkalarına güvenli, şifreli e-postalar gönderebileceksiniz ve alıcılarınız da güvenli bir şekilde yanıt verebilecek. Birçok güvenli e-posta sağlayıcısı, kullanıcıların e-postalarını güvence altına almak için OpenPGP şifrelemesini uygular ve kullanıcıların e-posta

istemcileriyle OpenPGP şifrelemesi etkinleştirilmiş başkalarıyla güvenli, şifreli e-postaları kolayca gönderip almalarını sağlar. Alıcınızda PGP etkin değilse, bu alıcıya yalnızca paylaşılan bir gizli kod dizesi kullanılarak açılabilen bir e-postayı güvenli bir şekilde gönderebilirsiniz.

Temel olarak, güvenli bir e-posta sağlayıcısı kullandığınızda, hassas iletileri şifreleyerek kolayca koruyabilirsiniz, bunların tümü Gmail, Yahoo! veya Outlook gibi büyük ad e-posta sağlayıcıları kadar kullanımı kolay bir platformda. Ancak bu büyük isim sağlayıcılarının aksine, güvenli bir e-posta sağlayıcısı sizi reklamlarla rahatsız etmeyecek veya e-postalarınızı izlemeyecektir (uçtan uca şifreleme sayesinde bunlara bile erişemediğinden).

Dezavantajı, güvenli bir e-posta sağlayıcısının tüm özelliklerine, genişletilmiş depolama alanına ve sınırsız mesajlaşmaya erişmek için ödeme yapmanız gerekmesidir. Bununla birlikte, en iyi güvenli e-posta sağlayıcılarının çoğu, ücretsiz olarak güvenli e-postalar gönderip almanıza olanak tanıyan ücretsiz bir katman (belirli sınırlamalarla) sunar. Yalnızca sınırlı sayıda güvenli e-posta göndereceksiniz, ücretsiz bir seçenek kesinlikle uygun bir çözüm olabilir, ancak e-posta yazışmalarınızın çoğunu güvenli bir şekilde yürütmeyi planlıyorsanız, premium abonelik satın almak gerekli olacaktır.

Bir e-posta aldığınızda,

•gönderenin kimliği garanti edilmez: gönderen ile iletinin içeriği arasındaki ilişkiyi kontrol eder;

•bilinmeyen kişilerden gelen veya meşru hesaplarla ilişkili ekleri değil, şüpheli konu ve içeriğe sahip iletileri açın. Kötü amaçlı yazılımlar (solucanlar, truva atları, casus yazılımlar, reklam yazılımı biçimleri vb. gibi kötü amaçlı yazılımlar veya kötü amaçlı yazılımlar) içerebilirler;

• Bir ekin meşru e-postalardan bile açılması kesinlikle gerekliyse, önce yüklü antivirüs çözümüyle indirilmeli ve taranmalı ve ardından ilişkili uygulamayla açılmalıdır;

•bağlantı içeren e-postalar söz konusu olduğunda, iletinin gövdesindeki bu bağlantıya doğrudan erişmeyin; muhtemelen, bu bağlantı başka bir tarayıcı sekmesinden kopyalanabilir ve açılabilir;

•Kişisel veya gizli veri talepleri (ör. PIN kodu ve banka kartı numarası) içeren e-postalara yanıt vermeyin.

E-postanıza bilinmeyen kişiler tarafından "erişildiğini" nereden biliyorsunuz?

•kişileriniz sizden spam e-postalar aldıklarını söylüyor;

•hatalı birçok e-posta alırsınız;

•iletiler siz göndermeden "gönderilenler" klasöründe görünür;

•oturum açma işlemindeki hesap konumu geçmişi geçerli etkinliğinize karşılık gelmiyor.

Parola güvenliği. Saldırılar, şifreyi tanımlamayı ve bu şifre tarafından kısıtlanan bilgilere erişmeyi amaçlamaktadır. Bu tür en çok kullanılan saldırı yöntemleri "sözlük saldırıları" ve "kaba kuvvet" tir.

"Sözlük saldırısı", önceden tanımlanmış bir kelime veya kelime öbeği listesinde bulunan şifreleri / şifre çözme anahtarlarını art arda deneyerek bazı kaynaklara veya bilgisayar sistemlerine yetkisiz erişimi amaçlamaktadır.

"Kaba kuvvet" saldırısı, deneme yanılma yöntemini uygulayan programlar aracılığıyla "kaba kuvvet" hesaplamasını kullanarak bir bilgisayar sistemine yetkisiz erişim veya şifrelenmiş içeriğin (şifreler gibi) kodunu çözme yöntemidir. Yöntem, ayrıntılı bir algoritma olmadan, olası tüm karakter kombinasyonlarını art arda denemekten ibarettir.

Önlemler: captcha sistemi, bir dizi başarısız erişimden sonra erişim zamanlaması.

•benzersiz kimlikler ve parolalar kullanın ve bunları diğer kullanıcılara iletmeyin;

• parolanın uzunluğu ve karmaşıklığı, tahmin edilmesi zor ancak hatırlanması kolay olacak şekilde seçilmelidir;

•periyodik olarak parola değişimi (1-3 ay arayla);

•farklı uygulamalar için farklı parolalar kullanmak;

•birden fazla kimlik doğrulama yönteminin kullanılması (PIN, parmak izi, uyarı mesajları vb.);

• Evde ve işte benzer parolalar kullanmaktan kaçınmak.

Şunları kullanmayın:

• Kendinizin, ailenizdeki bir başkasının veya en sevdiğiniz hayvanın adı,

• adresinizin öğeleri: bina adı, sokak, ülke,

•kurumun adı, proje vb.

•telefon numarası, kayıt numarası

• Favori yıldızın veya karakterin adı (veya filmin, kitabın vb.),

•sözlük kelimeleri;

•parolasını ayarladığınız hesabın adı;

Güçlü parolalar oluşturma yöntemleri

•fonetik yöntem: "Blu-Ray DVD'm olduğundan eminim!": St1u100%km1DVDBLr!

• ilk harf yöntemi: "Blu-Ray DVD'm olduğundan eminim!": "sSka1DVDBr!"

•ikame yöntemi (genellikle sesli harfler): "Tatilleri seviyorum": "@d0rc0nc#d11l#"

• ters ve ikame yöntemi: "Tatilleri seviyorum": "r0d@3l11d3cn0c"

•büyük/küçük harf, sayı/sembol ve değiştirme yöntemi: "Tatilleri seviyorum": "@D0rC)nC3d11L3"

•Kişisel bir şifre oluşturma sistemi oluşturmak için web sitelerine göre yöntemlerin özelleştirilmesi: Gmail - "G@D0rC)nC3d!1L3MAIL", Yahoo - "YA@D0rC)nC3d!1L3HOO", Wizzair - "WIZZ@D0rC)nC3d!1L3AIR".

Genel olarak bu ünite modülünde

Siber Güvenlik Stratejinizde Siber Öldürme Zincirini Etkili Bir Şekilde Nasıl Kullanırsınız?

Algıla – İzinsiz giriş girişimlerini analiz edin ve bulun.

İnkar et – Saldırıları gerçekleştikleri anda durdurun.

Kesintiye uğratın – Veri iletişimini durdurun

Degrade – Saldırının etkinliğini azaltın ve sınırlayın.

Aldatma – Saldırganları yanlış yöne yönlendirin.

İçerme – Saldırının erişimini gizleyin ve kısıtlayın, böylece kuruluşun yalnızca bir bölümünü etkiler.

Soru:

Sorular Tartışma Forumu kısa bir açıklama ile cevaplandırılacaktır. Mentorluk oturumları sırasında cevaplar mentor ile tartışılacaktır.

•Kötü Amaçlı Yazılım Nedir?

•Başlıca siber tehditler hangileridir?

•Güvenli Web Sunucusu'nun rolü hangisidir - SSL

•Daha güvenli tarama için bazı kuralları açıklayı?

•E-posta gönderme ve alma güvenliğini sağlamak için bazı önlemler sunun!

Öz değerlendirme soruları. Cevapladıktan sonra öğrenci sonuçları görebilir ve bunları platformda kayıtlı olanlarla karşılaştırabilir

•Kötü amaçlı yazılım

•Başlıcasiber tehditler

•Daha güvenli tarama için kurallar

•E-posta gönderme ve alma güvenliğini sağlamaya yönelik önlemler

Ekler (PowerPoint sunumu, dinleyici notları, baskılar, bağlantılar, video...):

Powerpoint ve Video dosyalarına bakın

Başvuru:

•Siber Güvenlik Nedir?

URL: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

•Kötü amaçlı yazılım veya kötü amaçlı yazılım

URL: https://www.malwarebytes.com/malware

•Herkes için siber güvenlik.

https://www.avast.com/c-malware

•Kötü Amaçlı Yazılım Temizleme Yazılımı 2022; Kişisel verilerinizin güvenliğini sağlayın

URL: Kötü amaçlı yazılım

•Siber Güvenlik Tehditleri Nedir?

URL: https://www.imperva.com/learn/application-security/cyber-security-threats/

•21 En İyi Siber Güvenlik Tehditleri ve Tehdit İstihbaratının Nasıl Yardımcı Olabileceği

URL: https://www.exabeam.com/information-security/cyber-security-threat/

•E-posta gönderme ve alma

URL: https://www.ibm.com/docs/en/i/7.1?topic=mail-sending-receiving-e

•E-posta oluşturma ve gönderme

URL: https://support.google.com/a/users/answer/9259846?hl=en

Siber Öldürme Zinciri: Bir Siber Saldırının Yedi Adımı

URL: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/