This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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

InCyT Eğitim Modülleri için Şablon

Yöneticiler için Bilgi Güvenliği **Ünite 3 - Hafta 6** **Birim (Modül) adı: Üçüncü taraf satıcı güvenliği**	
Öğrenme Aktiviteleri	❑ **Web Semineri** ❑ **Alıştırmaları** ❑ **Atölye Sunumu** ❑❑ **Diğer**
Öğrenme Sorumlusu	• George Matache – et al.
Öğrenme Etkinliği Hedefleri	1. Sosyal Ağlardaki Riskler 2. Sosyal Ağlarda Güvenlik ve Gizlilik Önlemlerine Yönelik Önlemler 3. Güvenlik teknikleri 4. Tedarik gereksinimleri
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?*** • Temel yönetim becerileri • Temel BT becerileri • Temel güvenlik becerileri

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.1

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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

Modül hakkında kısa bilgi

Giriş

Tedarik gereksinimleri, gerçekleştiren kuruluşun dışındaki kuruluşlardan edinilmesi gereken mal ve hizmetleri ifade eder. Çeşitli nedenlerden dolayı, bazen performans gösteren kuruluşlar, bir projeyi tamamlamak için gerekenleri sağlamak için satıcılara güvenir.

Örneğin, envanter izleme sistemlerini otomatikleştirmek için bir proje üstlenen widget üreticisini düşünün. Proje çalışma faaliyetlerinden bazıları, depolama kutularının ana depolarına taşınmasını içerir. İş faaliyetlerinden bazıları özel yazılım geliştirmeyi içerir. Yazılım geliştirme faaliyetlerine gelince, widget üreticisinin yazılım uygulamasını nasıl geliştireceğini bilen bir insan kaynağı yoktur. Yazılım geliştirme faaliyetleri ile ilgili olarak, widget üreticisi bu hizmetleri satın almalıdır.

Web tabanlı sosyal ağlar (WBSN'ler), kullanıcıların kaynakları (örneğin, kişisel veriler, ek açıklamalar, bloglar) yayınlamalarına ve iş, eğlence, din, buluşma vb. ile ilgili olabilecek amaçlar için muhtemelen farklı türde ilişkiler kurmalarına olanak tanıyan çevrimiçi topluluklardır. Son birkaç yılda, WBSN'lerin kullanımı ve yayılması artmakta olup, yaklaşık 300 Web sitesi 400 milyondan fazla kayıtlı kullanıcının bilgilerini toplamaktadır. Sonuç olarak, "net model" bugün şirketler ve kuruluşlar tarafından iletişim kurmak, bilgi paylaşmak, karar vermek ve "iş yapmak" için giderek daha fazla kullanılmaktadır.

Daha sonra, özel bilgileri koruyabilen ve paylaşılan kaynaklara erişimi düzenleyebilen sosyal ağlar için güvenlik mekanizmaları tasarlamak zor bir konudur. Bu makalede, Dünya Bankası ortamının özelliklerine ve koruma gereksinimlerine genel bir bakış sunmanın yanı sıra, Web 2.0 olarak adlandırılan teknolojilerle ilgili gelişmekte olan teknolojilere özellikle dikkat ederek, sosyal ağ güvenliğine yönelik mevcut yaklaşımları ve gelecekteki eğilimleri göstereceğiz.
Öğrenciler, ilgili metni okuyarak, akış web seminerlerini izleyerek ve alıştırmaları kendi hızlarında çözerek bu yönler hakkında bilgilendirilebilirler. Tüm bu dokümanlar dijital interaktif proje platformundadır.
Öğrenciler cevaplarını Öz değerlendirme alıştırmalarında test edebilirler. Diğer alıştırmalarla ilgili cevaplar ilgili tartışma forumuna kaydedilmeli ve haftada bir kez ortak organize toplantıda mentorla tartışılmalıdır. Öğrenci, özellikle toplantılar sırasında diğerleriyle işbirliği içinde çalışabilir ve mentorluk yapabilir. Eğitimin yansıtılması ve değerlendirilmesi için önemli olan e-portfolyo geliştirmeleri desteklenecektir.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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

Öğrenme Materyalinin İçeriği

Üçüncü taraf satıcı, başka bir şirkete (veya o şirketin müşterilerine) hizmet sağlayan bir kişi veya şirkettir. Satıcılar "üçüncü taraflar" olarak kabul edilirken, bazı endüstriler "üçüncü taraf satıcıyı" özellikle yazılı sözleşme kapsamında bir satıcı olarak ayırt eder, ancak tüm satıcılar bir sözleşme kapsamında çalışmaz. Netlik adına, bu makaledeki "üçüncü taraf satıcı" terimi, sözleşmeli veya sözleşmesiz olarak başka bir şirkete hizmet sağlayan herhangi bir birey veya şirketi ifade eder.

İşbirliği başarının anahtarıdır. Üçüncü taraflarla çalışmak, işletmelerin üretkenliklerini ve verimliliklerini artırmalarına, daha iyi ürün ve hizmetler üretmelerine, yüksek nitelikli uzmanlar istihdam etmelerine ve maliyetleri düşürmelerine yardımcı olur. Ancak tüm bu faydalar, artan siber güvenlik risklerinin bedeline karşılık geliyor. Üçüncü taraf satıcınızın güvenlik ve gizlilik rutinlerindeki küçük kusurlar, şirketiniz için siber güvenlik zayıflıklarına dönüşebilir. Bu makalede, üçüncü taraflarla ilgili belirli siber güvenlik risklerini ve bunları nasıl azaltabileceğinizi analiz ediyoruz.

Üçüncü taraf satıcılardan alınan mal ve hizmetler aşağıdakileri içerebilir, ancak bunlarla sınırlı değildir:

- Bulut web barındırma hizmetleri. Bir bulut barındırma satıcısı, disk alanı ve bant genişliğinden şifreleme ve yüksek teknoloji güvenlik çözümlerine kadar her şeyi sağlayabilir.
- Bulut tabanlı yazılım çözümleri. SaaS yazılım satıcıları, işletmeniz veya müşterileriniz için yazılım programlarına erişim sağlar. Örneğin, pazarlama otomasyon platformları, CRM'ler, muhasebe paketleri vb.
- Ekipman bakımı. Fotokopi makinenizi düzelten şirket ve ağ güvenliğinizi yöneten ekip üçüncü taraf satıcılardır.
- HVAC servisi. Biriminize hizmet veren yerel HVAC şirketi, üçüncü taraf satıcı hizmetleri sunmaktadır.
- Her türlü müteahhitler. Kısa veya uzun vadeli herhangi bir yüklenici, üçüncü taraf bir satıcıdır.
- Çağrı merkezi sağlayıcıları. Çağrı merkezinizi başka bir şirkette barındırıyorsanız, üçüncü taraf bir satıcı olarak kabul edilir.
- Defter tutma/mali denetçiler. Mali durumunuzu yönetmek, bütçenizi yönetmek veya mali durumunuzu denetlemek için işe alınan herhangi bir kişi veya işletme üçüncü taraf bir satıcıdır.
- Avukatlar. Bazen sözleşmeleri imzalamadan veya büyük satın alımlar yapmadan önce bir avukata danışmak gerekir. Tüm yasal hizmetler üçüncü taraf satıcılar olarak kabul edilir.

Kuruluşlar, temel hizmetleri sağlamak için üçüncü taraf satıcılara giderek daha fazla güvendikçe, satıcıyla ilgili siber güvenlik risklerine karşı da daha savunmasız hale geliyorlar. Yakın zamanda yapılan bir araştırma, şirketlerin yaklaşık% 60'ının geçen yıl üçüncü taraf bir satıcı nedeniyle veri

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

ihlali yaşadığını tespit etti. Ancak, kuruluşların farkında olması gereken en yaygın satıcı siber boşlukları nelerdir?

Hizmet sağlayıcılar için üçüncü taraf satıcıları kullanmanın avantajları nelerdir?
Günümüz dünyasında, üçüncü taraf satıcıları kullanmaktan kaçınmak imkansızdır. Şirketiniz kaç departman oluşturursa oluştursun, ihtiyacınız olan her hizmeti asla kapsayamazsınız. Şirketler, dış kaynaklı olanlara karşı iş için gerekli olan becerilerin doğru dengesini belirlemelidir. İşte bu dengeyi doğru kurduğunuzda ne olacağı:

Zaman kazanacaksınız. Hiç kimsenin her beceriyi öğrenmek veya bir işi yürütmek için gerekli olan her kişiyi işe almak için zamanı yoktur. Üçüncü taraf satıcılar, müşterileriniz için siparişleri yürütmek ve yerine getirmek için gereken tüm profesyonel hizmetleri alarak iş süreçlerinin sorunsuz çalışmasını sağlar.

Paradan tasarruf edeceksiniz. Belki de en büyük faydası maliyet tasarrufudur. Gerektiğinde iş için üçüncü taraf bir sağlayıcıyla sözleşme yapmak, şirket bordrosunda her zaman profesyonellere sahip olmaktan çok daha ucuz olabilir. Örneğin, bir avukatı hizmette tutmak yerine, ihtiyacınız olduğunda bir avukat tutmak çok daha ucuzdur.

Değerli uzmanlık kazanacaksınız. Şirketinizin yeni bir uzman ekibi geliştirmek için zamanı yok. Bunu yapmanın zamanı ve maliyeti çok büyük olurdu. Şirket içinde sahip olmadığınız uzmanlık için üçüncü taraf bir satıcıyı işe almak muhtemelen daha iyi sonuçlar verecektir.

Üçüncü taraf satıcıları kullanmanın riskleri nelerdir?
Üçüncü taraflar, ağ güvenliklerini sizin istediğiniz kadar ciddiye almayabilir. Bunu bilerek, bilgisayar korsanları şirketinize doğrudan saldırmamayı seçebilir. Bunun yerine, üçüncü taraf satıcılarınız arasında daha kolay bir hedef arayabilirler. Güvenliği ihlal edilmiş bir alt yüklenici, siber suçlular için kolayca bir giriş noktasına dönüştürülebilir.

Satıcılarınız teslim edemezse, siz de teslim edemezsiniz. Bununla birlikte, risk herhangi bir iş ilişkisinin doğasında vardır. Üçüncü taraf satıcıları kullanmak, çoğu azaltılabilecek birçok riskle birlikte gelir.

En büyük risk, güvenlik standartlarınıza uymayan bir üçüncü taraf ilişkisi seçmektir. Örneğin, ağ güvenliği ekibinizin belirli standartlarınıza uygun güvenlik protokollerini izlemesi gerekir. Şirketiniz sağlık sigortası gibi düzenlemelere bağlıysa, sağlık sigortası düzenlemelerine uymayan bir ağ güvenlik şirketini işe almayı göze alamazsınız. Düzenlemeleri anlayan ve bu düzenlemeleri karşılamak için uyum sağlamaya istekli bir satıcıya ihtiyacınız var.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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

Veri gizliliği düzenlemelerine bağlı olduğunuzda, tam olarak hangi güvenlik standartlarının uygulandığını bilmeniz gerekir ve satıcılarınız onlarla eşit değilse, bunu düzeltmeye çalışmalısınız. Aksi takdirde, şirketinizi veri ihlali gibi siber güvenlik risklerine maruz bırakmış olursunuz.

Veri ihlalleri, özellikle kişisel bilgilerinizi korurken son derece rahatsız edicidir. Ne yazık ki, veri ihlalleri artıyor ve her zamankinden daha yaygın. Veri ihlalleri operasyonlarda aksamalara, yıkıcı finansal sonuçlara, yasal işlemlere ve itibarın zedelenmesine neden olabilir. Bunlardan kaçınmak için, kendi güvenliğiniz veya satıcılarınızın güvenliği söz konusu olduğunda gardınızı düşüremezsiniz.

Üçüncü taraf satıcı uzlaşmasının niteliğine bağlı olarak, bir kuruluş farklı risklerle karşı karşıya kalabilir. En yaygın risk kategorilerine ve azaltmak için hazırlıklı olmanız gereken tehditlere bakalım. Güvenliği ihlal edilmiş bir üçüncü taraf satıcı, dört ana kategoriye ayrılabilecek birden fazla riske yol açabilir: Şekil 1

Siber güvenlik riskleri — Alt yükleniciler genellikle müşterilerinin farklı ortamlarına, sistemlerine ve verilerine meşru erişime sahiptir. Saldırganlar, değerli varlıklarınızı ele geçirmeye çalışmak için giriş noktası olarak üçüncü taraf bir satıcı kullanabilir.

Operasyonel riskler — Siber suçlular yalnızca verilerinizi değil, dahili sistemlerinizi ve kullandığınız hizmetleri hedefleyebilir. Bu, operasyonlarınızın kısmen kesintiye uğramasına veya hatta tamamen durdurulmasına neden olabilir.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

Uyumluluk riskleri — Uluslararası, yerel ve sektöre özgü standartlar ve düzenlemeler, kuruluşların karşılaması gereken katı siber güvenlik kriterlerini belirler. Ayrıca, bu kuruluşlarla çalışan üçüncü taraflar da bu gerekliliklere uymak zorundadır. Uyumsuzluk genellikle önemli para cezalarına ve itibar hasarına yol açar.

İtibar riskleri — Değerli verilerinizin ve sistemlerinizin güvenliğinin ihlal edilmesi, hem mevcut hem de gelecekteki iş ortaklarınız ve müşterileriniz için kırmızı bayrak görevi görür. Güvenlerini yeniden kazanmak çok zaman ve çaba gerektirecektir. Ve ne yazık ki, ciddi bir siber güvenlik olayından sonra itibarınızı başarılı bir şekilde geri kazanabileceğinizin garantisi yoktur.

Tedarik gereksinimleri

Çeşitli nedenlerden dolayı, bazen performans gösteren kuruluşlar, bir projeyi tamamlamak için gerekenleri sağlamak için satıcılara güvenir. Özellikle KOBİ'ler. Bu nedenle, üçüncü taraf satıcı güvenliği ile çalışmak için tedarik gereksinimleri son derece önemlidir.

Satın almanın son derece bireyselleştirilmiş bir süreç olduğu doğru olsa da, genellikle yönetim kurulu genelinde kullanılacak birkaç temel aşama da vardır.

Tedarik gereksinimleri, gerçekleştiren kuruluşun dışındaki kuruluşlardan edinilmesi gereken mal ve hizmetleri ifade eder. Çeşitli nedenlerden dolayı, bazen performans gösteren kuruluşlar, bir projeyi tamamlamak için gerekenleri sağlamak için satıcılara güvenir.

Satınalma Aşamaları
Aşama 1: Ürün ve/veya hizmetlere olan ihtiyacı belirleyin.
2. Aşama: Bir satın alma isteği oluşturun ve gönderin.
Aşama 3: Tedarikçileri/satıcıları değerlendirin ve seçin.
Aşama 4: Seçilen tedarikçi ile bir sözleşmenin şartlarını müzakere edin.
5. Aşama: Bir satınalma siparişini kesinleştirin.

Tedarik sürecindeki ilk adım, gereksinimleri belirlemektir. Tüm tedarik gereklilikleri bir ihtiyaç algısı ile başlar. Bir su kütlesini geçme ihtiyacı, bir köprü, feribot veya diğer ulaşım sistemleri inşa etmek için bir gereklilik yaratabilir.

Aşama 1: Ürün ve/veya hizmetlere olan ihtiyacı belirleme

Tedarik süreci başlamadan önce, belirli bir ihtiyacın tanınması gerekir. Örneğin, bir kuruluş yeni bilgisayar monitörleri satın almak, aylık kağıt ürünleri tedarikini yeniden sipariş etmek veya güncelleştirilmiş yazılım edinmekle ilgilenebilir. Şirket yapısına bağlı olarak, bu adım işletme sahipleri, departman başkanları, yönetici ekibi, personel ve / veya satın alma yöneticileri

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

tarafından yönetilebilir. Bu aşamada, bir bütçe belirlenecek ve harcamaların kapsamlı bir görünümü sıklıkla değerlendirilecektir.

Bu aşamada, ihtiyacı açıkça tanımlamak gerekir ve bu, su kütlesini geçmek için en iyi modu (mevcut durum ve öngörülen gelecekteki ihtiyaç göz önüne alındığında), daha sonra inşa edilecek köprünün türünü veya bir köprü ile diğer alternatifler arasındaki en iyi çözümü belirlemek için karşılaştırmalı bir maliyet / fayda analizini belirlemek için bir çalışma yoluyla yapılabilir. Çalışma, ihtiyacın şirket içinde mi yoksa sözleşmeli olarak mı karşılanabileceğini, ilk bütçe tahmininin niceliğini ve tedarik sağlama süresi hakkında bir fikri içermelidir.

2. Aşama: Satın alma isteği oluşturma ve gönderme
Bir satınalma talebi (veya satınalma talebi), mal veya hizmetler için resmi bir taleptir ve genellikle özel tedarik yazılımı kullanılarak gönderilir. Çoğu zaman, satın alma talebi bir çalışan veya yöneticiden kaynaklanır, ardından kuruluşun tedarik ekibi tarafından gözden geçirilir.

Bir satınalma isteği onaylandığında, bir satınalma siparişi haline gelir. Ancak, istek reddedilirse, genellikle kısa bir açıklama ile gönderene iade edilir. Reddedilen bir satın alma siparişi, ideal olmasa da, iyi bir öğrenme fırsatı olabilir.

3. Aşama: Tedarikçileri/satıcıları değerlendirin ve seçin
Bir sonraki adım, çeşitli satıcıları değerlendirmek ve ardından temel gereksinimleri karşılayan birini seçmektir. Bazı kuruluşlar, kendilerini kanıtlamış çeşitli tedarikçileri içeren onaylı satıcılardan oluşan bir katalog tutar.

Satıcıları talep etmek, kapsamı eldeki gereksinim (ler) tarafından belirlenen basitten karmaşığa kadar değişebilen bir süreçtir. Genellikle, çeşitli satıcılara birkaç teklif talebi (RFQ) gönderilir, böylece kuruluş/tedarik ekibi fiyatları ve seçenekleri karşılaştırabilir.

Bir satıcı seçerken fiyatın tek belirleyici olmaması gerektiğini unutmayın. En iyi sonuçlar için, aşağıdakiler de dahil olmak üzere bir satıcının neler sunabileceğinin "büyük resmini" göz önünde bulundurun:
-İletişim kolaylığı
-Şirket etiği
-Sorumluluk
-Üretim kabiliyetleri

Bir satıcı seçildikten sonra, ilişkiye zaman ve enerji yatırımı yapmak önemlidir. Bir tedarikçiyle iyi bir ilişki, uzun vadede maksimum değer sağlayarak daha iyi tasarruf ve hizmetin kilidini açabilir.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

Aşama 4: Seçilen tedarikçi ile bir sözleşmenin şartlarını müzakere edin

En uygun satıcıyı seçtikten sonra, sözleşme görüşmelerine geçmenin zamanı geldi. Başarılı tedarik açısından, bu şimdiye kadarki en kritik aşamalardan biridir. Bu aşamada, fiyatlandırmanın yanı sıra teslimat programları, belirli şartlar ve koşullar ve daha fazlası gibi ayrıntıları ana hatlarıyla belirtecek ve kabul edeceksiniz. İyileştirme fırsatlarını belirlemek için önceki sözleşmeleri değerlendirmek genellikle yararlı olabilir, bu da ileriye dönük olarak daha bilinçli bir yaklaşım benimsemenizi sağlar.

5. Aşama: Bir satınalma siparişini sonlandırma

Son sözleşme onaylandıktan sonra, bir sonraki iş emri satınalma siparişidir (PO). Sözleşme genellikle tam alıcı/tedarikçi ilişkisini yönetirken, bir satınalma siparişi belirli bir satın alma işlemine yakınlaşır.

Bu belgeyi, aşağıdakileri tam olarak ayrıntılandıran başka bir resmi sözleşme olarak düşünün:

-Toplam maliyet/fiyat

-Mal ve/veya hizmetlerin detaylı tanımı

-Miktar

-Diğer özel şartlar ve koşullar

6. Aşama: Sipariş yönetimi

Mallar / hizmetler teslim edilirken, tüm standartların teslimat tarihlerine, ürün miktarlarına ve kalitesine vb. Uyup uymadığını kontrol etmekten sorumlu biri, ideal olarak ürün veya hizmetlerin son kullanıcısı olmalıdır. Öğelerle ilgili sorunlar varsa (ör. hasarlı ürünler), teslimatı reddetme seçeneğiniz vardır. Herhangi bir teslimat sorunu olması durumunda satıcı ile açık iletişim çok önemlidir.

Teknoloji ve iletişim, işletmelerin tedarik zincirlerini genişletmelerine izin verdikçe, satıcı risk yönetiminin karmaşıklığı artmaktadır. İşletmeniz muhtemelen her zamankinden daha fazla satıcıyla çalışıyor ve bu satıcıların her biri kuruluşunuz için bir miktar risk oluşturacaktır.

Satıcı güvenliği risk yönetimi, tedarik zincirinizdeki satıcılar nedeniyle kuruluşunuzun karşılaştığı tehditlerin, güvenlik açıklarının ve zayıflıkların sayısını sınırlamak için tasarlanmış bir stratejidir. Bir satıcı genellikle işletmenizin çalışması için gereken bir ürün, hizmet veya ekipman parçası satan üçüncü taraf bir kuruluştur.

Her satıcı, kuruluşunuza bağlandıktan sonra, bir miktar siber güvenlik riski taşıyacaktır. Anlaşmanın sonunu koruyamazsa veya bir siber saldırının kurbanı olurlarsa, kuruluşunuzu doğrudan etkileyebilir. Etkili bir risk değerlendirmesi, daha büyük bir satıcı risk yönetimi planının bir parçası olarak, bu potansiyel başarısızlık noktalarını bir sorun haline gelmeden çok önce tanımlamaya ve

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

düzeltmeye çalışır.

Satıcı Risk Yönetimi Döngüsü

Satıcı güvenliği risk yönetimi devam eden bir süreçtir ve tedarik zincirinize getirdiğiniz her satıcıyla birlikte yürüteceğiniz bir süreçtir. Genellikle, işlem şöyle görünür:

Adım 1: Analiz – Şirket, ilişkinin doğal riskini ve yapılacak durum tespiti seviyesini tanımlar. Bu doğrultuda şirket, üçüncü tarafın güvenlik duruşunu değerlendirerek boşluk analizi yapar.
Adım 2: Katılım - Şirket ve üçüncü taraf, boşlukların nasıl giderileceği konusunda işbirliği yapar.
Adım 3: İyileştirme - Üçüncü taraf siber boşlukları düzeltir.
Adım 4: Onay – Şirket, üçüncü tarafı onaylar veya risk toleransına dayanarak reddeder.
Adım 5: İzleme - Şirket, herhangi bir siber boşluğu tespit etmek için üçüncü tarafı izlemeye devam ediyor

Sosyal ağlar ve satıcı güvenliği riskleri

Sosyal ağlar günümüz dünyasında çok popüler. Genellikle, bir sosyal ağ, kişisel, iş veya güven ilişkileri ile birbirine bağlı bir dizi bireyden (kişiler, gruplar, kuruluşlar) oluşan küçük bir dünya ağı olarak tanımlanır. Sosyal ağ o zaman Web bağlamında her türlü sanal topluluğa uygulanabilecek oldukça geniş ve genel bir kavramdır. Örneğin, Web postası, çevrimiçi dergiler veya abonelik gerektiren gazeteler gibi bir Web hizmetine kayıtlı kullanıcılar bir sosyal ağ olarak kabul edilebilir. Aşağıda, çevrimiçi bir topluluğun Web sitesinin yalnızca aşağıdaki koşulları yerine getirmesi durumunda Web tabanlı bir sosyal ağ olarak kabul edilebileceği tanımını benimsiyoruz:

- İlişkiler, üyeleri tarafından açıkça belirtilir ve mevcut etkileşimlerden çıkarılmaz (örneğin, örtük ilişkileri çıkarmak için bir posta listesi kullanılabilir).
- İlişkiler, veritabanı yönetim sistemleri gibi teknolojiler kullanılarak, ilişki analizine olanak tanıyan ve ilişki verilerine erişimi ve bunların alınmasını düzenleyen teknolojiler kullanılarak depolanır ve yönetilir.
- Üyeler ilişki bilgilerine en azından kısmen erişebilirler.

Anahtar Terimler

İlişkiye Dayalı Erişim Kontrolü: Belirli bir kaynağa erişmeye yetkili sosyal ağ üyelerinin, erişimi elde etmek için katılmaları gereken ilişkiler açısından gösterildiği, özellikle sosyal ağlara uyarlanmış bir erişim kontrolü paradigmasıdır.

Sosyal Ağ: Kişisel, iş veya güven ilişkileri ile birbirine bağlı bir dizi bireyden (kişiler, gruplar, organizasyon) oluşan küçük bir dünya ağı. Genellikle düğümlerin sosyal ağ üyelerine karşılık geldiği bir grafik olarak modellenirken, kenarlar aralarında var olan ilişkileri gösterir.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

Sosyal ağlar. Çevremizdekilerle iletişim kurmak ve bilgi paylaşmak herkesin hayatının bir parçasıdır ve basit metin mesajlarından e-postalara ve şimdi sosyal medya platformları dediğimiz şeye dönüşmüştür. Çok iyi bilinmeyen veya fark edilmeyen şey, çevrimiçi ortamda maruz kalmamızın birçok riski beraberinde getirdiğidir.

Sosyal medya ve sosyal ağ veya mesajlaşma uygulamaları, uygunsuz veya güvensiz bir şekilde kullanıldığında hem kuruluşlar hem de bireyler için bir dizi güvenlik ve gizlilik riski oluşturabilir. Sosyal ağlardaki en popüler ve yaygın platformlar:

- 1.300.000.000'dan fazla üyesi olan Facebook;
- Flickr, medya dosyalarını depolamak, düzenlemek ve paylaşmak için kullanılır;
- 300 milyondan fazla kullanıcısı olan LinkedIn;
- 30 milyondan fazla kullanıcısı olan Instagram;
- Bir milyardan fazla üyesi olan Twitter;
- Bir milyardan fazla kullanıcısı olan YouTube;
- Yaklaşık 12 milyon kullanıcısı olan Tinder;
- 800 milyondan fazla kullanıcısı olan TikTok.

Gizliliğe Duyarlı Erişim Kontrolü: Sosyal ağlar bağlamında, sosyal ağ üyelerinin erişim kontrolü gereksinimlerinin, katıldıkları ilişkiler hakkında özel bilgileri ifşa etmeden uygulandığı bir erişim kontrolü paradigmasını belirtir.

Web Tabanlı Sosyal Ağ: Kayıtlı üyelerinin diğer üyelerle ilişki kurmasına ve farklı bilgi türlerini (örneğin, kişisel veriler, kişiler, multimedya kaynakları) paylaşmasına izin veren Web tabanlı bir sistemdir.

Sosyal Ağ Analizi: Sosyal ağ topolojisinin analizinden istatistiksel veri toplamayı amaçlayan bir disiplin.

İlişki Güven Düzeyi: Bir sosyal ağda, belirli bir üyenin başka bir üyeyi ne kadar güvenilir gördüğünün bir ölçüsünü sağlayarak, bir güven ilişkisi ile ilişkili değeri gösterir. Kullanıldığı amaca bağlı olarak, bu kavramın farklı anlamları olabilir. Örneğin, işbirlikçi bir derecelendirme ortamında, belirli bir üyenin belirli bir konuyla ilgili olarak başka bir üyenin görüşlerine ne kadar güvendiğini (topikal güven) veya genel olarak (mutlak güven) gösterir. Buna karşılık, bir erişim kontrolü bağlamında, zorunlu erişim kontrol modellerinde kullanılan güvenlik seviyesi kavramıyla bazı benzerlikleri vardır.

Kenar Pertürbasyonu: Ağ grafiğinde bir dizi rastgele kenar silme / ekleme gerçekleştirerek gerçek

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

sosyal ağ ilişkilerini gizlemeyi amaçlayan grafik anonimleştirme tekniği.

Sosyal Ağ İlişkisi: Bir sosyal ağın iki üyesini ilgilendiren bir ilişki. WBSN'lerde, kişisel/iş ilişkilerinin (örneğin, arkadaş/meslektaş) yanı sıra, bir üyenin diğerine ne kadar güvendiğini gösteren güven ilişkileri de desteklenebilir. Bir sosyal ağın grafik gösteriminde, ilişkiler genellikle bir ilişki türü ve / veya bir ilişki güven düzeyi ile etiketlenmiş kenarlarla gösterilir.

Grafik Anonimleştirme: Sosyal ağ analizi yaparken sosyal ağ üyeleri hakkındaki özel bilgileri gizlemeyi amaçlayan tekniktir. Düğüm anonimleştirme ve kenar pertürbasyonu, şu anda kullanılan iki ana grafik anonimleştirme tekniğidir.

Düğüm Anonimleştirme: Karşılık gelen düğümleri rastgele tanımlayıcılarla etiketleyerek (naif anonimleştirme) veya düğümlerin ilgili kullanıcıyı tanımlamak için kullanılabilecek niteliklerle ilişkilendirilmesi durumunda, k-anonimliğe dayalı teknikler kullanarak sosyal ağ üyelerinin kimliklerini gizlemeyi amaçlayan grafik anonimleştirme tekniği (Sweeney, 2002).

Risk

Coğrafi etiketleme

- Coğrafi tanımlayıcı verilerin, konumunuzu okuyabilen veya ayarlarınızda bunu yapmasına izin verilen uygulamalar tarafından fotoğraflara, videolara, web sitelerine ve kısa mesajlara eklenmesini temsil eder;
- Tam konumunuzu, nerede çalıştığınızı veya nerede yaşadığınızı açıklamaktan kaçınmak için hassas konumlardaki coğrafi etiketleme özelliklerini kapattığınızdan emin olun.

"Kitle"

- Bu, yayınlarınızı kimlerin görebileceğini ve/veya yorum yapabileceğini ifade eden genel bir terimdir;
- Arkadaş grubunuz istediğiniz zaman değişebilir ve hakkınızda bilgi içeren bir gönderiyi görüntüleyebilir. Kasıtlı olarak "arkadaşlarınızla" bir şeyler paylaşabilirsiniz, ancak yayınla yaptıkları şey kişisel kontrolünüzün ötesindedir.

Kimlik

- Özellikle bir bireyle ilgili bilgi aralığını açıklar;
- Kimlik bilgilerini aramak için sosyal medyayı bir araştırma yöntemi olarak kullanan, kimlik hırsızlığı, dolandırıcılık, zimmete para geçirme veya korkutma gibi olası kötü niyetli kişiler olduğu unutulmamalıdır.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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

Önlemler

Parola

- Her çevrimiçi hesap için farklı bir şifre kullanılması önerilir;
- En az 10 karakter uzunluğunda olmalı ve büyük harfler, küçük harfler, sayılar ve özel karakterler içermelidir;
- Anlatmak istediğimiz kişi ne kadar yakın veya güvenilir olursa olsun, kimseye ifşa edilmemelidir.
- Bir şifre oluştururken kişisel bilgilerin kullanılmaması önerilir (örneğin: ebeveynlerin adları, doğum tarihi, evcil hayvanın adı, vb.);
- Parolanızı düzenli aralıklarla değiştirin;
- Size ait olmayan veya başka biri tarafından kullanılan bir cihazı kullanırken hesabınızdan çıkış yapın.

Güvenlik güncellemelerinizi zamanında yapın!

- Sosyal medya platformları düzenli olarak yeni gizlilik ve güvenlik ayarları sunar. Bunlar hesap ayarlarınızda bulunabilir ve bunları düzenli olarak kontrol etmeniz önerilir;
- Birinin hesabınızı hacklemeye çalışmadığından emin olmak için iki faktörlü kimlik doğrulama (2FA) seçeneğini kullanın.

Kimseden arkadaşlık isteği kabul etmeyin!

- Resmi profillerini takip etmeye özen göstererek yalnızca gerçek hayatta tanıştığınız kişilerden veya ilgilendiğiniz herkese açık kişilerden/kişilere arkadaşlık isteklerini kabul etmek veya göndermek;
- UNUTMAYIN! Belirli hesaplara bağlı hissediyorsanız, yayınlarınıza erişimlerini kısıtlayabilir veya hesabı engelleyebilirsiniz. Ayrıca, sahte hesap, sahte ad, uygunsuz içeriğe sahip gönderiler, şiddete teşvik, yanlış bilgi vb. gibi nedenlerle hesapları veya gönderileri şikayet etme seçeneğiniz de vardır.
- TIKLAMAYIN!
- Birçok saldırgan, daha sonra bilgiye erişmek için bir kişinin güvenini kazanmak için sosyal mühendisliği kullanır;
- Kaynaktan% 100 emin değilseniz sosyal medyadan bağlantıları ve ekleri açmayın (örneğin, ödül sunan web siteleri genellikle bilgi çalmayı amaçlamaktadır);
- Sohbetlerden, bir arkadaş farklı davranıyor gibi görünüyorsa (çok fazla soru soruyor, kişisel hayatını çok merak ediyor, para istiyorsa), hesabının saldırıya uğramış olması ve bir saldırganın kötü amaçlarla kullanması olasılığı vardır.

Göndermeden önce iki kez düşünün!

- Sosyal medya, olumsuz bir çevrimiçi itibar kadar olumlu bir çevrimiçi itibar yaratma fırsatı sunar, ayrıca bir gönderiyi "silsek" bile, çevrimiçi göründüğünde kalıcı olarak silinemez;

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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

- Sosyal medyada çok fazla kişisel ayrıntı açıklamayın! "Hakkımda" alanları isteğe bağlıdır.
- Çevrimiçi ortamda profesyonel ve kişisel yaşam arasındaki sınır
- İşvereniniz hakkındaki bilgileri çevrimiçi olarak ifşa etmeyin
- İşvereni kötü bir ışığa sokan iş fotoğrafları veya olumsuz mesajlar yayınlamayın.
- Göndermeden önce düşünün ve işinizi riske atmayın.

Eski hesapları kapatın!

- Sosyal medya platformlarında artık kullanmadığınız eski hesaplarınız veya aynı platformda eski hesaplarınız varsa, bunları kapatmaya çalışın. Bu şekilde, mevcut hesapların olası saldırganlardan daha fazla korunduğu mümkün olduğunca az bağlantı oluşturursunuz;
- Eski hesaplar veya platformlar bugünküler kadar güvenli olmayabilir.

Sosyal medya büyük riskler oluşturuyor

- Sosyal ağlar, merkezi mimarileri, herhangi bir bilgisayar korsanının sahip olmak isteyeceği kişisel olarak tanımlanabilir bilgilerin büyük deposu ve nüfusun sosyal medyanın nasıl düzgün kullanılacağı konusundaki genel cehaleti nedeniyle yüksek güvenlik ve gizlilik riskleri oluşturmaktadır. çevrimiçi güvenliklerini artırmak için gizlilik ayarları.
- Özellikle gençler arasında bir başka çok yüksek risk, diğer insanlara ve çevrimiçi olarak açıklanan kişisel bilgilerin türüne güvenmektir.
- Bu, teknolojik araçlar ve güvenlik politikalarının uygulanması yoluyla mücadele edilebilir.
- Sosyal medya aracılığıyla iletilen bilgilerin güvensiz olduğunu ve bu nedenle hassas bilgileri sosyal medya aracılığıyla iletmediğimizi düşünmeliyiz, bu nedenle güvende kalmanın birincil sorumluluğu KULLANICI'ya aittir.

Kötü sosyal medya alışkanlıkları

- Sosyal ağlar günümüzde kullanıcılar tarafından yaygın olarak kullanılan platformlardır. Çok çeşitli olanaklara sahibiz.
- Bazıları daha çok fotoğraf veya video yüklemeye, diğerleri fikrimize ve diğer durumlarda sadece arkadaşlarınızla ve ailenizle iletişimde kalmaya yöneliktir. Her durumda, dünya çapında birçok kullanıcısı olan platformlarla uğraşıyoruz.
- Bu aynı zamanda bilgisayar korsanlarının gözlerini buraya dikmelerini sağlar. Gizliliğimizi ve güvenliğimizi korumak istiyorsak sosyal ağlarda değiştirilmesi gereken bu alışkanlıklar hakkında konuşacağız.
- Ağda bulabileceğimiz ve bize arkadaşlarımıza veya ailemize mesaj gönderme, fotoğraflara, videolara yorum yapma fırsatı veren birçok platform türü var ...
- Bu, onları hem özel kullanıcılar hem de işletmeler için çok popüler bir ortam haline getirir.
- Ancak, bu aynı zamanda güvenliğimiz ve gizliliğimiz için bazı risklere sahip olmanıza neden olur. Bilgisayar korsanları saldırılarını gerçekleştirmek için burayı izleyebilirler. Özellikle bu platformları kullanırken kötü kullanıcı alışkanlıklarından yararlanabilirler.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

Değiştirilmesi gereken alışkanlıklar

- Gizlilik ve güvenlik, kullanıcılar için çok önemli faktörlerdir.
- Ancak, her zaman mevcut değildirler.
- Bu iki faktörü tehlikeye atan birçok saldırı türünün kurbanı olabiliriz.
- Sosyal medyayı kullanırken de hatalar yapabiliriz ve bu bizi etkiler.

Her türlü kişiyi ekleyin

- Sosyal ağlarda çok yaygın bir hata, her türlü kişiyi eklemektir. Bu, Facebook gibi platformlarda olabilir.
- Eklediğimiz şeyin gerçek bir kullanıcıdan ziyade bir bot olması mümkündür.
- Onları nasıl ayırt edeceğinizi bilmeniz ve davetinizin aldığı herhangi bir kişi türünü eklemekten kaçınmanız gerekir.
- Bazen botlar yalnızca kullanıcı verilerini toplamak için tasarlanmıştır. Bu, gizliliğimizi tehlikeye atabilir. Eklediğimiz kişiler üzerinde gerçek bir filtreye ihtiyacımız var.
- Arkadaşlarımız arasında güvenliğimiz ve gizliliğimiz için sorun olmayan kişilerin olması önemlidir.

Sosyal ağlara hiçbir yerden bağlanmayın

- Genellikle herhangi bir sitedeki sosyal ağlar üzerinden giriş yaparsınız. Bu çok rahat, ancak gizlilik için en iyisi değil.
- Kesinlikle birçok durumda bir sayfaya kaydolma veya Facebook veya Twitter üzerinden bir platforma bağlanma imkanı buluyoruz. Bu siteye kayıt olmaktan ve uzun bir form doldurmaktan kaçınıyoruz. Sorun şu ki, bu web sitesine Facebook aracılığıyla kişisel veriler sağlıyoruz. Paylaştığımız bu veriler/bilgiler üçüncü kişiler tarafından reklam amacıyla kullanılabilir.

Gerekenden daha fazla bilgi vermeyin

- Kesinlikle birçok kullanıcının sahip olduğu en kötü alışkanlıklardan biridir. Sosyal ağlara çok fazla kişisel veri, gerçekten gerekli olmayan bilgiler girerler.
- Örneğin, telefon numaramız, e-posta adresimiz, nerede yaşadığımızla ilgili bilgiler gibi veriler ... Tüm bunlar reklamlarımızı etkiler ve kötü amaçlar için kullanılabilir.
- Gerçekten gerekli olandan daha fazla bilgi vermeyin. Bu şekilde ağdaki gizliliğimizi artıracağız ve hatta bazı güvenlik sorunlarından kaçınabiliriz.

Sahte haberler yaymak

- Sahte haber sorunu bugün hala mevcuttur. Onlara birçok yolla ulaşabilirim, ancak şüphesiz sosyal ağlarda varlıklardan daha fazlasıdırlar.
- Bildiğimiz gibi, yem olarak kullandıkları ve hatta bazen kötü amaçlı yazılım dağıtabildikleri sahte haberlerdir.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

- Bu tür sahte haberleri paylaşmaktan kaçınmak ve ayrıca sosyal medyada gördüğümüzde erişmek önemlidir.
- Bu bizim güvenliğimizi artıracaktır.

Gizliliğimizi korumuyoruz

- Son bir hata, gizliliği düzgün bir şekilde korumamaktır. Örneğin, profillerimizi herkesin girmesi için açık bırakıyoruz.
- Bizim için bir profil oluşturmak ve hatta hedefli reklamlar göndermek veya güvenliğimizi etkileyen çeşitli saldırılar gerçekleştirmek için bu bilgileri toplayabilecek herkese bilgi sağlarız.

Disiplinlerarası bir bakış açısıyla sosyal mühendislik

•Bilgisayar korsanlarının kullandığı teknik nedeniyle bilgi teknolojisi, psikoloji, iş ve etik gibi disiplinler arası bir bakış açısıyla yaklaşmak gerekmektedir.

Bilgi teknolojisi disiplini

- Sosyal mühendislik, mevcut bilgi sistemleri ve bunların bir risk azaltma biçimi olarak kullanılan savunmaları bağlamında tartışılmalıdır.
- Çok faktörlü kimlik doğrulama, kuruluşların sistemlere erişen kişinin gerçekten bu erişime sahip olması gerektiğini onaylaması için yaygın ve genellikle etkili bir yoldur.
- Ek bir faktör, bir sanal özel ağın (VPN) kullanılması, yani kullanıcıyı daha fazla doğrulamak için kimlik doğrulaması olabilir.

Psikoloji disiplini

- Kavramı anlamak ve hem saldırganın hem de mağdurun düşüncelerini ve davranışlarını anlamak gerekir.
- Yöntemler sosyal mühendislik için önemlidir, çünkü davetsiz misafirleri tanımlamak için kullanılan güvenlik duvarları ve sistemler gibi mevcut olabilecek korumaları atlamak için kullanılırlar.
- Veri ihlallerinin ana nedenlerinden biri olan çalışan eylemlerini anlamaya yardımcı olur.

İş perspektifi

- Bu önemlidir, çünkü sosyal mühendislik birçok işletme türünü etkileyebilir ve kuruluşların nasıl yapılandırıldığı ve yönetildiği konusunda etkileri olabilir.
- sosyal mühendislik saldırılarını etkileyen faktörlerin belirlenmesine yardımcı olur ve aşağıdaki iş alanlarıyla ilgili olarak daha spesifik terimlerle ele alındığında faydalıdır: eğitim ve gelişim, belgelenmiş politikalar, iç denetim prosedürleri, bütçeler ve organizasyon kültürü.
- saldırılara katkıda bulunabilecek alanlardan herhangi birindeki eksiklikleri tespit edebilir.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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

Etik bakış açısı

- sosyal mühendislik ve ilgili araştırmalar bağlamında önemlidir, çünkü başka bir insanı manipüle etme fikri birçok etik ilkeyi ihlal eder.
- Bir sosyal mühendislik olayı durumunda, mağdurları tedavi etmeye yardımcı olur.

Aşağıdakileri dikkate almak önemlidir:

- her disiplin, konunun nasıl anlaşılacağı ve yorumlanacağı, farklı saldırı türlerine karşı korunma ve sosyal mühendisliğin etkisini hem insani hem de örgütsel açıdan anlama konusunda bilgi sağlar.
- Her disiplinin konuyu yorumlamasının ancak diğer disiplinler bağlamında bakıldığında yararlı olduğu.

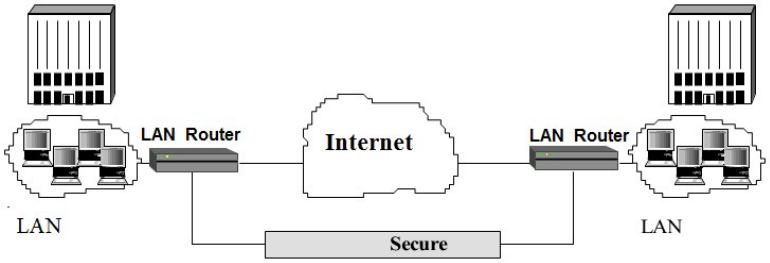
Güvenlik teknikleri

- Ekipman envanteri
- Uygulama ve işletim sistemlerinin envanteri
- Kablosuz ekipman kontrolü
- Ağ güvenliği tasarımı
- Ağ bağlantı noktalarını, iletişim protokollerini ve hizmetlerini sınırlama ve kontrol etme
- Çevre alanlarının korunması
- Konumlara fiziksel erişim
- Yönetici ayrıcalıklarının kontrollü kullanımı
- Kullanıcı hesaplarını izleme ve denetleme
- Beceri değerlendirmesi ve güvenlik eğitimi

VPN (Sanal Özel Ağ)

Sanal özel ağ, Internet gibi güvenli olmayan bir ağ üzerinden güvenli bir bağlantıdır. Sanal, topolojiden bağımsız olarak benzersiz bir ağın, yani iletişim kuran ve tek bir ağ olarak yönetilebilen coğrafi olarak dağıtılmış bir grup bilgisayarın varlığı anlamına gelir.

Özel, erişim denetimine sahip bir sanal ağ anlamına gelir. gizliliği, mesajların bütünlüğünü sağlar ve kullanıcılar ile iletişime katılan bilgisayarlar arasında kimlik doğrulaması yapar.

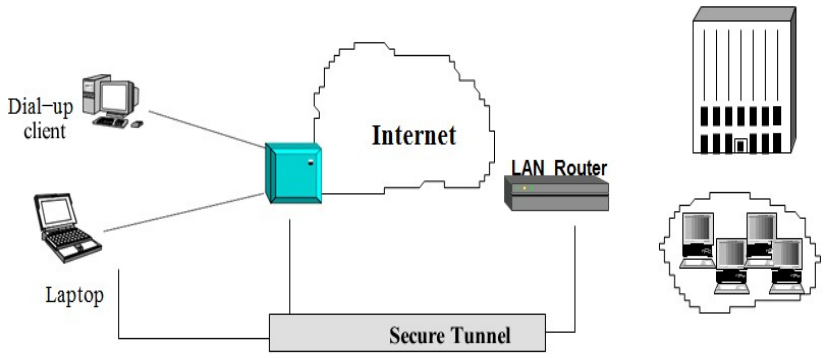


Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

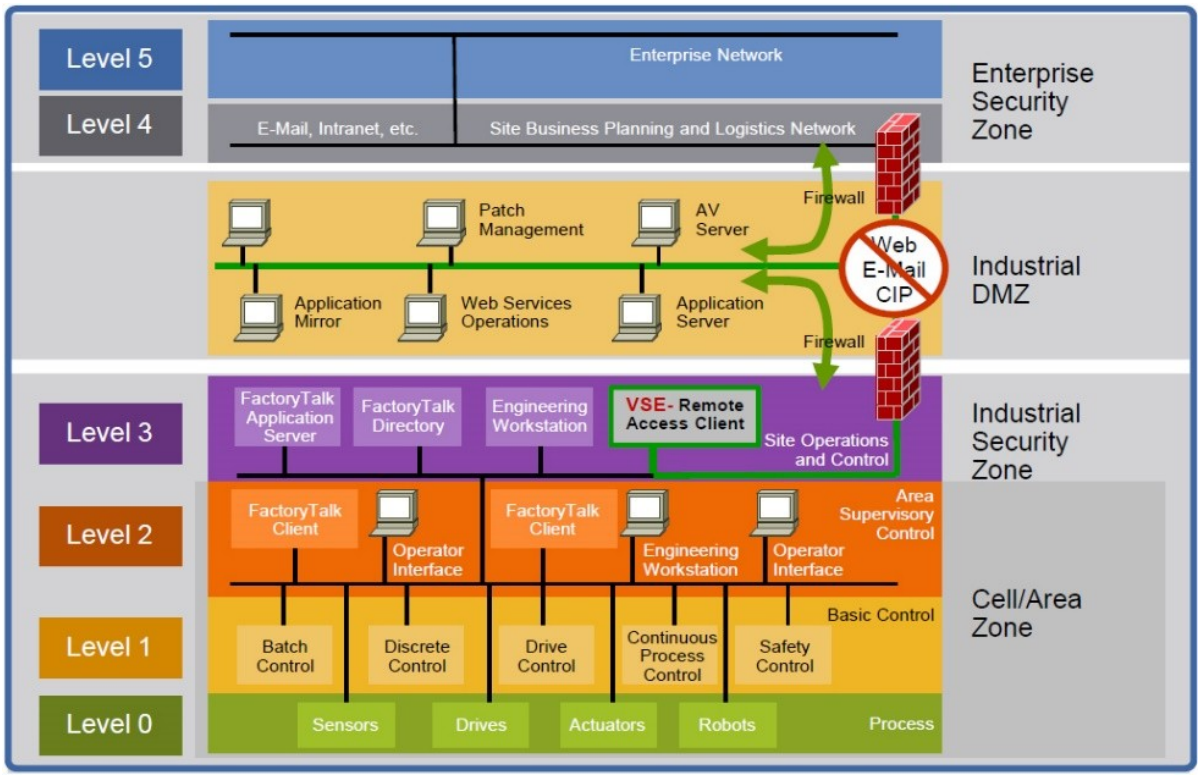
Co-funded by the Erasmus+ Programme of the European Union

Şekil 2: VPN (Sanal Özel Ağ)



Şekil 3: Uzaktan erişim için VPN

Güvenli bir endüstriyel altyapı oluşturmak



Şekil 4: ISA 95 Mantık Modeli - Endüstriyel Otomasyon ve Kontrol Sistemi (IACS)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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

- Derinlemesine Savunma (DiD) bu yaklaşımı destekler. Tek bir koruma noktasının yenilebileceği ve muhtemelen yenileceği fikrine dayanarak, DiD güvenliği fiziksel, elektronik ve prosedürel önlemlerin bir kombinasyonu yoluyla birden fazla koruma katmanı oluşturur.
- Bir banka, video kameralar, bir koruma ve kasa gibi birden fazla güvenlik önlemi kullanır ve bu, tehditlerin birden fazla savunma hattını karşılamasını sağlamaya yardımcı olur.
- Derinlemesine güvenlik yaklaşımı altı ana bileşenden oluşur:

1. Politika ve Prosedürler
2. Fiziksel
3. Ağ
4. Bilgisayar
5. Uygulama
6. Cihaz

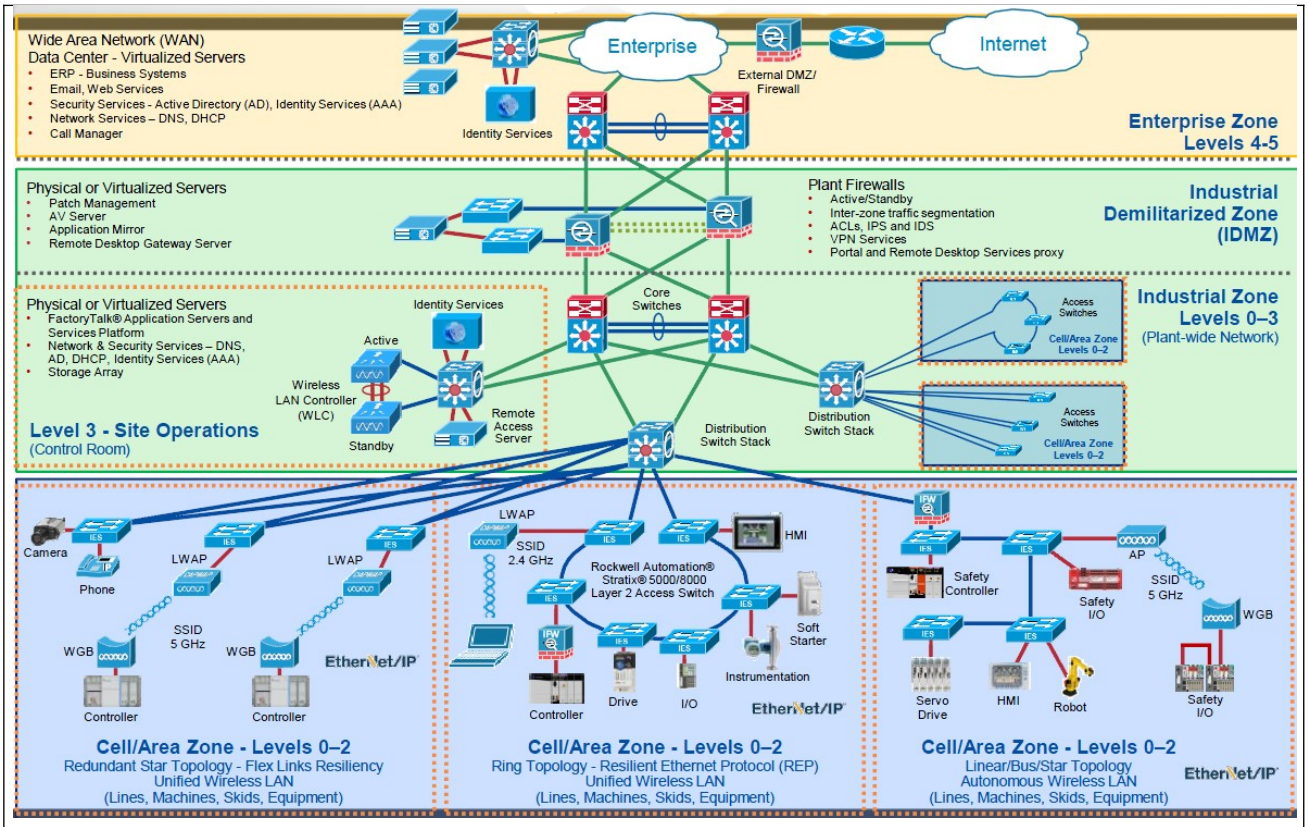
Güvenli bir endüstriyel altyapı oluşturmak

- Fiziksel güvenlik, personel erişimini yalnızca bir tesisin alanlarına değil, aynı zamanda kontrol panelleri, kablolar ve cihazlar gibi fiziksel ağ altyapısına giriş noktalarına da sınırlamalıdır.
- Tesis alanlarını sanal yerel alan ağlarına (VLAN'lar) bölmek, ağ genelinde en iyi güvenlik yöntemidir.
- Gerçek zamanlı iletişimlerde daha küçük VLAN'ların yönetilmesi ve bakımı daha kolaydır.
- Cihazları güvenliği ihlal edilmiş olanlardan izole etmeye yardımcı olabilirler, bu da olumsuz etkiyi tek bir VLAN içinde tutar.
- Tartışılan teknolojilerden biri, işletme ve endüstriyel alanlar arasında kritik bir koruyucu bariyer oluşturan endüstriyel silahsızlandırılmış bölge (IDMZ) olmalıdır.
- IDMZ, trafiğin doğrudan iki bölge arasında seyahat etmesini kısıtlar ve bilinen tehditler için kimlik doğrulamasını zorlayarak veya trafiği izleyerek erişimin daha iyi yönetilmesine yardımcı olabilir.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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



Şekil 5: IDMZ

Soru:

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

1.Sosyal Ağlardaki Riskler Nelerdir?

2.Sosyal Ağlarda Güvenlik ve Gizlilik Önlemlerine Yönelik Önlemler

3.Sosyal Ağlarda Temel Güvenlik Teknikleri Hangileridir?

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

- Sosyal Ağlardaki Riskler
- Sosyal Ağlarda Güvenlik ve Gizlilik
- Güvenlik teknikleri

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/4.0/

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

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

Ekte gör

Başvuru:

Tedarik Gereksinimleri
URL: Tedarik gereksinimleri
URL: https://www.ekransystem.com/en/blog/third-party-providers
Satınalma İhtiyacı Tespiti
URL: https://www.procurementclassroom.com/procurement-requirement-determination/
Sosyal Ağlarda Güvenlik ve Gizlilik
URL: https://www.igi-global.com/chapter/security-privacy-social-networks/14073
Sosyal Ağlarda Güvenlik ve Gizlilik
URL: https://sefcom.asu.edu/publications/security-privacy-social-ic2011.pdf
Çevrimiçi sosyal medyada Gizlilik ve Güvenlik
URL: https://www.geeksforgeeks.org/privacy-and-security-in-online-social-media/
Veri Güvenliği Teknikleri ve Gizlilik
URL: https://www.educba.com/data-security-techniques/
Güvenlik Teknikleri Nedir
URL: Güvenlik kavramları-gelişmeler-ve-gelecek-eğilimleri-
En Etkili Güvenlik Teknikleri
URL: https://dzone.com/articles/most-effective-security-techniques-part-1
URL: https://panorays.com/blog/what-is-a-third-party-vendor/

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.