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

InCyT Eğitim Modülleri

Çalışanlar için Bilgi Güvenliği **Ünite 1 Hafta 2** **Ünite adı: Bilgi Güvenliğine Giriş, iç kontrol sistemleri**	
Öğrenme aktiviteleri	❑ **Web Semineri** ❑ **Egzersizler** ❑ **Atölye** ❑ **Sunum** ❑**Diğer**
Öğrenme Sorumlusu	• Gabriel Vladut • Sevgililer Istratie
Öğrenme Etkinliği Hedefleri	1. Erasmus+ InCyT projesi hakkında tanıtım 2. Siber güvenlik 3. Kavramlar, tanımlar ve terimler 4. İç Kontrol Standardı 5. Siber güvenlik kontrollerinin detaylandırılması
Kazanılacak Beceriler	• TS3 Ağ Güvenliği • TS4 Sızma (istismar edilebilir güvenlik açıkları) testi • SS3 Bilişsel ve davranış analizi
Öğrenme faaliyetinin süresi	2 hafta
Öğrenme Gereksinimler	***İhtiyaç duyulan şey?***
	• Siber güvenlik farkındalığı kazanın ve Siber güvenlik saldırılarının ne olduğunu öğrenin • Saldırganların hassas verilere erişmek ve kurumsal güvenlik açıklarından yararlanmak için kullandıkları veri ihlallerini önleme yöntemlerini öğrenin • Siber güvenlik saldırısı durumunda nasıl ilerleyeceğinizi öğrenin

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.

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

Modül hakkında kısa bilgi

Tanım
Bilgi Güvenliği, iç kontrol sistemleri önemlidir ve çoğu zaman siber güvenlik için tehdit oluşturur Bilgilerin ve bilgi sistemlerinin, depolama, işleme veya aktarma sırasında yetkisiz erişime veya bilgilere değiştirilmesine ve yetkili kullanıcıların hizmet reddine karşı korunması. Bilgi güvenliği, bu tür tehditleri tespit etmek, belgelemek ve bunlara karşı koymak için gerekli önlemleri içerir. Bilgi güvenliği, bilgisayar güvenliği ve iletişim güvenliğinden oluşur. Bu kavram INFOSEC olarak da adlandırılır. Ayrıca bkz. iletişim güvenliği; bilgisayar Güvenliği; bilgi Güvenliği; bilgi sistemi. İç kontroller yönetim, BT güvenliği, finans, muhasebe ve operasyon ekipleri tarafından aşağıdaki hedeflere ulaşmak için kullanılır: 1. Mali bilgilerin güvenilirliğini ve doğruluğunu sağlayın – İç kontroller doğru, güncel ve eksiksiz bilgilerin muhasebe sistemlerine ve mali raporlara yansıtılmasını sağlar. Öğrenciler, ilgili metni okuyarak, akışlı web seminerlerini izleyerek ve alıştırmaları kendi hızlarında çözerek bu tür yönler hakkında bilgilendirilebilir. Tüm bu belgeler dijital interaktif proje platformunda yer almaktadır. Öğrenciler cevaplarını öz-değerlendirme alıştırmalarında test edebilirler. Diğer alıştırmalardaki cevaplar ilgili tartışma forumunda saklanmalı ve haftada bir düzenlenen ortak toplantıda mentor ile tartışılmalıdır. Öğrenen, özellikle toplantılar sırasında diğerleriyle ve mentorla işbirliği içinde çalışabilir. Eğitimin yansıtılması ve değerlendirilmesi için önemli olan e-portföy geliştirmeleri için desteklenecektir.

Öğrenme Materyali İçeriği

Siber saldırılar ve yetkinlik çerçevesi

Şirketler tarafından beceriye dayalı gereksinimleri, gerekli yetkinlikleri, çalışan becerilerini ve boşlukları anlamak için düzenli olarak bir yetkinlik çerçevesi kullanılır.

Şirketin profili ve çalışanların ilgi alanları dikkate alınarak bir yetkinlik çerçevesi geliştirildiğinde, performansı artırabilir ve her bir rol gereksinimi için netlik sağlayabilir ve işyerinde yetenek geliştirebilir. Son yıllarda, birçok siber saldırı nedeniyle , siber güvenlik çerçeveleri çoğunlukla büyük kuruluşlar (işletmeler, STK'lar ve diğer kuruluşlar) veya devlet aktörleri tarafından benimsenmiştir.

Başarılı bir siber saldırı , bir şirketin işine büyük zarar verebilir. Şirketin iş durumu ve tüketici

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.

güveninin yanı sıra kâr hanesini de etkileyebilir. Bir güvenlik ihlalinin etkisi üç kategoriye ayrılabilir: finansal, itibari ve yasal etki.

Siber saldırılar

Siber saldırılar genellikle kurumsal bilgilerin, finansal bilgilerin (ör. banka bilgileri veya ödeme kartı bilgileri), paranın, işlem kesintilerinin (ör. çevrimiçi işlem yapamama), iş veya sözleşme kaybından kaynaklanan önemli mali kayıplara neden olur. Bir siber ihlale maruz kalan işletmeler genellikle etkilenen sistemleri, ağları ve cihazları onarmak için para harcarlar.

Siber saldırılar bir şirketin itibarına ve müşterilerin şirkete duyduğu güvene zarar verebilir. Bu, müşteri kaybına, satış kaybına ve karda azalmaya yol açabilir. İtibar zedelenmesinin etkisi, şirketin tedarikçilerini veya ortakları, yatırımcıları ve şirketin işine dahil olan diğer üçüncü taraflarla olan ilişkileri bile etkileyebilir.

Bu nedenle, veri koruma ve gizlilik yasaları, şirket tarafından (kendi personeline veya müşterilerine ait) tutulan tüm kişisel verilerin güvenlik yönetimini gerektirir. Bu verilerin yanlışlıkla veya kasıtlı olarak tehlikeye atılması ve şirketin yeterli güvenlik önlemlerini uygulamaması halinde yasal cezalarla karşı karşıya kalabilir.

Şirketteki riskler

Risklerinizi buna göre yönetmek önemlidir. Bir saldırı meydana geldikten sonra, etkili bir siber güvenlik aracı veya olay müdahale planı, yani bir siber danışman kullanmak aşağıdakilere yardımcı olabilir:

- Saldırının etkisini azaltmak
- Olayı ilgili makama bildirin
- Etkilenen sistemleri temizle
- Mümkün olan en kısa sürede çalışır duruma getirin.

Bir organizasyonda bir siber strateji için sürekli farkındalık geliştirmek için kullanıcıları siber güvenlik alanında eğitmek ve eğitmek için yatırım yapmak gerekir .

Siber Güvenlik Çerçevesi

Bir siber güvenlik çerçevesi, bir kuruluş içinde BT güvenlik politikaları geliştirmek için kullanılan bir dizi en iyi uygulama ve belgelenmiş süreçtir. Ancak, kesinlikle yasal alanla ilgili geleneksel politikadan farklı olarak, bir siber güvenlik çerçevesi, bu politikalar tarafından kaçınılması gereken sorunların ve çerçevede açıklanan güvenlik politikalarını uygulamaya yönelik uygun süreçlerin ve yolların belgelenmiş örneklerini de içermelidir.

Hem çalışanlar ve kullanıcılar için bir rehber hem de yetkili harici taraflar (yetkililer gibi) tarafından

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.

danışılabilecek en iyi güvenlik uygulamalarının ilgi çekici bir özetidir. Siber güvenlik yeterlilik çerçevesi, saldırıları, açıkları ve iyileştirme önlemlerini önlemek için gereken yetkinliklerin daha iyi değerlendirilmesine de yardımcı olabilir .

Siber güvenlik

Artan farkındalığa ve cesur çabalara rağmen, Avrupa Birliği'nde siber güvenlik uzmanlarının son derece önemli ve büyüyen eksikliği ve dünya çapında siber saldırılardan kaçınmak için çalışanların bilgi ve becerileri biliniyor ve bu eksiklikler kamu ve özel sektör için büyük sorunlar oluşturmaya devam ediyor.

2019 SİBER GÜVENLİK İŞGÜCÜ 2019 Güçlü Siber Güvenlik Ekipleri Oluşturma ve Büyütme Stratejileri (ISC) araştırması, dünya genelinde 2,8 milyon siber güvenlik uzmanı olduğunu tahmin ederken, ihtiyacı karşılaması için gereken sayının aslında 4,07 milyon olduğunu tahmin ediyor.

Çalışma, Avrupa'daki mevcut açığın 291.000 olduğunu ve bu sayının önceki yıllara göre iki katına çıktığını belirtiyor. Uzmanlığı oldukça gelişmiş olan birçok ülke kendi yönetmelik ve belge setini oluşturmayı tercih eder, ancak birçok ülke ve küçük ve orta ölçekli şirket (KOBİ) bu bağlamda yardıma ihtiyaç duyar.

Sosyal mühendislik

- Saldırganın ilgisini çekecek verilere, belgelere ve bilgilere erişim elde etmek için (genellikle psikolojik yöntemler kullanarak) insanları manipüle etmek anlamına gelir.
- Günümüzde bilgi güvenliğine yönelik ana tehditlerden biridir ve etkili bir siber suç biçimidir.
- Veri ihlalleri gibi diğer tüm saldırı türlerinden daha tehlikeli sonuçlara yol açabilir.
- Saldırıların finansal bir amacı vardır ve bu nedenle kuruluşlar önemli miktarda para kaybetmiştir.
- Yazılım ve işletim sistemlerindeki güvenlik açıklarından çok insan hatasına dayandığından özellikle tehlikelidir.

Şirketler:

- Üretkenlik kaybı, çalışanların moralinde düşüş ve toparlanma güçlüğü yaşayabilirler.
- Müşteriler kuruluşun kendisini koruyabileceğine ikna olmadıkları için itibar zedelenmesi yaşarlar.
- Genellikle eski bir olay yanıtını tetikleme ihtiyacı duyar.
- Gelecekteki saldırıları önlemeye yardımcı olacak güvenlik yazılımı sağlamalıdır.
- Genellikle saldırılara hazır olmaları için çalışanları yeniden eğitmek zorunda kalırlardı.

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.

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

Sosyal mühendislik; Eğitim (siber farkındalık)

- Kurban olma riski yüksek olduğu için sosyal mühendislik saldırılarını tanımanın önemli olduğu çalışanlar ve yöneticiler.
- Topluluk, birey ve yurttaş güvenlik bilinçlendirme programlarına dahil edilebilir ve bireyleri ve kuruluşlarını koruyabilir.
- Daha az kaynağa sahip olan KOBİ'lerde özellikle eksiktir, bu nedenle siber farkındalık eğitimini ciddiye almaları ve çalışanlara bu eğitimi almaları için fırsatlar sağlamaları için onlara yardım edilmelidir.

Eğitim ve mentorluk

Geleceğin girişimcileri de dahil olmak üzere girişimciler, disiplinler arası öğrenmeyi gerektiren farklı sektörlerden bilgileri anlama ve bütünleştirme becerisine ve karmaşık düşünme biçimlerine ihtiyaç duyarlar. Karmaşık mühendislik problemleri neredeyse doğal bir şekilde disiplinler arası bir durum yaratmayı gerektirir.

Disiplinler arası bir yaklaşımda, öğrenciler farklı disiplinlerden ve alanlardan gelen bilgileri entegre etmelidir. Disiplinler arası bir anlayış geliştirirler, uzmanlık alanlarını ve disipline özgü düşünme biçimlerini entegre etmeyi öğrenirler.

Bu, bilişsel becerileri ve eleştirel düşünmeyi tek bir disiplin aracından daha fazla artırır.

Girişimcilik becerileri ve mentorluk

Öğrencilerin girişimcilik becerilerini geliştirmedeki performansını değerlendirmek, öğrenme ortamına ve öğrenme çıktılarına bir bakış da dahil olmak üzere bütüncül bir bakış açısı alabilir ve etkileşimli, etkili ve aktif öğrenmeyi kolaylaştırabilir.

Mentorluk, daha fazla bireysel öğrenmeyi desteklemek ve yeni meslekler için kişisel ve kariyer becerileri kazandırmak için deneyimli bir yöntemdir. Mentorluğun sonuçları hakkında genel olarak araştırma var, ancak mentorluk hakkında çok az araştırma var.

Mentorluk, şirketlerde eğitim gören çalışanlar için bir dizi avantaj sunar. Disiplinlerarası takım mentorluğu son yıllarda önem kazanmıştır ve çeşitli girişimcilik gelişmeleri ve alanları giderek daha çok disiplinli hale geldikçe mentorluğun oryantasyonunda bir değişiklik ihtiyacını yansıtmaktadır.

Disiplinlerarası mentorluk ve mentor ağları, gruplarda sinerji yaratabilir, yenilikçi fikirler ve zorluklara karşı karmaşık çözümler üretebilir ve işbirliği ve çalışma için fırsatlar yaratabilir.

Kavramlar, tanımlar ve terimler

" **Siberuzay** " terimi 1982 yılında William Gibson tarafından icat edildi. Terim, 1990'larda World

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.

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

Wide Web'in ortaya çıkışıyla günlük hayata girdi.

siber altyapılar - BT sistemleri, ilgili uygulamalar, ağlar ve elektronik iletişim hizmetlerinden oluşan bilgi ve iletişim teknolojisi altyapıları;

siber alan - işlenen, depolanan veya iletilen bilgi içeriği ve ayrıca kullanıcılar tarafından gerçekleştirilen eylemler dahil olmak üzere siber altyapılar tarafından oluşturulan sanal ortam;

siber güvenlik - elektronik formattaki bilgilerin, kamu veya özel kaynakların ve hizmetlerin siber uzayda gizliliğini, bütünlüğünü, kullanılabilirliğini, orijinalliğini ve reddedilmemesini sağlayan bir dizi proaktif ve reaktif önlemin uygulanmasından kaynaklanan normallik durumu .

Proaktif ve reaktif önlemler, güvenlik politikalarını, kavramlarını, standartlarını ve yönergelerini, risk yönetimini, eğitim ve bilinçlendirme faaliyetlerini, siber altyapıları korumak için teknik çözümlerin uygulanmasını, kimlik yönetimini, sonuç yönetimini içerebilir;

siber savunma - ulusal savunmaya özgü siber altyapıya yönelik tehditlere karşı koruma, izleme, analiz, tespit, saldırılara karşı koyma ve zamanında müdahale sağlama amacıyla siber alanda gerçekleştirilen eylemler;

bilgisayar ağlarındaki operasyonlar - düşmanın yeteneklerinin etkisiz hale getirilmesiyle eşzamanlı olarak bilgi üstünlüğü elde etmek için bilgisayar ağlarının korunması, kontrolü ve kullanımı için siber uzayda eylemleri planlama, koordine etme, senkronize etme, uyumlaştırma ve gerçekleştirme karmaşık süreci;

siber tehdit - siber güvenlik için potansiyel bir tehlike oluşturan durum veya olay;

siber saldırı - siber güvenliği etkilemesi muhtemel siber uzayda gerçekleştirilen düşmanca eylem;

siber olay - sonuçları siber güvenliği etkileyen siber uzayda meydana gelen olay;

siber terörizm - siber uzayda siyasi, ideolojik veya dini olarak motive edilen bireyler, gruplar veya kuruluşlar tarafından gerçekleştirilen, maddi yıkıma veya kurbanlara neden olabilecek, paniğe veya teröre neden olabilecek önceden tasarlanmış faaliyetler;

siber casusluk - bir devletin veya devlet dışı kuruluşun çıkarına yetkisiz gizli bilgileri elde etmek amacıyla siber alanda gerçekleştirilen eylemler;

bilgisayar suçları - siber altyapılar aracılığıyla veya bunlar üzerinde suçluluk duygusuyla işlenen ve sosyal tehlike oluşturan ceza kanunu veya diğer özel kanunlar tarafından öngörülen tüm fiiller;

siber uzayda güvenlik açığı - bir tehdit tarafından istismar edilebilecek siber altyapıların veya ilgili güvenlik önlemlerinin tasarımı ve uygulanmasındaki zayıflık;

siber uzayda güvenlik riski - siber altyapılara özgü belirli bir güvenlik açığından yararlanarak bir

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.

tehdidin gerçekleşme olasılığı;

risk yönetimi - her türlü kaybı önlemek için karmaşık tekniklerin ve araçların kullanımına dayalı olarak siber güvenlik risklerini belirleme, değerlendirme ve bunlara karşı koymaya yönelik karmaşık, sürekli ve esnek bir süreç;

kimlik yönetimi - belirli siber altyapılara eriştiklerinde kişilerin kimliğini doğrulama yöntemleri;

İç kontrolün bileşenleri

INTOSAI GOV 9100 Standardı "İç Kontrol Standartları Rehberi"ne göre. 2001 yılında, Uluslararası Yüksek Denetim Kurumları Örgütü (INCOSAI) Kongresinde, ilk olarak 1992'de yayınlanan INTOSAI Kamu Sektöründe İç Kontrol Standartları Rehberinin, son gelişmelerin tüm yönlerini belgeye dahil ederek güncellenmesine karar verildi. iç kontrol alanında ve COSO modelinin (İç Kontrol – Entegre Çerçeve) bir dizi unsurunu entegre etmek.

INTOSAI İç Kontrol Standartları Komitesi'nin operasyon grubu tarafından yürütülen bir faaliyet olan Kılavuz İlkelere entegre edilerek, Yüksek Denetim Kurumlarının temsilcileri tarafından yeni iç kontrol sisteminin nasıl çalıştığına dair birleşik bir anlayış elde edilmeye çalışılmıştır.

"Kamu Sektöründe İç Kontrol Standartları için INTOSAI Rehberi", INTOSAI GOV kategorisinin (iyi yönetişim rehberi) bir parçasıdır ve hem iç kontrol sistemini uygulamak zorunda olan kamu sektörü yöneticileri hem de dış kamu denetçileri için son derece yararlı kabul edilmektedir.

İç kontrol standartları

INTOSAI GOV 9100 Yönergelerine göre), iç kontrol birbirine bağlı beş bileşenden oluşur (COSO modelindekilerle aynı):

- Kontrol ortamı
- Risk değerlendirmesi
- Kontrol aktiviteleri
- Bilgi ve iletişim
- izleme

İç kontrol, kurumun genel hedeflerine ulaşılmasına ilişkin makul güvence sağlamak üzere tasarlanmıştır. Kurum başkanları tarafından açıkça belirlenmiş hedefler ve bütçenin uygun şekilde planlanması, etkili bir iç kontrol için zorunlu bir koşuldur.

Kontrol ortamı

Kontrol ortamı, yönetimin ve üst yönetimden sorumlu olanların, iç kontrol sistemi ve onun kurum içindeki önemine ilişkin genel tutumunu, farkındalığını ve aldığı önlemleri kapsar. Kontrol ortamı,

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.

personel düzeyinde kontrol bilincini etkileyerek organizasyonun tonunu belirler.

İç kontrol sisteminin etkin bir şekilde uygulanabilmesi için kurum içinde saygı duyulması gereken bir disiplin ve kurumun bir yapısını sağlayarak, iç kontrolün diğer tüm bileşenlerinin temelini oluşturur. İç kontrol ortamı, yolsuzluğun ve yolsuzluğun önlenmesinde etkili bir araçtır.

Kontrol ortamını tanımlayan unsurlar şunlardır:

- kişisel ve mesleki bütünlük, iç kontrole yönelik sürekli destekleyici bir tutum dahil olmak üzere yönetimin tüm personel için oluşturduğu etik değerler;
- personel yeterliliği için sürekli bir yönetim kaygısı;
- "yukarıdan verilen ton" (yönetimin felsefesi ve faaliyet tarzı);
- kuruluşun organizasyon yapısı;
- İK politikası ve uygulamaları.

Siber Güvenlik Kontrol Türleri

Siber güvenlik kontrolleri, siber tehditleri ve saldırıları önlemek, tespit etmek ve azaltmak için kullanılan mekanizmalardır. Mekanizmalar, güvenlik görevlileri ve güvenlik kameraları gibi fiziksel kontrollerden güvenlik duvarları ve çok faktörlü kimlik doğrulama gibi teknik kontrollere kadar uzanır.

Siber güvenliğe tek taraflı bir yaklaşım sadece modası geçmiş ve etkisizdir. Günümüz tehdit ortamında tüm saldırıları önlemek mümkün olmadığından, kuruluşlar varlıklarını iş için önem derecesine göre değerlendirmeli ve kontrolleri buna göre oluşturmalıdır.

Zorluklara ek olarak, tüm şirket varlıkları genelinde katı kontroller uygulanırsa çalışanların uyumluluk kurallarına uyma olasılığı düşüktür. Bir kontrolün ciddiyeti, varlık ve tehdit ortamını doğrudan yansıtmalıdır.

Örneğin, bir bilgisayar korsanının binlerce kişisel müşteri verisini bir bulut veritabanı aracılığıyla ifşa etmesinin sonuçları, bir çalışanın dizüstü bilgisayarının güvenliğinin ihlal edilmesinden çok daha büyük olabilir.

Siber güvenlik kontrolleri

Infosec Strategies and Best Practices ve siber güvenlik küresel kara kuşağı kitabının yazarı Joseph MacMillan, "Korumaya çalıştığınız şeyin doğasına bağlı olarak denetimleri uygulamanın birçok farklı yolu vardır" dedi .

"Korumaya çalıştığınız tehdidin doğası nedir?

Kötü niyetli bir aktör mü?

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.

Yoksa yıkıcı bir saldırı mı?”

Bilgi varlıklarının güvenliğini sağlama

Varlıklar için uygun bilgi güvenliği kontrollerinin uygulanmasını ifade eder. Uygun kontrolleri seçmeyi anlamak için güçlü ve etkili ideolojilere odaklandığımızdan emin olmak istiyoruz; bu, varlığın kritikliği ve sınıflandırmasına göre "yeterince güvenli" kabul edildiği anlamına gelir. Denetim türlerini ayıran farklı sınıflar vardır:

- İdari/yönetimsel kontroller, firmanın politikaları ve prosedürleridir. Yeni bir yazılım kontrolü kadar "havalı" değiller, ancak bireylere ve kuruluşun diğer üyelerine yapı ve rehberlik sağlamak için varlar ve kimsenin para cezasına çarptırılmamasını veya bir ihlale neden olmamasını sağlıyorlar.
- Sistemlere erişimi fiziksel bir şekilde sınırlayan fiziksel kontroller.
- Teknik / mantıksal kontroller, şifreleme, parmak izi okuyucular, kimlik doğrulama veya güvenilir platform modülleri (TPM) gibi donanım veya yazılıma dayalı olarak erişimi sınırlayan kontrollerdir.

Fiziksel kontrollerin yaptığı gibi fiziksel sistemlere erişimi sınırlamazlar, bunun yerine verilere veya içeriğe erişimi sınırlarlar. Operasyonel kontroller, süreçleri günlük olarak yürüten insanları içeren kontrollerdir. Örnekler farkındalık eğitimi, varlık sınıflandırması ve günlük dosyası incelemesini içerebilir.

Kontrol türleri

Önleyici kontroller, bir eylemi önlemek için mevcuttur ve güvenlik duvarlarını, çitleri ve erişim izinlerini içerir.

Dedektif komutları, yalnızca video gözetimi veya izinsiz giriş tespit sistemleri gibi bir olay sırasında veya sonrasında tetiklenir. Caydırıcılar, tehditleri "Watchdog" veya köpek işareti gibi bir güvenlik açığından yararlanmaya çalışmaktan caydırır . Düzeltici kontroller, bir durumdan diğerine eylem alma yeteneğine sahiptir. Başarısız açma ve başarısız kapalı komutları burada ele alınmaktadır.

Kurtarma komutları, bir sabit sürücüyü kurtarmak gibi bir kayıptan bir şeyler geri alır. Telafi edici kontroller, erişim günlüklerinin düzenli olarak gözden geçirilmesi gibi diğer kontrollerdeki eksiklikleri telafi etmeye çalışan kontrollerdir. Bu örnek aynı zamanda bir dedektif kontrolüdür, ancak telafi kontrolleri farklı türlerde olabilir.

Kontrol sırası

Oyuncuları, olmaması gereken bir şeye erişmeye çalışmaktan caydırır. Erişim izinleri veya kimlik doğrulama gibi önleyici bir kontrol aracılığıyla Erişimi Reddet/Engelle.

Uç nokta koruma yazılımı gibi, algılamayı kaydettiğinizden emin olarak riski algılayın. Parola girmek

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.

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

için "çok fazla deneme" özelliğinde olduğu gibi, işlemin riski tekrar etmesini geciktirin.

Bir olay müdahale planı gibi uzlaşmaya yanıt vererek durumu düzeltin. Bir sunucunun kullanılabilirliğini geri yükleyen bir yedekleme oluşturucu gibi güvenliği ihlal edilmiş bir durumdan kurtarın.

Ayrıca, sürekli iyileştirme alanında, herhangi bir değişiklik için her bir varlığın değerini izlemeliyiz. Bunun nedeni, zamanla veya kuruluşunuzdaki belirli önemli olaylar sırasında daha fazla veya daha az değerli hale gelirlerse, bu varlıkları korumak için kontrollerimizi yeniden düşünmemiz gerekebileceğidir.

Kontroller ve kurtarma

Kontrollere baktığımızda, iyileşmeyi de düşünmeliyiz, olumsuz durumlardan veya varlıklardaki ve değerlerindeki değişikliklerden kurtulabilmek istiyoruz. Örnek olarak yedekleme, yedeklilik, geri yükleme süreçleri ve benzerlerinden bahsediyoruz.

Özellikle bulut, SaaS , PaaS , IaaS , üçüncü taraf çözümler ve diğer tüm "başkasının bilgisayarı" biçimleri çağında hatırlanması gereken bir kavram, Hizmet Düzeyi Sözleşmelerinin (SLA'lar) net bir şekilde tanımlanmasını ve izin verilen maksimum kapalı kalma süresine sahip olmasını sağlamaktır. sözleşmeler ve bu sözleşmelere uyulmaması durumunda cezalar. Bu bir telafi edici kontrol örneğidir.

Sorular :

Sorular Tartışma Forumu kısa bir açıklama ile cevaplanacak. Cevaplar, mentorluk oturumları sırasında mentor ile tartışılacaktır.

1. Siber saldırılar için şirketteki riskler nelerdir?
2. Siber güvenlik kontrollerinin bazı türlerini söyleyin?
3. İç kontrol standartları hangileridir?
4. Bilgiler nasıl kontrol edilir ve kurtarılır?

Öz değerlendirme soruları. Öğrenci yanıtladıktan sonra sonuçları görebilir ve bunları platformda kayıtlı sonuçlarla karşılaştırabilir.

- Siber saldırılar için şirketteki riskler
- İç kontrol standartları ve kuralları
- Kontrol ortamı

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.

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

Ekler

Powerpoint sunum

Video filmler

Referanslar:

- Şirketlere Yönelik Siber Saldırılar: Risk Altında Mısınız?
- Siber saldırıların artan stratejik riskleri
- İşletmeler İçin Yaygın 10 Siber Güvenlik Riski
- Dahili Kontroller ve Veri Güvenliği: BT Güvenliği İhtiyaçlarınızı Karşılayan Kontroller Nasıl Geliştirilir?
- Bilgi Sistemleri Üzerindeki İç Kontroller

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.