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

InCyT Eğitim Modülleri

Çalışanlar için Bilgi Güvenliği **Ünite 1 Hafta 2** **Ünite adı: Bilgi Güvenliği, iç kontrol sistemlerine giriş**	
Öğrenme Aktiviteleri	❑ **Web Semineri** ❑ **Alıştırmaları** ❑ **Atölye Sunumu** ❑ **Diğer**
Öğrenme Sorumlusu	• Gabriel Vladut • Valentin Istratie
Öğrenme Etkinliği Hedefleri	1. Erasmus+ InCyT projesi hakkında giriş 2. Siber güvenlik 3. Kavramlar, tanımlar ve terimler 4. İç Kontrol Standardı 5. Siber güvenlik kontrollerinin detaylandırılması
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?*** • Siber güvenlik farkındalığı kazanın ve Siber güvenlik saldırısının ne olduğunu öğrenin. • Saldırganlar tarafından hassas verilere erişmek ve kurumsal güvenlik açıklarından yararlanmak için kullanılan veri ihlallerini önleme yöntemlerini öğrenin • Siber güvenlik saldırısı durumunda nasıl devam edeceğinizi 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

Giriş
Bilgi Güvenliği, iç kontrol sistemleri önemlidir ve çoğu zaman siber – güvenlik için tehdit oluşturur. Bilgi ve bilgi sistemlerinin, depolamada, işlemede veya nakliyede yetkisiz erişime veya bilgilerin değiştirilmesine ve yetkili kullanıcılara hizmet reddine karşı korunması gerekmektedir. 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 ifade aynı zamanda INFOSEC olarak da adlandırılır. Ayrıca bkz: iletişim güvenliği; bilgisayar güvenliği; bilgi güvenliği; bilgi sistemi. İç kontroller, yönetim, BT güvenliği, finansal, muhasebe ve operasyonel ekipler tarafından aşağıdaki hedeflere ulaşmak için kullanılır: 1. Finansal bilgilerin güvenilirliğini ve doğruluğunu sağlamak - İç kontroller, doğru, güncel ve eksiksiz bilgilerin muhasebe sistemlerine ve finansal raporlara yansıtılmasını sağlar. 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.

Öğrenme Materyalinin İçeriği

Siber saldırılar ve yetkinlik çerçevesi

Bir yetkinlik çerçevesi, şirketler tarafından beceri tabanlı gereksinimlerini, gerekli yetkinlikleri, çalışan becerilerini ve boşluklarını anlamak için düzenli olarak kullanılır.

Şirketin profili ve çalışan çıkarları 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 esas olarak büyük kuruluşlar (işletmeler, STK'lar ve diğer kuruluşlar) veya devlet aktörleri tarafından benimsenmektedir.

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

Başarılı bir siber saldırı, bir şirketin işine büyük zarar verebilir. Alt satırını, şirketin iş durumunu ve tüketici güvenini etkileyebilir. Bir güvenlik ihlalinin etkisi üç kategoriye ayrılabilir: finansal, itibar ve yasal.

Siber saldırılar

Siber saldırılar genellikle kurumsal bilgilerin, finansal bilgilerin (örneğin banka bilgileri veya ödeme kartı ayrıntıları), paranın, işlem kesintilerinin (örneğin çevrimiçi işlem yapamama), iş veya sözleşmenin kaybından kaynaklanan önemli finansal kayıplara neden olur. Siber ihlale maruz kalan işletmeler genellikle etkilenen sistemleri, ağları ve cihazları onarmakla ilgili para harcayacaktır.

Siber saldırılar bir şirketin itibarına ve müşterilerin şirkete olan güvenine zarar verebilir. Bu, müşteri kaybına, satış kaybına ve karların azalmasına neden olabilir. İtibar hasarının etkisi, şirketin tedarikçilerini bile etkileyebilir veya ortaklar, yatırımcılar ve şirketin işinde yer alan diğer üçüncü taraflarla ilişkileri etkileyebilir.

Bu nedenle, veri koruma ve gizlilik yasaları, şirket tarafından (kendi personelinin veya müşterilerinin) tutulan tüm kişisel verilerin güvenlik yönetimini gerektirir. Bu veriler yanlışlıkla veya kasıtlı olarak tehlikeye atılırsa ve şirket yeterli güvenlik önlemlerini uygulamazsa, düzenleyici cezalarla karşı karşıya kalabilir.

Şirketteki riskler

Risklerinizi buna göre yönetmeniz önemlidir. Bir saldırı gerçekleştikten 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 temizleme
- Şirketinizin işini mümkün olan en kısa sürede kurun ve çalıştırın.

Saldırılardan kaçınmak ve bir kişinin kuruluşunda bir siber strateji için sürekli farkındalık geliştirmek için kullanıcıları siber güvenlik alanında eğitmeye ve eğitmeye yatırım yapmak gerekir.

Siber Güvenlik Çerçevesi

Siber güvenlik çerçevesi, bir kuruluş içinde BT güvenlik politikaları geliştirmek için kullanılan bir dizi en iyi uygulama ve belgelenmiş süreçtir. Ancak, yasal alanla sıkı sıkıya ilgili geleneksel politikaların aksine, bir siber güvenlik çerçevesi, bu politikalar tarafından kaçınılması gereken sorunların belgelenmiş örneklerini ve çerçevede açıklanan güvenlik politikalarını uygulamak için uygun süreçleri ve yolları da içermelidir.

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

Hem çalışanlar hem de kullanıcılar için bir rehber hem de yetkili dış taraflarca (yetkililer gibi) danışılabilecek en iyi güvenlik uygulamalarının zorlayıcı bir özetidir. Bir siber güvenlik uzmanlık çerçevesi, saldırılardan, boşluklardan ve düzeltme önlemlerinden kaçınmak için gereken yetkinliklerin daha iyi değerlendirilmesine de yardımcı olabilir.

Siber güvenlik

Artan farkındalık ve cesur çabalara rağmen, Avrupa Birliği'ndeki siber güvenlik profesyonellerinin ve çalışanların dünya çapında siber saldırılardan kaçınma konusundaki bilgi ve becerilerinin son derece önemli ve büyüyen eksikliği bilinmektedir ve bu kıtlıklar kamu ve özel sektör için büyük sorunlar sunmaya devam etmektedir.

2019 SİBER GÜVENLİK İŞ GÜCÜ 2019 Güçlü Siber Güvenlik Ekipleri Oluşturma ve Büyütme Stratejileri (ISC) çalışması, küresel olarak 2,8 milyon siber güvenlik uzmanı olduğunu tahmin ederken, aradaki fark aslında 4,07 milyon.

Çalışma, Avrupa'daki mevcut boşluğun 291.000 olduğunu ve bu sayının önceki yıllara göre iki katına çıktığını belirtiyor. Son derece gelişmiş uzmanlığa sahip birçok ülke kendi yönetmelik ve belgelerini oluşturmayı tercih eder, ancak birçok ülke ve küçük ve orta ölçekli şirketler (KOBİ'ler) bu bağlamda yardıma ihtiyaç duyar.

Sosyal mühendislik

- Saldırganın ilgisini çeken verilere, belgelere ve bilgilere erişmek için insanları manipüle etmek (genellikle psikolojik yöntemler kullanarak) anlamına gelir.
- Günümüzde bilgi güvenliğine yönelik ana tehditlerden biridir ve etkili bir siber suç biçimidir.
- Veri ihlalleri gibi tehlikeli yankıları olabilir, diğer saldırı türlerinden daha fazla.
- Saldırıların finansal bir amacı var ve bu nedenle örgütler önemli miktarda para kaybetti.
- Özellikle tehlikelidir, çünkü yazılım ve işletim sistemlerindeki güvenlik açıklarından çok insan hatasına dayanır.

Şirketler:

- Üretkenlik kaybına, çalışanların moralinde bir düşüşe ve iyileşmede zorluklara maruz kalabilirler.
- İtibar hasarı var, çünkü müşteriler kuruluşun kendisini koruyabileceğine ikna olmuş değiller.
- Genellikle eski bir olay yanıtını tetiklemeniz gerekir.
- Gelecekteki saldırıları önlemeye yardımcı olmak için güvenlik yazılımı sağlamalıdır.
- Genellikle çalışanları saldırılara hazır olmaları için yeniden eğitmek zorunda kalacaklardı.

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

Social mühendislik; Eğitim (siber farkındalık)

- Sosyal mühendislik saldırılarını tanımanın önemli olduğu çalışanların ve yöneticilerin kurban olma riski yüksektir.
- toplumsal, bireysel ve vatandaş güvenliği farkındalık programlarına dahil edilebilir ve bireyleri ve kuruluşlarını koruyabilir.
- özellikle daha az kaynağa sahip KOBİ'lerde eksiktir, bu nedenle siber farkındalık eğitimini ciddiye almalarına ve çalışanların bunu almaları için fırsatlar sağlamalarına yardımcı olunmalıdır.

Eğitim ve mentorluk

Gelecektekiler de dahil olmak üzere girişimciler, karmaşık düşünme biçimlerine ve disiplinlerarası öğrenme gerektiren farklı sektörlerden gelen bilgileri anlama ve entegre etme yeteneğine ihtiyaç duyarlar. Karmaşık mühendislik problemleri, neredeyse doğal bir şekilde disiplinlerarası bir durum yaratmayı gerektirir.

Disiplinlerarası bir yaklaşımda, öğrenciler farklı disiplinlerden ve alanlardan gelen bilgileri bütünleştirmelidir. Disiplinlerarası bir anlayış geliştirirler, uzmanlık alanlarını ve disipline özgü düşünme biçimlerini bütünleştirmeyi öğrenirler.

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

Girişimcilik becerileri ve mentorluk

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

Mentorluk, daha bireysel öğrenmeyi desteklemek ve yeni meslekler için kişisel ve kariyer becerileri kazanmak için deneyimli bir yöntemdir. Genel olarak mentorluğun sonuçları hakkında araştırmalar vardır, ancak mentorluk hakkında çok az araştırma vardır.

Mentorluk, şirketlerde eğitim alan çalışanlar için bir dizi avantaj sunar. Disiplinlerarası ekip mentorluğu son yıllarda önem kazanmış, çeşitli girişimcilik gelişmeleri ve alanları giderek multidisipliner hale geldikçe mentorluk yöneliminde bir değişikliğe duyulan ihtiyacı yansıtmaktadır.

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

Kavramlar, tanımlar ve terimler

"**Siber uzay**" 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 çıkmasıyla günlük hayata girdi.

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

Siber uzay - işlenen, depolanan veya iletilen bilgi içeriğinin yanı sıra kullanıcılar tarafından gerçekleştirilen eylemler de dahil olmak üzere siber altyapılar tarafından oluşturulan sanal ortam;

Siber güvenlik - bilgilerin elektronik formatta, kamu veya özel kaynakların ve hizmetlerin, siber alanda gizliliğini, bütünlüğünü, kullanılabilirliğini, gerçekliğini ve reddedilmemesini sağlayan bir dizi proaktif ve reaktif önlemin uygulanmasından kaynaklanan normallik durumu.

Proaktif ve reaktif önlemler arasında güvenlik politikaları, kavramlar, standartlar ve kılavuzlar, risk yönetimi, eğitim ve farkındalık faaliyetleri, siber altyapıları korumak için teknik çözümlerin uygulanması, kimlik yönetimi, sonuç yönetimi;

Siber savunma - siber uzayda saldırganlıkları korumak, izlemek, analiz etmek, tespit etmek, karşı koymak ve ulusal savunmaya özgü siber altyapıya yönelik tehditlere karşı zamanında yanıt vermek amacıyla 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 eylemlerin planlanması, koordine edilmesi, senkronize edilmesi, uyumlaştırılması ve yürütülmesi karmaşık süreci;

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

Siber saldırı - siber güvenliği etkilemesi muhtemel siber alanda gerçekleştirilen düşmanca eylemler;

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

Siber terörizm - siber uzayda siyasi, ideolojik veya dini motivasyonlu bireyler, gruplar veya kuruluşlar tarafından yürütülen ve maddi yıkıma veya mağdurlara neden olabilecek, panik veya teröre neden olabilecek önceden tasarlanmış faaliyetler;

siber casusluk - bir devletin veya devlet dışı bir kuruluşun yararına yetkisiz gizli bilgiler elde etmek amacıyla siber uzayda gerçekleştirilen eylemler;

Bilgisayar suçu - ceza hukuku veya diğer özel yasalar tarafından öngörülen ve sosyal tehlike arz eden ve siber altyapılar aracılığıyla veya siber altyapılar üzerinde suçlulukla işlenen tüm eylemler;

Siber uzayda güvenlik açığı - siber altyapıların veya bir tehdit tarafından sömürülebilecek ilgili

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

güvenlik önlemlerinin tasarımında ve uygulanmasında zayıflık;

Siber uzayda güvenlik riski - siber altyapılara özgü belirli bir güvenlik açığından yararlanarak bir tehdidin gerçekleşme olasılığı;

Risk yönetimi - her türlü kaybı önlemek için karmaşık tekniklerin ve araçların kullanımına dayanan siber güvenlik risklerini tanımlamak, değerlendirmek ve bunlara karşı koymak için karmaşık, sürekli ve esnek bir süreç;

Kimlik yönetimi - belirli siber altyapılara eriştiklerinde insanların kimliğini doğrulama yöntemleri;

İç kontrolün bileşenleri

INTOSAI GOV 9100 Standardı "İç Kontrol Standartları Kılavuzu" na göre. 2001 yılında, Uluslararası Yüksek Denetim Kurumları Örgütü (INCOSAI) Kongresi'nde, ilk olarak 1992 yılında yayınlanan kamu sektöründeki iç kontrol standartları için INTOSAI Kılavuz İlkeleri'nin, iç kontrol alanındaki son gelişmelerin tüm yönlerini belgeye dahil ederek güncellenmesine ve COSO modelinin (İç Kontrol – Entegre Çerçeve) bir dizi unsurunun entegre edilmesine karar verilmiştir.

INTOSAI İç Kontrol Standartları Komitesi'nin operasyonel grubu tarafından yürütülen bir faaliyet olan Kılavuz İlkeler'e 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 Kılavuzları", INTOSAI GOV kategorisinin (iyi yönetişim rehberliği) bir parçasıdır ve hem iç kontrol sistemini uygulamak zorunda olan kamu sektörü yöneticileri hem de bu sistemi bilmesi ve değerlendirmesi gereken dış kamu denetçileri için son derece yararlı olduğu düşünülmektedir.

İç kontrol standartları

INTOSAI GOV 9100 Kılavuzlarına göre, iç kontrol birbirine bağlı beş bileşenden oluşur (COSO modelininkilerle aynıdır):

- Kontrol Ortamı
- Risk değerlendirmesi
- Kontrol faaliyetleri
- Bilgi ve iletişim
- Izleme

İç kontrol, kurumun genel hedeflerine ulaşılmasına ilişkin makul güvence sağlamak üzere tasarlanmıştır. İşletme başkanları tarafından açıkça belirlenen hedefler ve bütçenin uygun şekilde planlanması, etkin bir iç kontrol için zorunlu bir şarttır.

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

Kontrol ortamı

Kontrol ortamı, yönetimin ve yönetişimden sorumlu olanların iç kontrol sistemi ve işletme içindeki önemine ilişkin genel tutum, farkındalık ve eylemlerini kapsar. Kontrol ortamı, organizasyonun tonunu belirler ve personel düzeyinde kontrol bilincini etkiler.

İç kontrolün diğer tüm bileşenlerinin temelini temsil eder, iç kontrol sisteminin etkin bir şekilde uygulanabilmesi için kuruluş içinde saygı duyulması gereken bir disiplin ve işletmenin yapısını sağlar. İç kontrol ortamı, yolsuzluk ve dolandırıcılığın önlenmesinde etkili bir araçtır.

Kontrol ortamını tanımlayan unsurlar şunlardır:

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

Siber Güvenlik Denetimi Türleri

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

Siber güvenliğe tek taraflı bir yaklaşım sadece modası geçmiş ve etkisizdir. Ve günümüzün tehdit ortamında tüm saldırıları önlemek imkansız olduğundan, kuruluşlar varlıklarını işletme için önemine göre değerlendirmeli ve buna göre kontroller oluşturmalıdır.

Zorluklara ek olarak, tüm şirket varlıklarında sıkı kontroller uygulandığında çalışanların uyumluluk kurallarına uyma olasılıklarının düşük olmasıdır. Bir denetimin önem derecesi, varlık ve tehdit ortamını doğrudan yansıtmalıdır.

Örneğin, bir bilgisayar korsanının binlerce kişisel müşteri verisini bir bulut veritabanı aracılığıyla açığa çıkarmasının sonuçları, bir çalışanın dizüstü bilgisayarının tehlikeye girmesinden çok daha büyük olabilir.

Siber güvenlik kontrolleri

"Korumaya çalıştığınız şeyin doğasına bağlı olarak kontrolleri uygulamanın birçok farklı yolu var," diyor Microsoft'ta Infosec Stratejileri ve En İyi Uygulamaları ve siber güvenlik küresel siyah kuşağının yazarı Joseph MacMillan.

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

"Karşı korumaya çalıştığınız tehdidin doğası nedir?

Kötü niyetli bir aktör mü?

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 kritikliğine ve sınıflandırmasına göre "yeterince güvenli" olarak kabul edildiği anlamına gelir. Denetim türlerini bölen farklı sınıflar vardır:

- İdari / yönetsel kontroller firmanın politika ve prosedürleridir. Yeni bir yazılım kontrolü kadar "havalı" değiller, ancak bireylere ve kuruluşun diğer üyelerine yapı ve rehberlik sağlamak, kimsenin para cezasına çarptırılmamasını veya ihlale neden olmamasını sağlamak için varlar.
- Sistemlere erişimi fiziksel bir şekilde sınırlayan fiziksel kontroller.
- Teknik / mantıksal kontroller, şifreleme, parmak izi okuyucuları, kimlik doğrulama veya güvenilir platform modülleri (TPM) gibi donanım veya yazılımlara dayalı 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. Örnek olarak farkındalık eğitimi, varlık sınıflandırması ve günlük dosyası incelemesi verilebilir.

Denetim türleri

Önleyici denetimler bir eylemi önlemek için vardır 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 harekete geçebilir. Fail open ve fail closed komutları burada ele alınmıştır.

Kurtarma komutları, bir sabit sürücüyü kurtarmak gibi bir kayıptan bir şeyler geri alır. Telafi edici denetimler, erişim günlüklerinin düzenli olarak gözden geçirilmesi gibi diğer denetimlerdeki eksiklikleri telafi etmeye çalışan denetimlerdir. Bu örnek aynı zamanda bir dedektif denetimidir, ancak ücret denetimleri farklı türlerde olabilir.

Kontrollerin sırası

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

Aktörleri, olmamaları gereken bir şeye erişmeye çalışmaktan caydırır. Erişim izinleri veya kimlik doğrulaması gibi önleyici bir denetim aracılığıyla Erişimi Reddet/Engelle.

Uç nokta koruma yazılımı gibi algılamayı kaydettiğinizden emin olarak riski algılayın. İşlemin, parola girmek için "çok fazla deneme" özelliği gibi riski tekrar yinelemesini geciktirin.

Bir olay müdahale planı gibi uzlaşmaya yanıt vererek durumu düzeltin. Kullanılabilirliği bir sunucuya geri yükleyen bir yedek oluşturucu gibi güvenliği ihlal edilmiş bir durumdan kurtarın.

Ek olarak, sürekli iyileştirme alanında, herhangi bir değişiklik için her bir varlığın değerini izlemeliyiz. Bunun nedeni, zaman içinde veya kuruluşunuzdaki belirli önemli olaylar sırasında az ya da çok değerli hale gelmeleri durumunda bu varlıkları korumaya yönelik denetimlerimizi yeniden düşünmemiz gerekebileceğidir.

Kontroller ve kurtarma

Kontrollere baktığımızda toparlanmayı da düşünmeliyiz, varlıklardaki ve değerlerindeki olumsuz durumlardan veya değişikliklerden kurtulabilmek istiyoruz. Tıpkı örnekler gibi, yedeklemeler, artıklık, geri yükleme süreçleri ve benzerlerinden bahsediyoruz.

Özellikle bulut, SaaS, PaaS, IaaS, üçüncü taraf çözümleri ve diğer tüm "başkasının bilgisayarı" çağında hatırlanması gereken bir kavram, Hizmet Düzeyi Sözleşmelerinin (SLA'lar) açıkça tanımlandığından ve izin verilen maksimum kesinti süresi sözleşmelerine ve bu sözleşmelere uyulmamasına ilişkin cezalara sahip olduğundan emin olmaktır. Bu, telafi edici kontrolün bir örneğidir.

Soru:

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

1. Şirketler için siber saldırıları riskleri nelerdir?
2. Bazı siber güvenlik kontrollerini açıklayın.
3. İç kontrol standartlarını açıklayınız.
4. Bilgiler Nasıl Kontrol Edilir ve Kurtarılır?

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

- Şirkette siber saldırılara karşı 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

Ekleri

PowerPoint sunumu

Video filmler

Başvuru:

- Şirketlere Siber Saldırılar: Risk Altında mısınız?
- Siber saldırıların artan stratejik riskleri
- İşletmeler İçin 10 Ortak Siber Güvenlik Riski
- İç 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.