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

InCyT Eğitim Modülleri

Yöneticiler için Bilgi Güvenliği **Ünite (Modül) no: (2)-Hafta:4** **Birim (Modül) adı: Bilgi güvenliği yönetimi -2**	
Öğrenme Aktiviteleri	❑**Web semineri** ❑**Alıştırmalar** ❑**Çalıştay** ❑**Sunum** ❑**Diğer** Streaming Webinar, Metin, Öz Değerlendirme Alıştırmaları, Tartışma forumlarında cevapları olan alıştırmalar ve eğitmen / mentor ile tartışılacak
Öğrenme Sorumlusu	• Fatma Gökdemir • Ali Gökdemir
Öğrenme Etkinliği Hedefleri	1. Tehdit ve güvenlik açığı değerlendirmesi 2. Tehdit ve güvenlik açığı yönetimi 3. Güvenlik açığı değerlendirmesi türleri 4. Operasyonların Siber Sürekliliği 5. Siber Varlık 6. Siber güvenlik politikalarının etkinliğinin değerlendirilmesi
Kazanılacak Beceriler	• IS 1 • IS 3 • MS 5
Öğrenme aktivitesinin süresi	2 hafta
Öğrenme rdonatımları	***Neye ihtiyaç var?*** • Orta düzey bilgisayar becerile

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

Modül hakkında kısa bilgi

Giriş

Varlıkların yönetimi, ISO 27001 Bilgi Güvenliği Yönetim Sistemi kapsamında önemli bir yere sahiptir. Aslında, Bilgi Varlıklarının tanımlanması ve sınıflandırılması, bilgi güvenliği kurulumunun ilk adımlarından biridir. Bir kuruluştaki varlıklara değer belirlemek ve atamak, risk analizi sürecinde temel bir adımdır. Varlıklara değer atamak için bir varlık envanteri hazırlanır.

Varlık envanterinden önce tüm çalışanları kapsayan bir keşif çalışması yapılmalıdır. Bu çalışma ile bölümün varlık envanteri araştırılarak olası riskler ve gizlilik derecesi ile birlikte listelenmiştir. Varlık envanteri, kapsanan süreçler temelinde tek tek yapılmalıdır.

Varlık envanteri hazırlanırken; varlık grubu, belirtilen varlığın bulunduğu ortam, sınıflandırma kodu belirlenir ve varlık değeri (gizlilik, bütünlük, erişilebilirlik) hesaplanır. Hesaplama sonucuna göre öncelik durumu belirlenir ve eylem kararları alınır. Varlık stok çalışması tamamlandıktan sonra, tespit edilen yazılım-donanım stokları için detaylı bir stok listesi hazırlanır.

ISO27001 standardında varlık yönetimine ilişkin koşullar/kontroller Ek A.8 altında toplanmıştır. Bu modülde, A.8.1'de tanımlanan Varlıkların Sorumluluğu için şartları inceleyeceğiz.

Öğrenme Materyalinin İçeriği

1. Bilgi Güvenliği Yönetimini Değerlendirme

Varlık yönetiminin ilk aşamasında, öncelikle hangi varlıklara sahip olduğumuzu ortaya çıkarmak ve listelemek faydalı olacaktır. Bir kurumun neye sahip olduğu veya ne olmadığı önce bilinmelidir. O zaman sahipliklerinin tanımlanması gerekir. Hiçbir iş veya işlem gözetimsiz bırakılmamalıdır. Daha sonra, bu varlıkların kullanımına ilişkin kurallar belirlenmelidir.

Konunun detayları için ISO27002 standardı incelenmelidir. ISO27002'de Varlık yönetimine ilişkin beklentiler standardın 8. maddesinde yer almaktadır:

Varlık yönetimi ve varlıklar için sorumluluk

Amaç: Kuruluşun varlıklarını tanımlamak ve uygun koruma sorumluluklarını tanımlamak.

1. Varlık envanteri

Kontrol: Bilgi ve bilgi işlem tesisleri ile ilgili varlıklar belirlenmeli ve bu varlıkların envanteri çıkarılmalı ve muhafaza edilmelidir.

Uygulama kılavuzu: Bir kuruluş, bilgi yaşam döngüsündeki ilgili varlıkları tanımlamalı ve önemlerini belgelemelidir. Bilgi yaşam döngüsü oluşturma, işleme, depolama, iletme, silme ve imha etmeyi içermelidir. Dokümantasyon, mevcut envanterlere uygun olarak veya özellikle muhafaza edilmelidir.

Varlık envanteri; güncel, tutarlı, doğru ve diğer envanterlerle uyumlu olmalıdır.

Varlık mülkiyeti, tanımlanan her bir varlık için tahsis edilmeli (Madde 2'ye bakınız) ve sınıfı belirlenmelidir.

Diğer bilgiler: Varlık envanteri, etkili koruma sağlamaya yardımcı olur ve sağlık ve güvenlik, sigorta veya finansal (varlık yönetimi) nedenler gibi diğer amaçlar için de gerekli olabilir.

ISO/IEC 27005[11] standardı, varlıkları tanımlarken kuruluş tarafından dikkate alınması gerekebilecek varlık örnekleri sağlar. Bir varlık envanterinin derlenmesi süreci, risk yönetimi için önemli bir ön koşuldur (bkz. ISO/IEC 27000 ve ISO/IEC 27005[11]).

2. Varlıkların mülkiyeti

Kontrol: Stokta tutulan tüm varlıklar için sahip atamaları yapılmalıdır.

Uygulama kılavuzu: Varlık yaşam döngüsü için onaylanmış yönetim sorumluluğuna sahip bireyler ve diğer kuruluşlar, varlık sahibi olarak atanmaya uygundur.

Varlık sahipliğinin zamanında belirlenmesini sağlamak için genellikle bir süreç kullanılır. Sahiplik, varlıklar oluşturulduğunda veya kuruluşa devredildiğinde belirlenmelidir. Varlık sahibi, varlık yaşam döngüsü boyunca varlığın uygun şekilde yönetilmesinden sorumlu olmalıdır.

Varlık sahibi:

a) Varlık envanterinin kaydedilmesini sağlamak,

b) Varlıkların uygun şekilde sınıflandırılmasını ve korunmasını sağlamak,

c) Önemli varlıklara erişim ve bunların sınıflandırılması ile ilgili kısıtlamaları, yürürlükteki erişim kontrol politikasını dikkate alarak tanımlamak ve periyodik olarak gözden geçirmek,

d) Varlıkların silinmesi veya yok edilmesi için uygun önlemlerin alınmasını sağlamak.

Diğer bilgiler: Bir varlığı yaşam döngüsü boyunca kontrol etmek için yönetim sorumluluğu onayına sahip bir birey veya kuruluş olabilir. Tanımlanan sahibin, varlık üzerinde sahiplik menfaati yoktur.

Rutin görevler devredilebilir; (örneğin, bir varlığa günlük olarak bakan bir emanetçi) ancak sorumluluk varlık sahibine aittir.

Karmaşık bilgi sistemleri içindeki varlık gruplarını tanımlamak, birlikte işlevler sağlamada yararlı olabilir. Bu durumda, bu hizmet sahibi, varlıkların işletilmesi de dahil olmak üzere hizmetin tesliminden sorumludur.

3. Varlıkların kabul edilebilir kullanımı

Kontrol: Bilgi ve bilgi işlem tesislerine ilişkin bilgi ve varlıkların kabul edilebilir kullanımına ilişkin kurallar belirlenmeli, belgelendirilmeli ve uygulanmalıdır .

Uygulama kılavuzu: Kuruluşun varlıklarını kullanan veya bunlara erişimi olan çalışanlar ve dış kullanıcılar, kuruluşun bilgi ve bilgi işleme tesisleri ve kaynaklarıyla ilişkili varlıklarının bilgi güvenliği gereksinimleri konusunda bilgilendirilmelidir. Bu kullanıcılar, tüm bilgi işlem kaynaklarının kullanımından ve kendi sorumlulukları altında gerçekleşen her türlü kullanımdan sorumlu olmalıdır.

4. Varlıkların iadesi

Kontrol: Dış tarafların tüm çalışanları ve kullanıcıları, istihdam, sözleşme veya sözleşmenin feshi üzerine sahip oldukları tüm kurumsal varlıkları iade etmelidir .

Başvuru kılavuzu: Fesih süreci, kuruluşun daha önce verilmiş tüm fiziksel ve elektronik varlıklarının veya emanetlerinin mülkiyetinin iadesini içerecek şekilde formüle edilmelidir.

Bir çalışan veya dış kullanıcı kuruluşun ekipmanını satın aldığında veya kullandığında, ilgili tüm bilgilerin kuruluşa aktarılmasını ve ekipmandan güvenli bir şekilde silinmesini sağlamak için prosedürler izlenir.

Bir çalışanın veya harici kullanıcının devam eden operasyonlar için önemli olan bilgilere sahip olduğu durumlarda, bu bilgilerin belgelenmesi ve kuruluşa aktarılması gerekir.

Fesih bildirim süresi boyunca kuruluş; fikri mülkiyet gibi ilgili bilgilerin feshedilen çalışanlar ve yükleniciler tarafından yetkisiz olarak kopyalanmasını kontrol etmek.

2. Tehdit ve güvenlik açığı değerlendirmesi ve yönetimi

Hemen hemen her kuruluşun korunması gereken hassas ve değerli varlıkları vardır. Bununla birlikte, her kuruluşun bu varlıkları korumak için kapsamlı ve tamamen düşünülmüş bir stratejisi yoktur. Siber güvenlikte, güvenlik açığı yönetimi stratejileri güçlü savunmanın temelidir. Tipik olarak, güvenlik açığı yönetimi stratejileri bir kuruluşun sistemlerine, ağlarına, uygulamalarına vb. Yardımcı olmak için tasarlanmıştır. Güvenlik açıklarını yönetmek için bütünsel ve sürekli bir yaklaşım benimser Bu güvenlik açıkları daha sonra mümkün olan en kısa sürede tanımlanır, değerlendirilir ve düzeltilir.

Güvenlik tehditleri ve eğilimleri sürekli olarak gelişmektedir ve verilerinizi tehlikeye atabilecek tehditleri ve güvenlik açıklarını yönetmek için etkili, önleyici çabalar gerektirir. Bir ihlal veya saldırı için tüm potansiyel hedefleri belirlemek için, öncelikle bir varlık envanteri yapılarak riskinin azaltılması gerekir. Hedefler daha sonra sınıflandırılmalı ve yeni potansiyel güvenlik açıkları için sürekli izlenmelidir. Kuruluşun yüksek risk altındaki en değerli varlıklarını tanımlayan bir tehdit modeli daha sonra geliştirilmeli ve test edilmelidir. Tehdit ve Güvenlik Açığı test sürecinin (değerlendirme) temel amacı, varlıkların kritikliğini, bu varlıkların güvenlik açıklarını en iyi şekilde anlamak ve bu varlıkları etkili bir şekilde korumak için gerekli önlemleri azaltmaktır.

2.1. Güvenlik açığı değerlendirmesi nedir?

Güvenlik açığı değerlendirmesi, bilgisayar sistemlerindeki, uygulamalardaki ve ağ altyapılarındaki güvenlik açıklarını tanımlama, tanımlama, sınıflandırma ve önceliklendirme işlemidir.

Güvenlik açığı değerlendirmeleri ayrıca bir kuruluşa çevresine yönelik tehditleri anlamak ve bunlara yanıt vermek için gerekli bilgi, farkındalık ve risk geçmişini sağlar. Bir güvenlik açığı değerlendirme süreci, tehditleri ve oluşturdukları riskleri tanımlamayı amaçlar. Genellikle, sonuçları bir güvenlik açığı değerlendirme raporunda listelenen ağ güvenliği tarayıcıları gibi otomatik test araçlarının kullanılmasını içerir.

Her büyüklükteki kuruluş, hatta siber saldırı riski yüksek olan bireyler bile, bir tür güvenlik açığı değerlendirmesinden yararlanabilir, ancak devam eden saldırılara maruz kalan büyük kuruluşlar ve diğer kuruluş türleri güvenlik açığı analizinden en çok yararlanacaktır.

Güvenlik açıkları, bilgisayar korsanlarının BT sistemlerine ve uygulamalarına erişmesine izin verebildiğinden, kuruluşların güvenlik açıklarından yararlanmadan önce bunları tanımlaması ve düzeltmesi kritik önem taşır. Bir yönetim programı ile birleştirilen kapsamlı bir güvenlik açığı değerlendirmesi, şirketlerin sistemlerinin güvenliğini artırmalarına yardımcı olabilir.

2.2. Güvenlik açığı değerlendirmelerinin önemi

Güvenlik açığı değerlendirmesinin önemini daha iyi aydınlatmak için, fiziksel bir mülk sahibinin gözünden düşünelim. Değerli bir binanız varsa, muhtemelen onu korumak için bir dizi önlem

alırsınız: Bakımını yaparsınız, sigortalarsınız ve kapıların, pencerelerin kilitli olduğundan ve alarmların etkinleştirildiğinden emin olursunuz. Tüm bu adımlar, mülk ve içeriği üzerindeki riski yönetmek olarak adlandırılabilir.

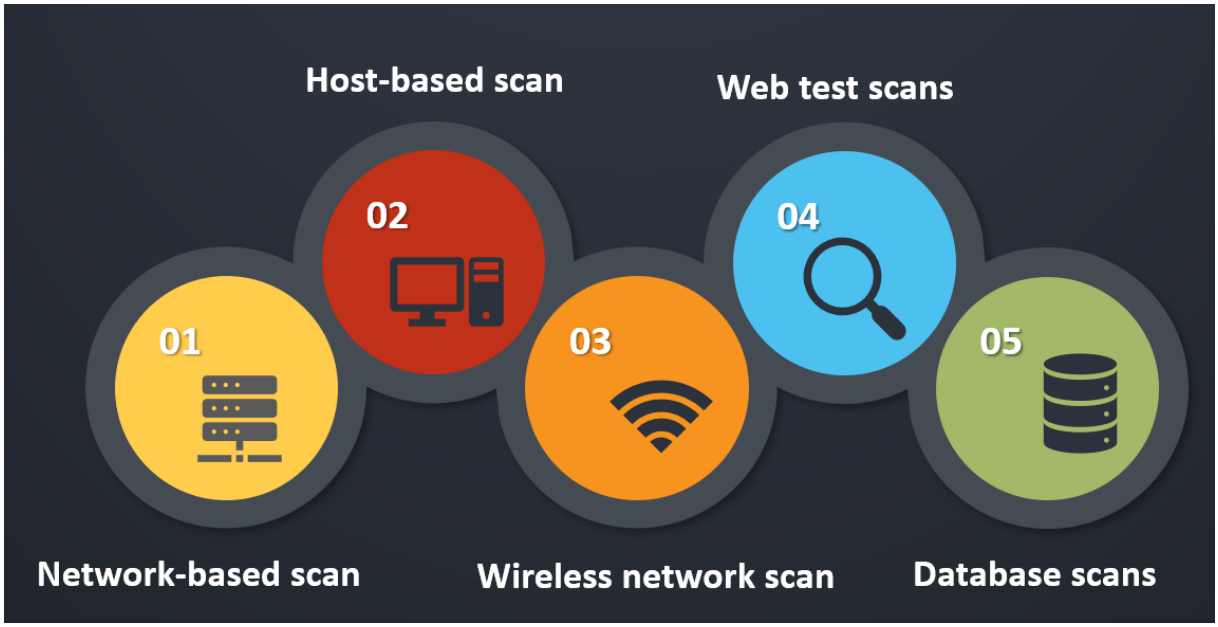
Peki ya alarmlarınızı ve dış savunmalarınızı test etmek ve raporlamak için birini işe alabilseydiniz? Siber güvenlik açıklarına da benzer şekilde yaklaşılmaktadır. Güvenlik açığı yönetimi kapsamlı ve devam eden bir stratejidir, güvenlik açığı değerlendirmeleri ise bu daha geniş yönetim stratejisinde kullanılan belirli bir araçtır.

Güvenlik açığı değerlendirmesi, kuruluşa ortamındaki güvenlik zayıflıkları hakkında ayrıntılı bilgi sağlar. Ayrıca, bu zayıflıklarla ilişkili risklerin nasıl değerlendirileceği konusunda da yön sağlar. Bu süreç, kuruluşun varlıklarını, güvenlik kusurlarını ve genel riskini daha iyi anlamasını sağlayarak bir siber suçlunun sistemlerini ihlal etme olasılığını azaltır ve işletmeyi hazırlıksız yakalar.

2.3. Güvenlik açığı değerlendirmesi türleri

Güvenlik açığı değerlendirmeleri farklı sistem veya ağ güvenlik açıklarını bulur. Bu, değerlendirme sürecinin güvenlik açıklarını, tehditleri ve riskleri tanımlamak için çeşitli araçlar, tarayıcılar ve metodolojiler kullanmayı içerdiği anlamına gelir.

Farklı güvenlik açığı değerlendirme tarama türlerinden bazıları şunlardır (Şekil 1):



Şekil 1. Güvenlik açığı değerlendirmesi türleri

- **Ağ tabanlı** taramalar, olası ağ güvenliği saldırılarını tanımlamak için kullanılır. Bu tür bir tarama, kablolu veya kablosuz ağlardaki savunmasız sistemleri de algılayabilir.
- **Ana bilgisayar tabanlı** taramalar, sunuculardaki, iş istasyonlarındaki veya diğer ağ ana bilgisayarlarındaki güvenlik açıklarını bulmak ve tanımlamak için kullanılır. Bu tür bir tarama genellikle ağ tabanlı taramalarda da görülebilen bağlantı noktalarını ve hizmetleri inceler. Bununla birlikte, eski sistemler de dahil olmak üzere taranan sistemlerin yapılandırma ayarları ve yama geçmişi hakkında daha fazla görünürlük sağlar.
- Bir kuruluşun Wi-Fi ağlarının kablosuz ağ taramaları genellikle kablosuz ağ altyapısındaki saldırı noktalarına odaklanır. Kablosuz ağ taraması, sahte erişim noktalarını tanımlamanın yanı sıra, bir şirketin ağının güvenli bir şekilde yapılandırıldığını da doğrulayabilir.
- **Web taraması** , uygulama, ağ veya web uygulamalarındaki bilinen yazılım güvenlik açıklarını ve yanlış yapılandırmaları tespit etmek için siteleri test eder.
- **Veritabanı taramaları** , kötü amaçlı saldırıları önlemek için veritabanındaki zayıf noktaları belirleyebilir. SQL ekleme saldırıları bunlara örnek olarak verilebilir.

2.4. Güvenlik açığı değerlendirmeleri ve sızma testleri

Bir güvenlik açığı değerlendirmesi genellikle bir kuruluşun personeli, prosedürleri veya süreçlerindeki güvenlik açıklarını tanımlamak için bir penetrasyon testi bileşeni içerir. Güvenlik açığı değerlendirmeleri, sızma testleriyle aynı özelliklerin çoğunu paylaşır, çünkü her ikisi de kuruluşların savunmalarını titizlikle incelemelerine izin verir. Bu güvenlik açıkları normalde ağ veya sistem taramaları tarafından algılanmayabilir. Süreç bazen güvenlik açığı değerlendirmesi / penetrasyon testi veya **VAPT** olarak adlandırılır.

Bununla birlikte, penetrasyon testi tam bir güvenlik açığı değerlendirmesi olarak yeterli değildir ve aslında ayrı bir süreçtir. Güvenlik açığı değerlendirmesi, bir ağdaki güvenlik açıklarını ortaya çıkarmayı ve riskleri azaltmak veya ortadan kaldırmak için uygun azaltma veya düzeltme önermeyi amaçlar.

Güvenlik açığı değerlendirmesi, otomatik ağ güvenliği tarama araçlarını kullanır. Sonuçlar, kuruluşlara düzeltilmesi gereken güvenlik açıklarının bir listesini sağlamaya odaklanan güvenlik açığı değerlendirme raporunda listelenmiştir. Ancak, bunu belirli saldırı hedeflerini veya senaryolarını değerlendirmeden yapar.

Kuruluşlar, özellikle değişiklikler yapıldığında, ağlarının güvenliğini sağlamak için düzenli olarak güvenlik açığı testleri gerçekleştirmelidir. Örneğin, hizmetler eklendiğinde, yeni ekipman kurulduğunda veya bağlantı noktaları açıldığında test yapılmalıdır.

Buna karşılık, penetrasyon testi, bir ağdaki güvenlik açıklarını tanımlamayı ve bunları sisteme saldırmak için kullanmaya çalışmayı içerir. Bazen güvenlik açığı değerlendirmeleriyle birlikte gerçekleştirilse de, sızma testinin birincil amacı, bir güvenlik açığının gerçekten var olup olmadığını kontrol etmektir. Ek olarak, sızma testi, bir güvenlik açığından yararlanmanın uygulamaya veya ağa zarar verebileceğini kanıtlamaya çalışır.

Bir güvenlik açığı değerlendirmesi genellikle çok çeşitli yamalanmamış güvenlik açıklarını kapsayacak şekilde otomatikleştirilirken, penetrasyon testi genellikle otomatik ve manuel teknikleri birleştirerek test uzmanlarının güvenlik açıklarını daha fazla araştırmalarına ve kontrollü bir ortamda ağ erişimi elde etmek için bunlardan yararlanmalarına yardımcı olur.

2.5. Güvenlik Açığı Yönetimi ve Risk Yönetimi

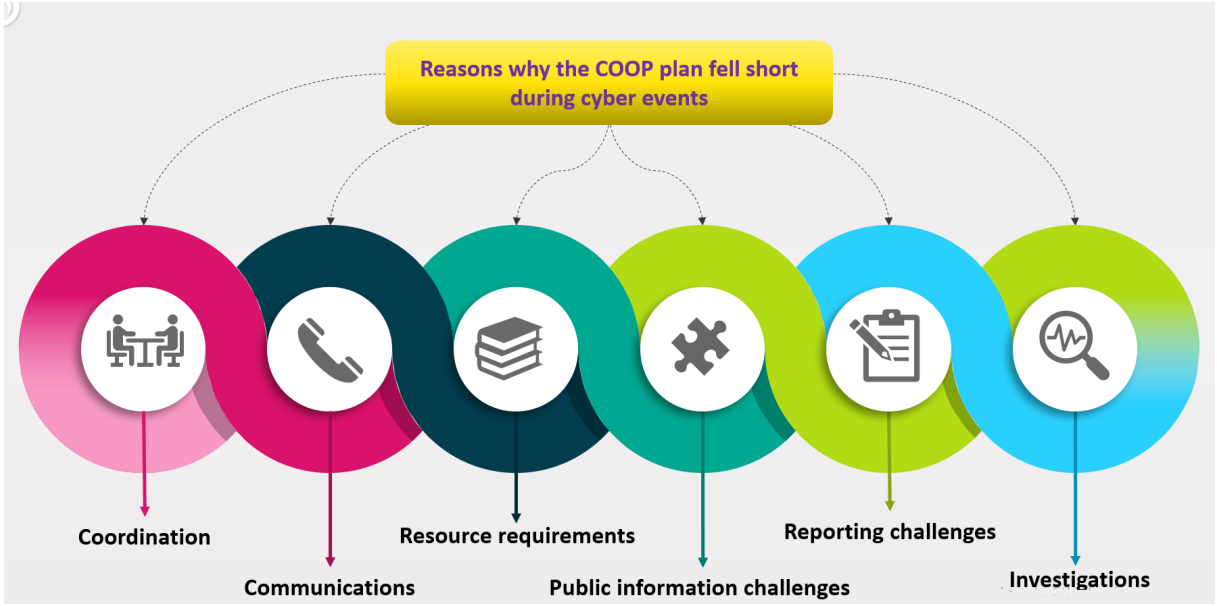
Güvenlik açığı yönetimi, güvenlik açıklarını yönetmek için devam eden bir süreç olsa da, risk yönetimi bir kuruluş için tehdit oluşturabilecek her şeye daha geniş bir bakış açısı getirir. Sağlam bir risk yönetimi stratejisi, risklerin tanımlanmasını, analiz edilmesini ve etkili bir şekilde azaltılmasını sağlar. Bu yaklaşım, kuruluşların yalnızca var olan güvenlik açıklarını değil, aynı zamanda kötüye kullanıldığında oluşabilecek hasarın ölçeğini de anlamalarına yardımcı olur. Risk yönetimi şemsiyesi altında yürütülen bir risk ve kırılganlık değerlendirmesi, örgütsel bir güvenlik duruşunun gücü hakkında özellikle geniş bir bakış açısı sağlayabilir.

3. Operasyonların Siber Sürekliliği

Yıkıcı kötü amaçlı yazılım tehditlerine karşı dayanıklılığı artırmak, mevcut güvenlik duruşu hakkında bilgi edinmeyi, önemli savunma eylemlerini planlamayı ve koordine etmeyi ve temel savunma kaynaklarını doğru şekilde hizalamayı gerektirir.

Siber olaylar da aynı şekilde temel süreklilik planlama çabalarına meydan okumuştur. Birçok yargı bölgesinde siber saldırıları tanımlamak, tespit etmek ve bunlara karşı korunmak için ekipman ve stratejiler bulunurken, çok daha azı gerçek bir saldırı yoluyla operasyonlarının sürekliliğinin zor gerçekleri üzerinde çalışmıştır. Siber saldırılar gerçekleştiğinde, etkilenen birçok yargı bölgesi, temel COOP planlarının tutmadığını fark eder. Planlar alternatif bir şantiyeye geçiş için yeterli olsa da, sistemlere ve veri personelinin misyonlarının temel işlevlerini yerine getirmesi gereken sistemlere ve verilere erişmeden çalışmak söz konusu olduğunda sunacakları çok daha az şey var. Mevcut planlar ayrıca yanıtı yönlendirmek için gereken özgüllükten yoksundur ve BT personelinin üyeleri gibi büyük paydaşlar genellikle yanıt yapılarına entegre edilmez. Ve planlar bir tatbikata veya gerçek dünyadaki bir olaya karşı test edilmemiştir.

Geleneksel COOP planları, siber olaylar sırasında süreklilik açısından çeşitli şekillerde yetersiz kalmaktadır (Şekil 5):



Şekil 5. COOP planlarının siber olaylar sırasında süreklilik için yetersiz kalmasının nedenleri

Koordinasyon: Fidye yazılımı söz konusu olduğunda karar alma sürecine kimlerin dahil olduğu, sistemleri çevrimdışı duruma getirme kararları ve yargı Acil Durum Operasyon Merkezi'ni etkinleştirme kararları dahil. Ek olarak, çoğu yerel yönetimin bir saldırı için net tırmanma düzeyleri veya her düzey için ilişkili eylem öğeleri yoktur. Yanıt liderliği ve personel alımı da belirsiz olabilir; Bir topluluğa bir siber olay boyunca rehberlik etmek için gereken konu uzmanlığı türleri, aşırı hava koşulları için gerekli olanlardan farklıdır.

İletişim: Bir siber saldırı iletişimi ciddi şekilde tehlikeye attığında yerel yöneticilerin personele nasıl hızlı bir şekilde bilgi sağlayacağı da dahil olmak üzere. Bu, hem saldırı başladığında ne yapılacağını açıklayan anlık iletişimleri hem de maaşların maaş gününe göre nasıl sağlanacağı gibi devam eden iletişimleri içerir. Her ikisi de yanıt için kritik öneme sahiptir ve yine de her ikisinin de tipik acil durum iletişim sistemlerinin yararı olmadan iletilmesi gerekebilir.

Kaynak gereksinimleri: Daha geleneksel bir yanıt için olanlardan çok farklı olabilir. Örneğin, personel temiz bilgisayarlara, temiz sunuculara, yerel yazıcılara ve hatta faks makinelerine ve kağıda ihtiyaç duyabilir. Daha da önemlisi, personel gereksinimleri, departmanlar ve ajanslar eksik veya şüpheli verileri çoğaltmak için mücadele ettikçe, kurtarma sırasında yanıt olarak olduğundan daha fazla artabilir.

Kamu bilgilendirme zorlukları: Siber güvenlik konusunda çok az eğitim veya deneyime sahip olan veya hiç deneyimi olmayan, önceden yazılmış mesajların eksikliği ve saldırı hakkındaki bilgilerin ne zaman kamuya açıklanması gerektiği konusunda anlaşmazlık yaşayan kamu bilgi görevlilerini reddediyorum. Halka bilgi sağlamak çok önemlidir, çünkü vatandaşlar verileri ve oylama ve adalet gibi kilit demokratik sistemlerin güvenilirliği konusunda endişe duymaktadır.

Raporlama zorlukları: Müdahaleler tutarlı bir şekilde raporlanmadığından müdahaleyi geciktirebilir ve BT departmanlarını bir saldırıyı hızlı bir şekilde belirlemek için gerekli ortak operasyonel aksiyondan mahrum bırakır. Buna ek olarak, raporlama hatları genellikle belirsizdir ve BT dışındaki çok az kişi, hangi sistemlerin hem yargı yetkisi içinde hem de dışında bağlı olduğunu anlar.

Araştırmalar: Birçok bölge için kara bir kutudur. Bir veya daha fazla federal örgütün katılımı ve soruşturmaların iyileştirme çabalarına getirdiği sınırlar iyi anlaşılmamıştır veya planlanmamıştır. Bu, süreklilik planlamasını son derece zorlaştırır, çünkü iyileştirmenin nasıl ve ne zaman başlayabileceği konusunda belirsizlik vardır.

3.1. Koordineli Savunma ile Acil Eylem için Öncelikler

• Temel prosedürler ve bilgiler içeren bir siber 'Go Bag' geliştirin.

  o COOP tarafından belirlenen bir tesiste siber dirençli TTP'lerin kurulması, uygulanması, sürdürülmesi ve sürekliliğinin sağlanması için prosedürler içeren mobil siber güvenlik araç setlerini bir araya getirmek

• Çalışma kitaplarını, rolleri, sorumlulukları ve araçları geliştirin, test edin ve doğrulayın.

  o Siber COOP'un uygulanmasını sağlamak için kullanılabilecek belirli siber rolleri, ilgili sorumlulukları ve siber araçları belirlemek.

  o Siber 'Go Bag' araçlarını ve elastik TTP'leri kullanarak bireysel veya siber ekip yürütme için standart siber COOP oyunlarını tanımlayın.

  o Siber 'Go Bag' ve taktik kitabını kullanarak farklı türde siber alıştırmalar (örneğin mini masa üstü tipi egzersizler) yapın.

• İşbirliği süreçlerini tanımlayın ve siber savunucular ve olay müdahale ekipleri için araçlar edinin.

  o Hem mobil hem de sabit siber COOP süreçlerinin, siber savunmaların yeterli yönetimini, tüm müdahale faaliyetleri arasında sinerjiyi ve kurtarma faaliyetleri sırasında güvenlik

kapsamı boşluklarının azaltılmasını teşvik etmek için iletişim ve koordinasyon eşgüdümünü içermesini sağlayın.

Temel COOP planları, yargı bölgelerinin karşılaştığı tehditlerin çoğuna karşı yerel hazırlığı daha da artırmış olsa da, normdan çok farklı bir ortam yaratan durumlarda yetersiz kalmaktadır. Ülkenin dört bir yanındaki BT departmanları sistemleri ve verileri mümkün olduğunca güvenli hale getirmeye devam ettikçe, hayal güçlerini genişletmek ve kritik sistemleri ve verileri ciddi şekilde etkileyen siber saldırıları planlamak acil durum yöneticilerine kalmıştır.

3.2. Yeniden Düzenleme ile Acil Eylem için Öncelikler

• Siber kaynaklara misyon ve iş fonksiyonu bağımlılıklarını tanımlayın.

o Kaynakların misyon amaçlarını belirlemek, böylece karşılık gelen herhangi bir görev faydası olmadan riski artıran kullanımlar belirlenebilir ve ortadan kaldırılabilir.

- ✓ Risklerin faydalarından daha ağır bastığı veri akışlarını ve bağlantılarını tanımlayın ve kaldırın veya değiştirin.

o NEF yeteneklerinin sağlanmasında kritik rolleri paylaşan misyon ve misyon dışı iş fonksiyonları ve kuruluşlar arasındaki karşılıklı bağımlılıkları göz önünde bulundurun.

- ✓ Kaynakları yeniden tahsis edin veya yönetim ve yönetim sorumluluğunu, misyon ve iş fonksiyonuna yönelik riske göre yeniden atayın.

• Siber kaynaklara veya siber kaynakların kullanımına misyon dışı ve iş fonksiyonu bağımlılıklarını tanımlamak.

o Belgelenmemiş görev bağımlılıklarını ortaya çıkarmak için görev akışı analizi, görev bağımlılığı analizi, masa başı alıştırmaları ve Red Teaming'den yararlanın.

o Misyon ve iş fonksiyonlarını bağımlılık modeli haritalama ve etki analizi faaliyetleri ve sonuçları ile gözden geçirin ve ilişkilendirin.

o Görev dışı kritik fonksiyonların sistemlerini, uygulamalarını ve süreçlerini ve bunları destekleyen kaynakları tanımlamak.

- ✓ Bu işlevleri, öncelikli operasyonlara uyum sağlamak ve daha iyi bağımlılık kullanımı veya ortadan kaldırmak için akıcı bir Cyber COOP uygulama stratejisine göre değerlendirin.

4. **Siber Varlık, Değişim ve Konfigürasyon Yönetimi**

- ✓ **Varlık:** Bir varlığın tanımıyla başlayalım. Bir varlığın sözlük tanımı, yararlı veya değerli bir şey veya kişidir. Benzer şekilde, bir BT hizmet sağlayıcısının varlıkları, araçları, uygulamaları, yapılandırma öğeleri ve müşterilere veya işletmeye hizmet sunmaya yardımcı olan diğer değerli öğelerdir. Varlıklar, hizmet varlığının ve yapılandırma yönetiminin bir parçasıdır.

- ✓ **Yapılandırma Öğesi:** Yapılandırma Öğesi CI olarak kısaltılır ve yapılandırma öğesi, bir BT Hizmeti sunmak için yönetilmesi gereken herhangi bir bileşendir. Yapılandırma öğelerine örnek olarak BT hizmetleri, donanım, yazılım, binalar, kişiler ve resmi belgeler verilebilir. Kısacası, müşteriye bir BT hizmeti sunmaya yardımcı olan herhangi bir bileşen veya öğe, bir Yapılandırma Öğesi olarak sınıflandırılır. Her yapılandırma öğesiyle ilgili bilgiler, Yapılandırma Yönetim Sistemi içindeki bir Yapılandırma Kaydına kaydedilir ve bu bilgiler Yapılandırma Yönetimi tarafından yaşam döngüsü boyunca korunur.

- ✓ **Yapılandırma Yönetimi Veritabanı:** Yapılandırma Yönetimi veritabanı CMDB olarak kısaltılır. CMDB, yapılandırma kayıtlarını yaşam döngüleri boyunca depolamak için kullanılan bir veritabanıdır. CMDB, seri numarası, MAC adresi veya IP adresi gibi tanımlayıcı bilgiler de dahil olmak üzere her biri benzersiz bir tanımlayıcı ile ayırt edilen CI'leriniz hakkındaki bilgileri depolar. Bunlar geçerli sürümü; konumu; ve satıcı ve tedarikçi bilgileridir.

- ✓ **Yapılandırma Yönetim Sistemi:** Yapılandırma Yönetim sistemi CMS olarak kısaltılır ve bir BT Servis Sağlayıcısının Yapılandırma Verilerini yönetmek için kullanılan bir dizi araç ve veritabanıdır. Yapılandırma öğeleriyle ilgili veriler yapılandırma kayıtlarında depolanır ve yapılandırma kayıtları Yapılandırma Yönetim Sistemi Veritabanlarına dahil edilir. Yapılandırma verilerini yönetmek için bir BT Hizmet sağlayıcısının CMDB'leri, hizmet varlığı ve yapılandırma yönetimi sürecine dahil edilir. Yapılandırma Yönetim Sistemi ayrıca olaylar, sorunlar, bilinen hatalar, değişiklikler ve sürümler, çalışanlar, tedarikçiler, konumlar, iş birimleri, müşteriler ve kullanıcılar hakkında bilgiler içerir. Özetle, yapılandırma öğeleri ve BT varlıkları hakkında gerekli tüm bilgiler Yapılandırma Yönetim Sistemi'ne dahil edilir. Gerektiğinde, bu bilgiler CMS'den alınır ve sırasıyla kullanılır.

Temel olarak yapılan değişikliklerin tanımlanması, kontrol edilmesi, izlenmesi ve denetlenmesi süreci olarak tanımlanan konfigürasyon yönetimi, güçlü bir güvenlik programının kritik bir parçasıdır. Bir kuruluştaki değişiklik ve yapılandırma yönetimi, neredeyse tüm güvenlik çerçeveleri ve düzenlemelerindeki denetim gereksinimleriyle güçlü bağlantılara sahiptir.

Yapılandırma yönetimi, çeşitli ürün sürümlerinin denetimine ve serbest bırakılmasına dayanır. İşletim sistemleri ve uygulamalar için varsayılan yapılandırmalar genellikle siber güvenlik en iyi uygulamalarına değil, dağıtım ve kullanım kolaylığına yöneliktir. Günümüzde yapılandırma yönetimi, özellikle kuruluşlar kullanıma hazır varsayılan yapılandırmalardan daha güvenli uygulama ve donanım yapılandırmalarına geçtikçe, önemli siber güvenlik etkileri olan talep gören bir disiplindir.

Bugün, yapılandırma yönetimi farklı insanlar için farklı şeyler ifade etmektedir. Bazı uygulamalarda, ağ aygıtlarının yapılandırılma şeklini ifade eder. Diğerlerinde, bir ekibin çalıştırdığı bir uygulamanın sürümüyle ilgilidir. Bazen sektördeki insanlar BT varlık yönetimini değişim ve yapılandırma yönetimi ile karıştırır. İş için benzer ve eşit derecede önemli olsalar da, aynı değildirler. BT yönetimi çözümleri, varlıkların yaşam tarzının tamamında varlıkları izler, optimize eder ve yönetir. Bu arada, CM tüm yapılandırma öğelerini toplar, depolar, yönetir, günceller ve analiz eder.

Birçok kuruluş olgunlaşmamış CM programlarına sahip olsa da, modern siber güvenlik ortamı için kritik öneme sahiptir ve tehdit ortamı gelişmeye devam ettikçe önemi artacaktır.

4.1. Yapılandırma Yönetimi ve Olağanüstü Durum Kurtarma

Modern olağanüstü durum kurtarma söz konusu olduğunda, yapılandırma yönetimi çok önemlidir. Bir siber güvenlik felaketi durumunda, (kuruluşların% 76'sı bir siber güvenlik olayı yaşamıştır), söz konusu yapılandırmanın belgesi yoksa, en son yapılandırmaya geri dönmek imkansız olabilir.

Aynı şey siber güvenlik için de geçerlidir: Dijital ortamı yapılandırmanın, değiştirmenin ve belgelemenin standartlaştırılmış bir yolu yoksa, ekiplerin bir şeylerin yanlış olup olmadığını bilmesi imkansızdır.

4.2. Değişiklik Yönetimi

Değişiklik yönetimi, yapılandırma yönetimi ile paralel çalışır, ancak iki şey aynı *değildir*. İnsanlar onları her zaman karıştırır.
Yapılandırma yönetimi, donanım bileşenlerini, yazılımlarını ve ilişkili ayarları tanımlama ve belgeleme işlemi olsa da, değişiklik yönetimi daha büyük yapılandırma yönetimi sürecinin altında yatan bir işlevdir. Değişiklik yönetimi, ilişkili süreçlerle ilgilidir ve bir sistem içinde istikrar yaratmayı ve kontrolsüz veya rastgele değişiklikleri önlemeyi veya kuruluş içinde ciroya sahip olduğunuzda değişiklik süreçlerini belgelemeyi amaçlar. Başka bir deyişle, şirketlerin sadece tepki vermek yerine değişim için plan yapmalarını sağlar.

4.2.1. Değişiklik Yönetimi Süreci

Bugün, iyi yapılandırılmış bir değişim yönetimi süreci aşağıdakileri içerecektir:

- Değişiklik isteği gönderimleri
- Risk ve etki değerlendirmeleri
- Değişiklik işlevlerini onaylama/reddetme
- Test etme
- Zamanlama/kullanıcı bildirimi/eğitim işlevleri
- Uygulama
- Doğrulama
- Belge

Değişim yönetiminin geliştiği yerlerden biri, değişikliklerin yapılması gereken acil durum kararları durumundadır. Değişiklik uygulandıktan sonra, daha sonra zaten kurulmuş olan doğrulama ve dokümantasyon protokollerinden yararlanacağı değişiklik yönetimi sürecine geri beslenmelidir.

4.3. Siber güvenlik varlık yönetimi

Siber güvenlik varlık yönetimi, aşağıdakiler dahil olmak üzere temel güvenlik işlevlerini güçlendirmek için varlık verilerini (cihazlar, bulut örnekleri ve kullanıcılar) toplama sürecidir:

- **Algılama ve yanıt:** Algılama ve yanıt yeteneklerinin sağlanması, kuruluş genelinde kapsama alanı sağlar
- **Güvenlik açığı yönetimi: Hangi varlıkların** istismarlara karşı savunmasız olabileceğini anlama ve tüm varlıkların güvenlik açıkları için değerlendirildiğinden emin olma
- **Bulut güvenliği:** Bulut bulut sunucularının güvenli olmasını ve hızlı bir şekilde devreye alınıp hizmet dışı bırakıldıklarında bile aşırı izin verilen erişim haklarını önleyecek şekilde yapılandırılmasını sağlama
- **Olay yanıtı:** Olay yanıtı araştırmalarını ve düzeltmelerini hızlandırmak için varlıklarla ilgili zenginleştirilmiş, ilişkilendirilmiş verileri kullanma
- **Sürekli kontrol izleme:** Güvenlik kontrollerinin ne zaman eksik olduğunu ve uygulanması gerektiğini belirleme

5. Siber güvenlik politikalarının etkinliğinin değerlendirilmesi

Bir bilgi sisteminin gelişimi, sorunun analiz edilmesinden sistemin uygulanmasına kadar birkaç farklı aşamadan geçer. Bu süreç boyunca her adım, bir fizibilite çalışmasından eğitim kılavuzlarına ve sistem dokümantasyonuna kadar uzanan bir dizi çıktıyla belgelenir. Bir güvenlik politikasının geliştirilmesinde bu kendi kendini belgeleme süreci genellikle gerçekleşmez.

Şu anda geliştirilen birçok politika, her şeyi güvenlik politikasına uydurmaya çalışmaktadır: önemin gerekçelendirilmesi ve özel sistem talimatları ve açıklamaları. Elbette, güvenlik politikasının kendisi, belgenin nasıl oluşturulduğu, üretiminde kime danışıldığı veya politika formülasyonunun

nasıl elde edildiği hakkında ayrıntılı bilgi sahibi olmadan, zaten yeterince uzun solukludur. Politikanın uygulanması sırasında ortaya çıkmış olabilecek siyasi sorunların veya insanların politika hakkında nasıl eğitileceğine dair herhangi bir belge de olmayacaktır. Bununla birlikte, politikanın geliştirilmesi sırasında dokümantasyon tekniklerinin kullanılmasıyla, bir güvenlik politikası tekrar bir ilke belgesi haline gelebilir. Güvenlik politikasının ilkeleriyle ilgili olmayan diğer konular, politikanın gerekçesiyle birlikte başka bir yerde belgelenecektir.

Bir kuruluştaki bir güvenlik ilkesini değerlendirmeye çalıştığımızda genellikle eksik veya yetersiz olan en önemli bilgi, gereksinim belgeleridir. Gereksinimlerin net bir şekilde anlaşılması olmadan, bir güvenlik politikasının kalitesinin değerlendirilmesi neredeyse imkansızdır. Kuruluşun karşılaştığı risklerin/tehditlerin analizi, bir güvenlik politikasının geliştirilmesi için gereken gereksinimlerin yalnızca bir parçasıdır. Örgütün hedefleri ve güvenlik politikasının geliştirilmesini, uygulanmasını ve kabul edilmesini etkileyen diğer siyasi konular da aynı derecede önemlidir. Kapsamlı bir gereksinim analizinin sonuçlarını içeren kapsamlı belgelerin mevcudiyeti, güvenlik politikasının değerlendirilmesinin, son ürünü yüzeysel olarak değerlendirmek yerine, daha derin bir derinliğe ulaşmasını sağlayacaktır. Örneğin, yalnızca politikanın belirli bir alanda uygulanıp uygulanmadığına odaklanmak yerine, değerlendirme artık bu alanın politika içinde nasıl geliştirildiğini de göz önünde bulundurabilir. Belgesel kanıtlar, politikanın hiçbirini sulandırmadan kalkınma içinde belirlenen tüm konuları yeterince kapsayıp kapsamadığını belirlemek için değerlendirilebilir. Bununla birlikte, güvenlik politikaları kuruluşun bağlamına bağlı olarak büyük ölçüde değişir ve gelişimlerinin de değişmesi beklenir. Hedef alanlar ayrılsa bile, politikalar arasında bazı ortaklıklar olacaktır. Bununla birlikte, ürün değerlendirmesinden farklı olarak, güvenlik politikası değerlendirmesinde birçok kriter öznel nitelikte olacaktır. Bunun nedeni, bir politika geliştirmenin ve politikanın uygulandığı ortamın öznel doğasıdır.

5.1. BT Güvenlik Politikalarının Etkinliğinin Korunması

Bilgi teknolojisi veya BT, tartışmasız yüzyılın teknolojisidir. Kesinlikle dünyayı dönüştürdü. Bununla birlikte, BT'nin tüm faydalarıyla birlikte, birçok güvenlik riski de hayatımıza nüfuz etti. Kuruluşlar, iş operasyonlarının kötü niyetli davetsiz misafirlere ve hırsızlara karşı verilere karşı güvende kalmasını sağlamak için etkili bilgi güvenliği ilkeleri tasarlamalıdır. İronik olarak, değişen BT risk ortamına karşı güvenlik politikalarının etkinliğini korumanın mükemmel bir yolu, daha fazla BT kullanmaktır.

BT'nin güvenlik politikalarının etkinliğini koruyabileceği yollardan bazıları şunlardır:

- **Daha iyi risk değerlendirmesi:** Güvenlik riski değerlendirmesi, herhangi bir bilgi güvenliği politikasının tasarlanmasında önemli bir ilk adımdır. Hızla gelişen BT sektöründen kaynaklanan tehditleri ele almak için, BT tek panzehirdir. Riskler sürekli değiştiğinden, yeni tehditleri kontrol altında tutmak için BT bir zorunluluktur. Önceki uyumluluk kayıtlarınıza

dayanarak yeni riskleri kolayca keşfetmenize, risk faktörlerini sıralamanıza ve sınıflandırmanıza ve neden olabileceği zararları değerlendirmenize olanak tanır. Bu nedenle, BT'deki yeni gelişmelerden - iyi ya da kötü - öğrenmek önemlidir. Bu, risk değerlendirmenizi ve bir tehdidin yakın olması durumunda hazırlıklı olmanızı artıracaktır.

- **Daha iyi uyumluluk**: BT, çalışanlarınızın ve kuruluşunuzun yöneticilerinin düzenleyici makamlarla ve kuruluşunuza özgü güvenlik ilkeleriyle ne kadar uyumlu kaldığını izlemenize yardımcı olur. Tek bir yazılım aracılığıyla, erişim yetkilerine, güvensiz veri paylaşımına, güvenli olmayan web gezintisine, yetersiz veri şifrelemesine ve güvenliğinizi ciddi şekilde etkileyebilecek sayısız diğer faktörlere göz kulak olabilirsiniz.
- **Sürekli yükseltme şarttır**: BT dünyası aldığımız her nefeste değiştiğinden, sisteminizi bozabilecek yeni değişiklikler için sürekli tetikte olmalısınız. Siber riskler, siber suçlar ve siber güvenlik dünyasındaki gelişmeleri izleyin. Bilgi güvenliği politikalarınızı ve güvenlik yazılımınızı sık sık ve düzenli olarak yükseltin, çünkü çok hızlı bir şekilde güncelliğini yitirebilirler. Bu şekilde, güvenlik politikalarınızın etkinliğini koruyabilirsiniz.
- **Hızlı azaltma**: Kuruluşunuz potansiyel veri kaybına veya hırsızlığına yol açabilecek yaklaşmakta olan bir güvenlik tehdidiyle karşı karşıyaysa, elinizin altında bir azaltma veya düzeltme planınız olmalıdır. BT, azaltmayı basit ve verimli bir şekilde planlamanıza yardımcı olur. BT ile, güvenlik ilkelerinizi tasarlarken risk azaltma adımlarını farklı potansiyel risklere atayabilir ve bağlayabilirsiniz. Bu, azaltmayı zamanında ve daha etkili hale getirecek, böylece güvenlik politikalarınızın etkinliğini koruyacaktır.
- **Geliştirilmiş hesap verebilirlik**: İnsanlar risklerden, uyumluluktan ve azaltmadan sorumlu ve sorumlu tutulmadığında hiçbir bilgi politikası etkili kalamaz. BT, düzeltici eylemin hesap verebilirliğini sağlamayı kolaylaştırır. Risklerin Görünürlüğünü ve Olgunluk değerlendirmesini, uyumluluğunu ve kuruluşunuzun üstlendiği düzeltme önlemlerini büyük ölçüde artırabilir. Bu, çalışanlarınızın bilgi güvenliği politikalarınızda listelenen adımlara karşı daha hızlı ve daha sorumlu olacağı anlamına gelir.

5.2. Güvenlik Risklerinin Değerlendirilmesi

Risk Değerlendirmesi, hangi bilgi varlıklarının korunacağı belirlendikten sonra risk değerlendirme yöntemi seçilir ve riskler tanımlanır. Seçilen risk değerlendirme yöntemine göre, bilgi varlıkları şekilde gösterilen risk haritası üzerinde konumlandırılır. Değerlendirme yapıldıktan sonra risk değerlendirme haritası, etkisi ve olasılığı yüksek tehditlere yönelik risklerin iyileştirilmesi ve kontrol altına alınması süreçlerini kapsamaktadır. Bilgi varlıklarının risk haritasındaki konumları değişebileceğinden, risk değerlendirme haritası düzenli olarak güncellenmeli ve gerekli önlemler alınmalıdır.

Risk, bir olayın olasılıklarının ve sonucunun birleşimi olarak tanımlanır. Risk yönetiminin bir adımı olan risk değerlendirmesi, risklerin tanımlandığı ve belirlenen bu risklerin etkilerinin ve

önceliklerinin belirlendiği bir süreçtir. Risk yönetimi, kabul edilebilir bir risk düzeyi belirlemek, mevcut riski değerlendirmek, bu riski kabul edilebilir bir düzeye indirmek için gerekli adımları atmak ve bu risk düzeyini korumaktır. Bilgi ve diğer varlıklar, bu varlıklara yönelik tehditler, mevcut sistemdeki güvenlik açıkları ve güvenlik sistemi kontrolleri mevcut riski belirleyen bileşenlerdir. Korunması gereken bilgi veya varlıkların belirlenmesi; bu varlıkların kuruluşlar için ne kadar değerli olduğunun belirlenmesi; bu varlıklara yönelik bilinen ve olası tehditlerden hangilerinin önlenmeye çalışılacağının ortaya konulması; olası kayıpların nasıl meydana gelebileceğini araştırmak; her bir varlığa yönelik olası tehditlerin kapsamını belirlemek; Bu varlıklarda oluşabilecek kayıpların kapsamını ve olasılığını azaltmak için öncelikle neler yapılabileceğinin incelenmesi ve ileriye dönük tehditlerin asgari düzeyde tutulması için atılacak adımların planlanması risk değerlendirmesinin belirli aşamalarıdır. Risk yönetimi sonucunda kurulacak ve uygulanacak güvenlik sisteminin maliyeti de dikkat edilmesi gereken bir diğer önemli konudur. Güvenlik sisteminin maliyeti, korunan bilginin değeri ve olası tehditler incelenerek belirlenen risk ile sınırlandırılmalıdır. %100 güvenliğin olmayacağı ilkesi ile birlikte bilgi güvenliğinin ideal konfigürasyonu üç süreç üzerinden gerçekleştirilmektedir. Bu süreçler önleme, algılama ve yanıttır (yanıt veya reaksiyon).

Önleme; Güvenlik sistemlerinin en çok odaklandığı ve çalıştığı süreçtir. Sistemi, bilgisayar sistemlerine yönelik tehdit ve saldırılara karşı yalıtmak için, bir evin bahçesini çitle çevirmek ve çelik kapı kullanmak gibi günlük hayatta kullanılan güvenlik önlemleri gibi çeşitli önlemler geliştirilmektedir. Kişisel bilgisayar güvenliği ile ilgili olarak, virüs tarama programlarının yüklü olması, bu programların ve işletim sistemi hizmet paketlerinin ve hata düzeltme ve güncellemelerinin düzenli aralıklarla gerçekleştirilmesi, bilgisayarda parola korumalı ekran koruyucu kullanılması, bilgisayardan uzun süre uzak kaldıktan sonra sistemden ayrılması, kullanılan şifrelerin tahmin edilmesi zordur. bu şifreleri belirlemek, gizli tutmak ve düzenli aralıklarla değiştirmek, disk paylaşımı konusunda dikkatli olmak, internetten indirilen veya e-posta ile gönderilen dosyalara dikkat etmek, önemli belgeleri şifre ile korumak veya şifreli tutmak, e-posta ile gizli veya önemli bilgileri, güvenlik sertifikası olmayan siteler. Basit görünebilen, ancak güvenli olmayan yollarla gönderilmemek, kullanılmadığında internet erişimini kapatmak, önemli bilgi ve belgelerin düzenli yedeklerini almak gibi hayat kurtaran önlemlerden bazıları. Kurumsal ortamlarda bilgisayar güvenliğinde uygulanacak önleme adımları daha geniş ve daha karmaşıktır. Güvenlik uzmanlarının çalıştığı bu tür sistemlerde önleme konusunda yapılan bazı şeyler:

- İşletim sistemi ve yazılımların hizmet paketlerini ve güncellemelerini periyodik olarak gözden geçirmek,
- Kullanıcı haklarını minimumda tutmak, kullanılmayan protokol, hizmet, bileşen ve süreçleri çalıştırmamak,
- Veri iletiminde şifreleme teknikleri, güvenlik açığı tarayıcıları,
- Sanal Özel Ağ Kullanma,

- Açık Anahtar Altyapısı ve e-imza kullanımı Biyometrik tabanlı sistemlerin kullanımı olarak sıralanabilir.

Aslında, önleme sürecinde belirlenen ilerleme mükemmel olabilseydi, daha ileri süreçlere hiç ihtiyaç duyulmazdı. Tüm saldırılar en kötü ihtimalle önlenebilirdi. Ancak hiçbir güvenlik ürünü mükemmel veya eksiksiz değildir. Ayrıca hemen hemen her gün iletim sistemlerinde, internet servislerinde, web teknolojilerinde ve güvenlik uygulamalarında çeşitli güvenlik açıkları tespit edilmektedir. Bu açıdan bakıldığında algılama ve eşleştirme süreçlerinin kullanılması artmaktadır.

Algılama; Güvenlik sadece bir önleme meselesi değildir. Örneğin bir müzenin iyi korunmuş olması, etrafının çitlerle çevrili olması, kapıların kapalı ve kilitli olması, o müzede geceleri muhafız kullanılmasını gerektirmez. Aynı şekilde, bilgisayar sistemlerindeki saldırı girişimlerini tespit etmek için yöntemlerin kullanımı da artmaktadır. Önleme, saldırıları daha güçlü (ancak imkansız olmayan) hale getiren veya saldırganları caydıran (ancak yok etmeyen) bir bariyer oluşturmaktır. Tespit ve müdahale olmadan önleme sadece sınırlı bir faydaya sahip olabilir. Sadece önleme yeterli olsaydı, çoğu saldırı bile bilinmeyecekti. Tespit ile daha önce bilinen veya yeni ortaya çıkan saldırılar raporlanabilir ve uygun yanıtlar verilebilir. Algılamada ilk ve en temel adım, sistemin tüm durumunu ve hareketini izlemek ve bu bilgilerin kayıtlarını tutmaktır. Bu şekilde, saldırı sonrası analiz için veri ve kanıtlar da toplanır. Güvenlik duvarları, saldırı tespit sistemleri, ağ trafiği monitörleri, port tarayıcıları, bal küpü kullanımı, gerçek zamanlı koruma virüsü ve casus yazılım araçları, dosya sağlama toplamı kontrol programları ve ağ Sniffer sensörleri algılama sürecinde kullanılan en yaygın yöntemlerden bazılarıdır.

Yanıt (AnswerBack); Muhafızlar, köpekler, güvenlik kameraları, sensörlerle donatılmış bir yerin hırsızların dikkatini çekebilmesi gibi, gerçek zamanlı algılama sistemlerine sahip bilgisayar sistemleri de bilgisayar korsanları ve saldırganlar için caziptir. Hızlı yanıt, bu saldırıları püskürtmek için güvenlik sistemini tamamlayan önemli bir unsur olarak ortaya çıkmaktadır. Yanıt, önleme süreci ile ele alınamayan ve tespit süreçleri ile belirlenen saldırı girişimlerine anında veya en kısa sürede yanıt verecek eylemlerin gerçekleştirilmesi olarak tanımlanabilir. İzinsiz giriş algılama sistemleri, bu algılamaya yanıt verecek biri veya sistem varsa mantıklı olabilir. Aksi takdirde bu durum kimsenin duymadığı ve umursamadığı bir araba alarmının faydasının ötesine geçmez. Bu bakımdan karşılıklılık, güvenlik sürecini tamamlayan önemli bir halkadır. Saldırı tamamen önlenmemiş olsa bile; Sistemin normal durumuna dönmesine, saldırının nedenlerini tespit etmesine, gerektiğinde saldırganı yakalamasına, güvenlik sistemi açıklarını tespit etmesine, önleme, algılama ve müdahale süreçlerini yeniden düzenlemesine olanak tanır. Bir saldırı tespit edildiğinde alınacak aksiyonların önceden planlanması, bu sürecin etkin bir şekilde işlemesini sağlayacak, zaman ve para israfı yaşanmayacaktır. Olağanüstü durum kurtarma, bu aşama için üstlenilen en kötü planların ön saflarında yer almaktadır.

Soru:

Ek olarak verilmiştir.

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

- BT sistemlerinin güvenlik açığı nelerdir
- Güvenlik Açığı Yönetimi ve Risk Yönetimi için açıklama ve örnek verme

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

Başvuru:

1. IS Güvenlik Politikası Geliştirme S.B. Maynard1 & A.B. Ruighaver2 Bilgi Sistemleri Bölümü Melbourne Üniversitesi Avustralya
2. https://www.bizzsecure.com/how-it-can-maintain-the-effectiveness-of-security-policies/
3. https://blog.masterofproject.com/service-asset-and-configuration-management/
4. https://www.apptega.com/blog/change-configuration-management-cybersecurity
5. https://cam.scmagazine.com/it-service-management-vs-cybersecurity-asset-management/
6. http://www2.mitre.org/public/industry-perspective/documents/06-ar-cyber-coop-planning.pdf
7. https://icma.org/articles/pm-magazine/cyber-continuity-planning-go-big-or-go-home
8. https://www.kroll.com/en/services/security-risk-management/security-consulting/threat-vulnerability-assessments
9. https://www.xmcyber.com/blog/what-is-the-difference-between-vulnerability-assessment-and-vulnerability-management/
10. https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis