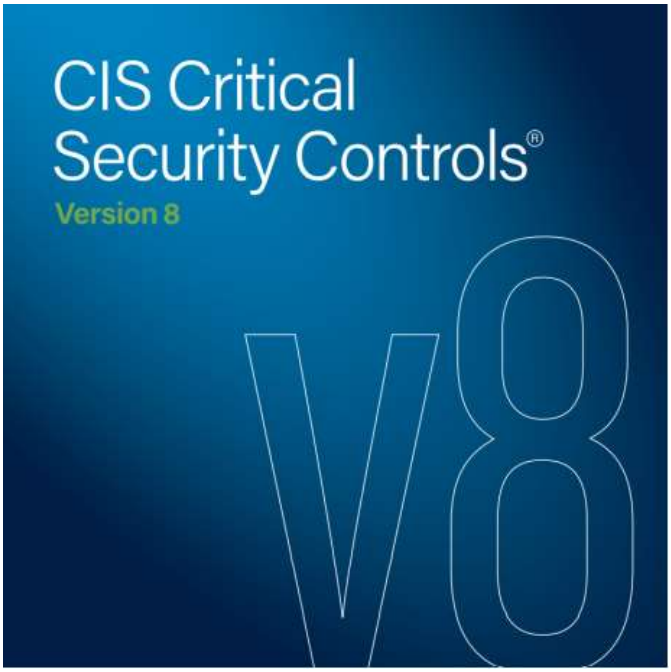

CIS CRITICAL SECURITY CONTROL V8

CIS Critical Security Controls (CIS Controls) , işletmeleri her gün etkileyen en yaygın ve önemli gerçek dünya siber saldırılarını belirlemek , bu bilgi ve deneyimi savunucular için olumlu , yapıcı eyleme dönüştürerek daha geniş kitleyle paylaşan yapıdır. Center for Internet Security® (CIS®) tarafından yönetilen CIS Kontrolleri , şunları gerçekleştiren gönüllü bireyler ve kurumlardan oluşan uluslararası topluluk haline gelmiştir ; Saldırılara ve saldırganlara ilişkin bilgileri paylaşarak temel nedenleri belirleyip bunu savunma eylemi sınıflarına dönüştürmek. Araçlar , çalışma yardımcıları ve benimseme , problem çözme hikayeleri oluşturup paylaşma. Uyum sağlayıp toplu öncelik getirmek ve bunlara odaklanmak için BDT Kontrollerini düzenleyici ve uyumluluk çerçeveleriyle eşleştirme. Ortak sorunları ve engelleri belirleyerek bunları topluluk olarak çözme girişimi.

CIS Kontrollerinin Yapısı ; Saldırıları engelleme , hafifletme veya tanımlamada Kontrolün öneminin açıklaması ve saldırganların Kontrolün yokluğundan nasıl etkin şekilde yararlandığına dair açıklama içerir.

Prosedürler ve araçlar ; Kontrolün uygulanmasını ve otomasyonunu sağlayan süreçlerin ve teknolojilerin daha teknik açıklamasıdır.

18 CIS Kritik Güvenlik Kontrolü ; Eskiden SANS Kritik Güvenlik Kontrolleri (SANS İlk 20) artık resmi olarak CIS Kritik Güvenlik Kontrolleri (CIS Kontrolleri) olarak adlandırılmaktadır. CIS Kontrolleri Sürüm 8 , cihazları kimin yönettiğinden ziyade faaliyetlere göre CIS Kontrollerini birleştirmektedir. Fiziksel cihazlar , sabit sınırlar ve ayrı güvenlik uygulama adaları daha az önemlidir. V8'de revize edilmiş terminoloji ve Koruma Önlemlerinin gruplandırılması yoluyla yansıtılır ve Kontrol sayısının 20'den 18'e düşmesine neden olmuştur.

CIS Kritik Güvenlik Uygulama Grubları ;

IG1 ; IG1 kuruluşu , BT varlıklarını ve personelini korumaya yönelik sınırlı BT ve siber güvenlik uzmanlığına sahip küçük ve orta ölçeklidir. Bu işletmelerin temel kaygısı , kesinti süresine karşı sınırlı toleransa sahip oldukları için işi çalışır durumda tutmaktır. Korumaya çalıştıkları verilerin hassasiyeti düşüktür ve esas olarak çalışan ve finansal bilgileri çevreler. IG1 için seçilen koruma önlemleri , sınırlı siber güvenlik uzmanlığı ile uygulanabilir olmalı ve genel , hedeflenmemiş saldırıları engellemeyi amaçlamalıdır. Bu korumalar tipik olarak küçük veya ev ofis ticari kullanıma hazır (COTS) donanım ve yazılımlarla birlikte çalışacak şekilde tasarlanacaktır.

IG2 (IG1'i içermektedir) ; IG2 kuruluşu , BT altyapısını yönetmekten ve korumaktan sorumlu kişileri istihdam eder. Bu kuruluşlar , iş işlevine ve misyonuna göre farklı risk profillerine sahip birden fazla departmanı destekler. Küçük işletme birimlerinin yasal uyumluluk yükleri olabilir. IG2 kuruluşları , genelde hassas müşteri veya kurumsal bilgileri depolayarak işler ve kısa hizmet kesintilerine dayanabilir. Önemli bir endişe de ihlal meydana gelirse kamu güveninin kaybıdır. IG2 için seçilen koruma önlemleri , güvenlik ekiplerinin artan operasyonel karmaşıklıkla başa çıkmasına yardımcı olur. Bazı koruma önlemleri , doğru şekilde kurmak ve yapılandırmak için kurumsal düzeyde teknolojiye ve özel uzmanlığa bağlı olacaktır.

IG3 (IG1 ve IG2'yi içermektedir) ; IG3 kuruluşu , siber güvenliğin farklı yönlerinde (risk yönetimi , sızma testi , uygulama güvenliği) uzmanlaşmış güvenlik uzmanları kullanır. IG3 varlıkları ve verileri , düzenleyici ve uyumluluk denetimine tabi olan hassas bilgiler veya işlevler içerir. IG3 kuruluşu , hizmetlerin kullanılabilirliğini ve hassas verilerin gizliliği ile bütünlüğünü ele almalıdır. Başarılı saldırılar , kamu refahına önemli zararlar verebilir. IG3 için seçilen koruma önlemleri , gelişmiş düşmandan gelen hedefli saldırıları azaltmalı ve sıfır gün saldırılarının etkisini azaltmalıdır.

CIS Kritik Güvenlik Kontrolü 1 - Envanter ve Kontrol Kurumsal Varlıklar ; Altyapıya fiziksel , sanal olarak bağlı tüm kurumsal varlıkları (taşınabilir ve mobil de dahil olmak üzere son kullanıcı cihazları , ağ cihazları , bilgi işlem dışı / Nesnelerin İnterneti (IoT) cihazları , sunucular) aktif olarak yöneterek kurum içinde izlenmesi ve korunması gereken varlıkların toplamını doğru şekilde bilmektir. Kaldırılacak veya düzeltilecek yetkisiz ve yönetilmeyen varlıkların belirlenmesini de destekleyecektir. İşletmeler sahip olduklarını bilmediklerini savunamazlar. Tüm kurumsal varlıkların yönetilen kontrolü , güvenlik izleme , olay müdahalesi , sistem yedekleme ve kurtarmada da kritik rol oynar. Kuruluşlar , kendileri için hangi verilerin kritik olduğunu bilmelidir ve uygun varlık yönetimi , uygun güvenlik kontrollerinin uygulanabilmesi için bu kritik verileri tutan veya yöneten kurumsal varlıkları belirlemeye yardımcı olacaktır. Harici saldırganlar , şirket ağına bağlı veya bulutta , hedef kuruluşların internet adres alanını sürekli olarak tarayarak kuruluşun ağına bağlı korumasız varlıkları belirler. Saldırganlar , yüklenen ancak güvenli şekilde yapılandırılmamış , yama uygulanmamış yeni varlıklardan yararlanabilir. Dahili olarak , tanımlanamayan varlıklar , onları web veya e-posta tabanlı kötü amaçlı yazılımlara karşı savunmasız hale getirebilecek zayıf güvenlik yapılandırmalarına da sahip olabilir ve saldırganlar , bir kez içeri girdikten sonra ağda gezinmek için zayıf güvenlik yapılandırmalarından yararlanabilir. Kuruluşun ağına bağlanan ek varlıklar (gösterim sistemleri , geçici test sistemleri , konuk ağları) , düşmanca erişimin kurumsal operasyonların güvenliğini etkilemesini önlemek için tanımlanmalı veya izole edilmelidir. Büyük , karmaşık , dinamik kuruluşlar , karmaşık , hızlı değişen ortamları yönetme zorluğuyla anlaşılır şekilde mücadele etmektedir. Fakat saldırganlar , fırsatlarını desteklemek için kurumsal varlıklarımızı çok büyük ölçekte envanter e kontrol etme becerisini , sabrını ve istekliliğini göstermişlerdir.

Diğer bir zorluk da taşınabilir son kullanıcı cihazlarının periyodik olarak bir ağa katılması ve sonrasında ortadan kaybolmasıyla mevcut varlıkların envanterini çok dinamik hale getirmiştir. Benzer şekilde , bulut ortamları ve sanal makineler , kapatıldıklarında veya duraklatıldıklarında varlık envanterlerinde takip edilmesi zor olabilir. Eksiksiz kurumsal varlık yönetiminin bir başka yararı ise hem ağdaki bir varlıktan ağ trafiğinin kaynağını araştırırken hem de olay sırasında benzer türdeki veya konumdaki potansiyel olarak savunmasız , etkilenen tüm varlıkları belirlerken olay yanıtını desteklemektir.

Prosedürler ve araçlar ; Yaşam döngüsü boyunca kurumsal varlıkların ve ilgili tüm verilerin envanterini oluşturan ve yöneten süreçte birleştirilmiş hem teknik hem de prosedürel eylemleri gerektirir. İş sürecinin her bir bileşeninden sorumlu olan veri / varlık sahipleri oluşturarak iş yönetişimiyle de bağlantı kurar. Kuruluşlar , BT varlık envanterlerini korumak için büyük ölçekli , kapsamlı kurumsal ürünler kullanabilir. Daha küçük kuruluşlar , bu verileri toplamak için kurumsal varlıklara önceden kurulmuş veya ağda kullanılan güvenlik araçlarından yararlanabilir. Güvenlik açığı tarayıcısıyla ağın keşif taraması yapmayı içererek kötü amaçlı yazılımdan koruma günlüklerini , uç nokta güvenlik portallarındaki günlükleri , anahtarlardan gelen ağ günlüklerini , kimlik doğrulama günlüklerini gözden geçirme , sonuçları elektronik tablo veya veritabanında yönetmeyi sağlayabiliriz.

Kurumsal varlıkların güncel ve doğru görünümünü sürdürmek , devam eden ve dinamik süreçtir. Kurumsal varlıklar her zaman BT departmanı tarafından sağlanmadığından veya kurulmadığından , kuruluşlar için bile nadiren tek gerçek kaynağı vardır. Gerçek şu ki , kurumsal varlıkların yüksek güvenilir sayısını belirlemek için çeşitli kaynakların kitle kaynaklı olması gerekir. Kuruluşlar , ağa bağlı varlıkları tanımlamak için çeşitli farklı paket türleri göndererek düzenli olarak aktif olarak tarama yapabilir. Küçük işletmeler için belirtilen varlık kaynaklarına ek olarak , daha büyük işletmeler , bulut portallarından ve kurumsal platformlardan günlüklerden veri toplayabilir ; Active Directory (AD) , Tekli Oturum Açma (SSO) , Çok Faktörlü Kimlik Doğrulama (MFA) , Sanal Özel Ağ (VPN) , Saldırı Tespit Sistemleri (IDS) , Derin Paket Denetimi (DPI) , Mobil Cihaz Yönetimi (MDM) ve güvenlik açığı tarama araçları. Mülk envanteri veritabanları , satınalma siparişi takibi ve yerel envanter listeleri , hangi cihazların bağlı olduğunu belirleyen diğer veri kaynaklarıdır. Bu kaynaklar arasında benzersiz olan cihazları tanımlamak için bu verileri normalleştiren araçlar ve yöntemler vardır.

Kaynak ; CIS Controls Cloud

Alınacak Güvenlik önlemleri ;

1.1 - Ayrıntılı Kurumsal Varlık Envanteri Oluşturup Bakımını Yapma ; Son kullanıcı cihazları (taşınabilir ve mobil dahil) , ağ cihazları , bilgi işlem dışı / IoT dahil olmak üzere , veri depolama veya işleme potansiyeline sahip tüm kurumsal varlıkların doğru , ayrıntılı ve güncel envanterini oluşturun ve sürdürmek önemlidir. Envanterin ağ adresini (statikse) , donanım adresini , makine adını , kurumsal varlık sahibini , her varlık için departmanını ve varlığın ağa bağlanmak için onaylanıp onaylanmadığını kaydettiğinden emin olunuz. Mobil son kullanıcı cihazları için uygun olduğunda MDM tipi araçlar bu süreci destekleyebilir. Bu envanter , altyapıya fiziksel , sanal , uzaktan ve bulut ortamlarındaki varlıkları içerir. İşletmenin kontrolünde olmasa bile işletmenin ağ altyapısına düzenli olarak bağlanan varlıkları içerir. Tüm kurumsal varlıkların envanterini iki yılda bir veya daha sık gözden geçirin ve güncelleyiniz.

1.2 - Yetkisiz Varlıkların Adresi ; Yetkisiz varlıkları haftalık olarak ele almak için bir sürecin var olduğundan emin olunuz. Kuruluş , varlığı ağdan kaldırmayı , varlığın ağa uzaktan bağlanmasını engellemeyi veya varlığı karantinaya almayı seçebilir.

1.3 - Aktif Keşif Aracını Kullanma ; Kuruluşun ağına bağlı varlıkları belirlemek için aktif keşif aracı kullanın. Etkin keşif aracını günlük veya daha sık çalışacak şekilde yapılandırınız.

1.4 - Kurumsal Varlık Envanterini Güncellemek için DHCP Günlüğünü Kullanma ; Kuruluşun varlık envanterini güncellemek için tüm DHCP sunucularında veya İnternet Protokolü (IP) adres yönetim araçlarında DHCP günlüğünü kullanınız. Kuruluşun varlık envanterini haftalık veya daha sık güncellemek için günlükleri inceleyin ve kullanınız.

1.5 - Pasif Varlık Keşif Aracı Kullanma ; Kuruluşun ağına bağlı varlıkları belirlemek için pasif keşif aracı kullanınız. Kuruluşun varlık envanterini en az haftada bir veya daha sık güncellemek için taramaları gözden geçirin ve kullanınız.

CIS Kritik Güvenlik Kontrolü 2 : Yazılım Varlıklarının Envanteri ve Kontrolü ; Ağdaki tüm yazılımları (işletim sistemleri ve uygulamaları) etkin şekilde yöneterek sadece yetkilendirilmiş yazılımlar kurulur ve çalıştırılır , yetkisiz ve yönetilmeyen yazılımlar bulunarak kurulum veya yürütmenin engellenmesi sağlanır. Eksiksiz yazılım envanteri , saldırıları önlemek için kritik temeldir. Saldırganlar , uzaktan yararlanılabilecek yazılımların savunmasız sürümlerini arayan hedef kuruluşları sürekli olarak tararlar. Kullanıcı güvenlik açığı bulunan tarayıcıyla kötü amaçlı web sitesi veya ek açarsa , saldırgan genelde saldırgana sistemin uzun vadeli kontrolünü veren arka kapı programlar ile botlar yükleyebilir. Saldırganlar bu erişimi ağda yanlamasına hareket etmek için de kullanabilir. Bu saldırılara karşı en önemli savunmalardan biri yazılımı güncellemek ve yama yapmaktır. Yazılım varlıklarının eksiksiz envanteri olmadan kuruluş , savunmasız yazılımlara sahip olup olmadığını veya olası lisans ihlalleri olup olmadığını belirleyemez. Yama henüz mevcut olmasa bile , eksiksiz yazılım envanter listesi , bir kuruluşun yama yayınlanana kadar bilinen saldırılara karşı koruma sağlamasına olanak tanır. Bazı gelişmiş saldırganlar , yazılım satıcısından henüz düzeltme eki yayınlamamış olan ve önceden bilinmeyen güvenlik açıklarından yararlanan " sıfır gün açıklarından yararlanma " kullanır. İstismarın ciddiyetine bağlı olarak , kuruluş , yama yayınlanana kadar saldırılara karşı korunmak için geçici azaltma önlemleri uygulayabilir. Yazılım varlıklarının yönetimi , gereksiz güvenlik risklerini belirlemek için de önemlidir. Kuruluş , iş amaçları için gerekli olmayan yazılım çalıştıran kurumsal varlıkları belirlemek için yazılım envanterini gözden geçirmelidir. Kurumsal varlık , potansiyel güvenlik riski oluşturan ve kuruluşa hiçbir fayda sağlamayan varsayılan yazılımlarla birlikte yüklenmiş olarak gelebilir. Bir kurumun altyapısına bağlı tüm yazılımların envanterini çıkarmak , anlamak , değerlendirmek , yönetmek çok önemlidir.

Prosedürler ve araçlar ; İzin verilenler listesi , ticari izin verilenler listesine ekleme araçları , politikaları veya kötü amaçlı yazılımdan koruma paketleri ve popüler işletim sistemleriyle birlikte gelen uygulama yürütme araçlarının kombinasyonu kullanılarak uygulanabilir. Ticari yazılım envanter araçları günümüzde birçok işletmede yaygın olarak bulunmakta ve kullanılmaktadır. Bu araçların en iyileri , işletmelerde kullanılan yüzlerce yaygın yazılımın envanter kontrolünü sağlar. Araçlar , en son sürüm olduğundan emin olmak ve Ortak Platform Numaralandırma (CPE) belirtiminde bulunanlar gibi standartlaştırılmış uygulama adlarından yararlanmak için yüklü her programın yama düzeyi hakkında bilgi alır. Kullanılabilecek yöntem örneği , Güvenlik İçeriği Otomasyon Protokolü'dür (SCAP). İzin verilenler listesini uygulayan özellikler , birçok modern uç nokta güvenlik paketine dahil edilmiştir ve büyük işletim sistemlerinin belirli sürümlerinde yerel olarak uygulanmaktadır. Ticari çözümler giderek artan şekilde kötü amaçlı yazılımdan koruma , casus yazılımdan koruma , kişisel güvenlik duvarı , host bilgisayar tabanlı IDS , İzinsiz Girişi Önleme Sistemi (IPS) ile birlikte uygulamaya izin verme ve engelleme listelemeyi bir araya getirmektedir. Özellikle , çoğu uç nokta güvenlik çözümü , uygulamanın korumalı makinede çalışmasına izin verilip verilmeyeceğini belirlemek için yürütülebilir dosyanın adına , dosya sistemi konumuna veya kriptografik hash değerine bakabilir. Bu araçların en etkilisi , yürütülebilir yol , hash veya normal ifade eşleşmesine dayalı özel izin verilenler listeleri sunar. Bazıları , yöneticilerin belirli kullanıcılar için ve günün belirli saatlerinde belirli yazılımların yürütülmesi için kurallar tanımlamasına olanak tanıyan , kötü amaçlı olmayan ancak onaylanmamış uygulama işlevi içerir.

Alınacak Güvenlik Önlemleri ;

2.1 - Yazılım Envanteri Oluşturup Bakımını Yapma; Kurumsal varlıklara kurulu tüm lisanslı yazılımların ayrıntılı envanterini oluşturun ve sürdürünüz. Yazılım envanteri , her giriş için başlığı , yayıncıyı , ilk kurulum / kullanım tarihini , iş amacını belgelemelidir.

Uygun olduğunda , Tekdüzen Kaynak Bulucu (URL) , uygulama mağaza , sürüm , dağıtım mekanizması ve kullanımdan kaldırma tarihini ekleyiniz. Yazılım envanterini yılda iki kez veya daha sık gözden geçirin ve güncelleyiniz.

2.2 - Yetkili Yazılımın Şu Anda Desteklendiğinden Emin Olma ; Kurumsal varlıklar için yazılım envanterinde sadece şu anda desteklenen yazılımın yetkili olarak belirlendiğinden emin olunuz. Yazılım desteklenmiyorsa ancak kuruluşun misyonunun yerine getirilmesi için gerekliyse , hafifletici kontrolleri ve artık risk kabulünü ayrıntılandıran istisna belgeleyin. İstisna belgesi olmayan desteklenmeyen yazılım için yetkisiz olarak atayınız. Yazılım desteğini en az ayda bir veya daha sık doğrulamak için yazılım listesini gözden geçiriniz.

2.3 - Yetkisiz Yazılımın Adresi ; Yetkisiz yazılımın kurumsal varlıklarda kullanımdan kaldırıldığından veya belgelenmiş istisna aldığından emin olunuz. Aylık veya daha sık gözden geçiriniz.

2.4 - Otomatikleştirilmiş Yazılım Envanteri Araçlarından Yararlanma ; Kurulu yazılımların keşfini ve dokümantasyonunu otomatikleştirmek için mümkün olduğunda kuruluş genelinde yazılım envanter araçlarını kullanınız.

2.5 - İzin Verilenler Listesindeki Yetkili Yazılım ; Sadece yetkili yazılımın çalıştırılabilmesini veya erişilebilmesini sağlamak için izin verilenler listesine uygulama gibi teknik kontrolleri kullanınız. İki yılda bir veya daha sık yeniden değerlendiriniz.

2.6 - İzin Verilen Yetkili Kütüphaneler ; Sadece belirli .dll , .ocx , .so vb. dosyaların bir sistem işlemine yüklenmesine izin verildiğinden emin olmak için teknik kontrolleri kullanınız. Yetkisiz kitaplıkların sistem işlemine yüklenmesini engelleyiniz. İki yılda bir veya daha sık yeniden değerlendiriniz.

2.7 - İzin Verilenler Listesi Yetkili Komut Dosyaları ; Sadece belirli .ps1 , .py vb. dosyalar gibi yetkili komut dosyalarının yürütülmesine izin verildiğinden emin olmak için dijital imzalar ve sürüm denetimi gibi teknik denetimleri kullanınız. Yetkisiz komut dosyalarının yürütülmesini engelleyiniz. İki yılda bir veya daha sık yeniden değerlendiriniz.

CIS Kritik Güvenlik Kontrolü 3 - Veri Koruma ; Verileri tanımlamak , sınıflandırmak , güvenli şekilde işlemek , saklamak ve elden çıkarmak için süreçler ve teknik kontroller geliştiriniz. Veriler artık yalnızca bir işletmenin sınırları içinde yer almıyor ; bulutta , kullanıcıların evden çalıştığı taşınabilir son kullanıcı cihazlarında bulunur ve genellikle dünyanın herhangi bir yerinde bulunabilecek ortaklarla veya çevrimiçi hizmetlerle paylaşılır. Bir işletmenin finans , fikri mülkiyet ve müşteri verileriyle ilgili olarak elinde bulundurduğu hassas verilere ek olarak , kişisel verilerin korunmasına yönelik çok sayıda uluslararası düzenleme de olabilir. Veri gizliliği giderek daha önemli hale gelerek şirketler , gizliliğin yalnızca şifreleme değil , verilerin uygun kullanımı ve yönetimi ile ilgili olduğunu öğrenmektedir. Veriler , tüm yaşam döngüsü boyunca uygun şekilde yönetilmelidir. Bu gizlilik kuralları , her büyüklükteki çok uluslu işletmeler için karmaşık olabilir fakat herkes için geçerli olabilecek temeller vardır. Saldırganlar bir kuruluşun altyapısına girdikten sonra ilk görevlerinden biri verileri bulmak ve sızdırmaktır. Kuruluşlar , veri çıkışlarını izlemedikleri için hassas verilerin ortamlarından ayrıldığının farkında olmayabilir. Ağ üzerinde birçok saldırı gerçekleşirken , diğerleri taşınabilir son kullanıcı cihazlarının fiziksel olarak çalınmasını , hizmet sağlayıcılara veya hassas verileri tutan diğer ortaklara yönelik saldırıları içerir. Diğer hassas kurumsal varlıklar , Denetleyici Kontrol ve Veri Toplama (SCADA) sistemleri gibi fiziksel sistemlerin yönetimini ve kontrolünü sağlayan bilgi işlem dışı cihazları da içerebilir. Kuruluşun korunan veya hassas veriler üzerindeki kontrolünü kaybetmesi , ciddi ve genellikle rapor edilebilir iş etkisidir. Hırsızlık veya casusluk sonucunda bazı veriler tehlikeye girer veya kaybolurken , büyük çoğunluğu yetersiz anlaşılan veri yönetimi kuralları ve kullanıcı hatasının sonucudur. Hem aktarım sırasında hem de kullanımda olmayan veri şifrelemesinin benimsenmesi , veri güvenliğinin ihlal edilmesini azaltabilir ve daha da önemlisi , çoğu kontrol edilen veri için düzenleyici gerekliliktir.

Prosedürler ve Araçlar ; Bir kuruluşun , veri yönetimi çerçevesi , veri sınıflandırma yönergeleri ve verilerin korunması , işlenmesi , saklanması ve elden çıkarılması için gereksinimleri içeren veri yönetimi süreci geliştirmesi önemlidir. Olay müdahale planına ve uyumluluk , iletişim planlarına bağlanan veri ihlali süreci olmalıdır. Veri duyarlılığı düzeylerini elde etmek için kuruluşların , temel veri türlerini ve kuruluş için genel kritikliği kataloglaması gerekir. Bu analiz , işletme için genel veri sınıflandırma şeması oluşturmak için kullanılacaktır. İşletmeler " Hassas " , " Gizli " , " Genel " gibi etiketler kullanabilir ve verilerini bu etiketlere göre sınıflandırabilir. Verilerin hassasiyeti tanımlandıktan sonra , çeşitli hassasiyet seviyelerinde verilere erişen yazılımları ve bu uygulamaları barındıran kurumsal varlıkları tanımlayan veri envanteri veya eşlemesi geliştirilmelidir. İdeal olarak , ağ , aynı hassasiyet seviyesindeki kurumsal varlıkların aynı ağ üzerinde olması ve farklı hassasiyet seviyelerine sahip kurumsal varlıklardan ayrılması için ayrılmalıdır. Mümkünse , güvenlik duvarlarının her segmente erişimi kontrol etmesi ve yalnızca işletme ihtiyacı olanların verilere erişmesine izin vermek için kullanıcı erişim kurallarının uygulanması gerekir.

Kaynak ; NIST SP 800-88r1 Guides for Media Sanitization , NIST® FIPS 140-2 , NIST® FIPS 140-3 .

Alınacak Güvenlik Önlemleri ;

3.1 - Veri Yönetim Süreci Oluşturma ve Sürdürme ; Veri yönetimi süreci oluşturun ve sürdürünüz. Süreçte , kurum için hassasiyet ve saklama standartlarına dayalı olarak veri hassasiyetini , veri sahibini , verilerin işlenmesini , veri saklama limitlerini ve elden çıkarma gerekliliklerini ele alınız. Belgeleri yıllık olarak veya korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyiniz.

3.2 - Veri Envanterinin Oluşturulması ve Sürdürülmesi ; Kuruluşun veri yönetimi sürecine dayalı olarak veri envanteri oluşturun ve sürdürünüz. En azından envantere duyarlı verilerdir. Envanteri , hassas verilere öncelik vererek , en azından yıllık olarak gözden geçirin ve güncelleyiniz.

3.3 - Veri Erişim Kontrol Listelerini Yapılandırma ; Kullanıcının bilme ihtiyacına göre veri erişim kontrol listelerini yapılandırınız. Erişim izinleri olarak da bilinen veri erişim kontrol listelerini yerel ve uzak dosya sistemlerine , veritabanlarına ve uygulamalara uygulayınız.

3.4 - Veri Saklamayı Zorlama ; Verileri , kurumun veri yönetimi sürecine göre saklayınız. Veri saklama hem minimum hem de maksimum zaman çizelgelerini içermelidir.

3.5 - Verilerin Güvenli Şekilde İmha Edilmesi ; Verileri , kurumun veri yönetimi sürecinde belirtildiği şekilde güvenli şekilde elden çıkarınız. Bertaraf süreci ve yönteminin veri hassasiyetiyle orantılı olduğundan emin olunuz.

3.6 - Son Kullanıcı Cihazlarındaki Verileri Şifreleyin ; Hassas veriler içeren son kullanıcı cihazlarındaki verileri şifreleyiniz. Örnek uygulamalar şunları içerebilir ; Windows BitLocker , Apple FileVault , Linux dm-crypt.

3.7 - Belge Veri Akışları ; Veri akışı belgeleri , hizmet sağlayıcı veri akışlarını içerir ve kuruluşun veri yönetimi sürecini temel almalıdır. Belgeleri yıllık olarak veya korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyiniz.

3.8 - Çıkarılabilir Ortamdaki Verileri Şifreleyin ; Çıkarılabilir ortamdaki verileri şifreleyiniz.

3.9 -Geçiş Halindeki Hassas Verileri Şifreleyin ; Aktarılan hassas verileri şifreleyiniz. Örnek uygulamalar şunları içerebilir ; Aktarım Katmanı Güvenliği (TLS) ve Açık Güvenli Kabuk (OpenSSH).

3.10 - Bekleyen Hassas Verileri Şifreleyin ; Hassas verileri içeren sunucularda , uygulamalarda ve veritabanlarında bekleyen hassas verileri şifreleyiniz. Sunucu tarafı şifreleme olarak da bilinen depolama katmanı şifrelemesi , korumanın minimum gereksinimini karşılar. Ek şifreleme yöntemleri , veri depolama aygıtına / cihazlarına erişimin düz metin verilerine erişime izin vermediği durumlarda , istemci tarafı şifreleme olarak da bilinen uygulama katmanı şifrelemesini içerebilir.

3.11 - Hassasiyete Dayalı Segment Veri İşleme ve Saklama ; Yerinde veya uzak hizmet sağlayıcıda bulunanlar da dahil olmak üzere kurumsal varlıklar aracılığıyla depolanan , işlenen veya iletilen tüm hassas verileri belirlemek , kuruluşun hassas verilerini güncellemek için Host bilgisayar tabanlı Veri Kaybını Önleme (DLP) aracı gibi otomatik araç uygulayın envanter.

3.12 - Veri Kaybını Önleme Çözümü Dağıtın ; Yerinde veya uzak hizmet sağlayıcıda bulunanlar da dahil olmak üzere kurumsal varlıklar aracılığıyla depolanan , işlenen veya iletilen tüm hassas verileri belirlemek , kuruluşun hassas verilerini güncellemek için host bilgisayar tabanlı Veri Kaybını Önleme (DLP) aracı gibi otomatik araç uygulayın envanter.

3.13 - Günlüğe Duyarlı Veri Erişimi ; Değişiklik ve imha dahil olmak üzere hassas veri erişimini günlüğe kaydediniz.

CIS Kritik Güvenlik Kontrolü 4 - Kurumsal Varlıkların ve Yazılımın Güvenli Yapılandırması ; Kurumsal varlıkların ve yazılımların güvenli yapılandırmasını oluşturun ve sürdürünüz. Üreticilerden ve satıcılardan teslim edildiği gibi , kurumsal varlıklar ve yazılımlar için varsayılan yapılandırmalar normalde güvenlikten ziyade dağıtım ve kullanım kolaylığına yöneliktir. Temel kontroller , açık hizmetler ve bağlantı noktaları , varsayılan hesaplar veya parolalar , önceden yapılandırılmış Etki Alanı Adı Sistemi (DNS) ayarları , daha eski (savunmasız) protokoller , gereksiz yazılımların önceden yüklenmesi , varsayılan durumlarında bırakılırsa tümü kötüye kullanılabilir. Güvenlik yapılandırma güncellemelerinin kurumsal varlıkların ve yazılımların yaşam döngüsü boyunca yönetilmesi ve sürdürülmesi gerekir. Uyumluluk açısından gözden geçirilebilecek , olay müdahalesi için yararlanılabilecek kayıt tutmak ve denetimleri desteklemek için yapılandırma güncellemelerinin izlenmesi , yapılandırma yönetimi iş akışı süreci aracılığıyla onaylanması gerekir. CIS Kontrolü , şirket içi cihazların yanı sıra uzak cihazlar , ağ cihazları ve bulut ortamları için önemlidir. Hizmet sağlayıcılar , özellikle küçük işletmeler için modern altyapılarda önemli rol oynamaktadır. Müşterilerine kendi güvenlik politikalarını uygulama esnekliği sağlamak için genelde en güvenli yapılandırmada varsayılan olarak kurulmazlar. Varsayılan yapılandırmalarda varsayılan hesapların veya parolaların varlığı , aşırı erişim veya gereksiz hizmetler yaygındır. Bunlar , hizmet sağlayıcıdan ziyade yazılımı kullanan kuruluşun sorumluluğunda olan zayıflıkları ortaya çıkarabilir. Bazı Hizmet Olarak Platform (PaaS) yalnızca işletim sistemini kapsadığından , devam eden yönetim ve güncellemeleri de kapsar. Bu nedenle barındırılan uygulamalara yama uygulama ve güncelleme işlemleri işletmenin sorumluluğundadır. Güçlü başlangıç yapılandırması geliştirilip uygulandıktan sonra bile , yazılım güncellenirken veya yama yapılırken , yeni güvenlik açıkları rapor edilirken ve yapılandırmalar yeni yazılımın yüklenmesine izin vermek veya desteklemek için ince ayar yapılırken güvenliğin düşmesini önlemek için sürekli olarak yönetilmelidir.

Prosedürler ve Araçlar ; Her sistem için birçok kullanılabilir güvenlik temel çizgisi vardır. Kuruluşlar , herkese açık olarak geliştirilmiş , incelenmiş ve desteklenen bu güvenlik kıyaslamaları, güvenlik kılavuzları veya kontrol listeleriyle başlamalıdır. İşletmeler , kurumsal güvenlik politikalarını ve endüstri ve devlet düzenleyici gereksinimlerini karşılamak için bu temelleri artırmalı veya ayarlamalıdır. Gelecekteki incelemeleri veya denetimleri kolaylaştırmak için standart konfigürasyonlardaki ve gerekçelerdeki sapmalar belgelenmelidir. Daha büyük veya daha karmaşık kuruluş için kurumsal varlık üzerindeki verilerin güvenlik gereksinimlerine veya sınıflandırmasına dayalı olarak birden çok güvenlik temel yapılandırması olacaktır. Güvenli temel görüntü oluşturma adımlarına örnek verecek olursak ; Kurumsal varlıkta işlenen / depolanan verilerin risk sınıflandırmasını belirleyin (Yüksek , orta , düşük risk). Kurumsal varlıkta kullanılan verileri korumaya yönelik gereksinimleri karşılayacak şekilde sistem güvenlik ayarlarını belirleyen bir güvenlik yapılandırması komut dosyası oluşturun. Karşılaştırma ölçütlerini kullanın. Temel işletim sistemi yazılımını yükleyin. Uygun işletim sistemi ve güvenlik yamalarını uygulayın. Uygun uygulama yazılım paketlerini , aracı ve yardımcı programları kurun. Yüklenen yazılıma uygun güncellemeleri uygulayın. Bu görüntüye yerel özelleştirme komut dosyalarını yükleyin. Uygun güvenlik düzeyini ayarlamak için oluşturulan güvenlik komut dosyasını çalıştırın. Temel görüntünün sistem ayarını kaydetmek / puanlamak için SCAP uyumlu araç çalıştırın. Güvenlik kalite güvence testi yapın. Bu temel görüntüyü güvenli bir yere kaydedin. CIS Yapılandırma Değerlendirme Aracı (CIS-CAT®) gibi ticari veya ücretsiz yapılandırma yönetimi araçları bu web sitesinden bulabilirsiniz. Ticari yapılandırma yönetimi araçları , yönetilen her sistemde yüklü bir aracının bir kombinasyonunu veya yönetici kimlik bilgilerini kullanarak her kurumsal varlıkta uzaktan oturum açarak sistemlerin aracısız denetimini kullanır. Bazen uzak oturumun başlatıldığı , tarama için hedef sisteme geçici veya dinamik bir ajanın yerleştirildiği ve ardından ajanın kaldırıldığı bir hibrit yaklaşım kullanılır.

Alınacak Güvenlik Önlemleri ;

4.1 - Güvenli Yapılandırma Süreci Oluşturma ve Sürdürme; Kurumsal varlıklar ve yazılımlar için güvenli yapılandırma süreci oluşturun ve sürdürünüz. Belgeleri yıllık olarak veya korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyiniz.

4.2 - Ağ Altyapısı için Güvenli Yapılandırma Süreci Oluşturma ve Sürdürme ; Ağ cihazları için güvenli yapılandırma süreci oluşturun ve sürdürünüz. Belgeleri yıllık olarak veya korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyiniz.

4.3 - Kurumsal Varlıklarda Otomatik Oturum Kilitlemeyi Yapılandırma ; Tanımlanmış etkinlik dışı kalma süresinden sonra kurumsal varlıklarda otomatik oturum kilitlemeyi yapılandırınız. Genel amaçlı işletim sistemlerinde süre 15 dakikayı geçmemelidir. Mobil son kullanıcı cihazlarında süre 2 dakikayı geçmemelidir.

4.4 - Sunucularda Güvenlik Duvarı Uygulamak ve Yönetmek ; Desteklendiği yerlerde sunucularda güvenlik duvarı uygulayın ve yönetiniz. Örnek uygulamalar arasında sanal güvenlik duvarı , işletim sistemi güvenlik duvarı veya üçüncü taraf güvenlik duvarı aracısı bulunur.

4.5 - Son Kullanıcı Cihazlarında Güvenlik Duvarı Uygulamak ve Yönetmek ; Son kullanıcı cihazlarında host bilgisayar tabanlı güvenlik duvarı veya bağlantı noktası filtreleme aracı uygulayın ve yönetin ve bu araç , açıkça izin verilen hizmetler ve bağlantı noktaları dışındaki tüm trafiği bırakan varsayılan reddet kuralıyla.

4.6 - Kurumsal Varlıkları ve Yazılımları Güvenle Yönetin ; Kurumsal varlıkları ve yazılımları güvenli şekilde yönetiniz. Örnek uygulamalar , sürüm kontrollü kod olarak altyapı aracılığıyla yapılandırmayı yönetmeyi ve Güvenli Kabuk (SSH) , Güvenli Köprü Metni Aktarım Protokolü (HTTPS) gibi güvenli ağ protokolleri üzerinden yönetici arabirimlerine erişmeyi içerir. Operasyonel olarak gerekli olmadıkça Telnet ve HTTP gibi güvenli olmayan yönetim protokollerini kullanmayınız.

4.7 - Kurumsal Varlıklar ve Yazılımlardaki Varsayılan Hesapları Yönetme ; Kök , yönetici ve diğer önceden yapılandırılmış satıcı hesapları gibi kurumsal varlıklar ve yazılımlardaki varsayılan hesapları yönetiniz. Örnek uygulamalar şunları içerebilir ; varsayılan hesapları devre dışı bırakmak veya kullanılamaz hale getirmektir.

4.8 - Kurumsal Varlıklar ve Yazılımlarda Gereksiz Hizmetleri Kaldırma veya Devre Dışı Bırakma ; Kullanılmayan dosya paylaşım hizmeti , web uygulama modülü veya hizmet işlevi gibi kurumsal varlıklar ve yazılımlardaki gereksiz hizmetleri kaldırın veya devre dışı bırakınız.

4.9 - Kurumsal Varlıklarda Güvenilir DNS Sunucularını Yapılandırma ; Kurumsal varlıklarda güvenilir DNS sunucularını yapılandırınız. Örnek uygulamalar şunları içerir ; varlıkları kurumsal kontrollü DNS sunucularını veya dışarıdan erişilebilen saygın DNS sunucularını kullanacak şekilde yapılandırma.

4.10 - Taşınabilir Son Kullanıcı Cihazlarında Otomatik Cihaz Kilitlemeyi Zorunlu Kıl ; Desteklendiği yerlerde , taşınabilir son kullanıcı cihazlarında önceden belirlenmiş yerel başarısız kimlik doğrulama girişimi eşiğinin ardından otomatik cihaz kilitlemeyi zorunlu kılınız. Dizüstü bilgisayarlar için 20'den fazla başarısız kimlik doğrulama girişimine izin vermeyiniz. Tabletler ve akıllı telefonlar için en fazla 10 başarısız kimlik doğrulama girişimi uygulayınız. Örnek uygulamalar arasında Microsoft® InTune Cihaz Kilidi ve Apple® Yapılandırma Profili maxFailedAttempts bulunmalıdır.

4.11 - Taşınabilir Son Kullanıcı Cihazlarında Uzaktan Silme Yeteneğinin Uygulanması ; Kayıp veya çalıntı cihazlar gibi uygun görüldüğünde veya bir kişi artık kuruluşu desteklemediğinde , kuruluşa ait taşınabilir son kullanıcı cihazlarından kurumsal verileri uzaktan siliniz.

4.12 - Mobil Son Kullanıcı Cihazlarında Ayrı Kurumsal Çalışma Alanları ; Desteklendiğinde , mobil son kullanıcı cihazlarında ayrı kurumsal çalışma alanlarının kullanıldığından emin olunuz. Örnek uygulamalar , kurumsal uygulamaları ve verileri kişisel uygulamalardan , verilerden ayırmak için Apple® Konfigürasyon Profili veya Android™ İş Profili kullanmayı içerir.

CIS Kritik Güvenlik Kontrolü 5 - Hesap Yönetimi ; Yönetici hesaplarının yanı sıra hizmet hesapları da dahil olmak üzere kullanıcı hesaplarına , kurumsal varlıklara ve yazılımlara yönelik kimlik bilgilerine yetki atamak ve yönetmek için süreçleri ve araçları kullanınız. Harici veya dahili tehdit aktörünün , ortamı hacklemek yerine geçerli kullanıcı kimlik bilgilerini kullanarak kurumsal varlıklara veya verilere yetkisiz erişim elde etmesi daha kolaydır. Kullanıcı hesaplarına gizlice erişim sağlamanın birçok yolu vardır ; zayıf parolalar , bir kullanıcı kuruluştan ayrıldıktan sonra hala geçerli olan hesaplar , atıl veya kalıcı test hesapları , aylar veya yıllar içinde değiştirilmemiş paylaşılan hesaplar , uygulamalara gömülü hizmet hesapları komut dosyaları için güvenliği ihlal edilmiş çevrimiçi hesap için kullandıkları parolayla aynı parolaya sahip kullanıcı , kullanıcının parolasını vermesi için sosyal mühendislik veya bellekte veya daha fazla parola veya belirteçleri yakalamak için kötü amaçlı yazılım kullanma. İdari veya yüksek ayrıcalıklı hesaplar , saldırganların başka hesaplar eklemesine veya varlıklarda onları diğer saldırılara karşı daha savunmasız hale getirebilecek değişiklikler yapmasına izin verdiği için belirli bir hedeftir. Hizmet hesapları da hassastır. Çünkü genelde şirket içi ve dışı ekipler arasında paylaşılır ve bazen bilinmez , yalnızca standart hesap yönetimi denetimlerinde ortaya çıkar. Son olarak , hesap günlüğü ve izleme , güvenlik operasyonlarının kritik bileşenidir. Hesap günlüğü ve izleme , CIS Kontrol 8'de (Denetim Günlüğü Yönetimi) kapsanırken , kapsamlı Kimlik ve Erişim Yönetimi (IAM) programının geliştirilmesinde önemlidir.

Prosedürler ve Araçlar ; Kimlik bilgileri , kuruluşa birinci giriş noktası olduklarından , kurumsal varlıklar ve yazılımlar gibi envantere alınması ve izlenmesi gereken varlıklardır. Şifrelerin tekrar kullanılmaması için uygun şifre politikaları ve rehberliği geliştirilmelidir.

Kaynak : CIS Şifre Politikası Kılavuzu .

Hesaplar da izlenmelidir , uykuda olan herhangi bir hesap devre dışı bırakılmalı ve sonunda sistemden kaldırılmalıdır. Tüm aktif hesapların kurumsal varlığın yetkili kullanıcılarına kadar izlenmesini sağlamak için periyodik denetimler yapılmalıdır. Özellikle yönetici ve hizmet hesapları olmak üzere , önceki incelemeden bu yana eklenen yeni hesapları arayınız. İdari veya yüksek ayrıcalıklı hesapları , hizmet hesaplarını belirlemek ve izlemek için çok dikkatli olunmalıdır. Yönetici veya diğer ayrıcalıklı erişime sahip kullanıcılar , daha yüksek yetkili görevler için ayrı hesaplara sahip olmalıdır. Bu hesaplar , normal kullanıcı hesaplarının tehlikeye girmesi durumunda riski azaltmak için yalnızca bu görevleri gerçekleştirirken veya özellikle hassas verilere erişirken kullanılacaktır. Birden fazla hesabı olan kullanıcılar için yönetimsel olmayan görevler için günlük olarak kullanılan temel kullanıcı hesaplarının yükseltilmiş ayrıcalığı olmamalıdır. Tek Oturum Açma (SSO) , bir kuruluşta bulut uygulamaları da dahil olmak üzere birçok uygulamaya sahip olduğunda kullanışlı ve güvenlidir. Bu da bir kullanıcının yönetmesi gereken parola sayısını azaltmaya yardımcı olur. Kullanıcıların , parolalarını güvenli şekilde saklamak için parola yöneticisi uygulamalarını kullanmaları önerilir ve bunları bilgisayarlarındaki elektronik tablolarda veya metin dosyalarında tutmamaları konusunda talimat verilmelidir. Uzaktan erişim için MFA önerilir.

Kaynak : NIST® Dijital Kimlik Yönergeleridir .

Alınacak Güvenlik Önlemleri ;

5.1 – Hesap Envanteri Oluşturma ve Muhafaza Etme ; Kuruluşta yönetilen tüm hesapların bir envanterini oluşturun ve sürdürünüz. Envanter hem kullanıcı hem de yönetici hesaplarını içermelidir. Envanter en azından kişinin adını , kullanıcı adını , başlangıç / bitiş tarihlerini ve departmanını içermelidir. Tüm aktif hesapların , en az üç ayda bir veya daha sık aralıklarla yinelenen bir programa göre yetkilendirildiğini doğrulayınız.

5.2 - Benzersiz Parolalar Kullanın ; Tüm kurumsal varlıklar için benzersiz parolalar kullanınız. En iyi uygulama uygulaması , MFA kullanan hesaplar için en az 8 karakterlik şifre ve MFA kullanmayan hesaplar için 14 karakterlik şifre içerir.

5.3 - Hareketsiz Hesapları Devre Dışı Bırak ; Destekleniyorsa , 45 günlük etkinlik dışı kalma süresinden sonra tüm etkin olmayan hesapları silin veya devre dışı bırakınız.

5.4 - Yönetici Ayrıcalıklarını Özel Yönetici Hesaplarıyla Kısıtlayın ; Yönetici ayrıcalıklarını , kurumsal varlıklarda özel olarak ayrılmış yönetici hesaplarıyla sınırlayınız. Kullanıcının birincil , ayrıcalıklı olmayan hesabından internette gezinme , e-posta ve üretkenlik paketi kullanımı gibi genel bilgi işlem etkinliklerini gerçekleştiriniz.

5.5 - Hizmet Hesapları Envanteri Oluşturma ve Koruma ; Hizmet hesaplarının envanterini oluşturun ve sürdürünüz. Envanter , en azından departman sahibini , gözden geçirme tarihini ve amacını içermelidir. Tüm etkin hesapların yetkilendirildiğini doğrulamak için en az üç ayda bir veya daha sık aralıklarla yinelenen programa göre hizmet hesabı incelemeleri gerçekleştiriniz.

5.6 - Merkezi Hesap Yönetimi ; Bir dizin veya kimlik hizmeti aracılığıyla merkezi hesap yönetimidir.

CIS Kritik Güvenlik Kontrolü 6 - Erişim Kontrolü Yönetimi ; Kurumsal varlıklar ve yazılımlar için kullanıcı , yönetici ve hizmet hesapları için erişim kimlik bilgileri ve ayrıcalıkları oluşturmak , atamak , yönetmek ve iptal etmek için süreçleri ve araçları kullanınız. CIS Control 5'in özellikle hesap yönetimiyle ilgili olduğu durumlarda , CIS Control 6 , bu hesapların hangi erişime sahip olduğunu yönetmeye , kullanıcıların yalnızca kendi rollerine uygun verilere veya kurumsal varlıklara erişiminin olmasını sağlamaya , kritik veya hassas kuruluşlar için güçlü kimlik doğrulamanın olmasını sağlamaya odaklanır. Hesaplar , yalnızca rol için gereken minimum yetkiye sahip olmalıdır. Her rol için tutarlı erişim hakları geliştirmek ve kullanıcılara roller atamak en iyi uygulamadır. Eksiksiz tedarik ve erişimin kaldırılması için program geliştirmek de önemlidir. Bu işlevi merkezileştirmek idealdir. Güvenilmeyen ağlardan erişildiklerinden veya diğer hesapları eklemeye , değiştirmeye veya kaldırmaya ya da işletim sistemlerinde , uygulamalarda yapılandırma değişiklikleri yapmaya olanak tanıyan yönetici işlevleri gerçekleştirmeleri nedeniyle kuruluş için daha büyük risk oluşturan bazı kullanıcı etkinlikleri vardır. Onları daha az güvenli hale getirin. Bu aynı zamanda MFA ve Privileged Access Management (PAM) araçlarının kullanılmasının önemini de ortaya koyar. Bazı kullanıcılar , rolleri için ihtiyaç duymadıkları kurumsal varlıklara veya verilere erişebilir. Bunun nedeni , tüm kullanıcılara tam erişim sağlayan olgunlaşmamış süreç veya kullanıcılar zaman içinde kuruluş içindeki rolleri değiştirdikçe kalıcı erişim olabilir.

Kullanıcı tarafından yüklenen veya indirilen herhangi bir kötü amaçlı kod , yönetici olarak çalışan kurumsal varlık üzerinde daha büyük bir etkiye sahip olabileceğinden , kullanıcıların dizüstü bilgisayarlarına yönelik yerel yönetici ayrıcalıkları da bir sorundur. Kullanıcı , yönetici ve hizmet hesabı erişimi , kurumsal rol ve ihtiyaca dayalı olmalıdır.

Prosedürler ve Araçlar ; Kullanıcı hesapları için ayrıcalıkların verildiği ve iptal edildiği bir süreç olmalıdır. Bu ideal olarak , rol tabanlı erişim yoluyla kurumsal rol ve ihtiyaca dayalıdır. Rol tabanlı erişim , şunlara dayalı olarak her hesap için erişim gereksinimlerini tanımlamaya ve yönetmeye yönelik tekniktir ; bilme ihtiyacı , en az ayrıcalık , gizlilik gereksinimleri veya görevler ayrılığı. Bu süreci yönetmeye yardımcı olacak teknoloji araçları vardır. Duruma göre daha ayrıntılı veya geçici erişim olabilir. MFA , tüm ayrıcalıklı veya yönetici hesapları için evrensel olmalıdır. Bu işlevi gerçekleştirmek için akıllı telefon uygulamalarına sahip birçok araç vardır ve dağıtımı kolaydır. Numara üreteci özelliğini kullanmak , yalnızca bir kerelik kod içeren Kısa Mesaj Servisi (SMS) mesajı göndermekten veya bir kullanıcının kabul etmesi için push uyarısı istemekten daha güvenlidir. Ayrıcalıklı hesap MFA'sı için ikisi de önerilmez. Ayrıcalıklı hesap kontrolü için PAM araçları mevcuttur ve her kullanım için kontrol edilmesi gereken tek seferlik şifre sağlar. Sistem yönetiminde ek güvenlik için atlama kutuları veya bant dışı terminal bağlantılarının kullanılması önerilir. Kapsamlı hesap yetkilendirmesinin kaldırılması önemlidir. Birçok kuruluş , çalışanlar kuruluştan ayrıldığında erişimi kaldırmak için tekrarlanabilir tutarlı süreçlere sahiptir. Bu süreç yükleniciler için her zaman tutarlı değildir ve standart provizyon kaldırma sürecine dahil edilmelidir. Ortak hata kodda açık metin belirteçleri veya parolalar bırakmak ve genel bulut tabanlı kod havuzlarına göndermek olduğundan , kuruluşlar hizmet hesaplarının envanterini çıkarmalı ve izlemelidir. Yüksek ayrıcalıklı hesaplar , web'de gezinme ve e-posta okuma gibi günlük kullanım için kullanılmamalıdır. Yöneticiler , günlük ofis kullanımı için yükseltilmiş ayrıcalıklara sahip olmayan ayrı hesaplara sahip olmalı ve yalnızca bu düzeyde yetki gerektiren yönetici işlevleri gerçekleştirirken yönetici hesaplarında oturum açmalıdır. Güvenlik personeli , herhangi bir tarayıcının veya e-posta okuyucunun yüksek ayrıcalıklarla çalışıp çalışmadığını belirlemek için düzenli aralıklarla çalışan işlemlerin bir listesini toplamalıdır.

Alınacak Güvenlik Önlemleri ;

6.1 - Erişim Verme Süreci Oluşturun ; Yeni işe alma , haklar verilmesi veya kullanıcının rol değişikliği üzerine kurumsal varlıklara erişim izni vermek için tercihen otomatikleştirilmiş süreç oluşturun ve izleyiniz.

6.2 - Erişim İptal İşlemi Oluşturun ; Kullanıcının feshi , haklarının iptali veya rol değişikliğinin hemen ardından hesapları devre dışı bırakarak , kurumsal varlıklara erişimi iptal etmek için tercihen otomatikleştirilmiş süreç oluşturun ve izleyiniz. Denetim izlerini korumak için hesapları silmek yerine hesapları devre dışı bırakmak gerekli olabilir.

6.3 - Harici Olarak Açıklanan Uygulamalar için MFA Gerektirir ; Desteklendiğinde , MFA'yı zorunlu kılmak için harici olarak açığa çıkan tüm kurumsal veya üçüncü taraf uygulamaları zorunlu kılınız. MFA'yı rehber hizmeti veya SSO sağlayıcısı aracılığıyla uygulamak , korumanın tatmin edici bir uygulamasıdır.

6.4 - Uzaktan Ağ Erişimi için MFA Gerektiri r; Uzak ağ erişimi için MFA gerektir.

6.5 - Yönetici Erişimi için MFA gerektir ; Desteklendiğinde , yerinde veya üçüncü taraf sağlayıcı aracılığıyla yönetilen tüm kurumsal varlıklarda tüm yönetim erişim hesapları için MFA gerektir.

6.6 - Kimlik Doğrulama ve Yetkilendirme Sistemleri Envanterinin Oluşturulması ve Sürdürülmesi ; Yerinde veya uzak hizmet sağlayıcısında barındırılanlar da dahil olmak üzere , kuruluşun kimlik doğrulama ve yetkilendirme sistemlerinin envanterini oluşturun ve sürdürün. Envanteri en azından yıllık olarak veya daha sık olarak gözden geçirin ve güncelleyiniz.

6.7 - Erişim Kontrolünü Merkezileştirin ; Desteklendiğinde , dizin hizmeti veya SSO sağlayıcısı aracılığıyla tüm kurumsal varlıklar için erişim kontrolünü merkezileştiriniz.

6.8 - Rol Tabanlı Erişim Kontrolünü Tanımlayın ve Bakımını Yapın ; Kuruluş içindeki her bir rolün kendisine verilen görevleri başarıyla yerine getirmesi için gerekli erişim haklarını belirleyerek ve belgeleyerek , rol tabanlı erişim kontrolünü tanımlayın ve sürdürünüz. Tüm ayrıcalıkların yetkilendirildiğini doğrulamak için en az yılda bir kez veya daha sık aralıklarla yinelenen bir programda kurumsal varlıkların erişim kontrolü incelemeleri gerçekleştiriniz.

CIS Kritik Güvenlik Kontrolü 7 - Sürekli Güvenlik Açığı Yönetimi ; Saldırganlar için fırsat penceresini düzeltmek ve en aza indirmek için kuruluşun altyapısındaki tüm kurumsal varlıklardaki güvenlik açıklarını sürekli olarak değerlendirmek ve izlemek için plan geliştiriniz. Yeni tehdit ve güvenlik açığı bilgileri için kamu ve özel sektör kaynaklarını izleyiniz. Siber savunucular , istismar etmek ve erişim elde etmek için altyapılarında güvenlik açıkları arayan saldırganlardan sürekli olarak meydan okumaktadır. Savunucular , yazılım güncellemeleri , yamalar , güvenlik önerileri , tehdit bültenleri vb. hakkında zamanında tehdit bilgilerine sahip olmalıdır ve saldırganlardan önce bu güvenlik açıklarını belirlemek için ortamlarını düzenli olarak gözden geçirmelidirler. Güvenlik açıklarını anlamak ve yönetmek , zaman , dikkat ve kaynaklara odaklanmayı gerektiren sürekli bir faaliyettir. Saldırganlar aynı bilgilere erişebilir ve güvenlik açıklarından genelde bir kuruluşun düzeltebileceğinden daha hızlı yararlanabilir. Güvenlik açığının ne zaman yamalandığının bilinmesi ile zaman içinde boşluk olsa da , savunucular , hangi güvenlik açıklarının kuruluş için en etkili olduğunu veya kullanım kolaylığı nedeniyle ilk olarak istismar edilmesinin muhtemel olduğunu önceliklendirebilir. Araştırmacılar veya topluluk yeni güvenlik açıkları bildirdiğinde , satıcıların yamalar , güvenlik ihlali göstergeleri (IOC) ve güncellemeler geliştirmesi ve dağıtması gerekir. Savunucuların , kuruluşa yönelik yeni güvenlik açığı riskini değerlendirmesi , regresyon testi yamaları ve yamayı yüklemesi gerekir. Bu süreçte asla mükemmellik yoktur. Saldırganlar , güvenlik topluluğu içinde bilinmeyen güvenlik açığından yararlanıyor olabilir. Sıfır gün istismarı olarak adlandırılan bu güvenlik açığına yönelik istismar geliştirmiş olabilirler. Toplulukta zafiyet belli olduktan sonra yukarıda bahsedilen süreç başlar. Bu nedenle , savunucular , güvenlik açığı geniş çapta sosyalleştiğinde istismarın zaten var olabileceğini akılda tutmalıdır. Bazen güvenlik açıkları , kamuya açıklanmadan haftalar , aylar veya yıllar önce kapalı toplulukta bilinebilir. Savunucular , her zaman düzeltemeyecekleri güvenlik açıkları olabileceğinin farkında olmalıdır ve bu nedenle hafifletmek için diğer kontrolleri kullanmaları gerekir. Altyapılarını güvenlik açıkları açısından değerlendirmeyen ve keşfedilen kusurları proaktif olarak ele almayan kuruluşlar , kurumsal varlıklarının tehlikeye girmesi konusunda önemli olasılık ile karşı karşıyadır. Savunucular , iyileştirmeyi tüm kuruluş genelinde ölçeklendirmede ve kuruluşun işini veya misyonunu etkilemeden , çelişen önceliklere sahip eylemlere öncelik vermede belirli zorluklarla karşı karşıyadır.

Prosedürler ve Araçlar ; Kurumsal varlıkların güvenlik yapılandırmasını değerlendirmek için çok sayıda güvenlik açığı tarama aracı mevcuttur. Bazı kuruluşlar , uzaktan yönetilen tarama araçlarını kullanan ticari hizmetlerin de etkili olduğunu bulmuşlardır. Kuruluş genelinde keşfedilen güvenlik açıklarının tanımlarının standartlaştırılmasına yardımcı olmak için güvenlik açıklarını şu endüstri tarafından tanınan güvenlik açığı , yapılandırma ve platform sınıflandırma şemaları ve dillerinden bir veya daha fazlasıyla eşleyen güvenlik açığı tarama araçlarının kullanılması tercih edilir ; Ortak Güvenlik Açıkları ve Etkilenmeler (CVE®) , Ortak Yapılandırma Numaralandırması (CCE) , Açık Güvenlik Açığı ve Değerlendirme Dili (OVAL®) , Ortak Platform Numaralandırması (CPE) , Ortak Güvenlik Açığı Puanlama Sistemi (CVSS) veya Genişletilebilir Yapılandırma Kontrol Listesi Açıklama Formatı (XCCDF). Bu şemalar ve diller SCAP'ın bileşenleridir.

Kaynak ; SCAP

Her satıcının değişen yama döngülerini hesaba katmak için kuruluşun varlıklarının çeşitliliği arttıkça tarama faaliyetlerinin sıklığı da artmalıdır.

Gelişmiş güvenlik açığı tarama araçları , kurumsal varlıkların kimliğini doğrulamak ve daha kapsamlı değerlendirmeler gerçekleştirmek için kullanıcı kimlik bilgileriyle yapılandırılabilir. Bunlara kimliği doğrulanmış taramalar denir. Ağ genelinde güvenlik açıklarını ve yanlış yapılandırmaları kontrol eden tarama araçlarına ek olarak , çeşitli ücretsiz ve ticari araçlar , kurumsal varlıkların güvenlik ayarlarını ve yapılandırmalarını değerlendirebilir. Bu tür araçlar , yapılandırmadaki yetkisiz değişikliklere veya yöneticilerden yanlışlıkla güvenlik zayıflıklarına giriş yapılmasına ilişkin ayrıntılı bilgiler sağlayabilir Etkili kuruluşlar , güvenlik açığı tarayıcılarını , güvenlik açıklarını düzeltme konusundaki ilerlemeyi izleyen ve raporlayan sorun bildirim sistemleriyle ilişkilendirir. Çözülmelerini sağlamak için üst yönetime yönelik , azaltılmamış kritik güvenlik açıklarının vurgulanmasına yardımcı olabilir. Kuruluşlar tespit edildikten veya yama yayınlandıktan sonra güvenlik açığının giderilmesinin ne kadar sürdüğünü de takip edebilir. Bunlar , dahili veya endüstri uyumluluk gereksinimlerini destekleyebilir. Bazı olgun işletmeler , iş etkisine dayalı iyileştirme çabalarına öncelik vermek için BT ve işletme liderlerini bir araya getiren BT güvenliği yönlendirme komitesi toplantılarında bu raporları gözden geçirecektir. Kuruluş , hangi güvenlik açıklarının düzeltileceğini veya yamaların uygulanacağını seçerken , NIST'in Ortak Güvenlik Açığı Puanlama Sistemini (CVSS) , tehdit aktörünün güvenlik açığını kullanma olasılığı veya istismarın kuruluş üzerindeki olası etkisi ile ilgili verilerle güçlendirmelidir. Sömürü olasılığına ilişkin bilgiler de en güncel tehdit bilgilerine dayalı olarak periyodik olarak güncellenmelidir. Yeni istismarın serbest bırakılması veya güvenlik açığından yararlanılmasına ilişkin yeni istihbarat , güvenlik açığının yama için dikkate alınması gereken önceliği değiştirmelidir. Bir işletmenin bu süreci ölçeklenebilir bir şekilde otomatikleştirmesini ve sürdürmesini sağlamak için çeşitli ticari sistemler mevcuttur. En etkili güvenlik açığı tarama araçları , ortamdaki güvenlik açıklarının zaman içinde nasıl değiştiğini belirlemek için mevcut taramanın sonuçlarını önceki taramalarla karşılaştırır. Güvenlik personeli , aydan aya güvenlik açığı eğilimlerini yürütmek için bu özellikleri kullanır. Son olarak , yapılandırma güncellemelerini veya yamaların doğru şekilde ve ilgili tüm kurumsal varlıklarda uygulandığını doğrulamak için bir kalite güvence süreci olmalıdır.

Alınacak Güvenlik Önlemleri ;

7.1 - Güvenlik Açığı Yönetim Süreci Oluşturma ve Sürdürme ; Kurumsal varlıklar için belgelenmiş güvenlik açığı yönetimi süreci oluşturun ve sürdürünüz. Belgeleri yıllık olarak veya korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyiniz.

7.2 - İyileştirme Süreci Oluşturma ve Sürdürme ; Aylık veya daha sık gözden geçirmelerle iyileştirme sürecinde belgelenen riske dayalı iyileştirme stratejisi oluşturun ve sürdürünüz.

7.3 - Otomatik İşletim Sistemi Yamasını Yönetmek ; Aylık veya daha sık aralıklarla otomatik yama yönetimi aracılığıyla kurumsal varlıklarda işletim sistemi güncellemeleri gerçekleştiriniz.

7.4 - Otomatik Uygulama Yama Yönetimini Gerçekleştirin ; Aylık veya daha sık aralıklarla otomatik yama yönetimi aracılığıyla kurumsal varlıklarda uygulama güncellemeleri gerçekleştiriniz.

7.5 - Dahili Kurumsal Varlıkların Otomatik Güvenlik Açığı Taramalarını Gerçekleştirin ; Dahili kurumsal varlıkların otomatik güvenlik açığı taramalarını üç ayda bir veya daha sık aralıklarla gerçekleştiriniz. SCAP uyumlu güvenlik açığı tarama aracı kullanarak hem kimliği doğrulanmış hem de kimliği doğrulanmamış taramalar gerçekleştiriniz.

7.6 - Dışarıdan Tespit Edilen Kurumsal Varlıkların Otomatik Güvenlik Açığı Taramalarını Gerçekleştirin ; SCAP uyumlu güvenlik açığı tarama aracı kullanarak harici olarak açığa çıkan kurumsal varlıkların otomatik güvenlik açığı taramalarını gerçekleştiriniz. Taramaları aylık veya daha sık aralıklarla gerçekleştiriniz.

7.7 - Algılanan Güvenlik Açıklarını Düzeltme ; Düzeltme sürecine bağlı olarak aylık veya daha sık aralıklarla süreçler ve araçlar aracılığıyla yazılımda algılanan güvenlik açıklarını gideriniz.

CIS Kritik Güvenlik Kontrolü 8 - Denetim Günlüğü Yönetimi ; Bir saldırıyı tespit etmeye , anlamaya veya saldırıdan kurtarmaya yardımcı olabilecek olayların denetim günlüklerini toplayın , uyarın , inceleyin ve saklayınız. Günlük toplama ve analiz , bir kuruluşun kötü amaçlı etkinlikleri hızlı şekilde tespit edebilmesi için kritik öneme sahiptir. Bazen denetim kayıtları başarılı saldırının tek kanıtıdır. Saldırganlar , birçok işletmenin uyumluluk amacıyla denetim günlükleri tuttuğunu bilir fakat bunları nadiren analiz eder. Saldırganlar bu bilgiyi konumlarını , kötü amaçlı yazılımları ve kurban makinelerdeki etkinliklerini gizlemek için kullanır. Kötü veya mevcut olmayan günlük analizi süreçleri nedeniyle , saldırganlar bazen hedef kuruluştaki hiç kimsenin haberi olmadan kurban makineleri aylarca veya yıllarca kontrol eder. Genel olarak ele alınan ve genelde bağımsız olarak yapılandırılan iki tür günlük vardır ; sistem günlükleri ve denetim günlükleri. Sistem günlükleri genellikle çeşitli sistem süreci başlangıç / bitiş zamanlarını , çökmeleri vb. gösteren sistem düzeyinde olaylar sağlar. Bunlar sistemlere özgüdür ve açılması daha az yapılandırma gerektirir. Denetim günlükleri genelde kullanıcı düzeyinde olaylar içerir ve kurulum için daha fazla planlama ve çaba gerektirir. Günlük kayıtları , olay müdahalesi için de kritik öneme sahiptir. Bir saldırı tespit edildikten sonra günlük analizi , kuruluşların saldırının kapsamını anlamasına yardımcı olabilir. Tam günlük kayıtları , örneğin , saldırının ne zaman ve nasıl gerçekleştiğini , hangi bilgilere erişildiğini ve verilerin sızdırılıp sızdırılmadığını gösterebilir. Bir takip araştırmasının gerekli olması veya bir saldırının uzun bir süre boyunca tespit edilememesi durumunda da günlüklerin tutulması kritik öneme sahiptir.

Prosedürler ve Araçlar ; Çoğu kurumsal varlık ve yazılım , günlük kaydı yetenekleri sunar. Bu tür günlükler , merkezileştirilmiş günlük sunucularına gönderilen günlüklerle etkinleştirilmelidir. Güvenlik duvarları , proksiler ve uzaktan erişim sistemleri (Sanal Özel Ağ - VPN) , çevirmeli ağ vb.) , yararlı olduğu durumlarda ayrıntılı günlük kaydı için yapılandırılmalıdır. Bir olay araştırmasının gerekli olması durumunda günlük verilerinin tutulması da önemlidir. Tüm kurumsal varlıklar , bir kullanıcı uygun ayrıcalıklar olmadan kaynaklara erişmeye çalıştığında erişim kontrol günlükleri oluşturacak şekilde yapılandırılmalıdır. Böyle bir günlük kaydının mevcut olup olmadığını değerlendirmek için kuruluş günlüklerini periyodik olarak taramalı ve ağa aktif olarak bağlı her yönetilen varlığın periyodik olarak günlükler oluşturduğundan emin olmak için CIS Kontrol 1'in bir parçası olarak toplanan kurumsal varlık envanteri ile karşılaştırmalıdır.

Alınacak Güvenlik Önlemleri ;

8.1 - Denetim Günlüğü Yönetim Süreci Oluşturma ve Sürdürme ; Kuruluşun günlük kaydı gereksinimlerini tanımlayan denetim günlüğü yönetim süreci oluşturun ve sürdürünüz. En azından kurumsal varlıklar için denetim günlüklerinin toplanması , gözden geçirilmesi ve saklanması konularını ele alınız. Belgeleri yıllık olarak veya korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyiniz.

8.2 - Denetim Günlüklerini Toplayın ; Denetim günlüklerini toplayınız. Kuruluşun denetim günlüğü yönetim süreci uyarınca günlük kaydının kurumsal varlıklar genelinde etkinleştirildiğinden emin olunuz.

8.3 - Yeterli Denetim Günlüğü Depolamasının Sağlanması ; Günlüğe kaydetme hedeflerinin , kuruluşun denetim günlüğü yönetimi sürecine uymak için yeterli depolamayı sürdürdüğünden emin olunuz.

8.4 - Zaman Senkronizasyonunu Standartlaştırın ; Zaman senkronizasyonunu standartlaştırınız. Destekleniyorsa , kurumsal varlıklar arasında en az iki senkronize zaman kaynağı yapılandırınız.

8.5 - Ayrıntılı Denetim Günlüklerini Toplayın ; Hassas veriler içeren kurumsal varlıklar için ayrıntılı denetim günlüğünü yapılandırınız. Adli soruşturmaya yardımcı olabilecek olay kaynağı , tarih , kullanıcı adı , zaman damgası , kaynak adresleri , hedef adresleri ve diğer yararlı öğeleri dahil ediniz.

8.6 - DNS Sorgu Denetim Günlüklerini Toplayın ; Uygun ve desteklenen yerlerde , kurumsal varlıklarda DNS sorgusu denetim günlüklerini toplayınız.

8.7 - URL Talebi Denetim Günlüklerini Toplayın ; Uygun ve desteklenen yerlerde , kurumsal varlıklarda URL istek denetim günlüklerini toplayınız.

8.8 - Komut Satırı Denetim Günlüklerini Toplayın ; Komut satırı denetim günlüklerini toplayınız. Örnek uygulamalar ; PowerShell , BASH ve uzak yönetim terminallerinden denetim günlüklerinin toplanmasını içerir.

8.9 - Denetim Günlüklerini Merkezileştirin ; Kurumsal varlıklar genelinde denetim günlüğü toplama ve saklamayı mümkün olduğu ölçüde merkezileştiriniz.

8.10 - Denetim Günlüklerini Saklayın ; En az 90 gün boyunca kurumsal varlıklar genelinde denetim günlüklerini saklayınız.

8.11 - Denetim Günlüğü İncelemelerinin Yürütülmesi ; Olası bir tehdidi gösterebilecek anormallikleri veya anormal olayları tespit etmek için denetim günlüklerini gözden geçiriniz. İncelemeleri haftalık veya daha sık aralıklarla gerçekleştiriniz.

8.12 - Hizmet Sağlayıcı Günlüklerini Toplayın ; Destekleniyorsa , servis sağlayıcı günlüklerini toplayınız. Örnek uygulamalar , kimlik doğrulama ve yetkilendirme olaylarını , veri oluşturma ve elden çıkarma olaylarını , kullanıcı yönetimi olaylarını toplamayı içerir.

CIS Kritik Güvenlik Kontrolü 9 - E-posta ve Web Tarayıcı Korumaları ; Saldırganların doğrudan etkileşim yoluyla insan davranışlarını manipüle etme fırsatları olduğundan , e-posta ve web vektörlerinden gelen tehditlerin korumasını ve algılamasını iyileştiriniz. Web tarayıcıları ve e-posta istemcileri , bir kuruluş içindeki kullanıcılarla doğrudan etkileşimleri nedeniyle saldırganlar için çok yaygın giriş noktalarıdır. İçerik , kullanıcıları kimlik bilgilerini ifşa etmeye , hassas veriler sağlamaya veya saldırganların erişim elde etmesine izin vermek için açık kanal sağlamaya ikna etmek veya yanıltmak için oluşturulabilir. Böylece kuruluş için risk artar. E-posta ve web , kullanıcıların harici ve güvenilmeyen kullanıcılar , ortamlarla etkileşime girmesinin ana araçları olduğundan , bunlar hem kötü amaçlı kod hem de sosyal mühendislik için ana hedeflerdir. Şirketler web tabanlı e-postaya veya mobil e-posta erişimine geçtikçe , kullanıcılar artık bağlantı şifreleme , güçlü kimlik doğrulama ve kimlik avı raporlama düğmeleri gibi yerleşik güvenlik kontrolleri sağlayan geleneksel tam özellikli e-posta istemcilerini kullanmıyor.

Prosedürler ve Araçlar ;

İnternet tarayıcısı ; Siber suçlular , web tarayıcılarından çeşitli şekillerde yararlanabilir. Güvenlik açığı bulunan tarayıcıların istismarlarına erişimleri varsa , güvenli olmayan veya yama uygulanmamış tarayıcıyla göz atıldığında bu güvenlik açıklarından yararlanabilecek kötü amaçlı web sayfaları oluşturabilirler. Alternatif olarak , tarayıcıya ve doğrudan işletim sistemine , uygulamaya bağlanmalarına izin verebilecek herhangi bir sayıda yaygın web tarayıcısı üçüncü taraf eklentisini hedeflemeye çalışabilirler. Bu eklentiler , bir ortamdaki diğer tüm yazılımlar gibi , güvenlik açıkları için gözden geçirilmeli , en son yamalar veya sürümlerle güncel tutulmalı ve kontrol edilmelidir. Birçoğu güvenilmeyen kaynaklardan geliyor ve bazıları kötü niyetlidir. Bu nedenle , kullanıcıların bu eklentilerin , uzantıların ve eklentilerin bazılarında gizlenmiş olabilecek kötü amaçlı yazılımları kasıtlı veya kasıtsız olarak yüklemelerini önlemek en iyisidir. Tarayıcıya yapılan basit yapılandırma güncellemeleri , eklentileri / uzantıları yükleme yeteneğini azaltarak ve belirli içerik türlerinin otomatik olarak yürütülmesini önleyerek kötü amaçlı yazılımların yüklenmesini çok daha zor hale getirebilir. Çoğu popüler tarayıcı , en yaygın tehditlere karşı koruma sağlamak için kimlik avı veya kötü amaçlı yazılım sitelerinden oluşan veritabanı kullanır. En iyi uygulama , bu içerik filtrelerini etkinleştirmek ve açılır pencere engelleyicilerini açmaktır. Pop-up'lar sadece can sıkıcı değildir , gömülü kötü amaçlı yazılımları doğrudan barındırabilir veya sosyal mühendislik hilelerini kullanarak kullanıcıları bağlantılara tıklamaya yönlendirebilirler. Bilinen kötü amaçlı etki alanlarının engellenmesini zorunlu kılmak için web sitelerine ağ düzeyinde erişim girişimlerini engellemek için DNS filtreleme hizmetlerine abone olmayı da düşününüz.

E-posta ; İnsanların kurumsal varlıklarla çalışmasının en etkileşimli yollarından birini temsil eder. Eğitim ve doğru davranışı teşvik etmek teknik ayarlar kadar önemlidir. E-posta , kimlik avı ve Kurumsal E-posta Uzlaşması (BEC) gibi taktikler yoluyla işletmelere karşı en yaygın tehdit vektörüdür. E-posta ağ geçidinde spam filtreleme aracı ve kötü amaçlı yazılım taraması kullanmak , kuruluşun ağına gelen kötü amaçlı e-postaların ve eklerin sayısını azaltır. Etki Alanı Tabanlı İleti Kimlik Doğrulaması , Raporlama ve Uygunluk (DMARC) başlatmak , spam ve kimlik avı etkinliklerini azaltmaya yardımcı olur. E-posta ve iletişimi güvence altına almak için şifreleme aracı yüklemek , başka kullanıcı ve ağ tabanlı güvenlik katmanı ekler. Göndericiye göre engellemenin yanı sıra , yalnızca kullanıcıların işleri için ihtiyaç duyduğu belirli dosya türlerine izin vermekte fayda var. Süreçlerinde kesinti olmamasını sağlamak için e-posta yoluyla ne tür dosyalar aldıklarını anlamak için farklı iş birimleriyle koordinasyon gerektirecektir. Kimlik avı e-posta teknikleri , SPAM filtre kurallarını aşmak için sürekli geliştiğinden , kullanıcıları kimlik avını nasıl tanımlayacakları konusunda eğitmek ve bir tanesini gördüklerinde BT Güvenliğini bilgilendirmek önemlidir. Kullanıcıları farklı örnekler konusunda eğitmek ve zaman içindeki gelişmelerini izlemek için kullanıcılara karşı kimlik avı testleri yapan birçok platform vardır. Bu bilgiyi BT Güvenlik ekiplerine kimlik avı konusunda bilgilendirmek için kitlesel kaynak sağlamak, e-posta tabanlı tehditlere karşı koruma ve algılamanın iyileştirilmesine yardımcı olur.

Alınacak Güvenlik Önlemleri ;

9.1 - Yalnızca Tam Olarak Desteklenen Tarayıcıların ve E-posta İstemcilerinin Kullanılmasını Sağlayın ; Yalnızca satıcı tarafından sağlanan tarayıcıların ve e-posta istemcilerinin en son sürümünü kullanarak kuruluşta yalnızca tam olarak desteklenen tarayıcıların ve e-posta istemcilerinin çalışmasına izin verildiğinden emin olunuz.

9.2 - DNS Filtreleme Hizmetlerini Kullanın ; Bilinen kötü amaçlı etki alanlarına erişimi engellemek için tüm kurumsal varlıklarda DNS filtreleme hizmetlerini kullanınız.

9.3 - Ağ Tabanlı URL Filtrelerini Koruma ve Uygulama ; Kurumsal varlığın potansiyel olarak kötü amaçlı veya onaylanmamış web sitelerine bağlanmasını sınırlamak için ağ tabanlı URL filtrelerini zorunlu kılın ve güncelleyiniz. Örnek uygulamalar , kategori tabanlı filtrelemeyi , itibar tabanlı filtrelemeyi veya engelleme listelerinin kullanımını içerir. Tüm kurumsal varlıklar için filtreler uygulayınız.

9.4 - Gereksiz veya Yetkisiz Tarayıcı , E-posta İstemcisi Uzantılarını Kısıtlama ; Yetkisiz veya gereksiz tarayıcı , e-posta istemcisi eklentilerini , uzantılarını ve eklenti uygulamalarını kaldırarak veyahut devre dışı bırakarak kısıtlayınız.

9.5 - DMARC'yi Uygulamak ; Geçerli alanlardan gelen sahte veya değiştirilmiş e-postaların olasılığını azaltmak için Gönderen Politikası Çerçevesi (SPF) ve Etki Alanı Anahtarları Tanımlanmış Posta (DKIM) standartlarını uygulamaya başlayarak DMARC politikasını ve doğrulamasını uygulayınız.

9.6 - Gereksiz Dosya Türlerini Engelleyin ; Kuruluşun e-posta ağ geçidine girmeye çalışan gereksiz dosya türlerini engelleyiniz.

9.7 - E-posta Sunucusu Kötü Amaçlı Yazılımdan Koruma Korumalarını Dağıtın ve Bakımını Yapın ; Ek tarama veya korumalı alan oluşturma gibi e-posta sunucusu kötü amaçlı yazılıma karşı korumaları dağıtın ve sürdürünüz.

CIS Kritik Güvenlik Kontrolü 10 - Kötü Amaçlı Yazılım Savunmaları ; Kurumsal varlıklar üzerinde kötü amaçlı uygulamaların , kodların veya komut dosyalarının yüklenmesini , yayılmasını ve yürütülmesini önleyin veya kontrol ediniz. Kötü amaçlı yazılımlar (virüsler veya Truva atları olarak sınıflandırılır) , internet tehditlerinin ayrılmaz ve tehlikeli bir yönüdür. Kimlik bilgilerini ele geçirmek , verileri çalmak , ağ içindeki diğer hedefleri belirlemek ve verileri şifrelemek veyahut yok etmek gibi birçok amacı olabilir. Modern türevleri makine öğrenimi tekniklerinden yararlandığından , kötü amaçlı yazılımlar sürekli olarak gelişmektedir ve uyarlanabilirdir. Kötü amaçlı yazılım bir kuruluşa son kullanıcı cihazlarında , e-posta eklerinde , web sayfalarında , bulut hizmetlerinde , mobil cihazlarda ve çıkarılabilir medyadaki güvenlik açıkları aracılığıyla girer. Kötü amaçlı yazılımlar genelde bağlantıları tıklama , ekleri açma , yazılım veya profil yükleme , USB flash sürücüleri takma gibi güvenli olmayan son kullanıcı davranışlarına dayanır. Modern kötü amaçlı yazılımlar , savunmaları önlemek , aldatmak veya devre dışı bırakmak için tasarlanmıştır. Kötü amaçlı yazılım savunmaları , otomasyon , zamanında ve hızlı güncelleme ve güvenlik açığı yönetimi ve olay yanıtı gibi diğer süreçlerle entegrasyon yoluyla bu dinamik ortamda çalışabilmelidir. Kötü amaçlı yazılım veya kodun yürütülmesini tespit etmek , yayılmasını önlemek veya kontrol etmek için tüm olası giriş noktalarında ve kurumsal varlıklarda konuşlandırılmalıdırlar.

Prosedürler ve Araçlar ; Etkili kötü amaçlı yazılım koruması , geleneksel uç nokta kötü amaçlı yazılım önleme ve algılama paketlerini içerir. Kötü amaçlı yazılım IOC'lerinin güncel olduğundan emin olmak için kuruluşlar , diğer güvenlik açığı veya tehdit verilerini zenginleştirmek için satıcıdan otomatik güncellemeler alabilir. Bu araçlar , altyapı genelinde tutarlılık sağlamak için en iyi şekilde merkezi olarak yönetilir. Kötü amaçlı yazılımları engelleyebilmek veya tanımlayabilmek bu CIS Denetiminin yalnızca bir parçasıdır. Uyarı , tanımlama ve olay yanıtını desteklemek için günlükleri merkezi olarak toplamaya da odaklanılır. Kötü niyetli aktörler metodolojilerini geliştirmeye devam ettikçe , birçoğu yakalanma olasılığını en aza indirmek için LotL yaklaşım benimsemeye başlamaktadır. Bu yaklaşım , hedef ortamda zaten var olan araçları veya özellikleri kullanan saldırgan davranışına atıfta bulunur. CIS Control 8'deki Korumalar uyarınca günlüğe kaydetmeyi etkinleştirmek , kuruluşun ne olduğunu ve neden olduğunu anlamak için olayları takip etmesini önemli ölçüde kolaylaştıracaktır.

Alınacak Güvenlik Önlemleri ;

10.1 - Kötü Amaçlı Yazılımdan Koruma Yazılımını Dağıtın ve Bakımını Yapma ; Tüm kurumsal varlıklarda kötü amaçlı yazılımdan koruma yazılımı dağıtın ve bakımını yapınız.

10.2 - Otomatik Kötü Amaçlı Yazılımdan Koruma İmza Güncellemelerini Yapılandırma ; Tüm kurumsal varlıklarda kötü amaçlı yazılımdan koruma imza dosyaları için otomatik güncellemeleri yapılandırınız.

10.3 - Çıkarılabilir Medya için Otomatik Çalıştırma ve Otomatik Yürütmeyi Devre Dışı Bırakma ; Çıkarılabilir medya için otomatik çalıştırma işlevini devre dışı bırakınız.

10.4 - Çıkarılabilir Ortamın Otomatik Kötü Amaçlı Yazılımdan Koruma Taramasını Yapılandırma ; Çıkarılabilir medyayı otomatik olarak taramak için kötü amaçlı yazılımdan koruma yazılımını yapılandırınız.

10.5 - Sömürü Önleme Özelliklerini Etkinleştirin ; Microsoft Data Execution Prevention (DEP) , Windows® Defender Exploit Guard (WDEG) veya Apple® System Integrity Protection (SIP) , Gatekeeper™ gibi kurumsal varlıklarda ve yazılımlarda , mümkün olduğunda, istismar önleme özelliklerini etkinleştiriniz.

10.6 - Kötü Amaçlı Yazılımdan Koruma Yazılımını Merkezi Olarak Yönetin ; Kötü amaçlı yazılımdan koruma yazılımını merkezi olarak yönetiniz.

10.7 - Davranış Tabanlı Kötü Amaçlı Yazılımdan Koruma Yazılımı Kullanın ; Davranış tabanlı kötü amaçlı yazılımdan koruma yazılımı kullanınız.

CIS Kritik Güvenlik Kontrolü 11 - Veri Kurtarma ; Kapsam dahilindeki kurumsal varlıkları olay öncesi ve güvenilir duruma geri yüklemek için yeterli veri kurtarma uygulamalarını oluşturun ve sürdürünüz. Siber güvenlik üçlüsünde ; Gizlilik , Bütünlük ve Erişilebilirlik (CIA) , verilerin kullanılabilirliği , bazı durumlarda gizliliğinden daha kritiktir. İşletmeler , iş kararları vermek için birçok veri türüne ihtiyaç duyarak bu veriler mevcut olmadığında veya güvenilir olmadığında , işletmeyi etkileyebilir. Saldırganlar varlıkların güvenliğini ihlal ettiğinde yapılandırmalarda değişiklikler yapar , hesaplar ekler ve genelde yazılım veya komut dosyaları ekler. Saldırganlar güvenilen uygulamaları bozmuş veya kötü amaçlı sürümlerle değiştirmiş olabileceğinden veya değişiklikler standart görünümlü hesap adları gibi görünebileceğinden , bu değişiklikleri belirlemek her zaman kolay değildir. Yapılandırma değişiklikleri , kayıt defteri girdilerini ekleme veya değiştirmeyi , bağlantı noktalarını açmayı , güvenlik hizmetlerini kapatmayı , günlükleri silmeyi veya sistemi güvensiz hale getiren diğer kötü amaçlı eylemleri içerebilir. Bu eylemlerin kötü niyetli olması gerekmez. İnsan hatası da bunların her birine neden olabilir. Bu nedenle , kurumsal varlıkları ve verileri bilinen güvenilir duruma geri döndürmek için en son yedeklemelere veya geri dönüş noktalarına sahip olmak önemlidir. Son birkaç yılda fidye yazılımlarında üstel artış olmuştur. Saldırganların para kazanması için güvenilir yöntem olarak daha ticari hale gelmesine ve organize olmasına rağmen , yeni tehdit değildir. Saldırgan bir kuruluşun verilerini şifreler ve geri yüklenmesi için fidye talep ederse , bilinen , güvenilir duruma kurtarmak için yakın zamanda alınmış yedeklemeye sahip olmak yardımcı olabilir. Bununla birlikte , fidye yazılımı geliştikçe , verilerin şifrelenmeden önce sızdırıldığı ve saldırganın kuruluşun verilerini geri yüklemek , bunların satılmasını veya halka açıklanmasını önlemek için ödeme istediği gasp tekniği haline gelmiştir. Bu durumda , geri yükleme sadece sistemlerin güvenilir duruma geri yüklenmesi ve operasyonların sürdürülmesi sorununu çözecektir. Saldırganlar genelde güvenli olmayan sistemlerde daha eski veya temel açıklardan yararlandığından , CIS Kontrolleri içindeki rehberlikten yararlanmak , iyileştirilmiş siber hijyen yoluyla fidye yazılımı riskini azaltmaya yardımcı olacaktır.

Prosedürler ve Araçlar ; Veri kurtarma prosedürleri , CIS Kontrolü 3 , Veri Koruma'da açıklanan veri yönetimi sürecinde tanımlanmalıdır. Veri değeri , hassasiyet veya saklama gereksinimlerine dayalı yedekleme prosedürlerini içermelidir. Yedekleme sıklığı ve türü geliştirmeye yardımcı olacaktır. Her üç ayda bir veya yeni yedekleme süreci veya teknolojisi tanıtıldığında , test ekibi rastgele yedek örneklemeyi değerlendirmeli ve bunları test ortamı ortamında geri yüklemeye çalışmalıdır. Geri yüklenen yedeklemeler , işletim sistemi , uygulama ve yedeklemedeki verilerin eksiksiz ve işlevsel olduğundan emin olmak için doğrulanmalıdır. Kötü amaçlı yazılım bulaşması durumunda, geri yükleme prosedürleri , orijinal enfeksiyondan önceki yedekleme sürümünü kullanmalıdır .

Alınacak Güvenlik Önlemleri ;

11.1 - Veri Kurtarma Süreci Oluşturma ve Sürdürme ; Veri kurtarma süreci oluşturun ve sürdürünüz. Bu süreçte , veri kurtarma etkinliklerinin kapsamını , kurtarma önceliklendirmesini ve yedekleme verilerinin güvenliğini ele alınız. Belgeleri yıllık olarak veya etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyiniz.

11.2 - Otomatik Yedeklemeler Gerçekleştirme ; Kapsam dahilindeki kurumsal varlıkların otomatik yedeklemelerini gerçekleştiriniz. Verilerin hassasiyetine bağlı olarak yedeklemeleri haftalık olarak veya daha sık çalıştırınız.

11.3 - Kurtarma Verilerini Koruma ; Kurtarma verilerini orijinal verilere eşdeğer kontrollerle koruyunuz. Gereksinimlere göre referans şifreleme veya veri ayrımı kullanınız.

11.4 - Kurtarma Verilerinin İzole Edilmiş Eşgörünümünün Oluşturulması ve Sürdürülmesi ; Yalıtılmış kurtarma verisi örneği oluşturun ve sürdürünüz. Örnek uygulamalar , çevrimdışı , bulut veya site dışı sistemler veya hizmetler aracılığıyla sürüm kontrol eden yedekleme hedeflerini içerir.

11.5 - Test Veri Kurtarma ; Kapsam dahilindeki kurumsal varlıkların bir örneklemesi için yedek kurtarmayı üç ayda bir veya daha sık test ediniz.

CIS Kritik Güvenlik Kontrolü 12 - Ağ Altyapısı Yönetimi ; Saldırganların savunmasız ağ hizmetlerinden ve erişim noktalarından yararlanmasını önlemek için ağ cihazlarını kurun , uygulayın ve aktif olarak yönetiniz (izleyin , raporlayın , düzeltin). Güvenli ağ altyapısı , saldırılara karşı önemli bir savunmadır. Uygun güvenlik mimarisini , çoğu zaman varsayılan ayarlarla sunulan güvenlik açıklarını ele alan , değişiklikleri izlemeyi ve mevcut yapılandırmaların yeniden değerlendirilmesini içerir. Ağ altyapısı , fiziksel ve sanallaştırılmış ağ geçitleri , güvenlik duvarları , kablosuz erişim noktaları , yönlendiriciler ve anahtarlar gibi cihazları içerir. Ağ cihazları için varsayılan yapılandırmalar , güvenlik için değiı l, dağıtım kolaylığı ve kullanım kolaylığı için tasarlanmıştır. Potansiyel varsayılan güvenlik açıkları arasında açık hizmetler ve bağlantı noktaları , varsayılan hesaplar ve parolalar , daha eski güvenlik açığı bulunan protokoller için destek ve gereksiz yazılımların önceden yüklenmesi yer alır. Saldırganlar , güvenlik duvarı kural kümelerinde , yönlendiricilerde ve anahtarlarda savunmasız varsayılan ayarları , boşlukları veya tutarsızlıkları arayarak bu delikleri savunmalara nüfuz etmek için kullanır. Ağlara erişim sağlamak , ağdaki trafiği yeniden yönlendirmek ve iletim sırasında verileri kesmek için bu cihazlardaki kusurlardan yararlanırlar. Ağ güvenliği , mimari diyagramların , konfigürasyonların , erişim kontrollerinin ve izin verilen trafik akışlarının düzenli olarak yeniden değerlendirilmesini gerektiren sürekli değişen ortamdır. Saldırganlar , kullanıcılar belirli iş ihtiyaçları için istisnalar talep ettikçe zamanla daha az güvenli hale gelen ağ cihazı yapılandırmalarından yararlanır. Bazen istisnalar devreye alınır fakat artık işletmenin ihtiyaçları için geçerli olmadığında kaldırılmazlar. Bazı durumlarda , bir istisnanın güvenlik riski ne düzgün şekilde analiz edilir ne de ilgili iş ihtiyacına göre ölçülür ve zamanla değişebilir.

Prosedürler ve Araçlar ; Kuruluşlar , ağ altyapısının tamamen belgelendiğinden ve mimari diyagramların güncel tutulduğundan emin olmalıdır. Önemli altyapı bileşenlerinin yamalar ve özellik yükseltmeleri için satıcı desteğine sahip olması önemlidir. Kullanım Ömrü Sonu (EOL) bileşenlerini , destek dışı kalacakları tarihten önce yükseltin veya izole etmek için hafifletici kontroller uygulayınız. Kuruluşların , ağ cihazlarını altyapıyı etkilemeyen en son güvenli ve kararlı sürüme yükseltmelerini gerektirecek güvenlik açıkları için altyapı sürümlerini ve yapılandırmalarını izlemeleri gerekir. Erişim kontrolü , günlük kaydı ve izleme için eksiksiz hesap yönetimine sahip olmaktır. Son olarak , altyapı yönetimi yalnızca güçlü kimlik doğrulama (PAM için MFA) ile güvenli protokoller üzerinden ve özel yönetim aygıtlarından , bant dışı ağlardan gerçekleştirilmelidir. Ağ filtrelerinin otomatik akıl sağlığı kontrolünü sağlar. Bu araçlar , ağ aygıtı aracılığıyla istenmeyen hizmetlere izin verebilecek kural kümelerinde veya Erişim Kontrol Listelerinde (ACL) hataları arar. Bu tür araçlar , güvenlik duvarı kural kümelerinde , yönlendirici ACL'lerinde veya diğer filtreleme teknolojilerinde her önemli değişiklik yapıldığında çalıştırılmalıdır.

Alınacak Güvenlik Önlemleri ;

12.1 - Ağ Altyapısının Güncel Olduğundan Emin Olma ; Ağ altyapısının güncel tutulmasını sağlayınız. Örnek uygulamalar , yazılımın en son kararlı sürümünü çalıştırmayı veya şu anda desteklenen hizmet olarak ağ (NaaS) tekliflerini kullanmayı içerir. Yazılım desteğini doğrulamak için yazılım sürümlerini aylık olarak veya daha sık gözden geçiriniz.

12.2 - Güvenli Ağ Mimarisi Kurmak ve Sürdürmek ; Güvenli ağ mimarisi oluşturun ve sürdürünüz. Güvenli ağ mimarisi , en azından segmentasyon , en az ayrıcalık ve kullanılabilirliği ele almalıdır.

12.3 - Ağ Altyapısını Güvenli Şekilde Yönetme ; Ağ altyapısını güvenli şekilde yönetiniz. Örnek uygulamalar , sürüm kontrollü kod olarak altyapıyı ve SSH ile HTTPS gibi güvenli ağ protokollerinin kullanımını içerir.

12.4 - Mimari Diyagramların Oluşturulması ve Sürdürülmesi ; Mimari şemaları veya diğer ağ sistemi belgelerini oluşturun ve sürdürünüz. Belgeleri yıllık olarak veya etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyiniz.

12.5 - Ağ Kimlik Doğrulaması , Yetkilendirme ve Denetimi (AAA) Merkezileştirme ; Ağı merkezileştiren AAA.

12.6 - Güvenli Ağ Yönetimi ve İletişim Protokollerinin Kullanımı ; Güvenli ağ yönetimi ve iletişim protokollerini kullanın (802.1X , Wi-Fi Protected Access 2 (WPA2) Enterprise veya üstü).

12.7 - Uzak Cihazların VPN Kullandığından ve Kuruluşun AAA Altyapısına Bağlandığından Emin Olma ; Kullanıcıların , son kullanıcı cihazlarındaki kurumsal kaynaklara erişmeden önce kurumsal olarak yönetilen VPN ve kimlik doğrulama hizmetlerinde kimlik doğrulaması yapmasını zorunlu kılınız.

12.8 - Tüm İdari İşler için Özel Bilgi İşlem Kaynakları Oluşturun ve Bakımını Yapma ; Tüm idari görevler veya idari erişim gerektiren görevler için fiziksel veya mantıksal olarak ayrılmış özel bilgi işlem kaynakları oluşturun ve sürdürünüz. Bilgi işlem kaynakları , işletmenin birinci ağından bölümlere ayrılmalı ve internet erişimine izin verilmemelidir.

CIS Kritik Güvenlik Kontrolü 13 - Ağ İzleme ve Savunma ; Kuruluşun ağ altyapısı ve kullanıcı tabanı genelinde kapsamlı ağ izleme ve güvenlik tehditlerine karşı savunma oluşturmak ve sürdürmek için süreçleri ve araçları çalıştırınız. Mükemmel olmak için ağ savunmalarına güvenemeyiz. Düşmanlar , güvenlik kontrollerine yönelik açıklardan yararlanmalar ve atlamalar hakkında toplulukları arasında bilgi paylaştıkça veya sattıkça gelişmeye ve olgunlaşmaya devam etmektedir. Güvenlik araçları çalışsa bile , etkili olmaları için bunları yapılandırmak , ayarlamak ve günlüğe kaydetmek için kurumsal risk duruşunu anlamak gerekir. Çoğu zaman , insan hatasından veya araç yetenekleri konusundaki bilgi eksikliğinden kaynaklanan yanlış yapılandırmalar , işletmelere yanlış güvenlik duygusu verir. Güvenlik araçları , yalnızca personelin uyarılmasına ve güvenlik olaylarına yanıt vermesine olanak tanıyan sürekli izleme sürecini destekliyorsa etkili olabilir. Tamamen teknoloji odaklı yaklaşımı benimseyen kuruluşlar , araçlardan gelen uyarılara aşırı güvenmeleri nedeniyle daha fazla yanlış pozitifle karşılaşacaklardır. Bu tehditleri belirlemek ve bunlara yanıt vermek , altyapının tüm tehdit vektörlerinin görünürlüğünü ve algılama , analiz ve yanıt sürecinde insanlardan yararlanmayı gerektirir. Büyük veya yoğun şekilde hedeflenen kuruluşların , siber tehditleri işletmeyi etkilemeden önce önleme , tespit etme ve hızlı şekilde yanıtlama için güvenlik operasyonları yeteneğine sahip olması kritik önem taşır. Bu süreç , güvenlik politikalarının geliştirilmesine yardımcı olacak ve birçok kuruluş için mevzuat uyumluluğunu destekleyecek faaliyet raporları ve ölçümler oluşturacaktır. Basında birçok kez gördüğümüz gibi , işletmeler keşfedilmeden haftalar , aylar veya yıllar önce tehlikeye atılmıştır. Kapsamlı durumsal farkındalığa sahip olmanın birinci faydası , algılama ve yanıt verme hızını artırmaktır. Kötü amaçlı yazılım keşfedildiğinde , kimlik bilgileri çalındığında veya kurum üzerindeki etkiyi azaltmak için hassas veriler tehlikeye girdiğinde hızlı şekilde yanıt vermek için kritik öneme sahiptir. İyi durumsal farkındalık (güvenlik operasyonları) aracılığıyla , kuruluşlar Taktikler , Teknikler ve Prosedürleri belirleyecek ve kataloglayacaktır. Kuruluşun gelecekteki tehditleri veya olayları belirlemede daha proaktif olmasına yardımcı olacak IOC'leri de dahil olmak üzere saldırganların (TTP). Müdahale , etkin müdahale stratejileri geliştirmek için çevre ve kurumsal yapı hakkında eksiksiz bilgilere eriştiğinde kurtarma daha hızlı gerçekleştirilebilir.

Prosedürler ve Araçlar ; Çoğu kuruluş , durumsal farkındalık kazanmak için Güvenlik Operasyon Merkezi (SOC) kurmaya ihtiyaç duymaz. Öncelikle kritik iş fonksiyonlarını , ağ ve sunucu mimarilerini , veri ve veri akışlarını , satıcı hizmetini ve iş ortağı bağlantısını ve son kullanıcı cihazlarını , hesaplarını anlamakla başlar. Güvenlik mimarisinin , teknik kontrollerin , günlüğe kaydetme , izleme ve yanıt prosedürlerinin geliştirilmesi hakkında bilgi verir. Bu sürecin merkezinde , olay tespiti , analizi ve hafifletme süreçlerini uygulayan eğitimli ve organize ekip bulunur. Bu yetenekler dahili olarak veya danışmanlar veya yönetilen hizmet sağlayıcı aracılığıyla yürütülebilir. Kuruluşlar ağ , kurumsal varlık , kullanıcı kimlik bilgileri ve veri erişim faaliyetlerini dikkate almalıdır. Teknoloji , tüm verileri toplamak ve analiz etmek , kurum içinde ve dışında ağları ile kurumsal varlıkları izlemek için çok önemli bir rol oynayacaktır. Kuruluşlar , şirket içi güvenlik teknolojisiyle uyumlu olmayabilecek bulut platformlarına yönelik görünürlük içermelidir.

Tüm önemli günlükleri Güvenlik Bilgileri ve Olay Yönetimi (SIEM) çözümleri gibi analitik programlara iletmek değer sağlayabilir. Eşikleri ayarlamak ve anormal olayları belirlemek için haftalık günlük incelemeleri gereklidir. Korelasyon araçları , sonraki manuel inceleme için denetim günlüklerini daha kullanışlı hale getirebilir. Bu araçlar , yetenekli bilgi güvenliği personeli ve sistem yöneticilerinin yerini tutmaz. Otomatik günlük analiz araçlarıyla bile , saldırıları belirlemek ve anlamak için genelde insan uzmanlığı ve sezgisi gerekir. Bu süreç olgunlaştıkça , işletmeler , iç tehdit istihbarat yeteneği geliştirerek , iş risklerini anlamaya ve değerlendirmeye yardımcı olacak bilgi tabanı oluşturacak , sürdürecek ve geliştirecektir. Tehdit istihbaratı , olaylardan ve düşmanlardan gelen TTP'lerin toplanmasıdır. Bunu başarmak için durumsal farkındalık programı , saldırıları tespit etmek , raporlamak ve ele almak için hangi bilgi kaynaklarının alakalı olduğunu tanımlayacak ve değerlendirecektir. Çoğu olgun kuruluş , anormallikleri bulmak için eğitimli personelin sistem ve kullanıcı günlüklerini , veri akışlarını ve trafik modellerini manuel olarak gözden geçirdiği tehdit avcılığına dönüşebilir.

Alınacak Güvenlik Önlemleri ;

13.1 - Güvenlik Olayı Uyarısını Merkezileştirin ; Günlük korelasyonu ve analizi için güvenlik olayı uyarılarını kurumsal varlıklar genelinde merkezileştiriniz. En iyi uygulama uygulaması , satıcı tanımlı olay bağıntı uyarılarını içeren SIEM kullanımını gerektirir. Güvenlikle ilgili korelasyon uyarılarıyla yapılandırılmış günlük analizi platformu da bu korumayı karşılar.

13.2 - Host Bilgisayar Tabanlı Saldırı Tespit Çözümü Dağıtın ; Uygun olduğunda veya desteklendiğinde kurumsal varlıklara host bilgisayar tabanlı saldırı tespit çözümü dağıtınız.

13.3 - Ağa İzinsiz Giriş Tespit Çözümü Dağıtın ; Uygun olduğunda kurumsal varlıklara ağ saldırı tespit çözümü dağıtınız. Örnek uygulamalar , Ağ İzinsiz Giriş Tespit Sistemi (NIDS) veya eşdeğer bulut hizmeti sağlayıcısı (CSP) hizmetinin kullanımını içerir.

13.4 - Ağ Segmentleri Arasında Trafik Filtreleme Yapın ; Uygun olduğunda , ağ segmentleri arasında trafik filtrelemesi gerçekleştiriniz.

13.5 - Uzak Varlıklar için Erişim Kontrolünü Yönetme ; Kurumsal kaynaklara uzaktan bağlanan varlıklar için erişim kontrolünü yönetin. Şunlara dayalı olarak kurumsal kaynaklara erişim miktarını belirleyiniz ; yüklü güncel kötü amaçlı yazılımdan koruma yazılımı , kuruluşun güvenli yapılandırma süreciyle yapılandırma uyumluluğu ve işletim sistemi ve uygulamaların güncel olmasını sağlama.

13.6 - Ağ Trafiği Akış Günlüklerini Toplayın ; Gözden geçirmek ve ağ cihazlarından uyarı almak için ağ trafiği akış günlüklerini veya ağ trafiğini toplayınız.

13.7 - Host Bilgisayar Tabanlı Saldırı Önleme Çözümü Dağıtın ; Uygun olduğunda veya desteklendiğinde , kurumsal varlıklara host bilgisayar tabanlı izinsiz giriş önleme çözümü dağıtın. Örnek uygulamalar, Uç Nokta Algılama ve Yanıt (EDR) istemcisinin veya host bilgisayar tabanlı IPS aracısının kullanımını içerir.

13.8 - Ağa İzinsiz Girişi Önleme Çözümü Dağıtın ; Uygun olduğunda , ağa izinsiz giriş önleme çözümü dağıtınız. Örnek uygulamalar , Ağa İzinsiz Giriş Önleme Sistemi (NIPS) veya eşdeğer CSP hizmetinin kullanımını içerir.

13.9 - Bağlantı Noktası Düzeyinde Erişim Denetimi Dağıtma ; Bağlantı noktası düzeyinde erişim denetimi dağıtınız. Bağlantı noktası düzeyinde erişim kontrolü , 802.1x veya sertifikalar gibi benzer ağ erişim kontrolü protokollerini kullanır ve kullanıcı veya cihaz kimlik doğrulamasını içerebilir.

13.10 - Uygulama Katmanı Filtreleme Gerçekleştirin ; Uygulama katmanı filtrelemesi gerçekleştiriniz. Örnek uygulamalar arasında filtreleme proksisi , uygulama katmanı güvenlik duvarı veya ağ geçidi bulunur.

13.11 - Güvenlik Olayı Uyarı Eşiklerini Ayarlayın ; Hassas verileri içeren sunucularda , uygulamalarda ve veritabanlarında bekleyen hassas verileri şifreleyiniz. Sunucu tarafı şifreleme olarak da bilinen depolama katmanı şifrelemesi , korumanın minimum gereksinimini karşılar. Ek şifreleme yöntemleri , veri depolama aygıtına / cihazlarına erişimin düz metin verilerine erişime izin vermediği durumlarda , istemci tarafı şifreleme olarak da bilinen uygulama katmanı şifrelemesini içerebilir.

CIS Kritik Güvenlik Kontrolü 14- Güvenlik Bilinci ve Becerileri Eğitimi ; Kuruma yönelik siber güvenlik risklerini azaltmak için güvenlik bilincine sahip ve uygun becerilere sahip olmak için işgücü arasındaki davranışları etkilemek için güvenlik bilinci programı oluşturun ve sürdürünüz. İnsanların eylemleri , kuruluşun güvenlik programının başarısında veya başarısızlığında kritik rol oynar. Saldırganın , kuruluşa girmek için kötü amaçlı yazılım yüklemek üzere kullanıcıyı bir bağlantıyı tıklamaya veya bir e-posta ekini açmaya ikna etmesi , bunu doğrudan yapmak için ağ istismarı bulmaktan daha kolaydır. Hassas verilerin yanlış kullanılması , hassas veriler içeren e-postanın yanlış alıcıya gönderilmesi , taşınabilir son kullanıcı cihazının kaybedilmesi , zayıf parolaların kullanılması veya genel sitelerde kullandıkları parolanın aynısının kullanılması sonucunda olaylara neden olur. Hiçbir güvenlik programı etkili şekilde ele alamaz. İşletmenin her seviyesindeki kullanıcılar farklı risklere sahiptir. Yöneticiler daha hassas verileri yönetirken sistem yöneticileri , sistemlere ve uygulamalara erişimi kontrol etme becerisine sahiptir. Finans , insan kaynakları ve sözleşmelerdeki kullanıcıların tümü , kendilerini hedef haline getirebilecek farklı türde hassas verilere erişebilir. Eğitim düzenli olarak güncellenmelidir. Güvenlik kültürünü artıracak ve riskli geçici çözümleri caydıracaktır.

Prosedürler ve Araçlar ; Etkili güvenlik bilinci eğitim programı , yalnızca düzenli kimlik avı testiyle birlikte yılda bir kez hazır eğitim videosu olmamalıdır. Yıllık eğitim gerekli olmakla birlikte , güvenlikle ilgili daha sık , güncel mesajlar ve bildirimler de olmalıdır. Şunlarla ilgili mesajları içerebilir ; medya raporuna denk gelen parola dökümü , vergi döneminde kimlik avının artması veya tatillerde kötü niyetli paket teslimatı e-postalarının farkındalığının artması. Finans firmaları , veri işleme ve kullanımı , sağlık işletmeleri sağlık verilerinin işlenmesi ve satıcılar için kredi kartı verileri konusunda uyumlulukla ilgili daha fazla eğitime sahip olabilir. Kimlik avı testleri gibi sosyal mühendislik eğitimleri , farklı rolleri hedefleyen taktiklerin farkındalığını da içermelidir. Finans ekibi , para havalesi yapmak isteyen yöneticiler gibi görünen BEC girişimleri veya güvenliği ihlal edilmiş ortaklardan veya satıcılardan sonraki ödemeleri için banka hesap bilgilerini değiştirmelerini isteyen e-postalar alacaktır.

Kaynaklar ; NIST® SP 800-50 Infosec Awareness Training , National Cyber Security Centre , EDUCAUSE , National Cyber Security Alliance (NCSA) , SANS , Telework and Small Office Network Security Guide .

Alınacak Güvenlik Önlemleri ;

14.1 - Güvenlik Farkındalık Programı Oluşturma ve Sürdürme ; Güvenlik bilinci programı oluşturun ve sürdürünüz. Güvenlik bilinci programının amacı , kurumun iş gücünü kurumsal varlıklar ve verilerle güvenli şekilde nasıl etkileşime gireceği konusunda eğitmektir. Eğitimi işe alarak ve en azından yıllık olarak gerçekleştiriniz. İçeriği yıllık olarak veya korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyiniz.

14.2 - İşgücü Üyelerini Sosyal Mühendislik Saldırılarını Tanıyacak Şekilde Eğitmek ; İş gücü üyelerini kimlik avı , ön mesaj gönderme ve takip etme gibi sosyal mühendislik saldırılarını tanımaları için eğitiniz.

14.3 - İş Gücü Üyelerini Kimlik Doğrulama En İyi Uygulamaları konusunda Eğitin ; İş gücü üyelerini en iyi kimlik doğrulama uygulamaları konusunda eğitiniz. Örnek konular arasında MFA , parola oluşturma ve kimlik bilgisi yönetimi yer alır.

14.4 - İş Gücünü Veri İşleme En İyi Uygulamaları konusunda Eğitin ; İş gücü üyelerini hassas verilerin nasıl tanımlanacağı ve uygun şekilde depolanacağı , aktarılacağı , arşivleneceği ve imha edileceği konusunda eğitiniz.

Kurumsal varlıklarından uzaklaştıklarında ekranlarını kilitleme , toplantıların sonunda fiziksel ve sanal beyaz tahtaları silme , veri ve varlıkları güvenli şekilde depolama gibi net ekran ve masa üstü en iyi uygulamaları konusunda iş gücü üyelerine eğitim vermeyi de içerir.

14.5 - İşgücü Üyelerini Kasıtsız Verilere Maruz Kalma Nedenleri Konusunda Eğitin ; İşgücü üyelerini , kasıtsız veri maruziyetinin nedenlerinin farkında olmaları için eğitiniz. Örnek konular arasında hassas verilerin yanlış teslimi , taşınabilir son kullanıcı cihazının kaybolması veya istenmeyen kitlelere veri yayınlanması sayılabilir.

14.6 - İşgücü Üyelerini Güvenlik Olaylarını Tanıma ve Raporlama konusunda Eğitin ; Potansiyel bir olayı fark edebilmek ve böyle bir olayı rapor edebilmek için işgücü üyelerini eğitiniz.

14.7 - İşgücünü Kurumsal Varlıklarında Güvenlik Güncelleştirmelerinin Eksik Olup Olmadığını Belirleme ve Raporlama Konusunda Eğitme ; Güncel olmayan yazılım yamalarının veya otomatik süreçler ile araçlarda ki herhangi bir arızanın nasıl doğrulanacağını ve raporlanacağını anlamak için işgücünü eğitiniz. Bu eğitimin bir kısmı , otomatikleştirilmiş süreçler ve araçlardaki herhangi bir arızanın BT personeline bildirilmesini içermelidir.

14.8 - İşgücünü Güvensiz Ağlara Bağlanmanın ve Kurumsal Verileri İletmenin Tehlikeleri Konusunda Eğitme ; Uygun olduğunda , ağa izinsiz giriş önleme çözümü dağıtın. Örnek uygulamalar , Ağa İzinsiz Giriş Önleme Sistemi (NIPS) veya eşdeğer CSP hizmetinin kullanımını içerir.

14.9 - Role Özgü Güvenlik Farkındalığı ve Becerileri Eğitimi Yürütme ; Role özel güvenlik farkındalığı ve becerileri eğitimi gerçekleştiriniz. Örnek uygulamalar arasında BT uzmanları için güvenli sistem yönetimi kursları , web uygulaması geliştiricileri için OWASP® En İyi 10 güvenlik açığı farkındalığı ve önleme eğitimi , yüksek profilli roller için gelişmiş sosyal mühendislik farkındalık eğitimi yer alır.

CIS Kritik Güvenlik Kontrolü 15 - Servis Sağlayıcı Yönetimi ; Hassas verileri elinde bulunduran veya bir kuruluşun kritik BT platformlarından veya süreçlerinden sorumlu olan hizmet sağlayıcıların bu platformları ve verileri uygun şekilde koruduğundan emin olmak için süreç geliştiriniz. Modern , bağlantılı dünyamızda kuruluşlar , verilerini yönetmeye yardımcı olmaları için satıcılara ve ortaklara ya da temel uygulamalar veya işlevler için üçüncü taraf altyapısına güvenirler. Üçüncü taraf ihlallerinin işletmeyi önemli ölçüde etkilediği çok sayıda örnek olmuştur. Doğrudan bağlanırsa , fidye yazılımı saldırısı ana kuruluştaki verileri şifreleyebilir. Çoğu veri güvenliği ve gizlilik düzenlemesi , korumalarının , Sağlık Sigortası Taşınabilirlik ve Hesap Verebilirlik Yasası (HIPAA) Sağlık hizmetlerindeki İş Ortağı anlaşmaları , finans sektörü için Federal Finansal Kurumlar İnceleme Konseyi (FFIEC) gereksinimleri gibi üçüncü taraf hizmet sağlayıcılarını kapsamasını gerektirir. Üçüncü taraf güveni , kuruluş içinde yönetilmeyen riskler kuruluş dışındaki kuruluşlara devredildiğinden , temel Yönetişim Riski ve Uyumluluk (GRC) işlevidir. Üçüncü şahısların güvenliğini gözden geçirmek on yıllardır gerçekleştirilen görev olsa da , güvenliği değerlendirmek için evrensel standart yoktur ve birçok hizmet sağlayıcı , müşterileri tarafından ayda birkaç kez denetleniyor ve bu da kendi üretkenliklerini etkiliyor. Bunun nedeni , her işletmenin hizmet sağlayıcıyı derecelendirmek için farklı kontrol listesi veya bir dizi standardı olmasıdır. Finans alanında , Paylaşılan Değerlendirmeler programıyla veya Yüksek Öğrenim Topluluk Satıcısı Değerlendirme Araç Seti (HECVAT) ile yüksek öğrenimde olduğu gibi yalnızca birkaç endüstri standardı vardır. Siber güvenlik poliçesi satan sigorta şirketlerinin de kendi ölçüleri vardır. Bir kuruluş , e-postalarını veya kritik iş uygulamalarını barındırdıkları için büyük bulut veya uygulama barındırma şirketlerini çok fazla incelemeye tabi tutabilirken , daha küçük şirketler genelde daha büyük risk taşır. Çoğu zaman , üçüncü taraf hizmet sağlayıcı , diğer eklentileri veya hizmetleri sağlamak için ek taraflarla sözleşme yapar.

Prosedürler ve Araçlar ; Çoğu kuruluş , ISO 27001 veya CIS Kontrolleri gibi standart kontrol listelerini geleneksel olarak kullanmıştır. Çoğu zaman , bu süreç elektronik tablolar aracılığıyla yönetilir fakat artık bu sürecin merkezi yönetimine izin veren çevrimiçi platformlar vardır. Bu CIS Kontrolünün odak noktası kontrol listesinde yer almasa da , bunun yerine programın temelleri üzerindedir. İlişkiler ve veriler değişebileceğinden , her yıl tekrar ziyaret ettiğinizden emin olunuz. İşletmenin büyüklüğü ne olursa olsun , hizmet sağlayıcıları , bu satıcıların envanterini ve olay durumunda işletme üzerindeki potansiyel etkileriyle ilişkili bir risk derecelendirmesini gözden geçirme politikası olmalıdır. İşletmeyi etkileyen olay olduğunda onları sorumlu tutmak için sözleşmelerde dil olmalıdır. Sektöre merkezi bakış sağlamaya çalışan , binlerce hizmet sağlayıcı envanterine sahip üçüncü taraf değerlendirme platformları vardır. işletmelerin daha bilinçli risk kararları almalarına yardımcı olmaktır. Bu platformlar genellikle pasif teknik değerlendirmelere dayalı veya diğer firmaların üçüncü taraf değerlendirmeleriyle zenginleştirilmiş hizmet sağlayıcılar için dinamik risk puanına sahiptir. İncelemeleri gerçekleştirirken , sağlayıcının işletmeyi destekleyen hizmetlerine veya bölümlerine odaklanınız. Yönetilen güvenlik hizmeti sözleşmesine veya hizmet sağlayıcısına sahip olan , siber güvenlik sigortasına sahip üçüncü taraf da riskin azaltılmasına yardımcı olabilir. Sözleşmeler tamamlandığında veya feshedildiğinde hizmet sağlayıcıların güvenli şekilde hizmet dışı bırakılması da önemlidir. Hizmetten çıkarma faaliyetleri , kullanıcı ve hizmet hesabının devre dışı bırakılmasını , veri akışlarının sonlandırılmasını ve hizmet sağlayıcı sistemlerinde kurumsal verilerin güvenli bir şekilde elden çıkarılmasını içerebilir.

Alınacak Güvenlik Önlemleri ;

15.1 - Hizmet Sağlayıcıların Envanterinin Oluşturulması ve Bakımının Yapılması ; Hizmet sağlayıcıların envanterini oluşturun ve sürdürünüz. Envanter , bilinen tüm hizmet sağlayıcıları listelemek , sınıflandırmaları dahil etmek ve her bir hizmet sağlayıcı için bir kurumsal irtibat kişisi belirlemek içindir. Envanteri yıllık olarak veya korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyiniz.

15.2 - Hizmet Sağlayıcı Yönetim Politikasının Oluşturulması ve Sürdürülmesi ; Hizmet sağlayıcı yönetim politikası oluşturun ve sürdürünüz. Politikanın hizmet sağlayıcıların sınıflandırılmasını , envanterini , değerlendirmesini , izlenmesini ve hizmetten çıkarılmasını ele aldığından emin olunuz. Politikayı yıllık olarak veya korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyiniz.

15.3 - Hizmet Sağlayıcıları Sınıflandırın ; Servis sağlayıcıları sınıflandırınız. Sınıflandırma değerlendirmesi , veri duyarlılığı , veri hacmi , kullanılabilirlik gereksinimleri , geçerli düzenlemeler , yapısal risk ve azaltılmış risk gibi bir veya daha fazla özelliği içerebilir. Sınıflandırmaları yıllık olarak veya korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde güncelleyin ve gözden geçiriniz.

15.4 Hizmet Sağlayıcı Sözleşmelerinin Şunları Kapsadığından Emin Olun ; Servis sağlayıcı sözleşmelerinin güvenlik gereksinimlerini içerdiğinden emin olunuz. Örnek gereksinimler , minimum güvenlik programı gereksinimleri , güvenlik olayı veya veri ihlali bildirimi ve yanıtı , veri şifreleme gereksinimleri ve veri imha taahhütlerini içerebilir. Bu güvenlik gereksinimleri , işletmenin hizmet sağlayıcı yönetim politikasıyla tutarlı olmalıdır.

15.5 - Hizmet Sağlayıcıları Değerlendirme ; Kuruluşun hizmet sağlayıcı yönetim politikasına uygun olarak hizmet sağlayıcıları değerlendiriniz. Değerlendirme kapsamı , sınıflandırmalara göre değişiklik gösterebilir ve Hizmet Organizasyonu Kontrolü 2 (SOC 2) ve Ödeme Kartı Endüstrisi (PCI) Uygunluk Teyidi (AoC) , özelleştirilmiş anketler veya diğer uygun şekilde standartlaştırılmış değerlendirme raporlarının gözden geçirilmesini içerebilir. Hizmet sağlayıcıları en azından yıllık olarak veya yeni ve yenilenmiş sözleşmelerle yeniden değerlendiriniz.

15.6 - Hizmet Sağlayıcıları İzleme ; Kuruluşun hizmet sağlayıcı yönetim politikasına uygun olarak hizmet sağlayıcıları izleyiniz. İzleme , hizmet sağlayıcı uyumluluğunun periyodik olarak yeniden değerlendirilmesini , hizmet sağlayıcı sürüm notlarının izlenmesini ve karanlık web izlemesini içerebilir.

15.7 - Güvenli Hizmetten Çıkarma Hizmet Sağlayıcıları ; Güvenli şekilde hizmetten çıkarma hizmeti sağlayıcılarıdır Örnek hususlar , kullanıcı ve hizmet hesabının devre dışı bırakılmasını , veri akışlarının sonlandırılmasını ve hizmet sağlayıcı sistemlerinde kurumsal verilerin güvenli bir şekilde elden çıkarılmasını içerir.

CIS Kritik Güvenlik Kontrolü 16 - Uygulamalar Yazılım Güvenliği ; Güvenlik zayıflıklarını işletmeyi etkilemeden önce önlemek , tespit etmek ve gidermek için kurum içinde geliştirilen , barındırılan veya satın alınan yazılımların güvenlik yaşam döngüsünü yönetmeniz gereklidir. Uygulamalar , kullanıcıların verilere işletme işlevleriyle uyumlu şekilde erişmesine ve bunları yönetmesine olanak tanıyan insan dostu arayüz sağlar. Kullanıcıların dosyaları eklemek veya değiştirmek için veritabanına giriş yapmak gibi karmaşık ve potansiyel olarak hataya açık sistem işlevleriyle doğrudan ilgilenme ihtiyacını da en aza indirirler. Kuruluşlar , en hassas verilerini yönetmek ve sistem kaynaklarına erişimi kontrol etmek için uygulamaları kullanır. Bu nedenle , saldırgan , ağ güvenlik kontrollerini ve sensörlerini atlamaya çalışan ayrıntılı ağ ve sistem korsanlığı dizisi yerine verileri tehlikeye atmak için uygulamanın kendisini kullanabilir. Bu nedenle , CIS Control 6'da tanımlanan kullanıcı kimlik bilgilerinin (özellikle uygulama kimlik bilgilerinin) korunması çok önemlidir. Kimlik bilgilerinin olmaması , uygulama kusurları tercih edilen saldırı vektörüdür. Günümüz uygulamaları oldukça karmaşık , çeşitli ve dinamik ortamda geliştirilmekte , işletilmekte ve sürdürülmektedir. Uygulamalar birden çok platformda çalışır ; eski istemci-sunucu veya veritabanı-web sunucusu yapılarından daha karmaşık uygulama mimarileriyle web , mobil , bulut vb. . Geliştirme yaşam döngüleri , uzun şelale metodolojilerinde aylar veya yıllardan sık kod güncellemeleriyle DevOps döngülerine geçiş yaparak kısalmıştır. Uygulamalar nadiren sıfırdan oluşturulur ve genelde geliştirme çerçevelerinin , kitaplıkların , mevcut kodun ve yeni kodun karmaşık karışımından birleştirilir. Kullanıcı gizliliğiyle ilgili modern ve gelişen veri koruma düzenlemeleri de vardır. Bölgesel veya sektöre özel veri koruma gereksinimlerine uyumu gerektirebilir. Bu faktörler , kontrol (süreçler , kod kaynakları , çalışma zamanı ortamı vb.) , inceleme ve test etme gibi geleneksel güvenlik yaklaşımlarını çok daha zorlu hale getirir. Uygulama güvenlik açığının getirdiği risk , belirli operasyonel ortam veya bağlam dışında anlaşılmayabilir. Uygulama güvenlik açıkları birçok nedenden dolayı mevcut olabilir ; güvenli olmayan tasarım , güvenli olmayan altyapı , kodlama hataları , zayıf kimlik doğrulama , olağandışı veya beklenmedik koşullar için test yapılmaması. Saldırganlar , arabellek taşmaları , Yapılandırılmış Sorgu Dili (SQL) enjeksiyonuna maruz kalma , siteler arası komut dosyası çalıştırma , siteler arası istek sahteciliği ve hassas verilere erişim elde etmek veya savunmasız varlıklar üzerinde kontrolü ele geçirmek için koda tıklama dahil olmak üzere belirli güvenlik açıklarından yararlanabilir. Uygulamalar ve web siteleri , kimlik bilgilerini , verileri toplamak veya bunlara erişen kullanıcılara kötü amaçlı yazılım yüklemeye çalışmak için de kullanılabilir. Yazılımın tamamen üçüncü taraf aracılığıyla geliştirildiği ve yönetildiği Hizmet Olarak Yazılım (SaaS) platformlarını satın almak artık daha yaygındır. Bunlar dünyanın herhangi bir yerinde barındırılabilir. Bu platformları kullanırken hangi riskleri kabul ettiklerini bilmesi gereken işletmeler zorluklarla karşılaşmakta ve genelde bu platformların geliştirme ve uygulama güvenliği uygulamalarına ilişkin görünürlükleri yoktur. Bu SaaS platformlarından bazıları , arayüzlerinin ve veritabanlarının özelleştirilmesine izin verir. Bu uygulamaları genişleten kuruluşlar , temelden müşteri geliştirme yapıyormuş gibi CIS Kontrolünü izlemelidir.

Prosedürler ve Araçlar ; Sürüm 8 için CIS , bu güncellenmiş Uygulama Yazılımı Güvenlik Kontrolü için prosedürlerin ve korumaların geliştirilmesine yardımcı olmak için SAFECode ile ortaklık kurmuştur. Uygulama yazılımı güvenliği başlı başına geniş konudur. Bunlar , SAFECode'un geliştirdiği uygulama yazılımı güvenliğine ilişkin , konunun daha derinlemesine ele alınmasını sağlayan ve SAFECode'un mevcut içerik yapısıyla tutarlı olan tamamlayıcı belgeden türetilmiştir. SAFECode , okuyucuların geliştirme programları için olgunluk ölçeği olarak hangi Geliştirme Grubuna (DG) uyduklarını belirlemelerine yardımcı olmak için üç aşamalı yaklaşım geliştirmiştir. Koruma Tedbirlerinde kullanılan üç CIS IG seviyesi , şu DG'lere yönelik yaklaşımlarına ilham vermiştir ;

Geliştirme Grubu 1 ; Kuruluş , büyük ölçüde kullanıma hazır veya Açık Kaynaklı Yazılımlara (OSS) , sadece ara sıra küçük uygulamaların veya web sitesi kodlamasının eklendiği paketlere dayanır. Kuruluş , temel operasyonel ve prosedüre ilişkin en iyi uygulamaları uygulama ve satıcı tarafından sağlanan yazılımın güvenliğini CIS Kontrollerinin kılavuzluğunu izlemenin sonucu olarak yönetme yeteneğine sahiptir.

Geliştirme Grubu 2 ; Kuruluş , üçüncü taraf bileşenlerle entegre bazı özel (şirket içi veya yüklenici tarafından geliştirilen) web veya yerel kod uygulamalarına güvenerek şirket içinde veya bulutta çalışır. Kuruluş , yazılım geliştirme en iyi uygulamalarını uygulayan geliştirme ekibine sahiptir. İşletme , bağlı olduğu üçüncü taraf açık kaynak veya ticari kodun kalitesine ve bakımına özen gösterir.

Geliştirme Grubu 3 ; İşletme , işini yürütmek ve müşterilerine hizmet vermek için ihtiyaç duyduğu özel yazılımlara büyük yatırım yapar. Yazılımı kendi altyapısında , bulutta veya her ikisinde barındırabilir. Çok çeşitli üçüncü taraf açık kaynak ve ticari yazılım bileşenlerini entegre edebilir. SaaS sağlayan yazılım satıcıları ve kuruluşlar , Geliştirme Grubu 3'ü minimum gereksinimler dizisi olarak değerlendirmelidir.

Uygulama güvenlik programı geliştirmenin ilk adımı , güvenlik açığı yönetimi sürecini uygulamaktır. Bu süreç , geliştirme yaşam döngüsüne entegre olmalı ve standart hata düzeltme ilerlemesine eklemek için hafif olmalıdır. Süreç , gelecekteki güvenlik açıklarını azaltmak için altta yatan kusurları düzeltmek için kök neden analizini ve iyileştirme çabalarına öncelik vermek için önem derecesini içermelidir. Geliştiricilerin uygulama güvenliği kavramları ve güvenli kodlama uygulamaları konusunda eğitilmesi gerekir. Güvenlik kusurları oluşturmadıklarından emin olmak için uygulamada kullanılan üçüncü taraf yazılımları , modülleri ve kitaplıkları edinme veya değerlendirme sürecini içerir. Geliştiricilere ne tür modülleri güvenli şekilde kullanabilecekleri , nereden güvenli şekilde edinilebilecekleri ve hangi bileşenleri kendilerinin geliştirip geliştirmemeleri gerektiği öğretilmelidir. Bu uygulamaları destekleyen altyapıdaki zayıflıklar risk oluşturabilir. CIS Kontrolleri ve saldırı yüzeyini en aza indirme konsepti , uygulama içinde kullanılan ağların , sistemlerin ve hesapların güvenliğini sağlamaya yardımcı olabilir.

İdeal uygulama güvenliği programı , güvenliği yazılım geliştirme yaşam döngüsüne mümkün olduğunca erken getiren programdır. Güvenlik sorunlarının yönetimi , geliştirme kaynakları için rekabet eden ayrı bir sürecin aksine , standart yazılım kusur / hata yönetimi ile tutarlı ve entegre olmalıdır. Daha büyük veya daha olgun geliştirme ekipleri , tasarım aşamasında tehdit modelleme uygulamasını dikkate almalıdır. Tasarım düzeyindeki güvenlik açıkları , kod düzeyindeki güvenlik açıklarından daha az yaygındır. Genelde çok şiddetlidir ve hızlı şekilde düzeltilmesi çok daha zordur. Tehdit modelleme , kod oluşturulmadan önce uygulama güvenliği tasarım kusurlarını belirleme ve giderme sürecidir. Tehdit modellemesi , özel eğitim , teknik ve iş bilgisi gerektirir. Her geliştirme ekibinde , o ekibin yazılımı için tehdit modelleme uygulamalarına liderlik etmek üzere en iyi şekilde dahili güvenlik şampiyonları aracılığıyla yürütülür. Kök neden analizi ve güvenlik testi gibi aşağı akış faaliyetleri için değerli bağlam sağlar. Daha büyük veya ticari geliştirme ekipleri , uygulamalarında kusurları bulmak için bireylere ödeme yapılan hata ödül programı da düşünebilir. Böyle bir program en iyi şekilde kurum içi güvenli geliştirme sürecini desteklemek için kullanılır ve sürecin odaklanması gereken güvenlik açıklarının sınıflarını belirlemek için etkili mekanizma sağlayabilir.

Kaynaklar ; NIST® SSDF , NIST® FIPS 140-3 , The Software Alliance , OWASP® .

Alınacak Güvenlik önlemleri ;

16.1 - Güvenli Uygulama Geliştirme Süreci Oluşturma ve Sürdürme ; Güvenli uygulama geliştirme süreci oluşturun ve sürdürünüz. Bu süreçte , güvenli uygulama tasarım standartları , güvenli kodlama uygulamaları , geliştirici eğitimi , güvenlik açığı yönetimi , üçüncü taraf kodunun güvenliği , uygulama güvenliği test prosedürleri gibi öğeleri ele alınız. Belgeleri yıllık olarak veya korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyiniz.

16.2 - Yazılım Açıklarını Kabul Etmek ve Ele Almak için Süreç Oluşturma ve Sürdürme ; Harici varlıkların raporlaması için araç sağlamak da dahil olmak üzere , yazılım güvenlik açıklarının raporlarını kabul etmek ve ele almak için süreç oluşturun ve sürdürünüz. Süreç , şu öğeleri içerecektir ; raporlama sürecini tanımlayan güvenlik açığı işleme politikası , güvenlik açığı raporlarının işlenmesinden sorumlu taraf ve alım , atama ve iyileştirme testi için süreç.

Sürecin bir parçası olarak , güvenlik açıklarının tanımlanması , analizi ve düzeltilmesi için zamanlamayı ölçmek için önem dereceleri ve ölçümler içeren güvenlik açığı izleme sistemi kullanınız. Belgeleri yıllık olarak veya korumayı etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçirin ve güncelleyiniz. Üçüncü taraf uygulama geliştiricilerinin bunu , dış paydaşlar için beklentileri belirlemeye yardımcı olan , dışa dönük politika olarak görmesi gerekir.

16.3 - Güvenlik Açıkları Üzerinde Kök Neden Analizi Gerçekleştirme ; Güvenlik açıkları üzerinde kök neden analizi yapınız. Güvenlik açıklarını gözden geçirirken , kök neden analizi , kodda güvenlik açıkları oluşturan temel sorunları değerlendirme görevidir ve geliştirme ekiplerinin yalnızca ortaya çıktıkları anda tek tek güvenlik açıklarını düzeltmenin ötesine geçmesine olanak tanır.

16.4 - Üçüncü Kişi Yazılım Bileşenleri Envanterini Oluşturma ve Yönetme ; Geliştirmede kullanılan ve genelde malzeme listesi olarak adlandırılan üçüncü taraf bileşenlerinin yanı sıra gelecekte kullanılmak üzere planlanmış bileşenlerin güncellenmiş envanterini oluşturun ve yönetiniz. Bu envanter , her bir üçüncü taraf bileşeninin oluşturabileceği riskleri içerecektir. Bu bileşenlerde yapılan değişiklikleri veya güncellemeleri belirlemek için listeyi en az ayda bir değerlendirin ve bileşenin hala desteklendiğini doğrulayınız.

16.5 - Güncel ve Güvenilir Üçüncü Kişi Yazılım Bileşenlerini Kullanma ; Güncel ve güvenilir üçüncü taraf yazılım bileşenlerini kullanınız. Mümkün olduğunda , yeterli güvenlik sağlayan yerleşik ve kanıtlanmış çerçeveler ve kitaplıklar seçiniz. Bu bileşenleri güvenilir kaynaklardan edinin veya kullanmadan önce yazılımı güvenlik açıkları açısından değerlendiriniz.

16.6 - Uygulama Güvenlik Açıkları için Önem Derecelendirme Sistemi ve Süreci Oluşturma ile Sürdürme ; Keşfedilen güvenlik açıklarının düzeltildiği sıraya öncelik verilmesini kolaylaştıran uygulama güvenlik açıkları için bir önem derecesi derecelendirme sistemiyle süreci oluşturun ve sürdürünüz. Bu süreç , kod veya uygulamaların serbest bırakılması için minimum güvenlik kabul edilebilirliği düzeyini ayarlamayı içerir. Önem dereceleri , risk yönetimini geliştiren ve en ciddi hataların ilk önce düzeltilmesini sağlamaya yardımcı olan güvenlik açıklarını tetiklemek için sistematik bir yol sunar. Sistemi ve süreci yıllık olarak gözden geçirin ve güncelleyiniz.

16.7 - Uygulama Altyapısı için Standart Sertleştirme Yapılandırma Şablonlarını Kullanma ; Uygulama altyapısı bileşenleri için standart , endüstri tarafından önerilen sağlamlaştırma yapılandırma şablonlarını kullanınız. Temel sunucuları , veritabanlarını ve web sunucularını içerir ve bulut kapsayıcıları , Hizmet olarak Platform (PaaS) bileşenleri ve SaaS bileşenleri için geçerlidir. Şirket içinde geliştirilen yazılımın yapılandırma sağlamlaştırmasını zayıflatmasına izin vermeyiniz.

16.8 - Ayrı Üretim ve Üretim Dışı Sistemler ; Üretim ve üretim dışı sistemler için ayrı ortamlar sağlayınız.

16.9 - Geliştiricileri Uygulama Güvenliği Kavramları ve Güvenli Kodlama Konusunda Eğitme ; Tüm yazılım geliştirme personelinin , kendi özel geliştirme ortamları ve sorumlulukları için güvenli kod yazma konusunda eğitim almalarını sağlayın. Eğitim , genel güvenlik ilkelerini ve uygulama güvenliği standart uygulamalarını içerebilir. En az yılda bir kez eğitim yapın ve geliştirme ekibi içinde güvenliği teşvik edecek şekilde tasarım yapın ve geliştiriciler arasında güvenlik kültürü oluşturunuz.

16.10 - Güvenli Tasarım İlkelerini Uygulama Mimarilerinde Uygulamak ; Uygulama mimarilerinde güvenli tasarım ilkelerini uygulayınız. Güvenli tasarım ilkeleri , en az ayrıcalık kavramını ve kullanıcının yaptığı her işlemi doğrulamak için arabuluculuğu zorunlu kılarak " kullanıcı girdisine asla güvenme " kavramını teşvik eder. Tüm girdiler için açık hata denetiminin gerçekleştirilmesini ve belgelenmesini içerir. Güvenli tasarım , korumasız bağlantı noktalarını ve hizmetleri kapatmak , gereksiz programları ve dosyaları kaldırmak ve varsayılan hesapları yeniden adlandırmak veya kaldırmak gibi uygulama altyapısı saldırı yüzeyini en aza indirmek anlamına gelir.

16.11 - Uygulama Güvenliği Bileşenleri için Kontrol Edilen Modüller veya Hizmetlerden Yararlanma ; Kimlik yönetimi , şifreleme ve denetleme , günlüğe kaydetme gibi uygulama güvenliği bileşenleri için onaylanmış modüllerden veya hizmetlerden yararlanınız. Platform özelliklerinin kritik güvenlik işlevlerinde kullanılması , geliştiricilerin iş yükünü azaltacak ve tasarım veya uygulama hataları olasılığını en aza indirecektir. Modern işletim sistemleri , tanımlama , kimlik doğrulama ve yetkilendirme için etkili mekanizmalar sağlar ve bu mekanizmaları uygulamalar için kullanılabilir hale getirir. Yalnızca standartlaştırılmış , şu anda kabul edilmiş ve kapsamlı şekilde gözden geçirilmiş şifreleme algoritmalarını kullanınız. İşletim sistemleri güvenli denetim günlükleri oluşturmak ve sürdürmek için mekanizmalar sağlar.

16.12 - Kod Düzeyinde Güvenlik Kontrolleri Uygulama ; Güvenli kodlama uygulamalarının takip edildiğini doğrulamak için uygulama yaşam döngüsü içinde statik ve dinamik analiz araçları uygulayınız.

16.13 - Uygulama Sızma Testini Gerçekleştirme ; Uygulama penetrasyon testi yapınız. Kritik uygulamalar için kimliği doğrulanmış sızma testi , iş mantığı güvenlik açıklarını bulmak için kod tarama ve otomatik güvenlik testinden daha uygundur. Penetrasyon testi , test cihazının uygulamayı kimliği doğrulanmış ve kimliği doğrulanmamış kullanıcı olarak manuel olarak değiştirme becerisine dayanır.

16.14 - Tehdit Modelleme Davranışı ; Tehdit modellemesi yapınız. Tehdit modelleme , kod oluşturulmadan önce tasarımdaki uygulama güvenliği tasarım kusurlarını belirleme ve ele alma sürecidir. Uygulama tasarımını değerlendiren ve her giriş noktası ve erişim seviyesi için güvenlik risklerini ölçen özel eğitimli kişiler tarafından gerçekleştirilir. Amaç , zayıflıklarını anlamak için uygulamayı , mimariyi ve altyapıyı yapılandırılmış şekilde haritalandırmaktır.

CIS Kritik Güvenlik Kontrolü 17 - Olay Müdahale Yönetimi ; Saldırıyı hazırlamak , tespit etmek ve hızlı şekilde yanıt vermek için olay müdahale yeteneği (politikalar , planlar , prosedürler , tanımlanmış roller , eğitim , iletişimler) geliştirmek ve sürdürmek için program oluşturunuz. Kapsamlı siber güvenlik programı , koruma , algılama , yanıt ve kurtarma özelliklerini içerir. Çoğu zaman , son ikisi olgunlaşmamış işletmelerde gözden kaçar veya tehlikeye atılmış sistemlere yanıt verme tekniği , onları orijinal hallerine yeniden getirerek devam etmektir. Olay müdahalesinin birinci amacı , kuruluştaki tehditleri belirleyerek yayılmadan önce bunlara yanıt vermek ve zarar vermeden önce onları düzeltmektir. Olayın tam kapsamını , nasıl olduğunu ve tekrar olmasını önlemek için ne yapılabileceğini anlamadan , savunucular sürekli köstebek vurma düzeni içinde olacaklardır. Korumalarımızın her zaman %100 etkili olmasını bekleyemeyiz. Olay meydana geldiğinde , bir kuruluşun belgelenmiş planı yoksa , doğru soruşturma prosedürlerini , raporlamayı , veri toplamayı , yönetim sorumluluğunu , yasal protokolleri ve kuruluşa izin verecek iletişim stratejisini bilmek neredeyse imkansızdır. Tespit , sınırlama ve yok etme ile birlikte paydaşlarla iletişim anahtardır. Siber olay nedeniyle maddi etki olasılığını azaltacaksak , işletmenin liderliği , işletmeyi en iyi destekleyen iyileştirme veya restorasyon kararlarına öncelik verilmesine yardımcı olabilmeleri için olası etkilerin neler olabileceğini bilmelidir. Bu iş kararları , mevzuata uygunluk , ifşa kuralları , ortaklar veya müşterilerle hizmet düzeyi anlaşmaları , gelir veya görev etkilerine dayanabilir. Saldırının gerçekleştiği andan tanımlandığı ana kadar geçen bekleme süresi günler , haftalar veya aylar olabilir. Saldırgan kuruluşun altyapısında ne kadar uzun süre kalırsa , o kadar yerleşik hale gelir ve sonunda keşfedildiklerinde kalıcı erişimi sürdürmek için daha fazla yol geliştirir. Saldırganlar için istikrarlı para kaynağı olan fidye yazılımlarının yükselişiyle birlikte , bu bekleme süresi , özellikle fidye için şifrelemeden önce verileri çalmaya yönelik modern taktikler açısından kritik önem taşıyor.

Prosedürler ve araçlar ; Kuruluş, kuruluş içinde olay yanıtını yürütmek için kaynaklara sahip olmasa bile , bir plana sahip olmak yine de kritik öneme sahiptir. Korumalar ve tespitler için kaynakları , yardım için kimlerin aranacağının listesini ve bilgilerin liderlere , çalışanlara , düzenleyicilere , ortaklara ve müşterilere nasıl iletileceğine ilişkin iletişim planlarını içerecektir. Olay müdahale prosedürlerini tanımladıktan sonra , olay müdahale ekibi veya üçüncü taraf , işletmenin karşı karşıya kaldığı tehditlere ve olası etkilere göre ince ayarlı dizi saldırı senaryosu üzerinden çalışarak , periyodik olarak senaryo tabanlı eğitime katılmalıdır. Bu senaryolar , kurumsal liderliğin ve teknik ekip üyelerinin , olayları ele almaya hazırlamaya yardımcı olmak için olay müdahale sürecindeki rollerini anlamalarına yardımcı olur. Tatbikat ve eğitim senaryolarının , planlar ve süreçlerdeki boşlukları ve daha sonra plana güncellenebilecek beklenmedik bağımlılıkları belirlemesi kaçınılmazdır. Daha olgun işletmeler , olay müdahale süreçlerine tehdit istihbaratını veya tehdit avcılığını dahil etmelidir. Ekibin TTP'lerini izlemek veya aramak için kuruluşlarına veya sektörlerine yönelik kilit veya birinci saldırganları belirleyerek daha proaktif hale gelmesine yardımcı olacaktır. Tespitlere odaklanmaya ve daha hızlı tespit ve düzeltme için yanıt prosedürlerini tanımlamaya yardımcı olacaktır. CIS Kontrolü 17'deki eylemler , kurumsal güvenliği artırabilecek ve kapsamlı olay ile müdahale planının bir parçası olması gereken belirli , yüksek öncelikli adımlar sağlar.

Kaynaklar ; CREST

Alınacak Güvenlik önlemleri ;

17.1 - Olay Yönetimini Yönetecek Personeli Belirleme ; Kuruluşun olay işleme sürecini yönetecek kilit kişi ve en az bir yedek belirleyiniz. Yönetim personeli , olay müdahalesi ve kurtarma çabalarının koordinasyonu ile belgelenmesinden sorumludur. Kuruluş içindeki çalışanlardan , üçüncü taraf satıcılardan veya hibrit yaklaşımdan oluşabilir. Üçüncü taraf satıcı kullanıyorsanız , üçüncü taraf çalışmasını denetlemek için kuruluş içinden en az bir kişi atayınız. Yıllık olarak veya etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçiriniz.

17.2 - Güvenlik Olaylarını Bildirmek için İletişim Bilgilerini Oluşturup Muhafaza Etme ; Güvenlik olayları hakkında bilgilendirilmesi gereken taraflar için iletişim bilgilerini oluşturun ve koruyunuz. İlgili kişiler , dahili personel , üçüncü taraf satıcılar , kolluk kuvvetleri , siber sigorta sağlayıcıları , ilgili devlet kurumları , Bilgi Paylaşımı ve Analiz Merkezi (ISAC) ortakları veya diğer paydaşları içerebilir. Bilgilerin güncel olduğundan emin olmak için kişileri yıllık olarak doğrulayınız.

17.3 - Olayları Raporlamak için Kurumsal Sürecin Oluşturulması ve Sürdürülmesi ; İş gücünün güvenlik olaylarını bildirmesi için kurumsal süreç oluşturun ve sürdürünüz. Süreç , raporlama zaman çerçevesini , rapor edilecek personeli , raporlama mekanizmasını ve rapor edilecek minimum bilgiyi içerir. Sürecin tüm işgücü için kamuya açık olduğundan emin olunuz. Yıllık olarak veya etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçiriniz.

17.4 - Olay Müdahale Süreci Oluşturma ve Sürdürme ; Rolleri ve sorumlulukları , uyumluluk gereksinimlerini ve iletişim planını ele alan olay müdahale süreci oluşturun ve sürdürünüz. Yıllık olarak veya etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçiriniz.

17.5 - Kilit Rolleri ve Sorumlulukları Atama ; Hukuk , BT , bilgi güvenliği , tesisler , halkla ilişkiler , insan kaynakları , olay müdahale ekipleri , uygun olduğu şekilde analistlerden oluşan personel de dahil olmak üzere olay müdahalesi için kilit roller ve sorumluluklar atayınız. Yıllık olarak veya etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçiriniz.

17.6 - Olay Müdahalesi Sırasında İletişim İçin Mekanizmaları Tanımlama ; Güvenlik olayı sırasında iletişim kurmak ve raporlamak için hangi birinci ve ikinci mekanizmaların kullanılacağını belirleyiniz. Mekanizmalar telefon görüşmelerini , e-postaları veya mektupları içerebilir. Güvenlik olayı sırasında e-postalar gibi belirli mekanizmaların etkilenebileceğini unutmayınız. Yıllık olarak veya etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçiriniz.

17.7 - Rutin Olay Müdahale Tatbikatlarının Yapılması ; Gerçek dünyadaki olaylara müdahale etmeye hazırlanmak için olay müdahale sürecine dahil olan kilit personel için rutin olay müdahale tatbikatları ve senaryoları planlayın ve yürütünüz. Alıştırmaların iletişim kanallarını , karar vermeyi ve iş akışlarını test etmesi gerekir. En azından yıllık bazda testler yapınız.

17.8 - Olay Sonrası İncelemelerin Yapılması ; Olay sonrası incelemeler yapınız. Olay sonrası incelemeler , öğrenilen dersleri ve takip eylemini belirleyerek olayın tekrarını önlemeye yardımcı olur.

17.9 - Güvenlik Olayı Eşiklerinin Oluşturulması ve Sürdürülmesi ; Asgari olarak olay ve olay arasında ayrım yapmak dahil olmak üzere güvenlik olayı eşiklerini oluşturun ve sürdürünüz. Örnekler şunları içerebilir ; anormal etkinlik , güvenlik açığı , güvenlik zayıflığı , veri ihlali , gizlilik olayı vb. Yıllık olarak veya etkileyebilecek önemli kurumsal değişiklikler meydana geldiğinde gözden geçiriniz.

CIS Kritik Güvenlik Kontrolü 18 - Sızma Testi ; Denetimlerdeki (insanlar , süreçler , teknoloji) zayıflıkları belirleyip bunlardan yararlanarak ve saldırganın amaçları ile eylemlerini simüle ederek kurumsal varlıkların etkinliğini ve esnekliğini test ediniz. Başarılı savunma duruşu , kapsamlı etkili politikalar ve yönetişim programı , güçlü teknik savunmalar , insanlardan uygun eylemler gerektirir. Nadiren bunlar mükemmeldir. Teknolojinin sürekli geliştiği ve yeni saldırgan ticaret araçlarının düzenli olarak ortaya çıktığı karmaşık ortamda , kuruluşlar boşlukları belirlemek ve esnekliklerini değerlendirmek için kontrollerini periyodik olarak test etmelidir. Bu test harici ağ , dahili ağ , uygulama , sistem veya cihaz perspektifinden olabilir. Kullanıcıların sosyal mühendisliğini veya fiziksel erişim kontrolü atlamalarını içerebilir.

Sızma testleri genellikle belirli amaçlar için yapılır ; Genelde karar vericileri işletmelerinin zayıf yönlerine ikna etmek için yapılan saldırının dramatik gösterimi olarak. Kurumsal savunmaların doğru çalışmasını test etmenin bir yolu olarak doğrulama. İşletmenin ilk etapta doğru savunmaları oluşturduğunu test etmek.

Bağımsız sızma testi , kurumsal varlıklarda ve insanlarda güvenlik açıklarının varlığı ve kurum üzerindeki olumsuz etkilere karşı koruma sağlamak için savunmaların ve hafifletici kontrollerin etkinliği hakkında değerli , nesnel bilgiler sağlayabilir. Kapsamlı ve devam eden güvenlik yönetimi ve iyileştirme programının parçasıdırlar. Eksik veya tutarsız yapılandırma yönetimi veya son kullanıcı eğitimi gibi süreç zayıflıklarını da ortaya çıkarabilirler. Sızma testi , CIS Kontrolü 7'de açıklanan güvenlik açığı testinden farklıdır. Güvenlik açığı testi yalnızca bilinen , güvenli olmayan kurumsal varlıkların varlığını kontrol ederek orada durur. Sızma testi , saldırganın ne kadar ileri gidebileceğini ve bu güvenlik açığından yararlanılarak hangi iş süreçlerinin veya verilerin etkilenebileceğini görmek için bu zayıflıklardan yararlanmak için daha da ileri gider. Bu önemli bir ayrıntıdır ve genelde sızma testi ile güvenlik açığı testi yanlış şekilde birbirinin yerine kullanılır. Güvenlik açığı testi , bazen yanlış pozitiflerin manuel olarak doğrulanmasıyla özel olarak otomatikleştirilmiş taramadır , oysa sızma testi , bazen özel araçlar veya komut dosyaları kullanılarak desteklenen daha fazla insan katılımı ve analizi gerektirir. Güvenlik açığı testi genelde sızma testi için bir başlangıç noktasıdır. Diğer bir yaygın terim ise Kırmızı Takım egzersizleridir. Güvenlik açıklarından yararlanıldığı için sızma testlerine benzer fakat fark odak noktasıdır. Red Teams , kuruluş ortamının belirli bir rakipten veya rakip kategorisinden gelen saldırıya nasıl dayanacağını değerlendirmek için belirli saldırgan TTP'lerini simüle eder.

Prosedürler ve Araçlar ; Sızma testi , kuruluşun ve ortamın keşfi ve kuruluşa giriş olarak kullanılabilecek güvenlik açıklarının belirlenmesi için tarama yapılmasıyla başlar. Kapsam dahilinde olan ve sadece eski veya eksik olabilecek statik listeye dayanmayan tüm kurumsal varlıkların keşfedildiğinden emin olmak önemlidir. Sonrasında bu hedeflerdeki güvenlik açıkları belirlenecektir. Bu güvenlik açıklarından yararlanmalar , saldırganın işletmenin güvenlik hedeflerini nasıl alt edebileceğini veya belirli düşmanca hedeflere nasıl ulaşabileceğini nasıl gerçekleştirebileceğini özellikle göstermek için yürütülür. Sonuçlar , çeşitli güvenlik açıklarının iş risklerine ilişkin gösterim yoluyla daha derin içgörü sağlar.

Fiziksel erişim kontrollerine , ağ , sistem veya uygulama katmanlarına karşı olabilir ve genelde sosyal mühendislik bileşenlerini içerir. Penetrasyon testleri pahalıdır , karmaşıktır ve potansiyel olarak kendi risklerini ortaya çıkarır. Saygın satıcılardan deneyimli kişiler bunları gerçekleştirmelidir. Bazı riskler , kararsız olabilecek sistemlerin beklenmedik şekilde kapatılmasını , verileri veya yapılandırmaları silebilecek veya bozabilecek istismarları , nasıl girileceğine dair adım adım talimatlar verdiği için kendisinin korunması gereken test raporunun çıktısını içerir. Kritik varlıkları veya verileri hedeflemelidir. Her kuruluş , sızma testi için net kapsam ve katılım kuralları tanımlamalıdır. Bu tür projelerin kapsamı , asgari olarak , en yüksek değerli bilgi ve üretim işleme işlevselliğine sahip kurumsal varlıkları içermelidir. Diğer düşük değerli sistemler , daha yüksek değerli hedeflerden ödün vermek için pivot noktaları olarak kullanılıp kullanılamayacaklarını görmek için test edilebilir. Sızma testi analizleri için katılım kuralları , asgari olarak , test için günün saatlerini , testlerin süresini ve genel test yaklaşımını tanımlamalıdır. Sızma testinin ne zaman yapıldığını işletmede sadece birkaç kişi bilmeli ve sorun çıkması durumunda işletmede birinci irtibat noktası belirlenmelidir. Son zamanlarda giderek daha popüler hale gelen uygulama , sızma testi raporunun ifşa edilmesini önlemek için üçüncü taraf hukuk danışmanı aracılığıyla gerçekleştirilen sızma testleridir. Bu CIS Kontrolündeki Korumalar , kurumsal güvenliği artırabilecek ve sızma testinin bir parçası olması gereken belirli , yüksek öncelikli adımlar sağlar.

Kaynaklar ; OWASP Sızma Testi Metodolojileri , PCI Güvenlik Standartları Konseyi .

Alınacak Güvenlik Önlemleri ;

18.1 - Sızma Testi Programının Oluşturulması ve Sürdürülmesi ; İşletmenin büyüklüğüne , karmaşıklığına ve olgunluğuna uygun sızma testi programı oluşturun ve sürdürünüz. Sızma testi programı özellikleri , ağ , web uygulaması , Uygulama Programlama Arayüzü (API) , barındırılan hizmetler ve fiziksel öncül kontroller gibi kapsamı ; Sıklık ; kabul edilebilir saatler ve hariç tutulan saldırı türleri gibi sınırlamalar ; iletişim noktası bilgileri ; bulguların dahili olarak nasıl yönlendirileceği gibi iyileştirme ve geriye dönük gereksinimler.

18.2 - Periyodik Dış Penetrasyon Testlerini Gerçekleştirme ; En az yılda bir olmak üzere , program gereksinimlerine dayalı olarak periyodik dış sızma testleri gerçekleştiriniz. Harici sızma testi , sömürülebilir bilgileri tespit etmek için kurumsal ve çevresel keşifleri içermelidir. Penetrasyon testi , özel beceriler ve deneyim gerektirir ve kalifiye taraf aracılığıyla gerçekleştirilmelidir. Test şeffaf kutu veya opak kutu olabilir.

18.3 - Düzeltici Penetrasyon Testi Bulguları ; Kuruluşun iyileştirme kapsamı ve önceliklendirme politikasına dayalı olarak sızma testi bulgularını düzeltiniz.

18.4 - Güvenlik Önlemlerini Doğrulama ; Her sızma testinden sonra güvenlik önlemlerini doğrulayınız. Gerekirse , test sırasında kullanılan teknikleri tespit etmek için kural kümelerini ve yetenekleri değiştiriniz.

18.5 - Periyodik İç Penetrasyon Testlerini Gerçekleştirme ; En az yılda bir olmak üzere , program gereksinimlerine dayalı olarak periyodik dahili sızma testleri gerçekleştiriniz. Test şeffaf kutu veya opak kutu olabilir.