TANITIM BELGESİ

Modern BT Ortamlarında Güvenlik Standartlarına Uygunluğa Yönelik Denetime Hazırlıklı Olma

Runecast | Value-Added Distributor OTD BİLİŞİM www.onlineteknikdestek.com

ICT OTD PREFER EXPERIENCE ONLINE Since 2011

Yazarlar: Kev Johnson ve Steve Salisbury
Runecast Solutions Ltd. Sistem Mühendisleri
Yayınlanma Tarihi: Ağustos 2020

İçindekiler Tablosu

Modern BT ortamları oldukça karmaşıktır. Bazı şirketler tamamen yerinde faaliyet göstermekte veya VMware'in amiral gemisi vSphere suit gibi ürünleri kullanarak özel bulut modelinden faydalanmaktadır. Ve giderek bir şeyleri Amazon Web Servisleri (AWS) üzerinde kullanılan VMware Bulut gibi hibrit bulut model ile karıştırma trendi yaygınlaşmaktadır.
Bazı kurumlar tamamen AWS gibi teknolojilerle halka açık bulut sistemi kullanmaktadır. Gerçekçi olmak gerekirse, çoğu kurum her birinin bazı kombinasyonlarını kullanmaktadır ve güvenlik standartlarına uygunluğun takibi önemli ölçüde çalışmalar yapılmasını gerektirebilir. Ortamların en güncel standartlara ve en iyi uygulamalara ayak uydurmasını sağlamak otomatik süreçlerden yardım almadan vakit alan ve maliyetli süreçlerdir.
Bu tanıtım belgesi daha yaygın olan güvenlik standartlarından bazılarına, bu standartların ilgili problemlerine ve BT Sistem Yöneticilerinin güvenli, özel, hibrit ve halka açık bulut ortamlarını kullanmak için bu standartlara nasıl uyulacağına dair genel bilgiler vermektedir.

Genel Sorunlar1

• Ortamın uygunluk durumuna ilişkin görünürlük yetersizliği.

• Manuel kontrol ve çözümler için gereken zaman.

• Yapılandırma kaymasının uzun süreli olması ve buna ilişkin görünürlük.

• Dar Boğazlar / Kaynak kısıtlamaları.

• Proaktif değil, reaktif düzeltme maliyetleri.

• Sektörün güvenlik standartlarına uyulmamasına ilişkin cezalar.
• Organizasyonel itibara zarar gelmesi ve daha sonra gelir kaybı.
• İhlal sonrası dönemle başa çıkması için dış Danışman ihtiyacı.
Güvenlik denetimi ve uygunluğu süreklilik arz eden bir sorundur. Sektörel güvenlik standartlarının birçoğu eşdeğer görünmek için evrensellik esasıyla oluşturulur.
Uygunluğu sağlamak ve sürdürmek amacıyla ortam ayarlarınıza ilişkin sayısız denetim ve güvenlik standardı gerekliliklerini çevirmek zor olabilir.
Bu standartlar dinamik, geniş kapsamlı olduğu ve sektörlerin ötesine geçtiği için, Sistem Adminlerinin meydana geldikçe değişimleri yakalamasını gerektirir. Sizin de görebileceğiniz üzere, bu göz korkutucu bir görev gibi gözükebilir.
Zaman harcatan güvenlik denetimleri
Hızlıca gelişen BT dünyasında en yeni güvenlik standartlarının ve en iyi uygulamaların en üstünde olmak ne kadar iyi bir kadroya sahip olduğu önemli olmaksızın her BT departmanı için zor ve vakit alan bir durumdur. Bu standartlar mümkün olan durumların tamamını kapsayacak şekilde geniş bir yelpazede amacına uygun olarak tanımlanan yeni teknolojilerle geçişlerden etkilenmeyecek bir şekilde yazılmaktadır.
BT ekiplerinin bu gereklilikleri teknik kontrollere çevirmesi oldukça zor olabilir. HIPAA, NIST 800-53, ve PCI DSS bu standartlara örnektir.

1) Adminlerin karşılaştığı en yaygın sorunlar ile ilgili daha fazla bilgi almak için VMware Adminlerinin Karşılaştığı En Yaygın 10 Sorun (Runecast, 2020) başlıklı bölüme göz atın.

Genel Sorunlar

• BT ekipleri genellikle bu standartları karşılayan güvenlik politikalarını oluşturacak ve yönetecek kaynaklara veya becerilere sahip değildir.

• Güvenlik denetimleri çok daha sık gerçekleştirilmekte ve uygunsuzluk giderek daha maliyetli bir hale gelir.

• Yapılandırmanın kaymasına ilişkin görünürlük yetersizlik, geçen hafta denetimden geçmenize rağmen artık uygun olmayabileceğiniz anlamına gelir.

• Her ürün veya hizmetin kendine özel en iyi uygulamaları vardır.

• Her en iyi uygulama belli bir riski ortadan kaldırabilir. Hepsini toplamak, tamamlanmasını sağlamak, önceliklendirmek ve ortamınızda uygulanabilir olup olmadığını değerlendirmek maliyetli olabilir.
• Fiziksel katmanı kontrol ederken düzgün çalışmayan geleneksel güvenlik politikaları bulut tabanlı model için de düzgün çalışmaz.

Denetime Hazırlıklı Olmak için Bir Çözüm

Denetime hazırlıklı olmaya yardımcı olabilecek birkaç araç mevcuttur. Standartların politika gereklilikleri ile BT personeli tarafından net bir şekilde anlaşılabilecek daha teknolojiye özgü kontroller arasında karşılıklı ilişki kurabilen bir çözüm gereklidir. Her sektör, iş ve kurum uygunluk problemi olması halinde zaman, para ve iş saygınlığını tüketebilecek güvenlik standartlarına tabidir. Yukarıda belirtilen genel sorunlar birçok sebepten ortaya çıkabilir, bu sebepler arasında en tecrübeli Sistem Adminlerinin dahi işlerinin bir insanın bile gerçekleştiremeyeceği yönleri olduğunu anlamaları yer alır.

Güvenlik uygunluğu alanında tek bir referans noktası olarak kullanılabilen otomatik bir çözüme ihtiyaç vardır. Sayısız sanayi kaynaklarından alınan okunabilir dilin güvenli bir şekilde çalışan (hem yerinde hem de çevrim dışı) makine tarafından okunabilir bir dile tercüme edilmesi gerekir. Yazılım tanımlı veri merkezleri (SDDC) için en ilişkili ve karmaşık güvenlik standartlarının giderek büyüyen bir listesi hakkında denetimler sağlar. Çözümün belirli yapılandırmaları tarayabiliyor ve keşfettiği her türlü sorun için düzeltme adımlarını oluşturmanın yanı sıra güvenlik güçlendirme kontrolleri için boşluk analizi raporlarını iletebiliyor olması gerekir. Genel şartlar arasında şunlar yer alır:

• İyileştirilmiş Uygunluk, Yönetilebilirlik, Performans, Geri Kazanılabilirlik ve Güvenlik (UYPGG).

• Kullanımdaki çözümlere ilişkin en iyi uygulamalar analizi.

• BSI IT-Grundschutz, CIS SC, DISA STIG 6, HIPAA, NIST 800-53 ve PCI DSS gibi standartlara yönelik sürekli denetim.

• Gidermeye yönelik yaklaşıma ilişkin tavsiyeler ile birlikte kolaylıkla filtrelenen ve gruplandırılan sorunlar.

• Manuel çalışmayı ortadan kaldıran ve BT ortamlarınızın en iyi şekilde çalışmasını sağlayan otomatik taramalar.

• Bilinen güvenlik açıklarına ilişkin görünürlük: Hayalet, Erime, L1TF, MDS ve dahası.

• Mevcut yapılandırma sorunlarının ve zamanla değişen trendlerinin bir özeti.

• Sorun keşfi ve düzeltmelerine ilişkin zaman ilerlese dahi uygunluğun kanıtlanmasına yardımcı olan geçmiş veriler (ortamı etkileyen şeyin ne olduğunu
takip etmek için yapılandırma yönetimi veya BT yardım masası raporlaması ile eşleşecek şekilde ideal).

• Sorunlarla birlikte göstererek nesneleri kolaylıkla izleyebilme işlevi.

• Hem altyapı, hem de tasarım kaliteleri genelindeki etkiyi göstermek için bölünmüş sorunların görsel bir temsili.

• Altyapınızın her bir alanı için özel bir özet durumu ile birlikte loglardaki yaygın sorunların bir özeti.
• Ortamlarınızdaki tüm sorunlara yönelik ayrıntılı, birleşik ve granüler raporlama işlevleri.
Aşağıdaki bölümlerde birçok güvenlik standardına karşı otomatik güvenlik uygunluğunun sağlanması ile ilgili belli sorunlar ve gereklilikler açıklanmaktadır.

BSI IT-Grundschutz

Alman BT Veritabanı Koruma (IT-Grundschutz) standardı, Almanya Bilgi Güvenliği Federal Ofisi (BSI) tarafından etkili ve sürdürülebilir bir bilgi güvenliği yönetim sistemi (BGYS) olarak oluşturulmuştur. IT-Grundschutz eşit ölçüde teknik, organizasyonel, altyapısal ve personel hususlarını kapsar. Geniş kapsamı sayesinde,

IT-Grundschutz ISO/IEC/27001 ile uyumlu olarak bilgi güvenliğine sistematik bir yaklaşım getirir.
IT-Grundschutz, BSI Standartları ile birlikte BGYS kurmak isteyen her türden kurum için gerekli yayınları sunmaktadır:

•BSI Standardı 200-1
Bir BGYS için genel şartları tanımlar.

•BSI Standardı 200-2
üç farklı yaklaşımın biri esas alınarak BGYS'nin nasıl oluşturulabileceğini açıklar.

•BSI Standardı 200-3 risk ile ilgili tüm görevleri içerir.

•BSI Standardı 100-4 İş Sürekliliği Yönetimini (İSY) kapsar.
IT-Grundschutz'un dış dünya ile şeffaf bir şekilde başarılı olarak uygulanmasını sağlamak adına şirketler veya kamu kuruluşları IT-Grundschutz esas alınarak ISO 27001'e göre sertifika alabilir. Bu sertifika BT güvenliği kapsamının ISO 27001 gerekliliklerini karşıladığını tasdik eder.

Bu, bilgi güvenliğine ilişkin yöntemler, süreçler, prosedürler, yaklaşımlar ve ölçümler ile ilgili tavsiyeler sağlayan bir müşteri koruma yönetmeliğidir.

BSI kamu kuruluşlarında ve şirketlerdeki uygun, pratik, ulusal veya uluslararası yaklaşımların oluşturulduğu bilgi güvenliği için önemli olan sorunları ele alır.

BSI bir Almanya federal standardı olmasına rağmen, Almanya'da özellikle kamu ve hukuk sektörlerinde müşteri tabanına sahip bütün kurumlarda uygulanabilir (hangi ülkede oldukları önemli olmaksızın).

Sorunlar

Almanya'nın kamu ve hukuk sektörleri içerisindeki projelere yönelik teklif vermek için bir

BSI taban koruma sertifikası gereklidir.
BSI taban koruma kataloğu kamu kuruluşları için 2017 Ulusal Eylem Planına ilişkin bir kriterdir.

IT-Grundschutz Külliyatının farklı modüllerinde birçok farklı konuya yönelik güvenlik tavsiyeleri yer alır. IT- Grundschutz modüllerine yönelik uygulama kılavuzlarında yer alan detaylı tavsiyeler ve tedbirler, kılavuzların anlaşılması ve uygulanması düzeltme işlemleri için zaman harcayan ve acılı bir süreç olsa dahi bilgi güvenliği çalışanlarının günlük işlerinde bilgi güvenliğini sağlayabilmelerini kolaylaştıracak şekilde tasarlanmaktadır.

Otomatik BSI uygunluğu için gereklilikler

• Mevcut BSI yapılandırma sorunlarının ve trendlerinin bir özeti.

• BSI standartları 200-1, 200-2, 200- 3, and 200-4'e karşı ihlallere yönelik sürekli izleme.

• Güvenlik ekipleri ve denetçilerle eşit ölçüde iletişime imkan vererek sistem Adminlerinin anlayabileceği bir formata dönüştürülen karmaşık hukuki ve teknik terminoloji.

• BSI'ye uygun bir ortama yönelik otomatik tarama ve raporlama.

• Detaylandırılan sorunlarla birlikte yapılandırılmış veya arızalı bulguları gösteren sonuçlar.

• Her bir bulgunun BSI standardı içerisindeki ilgili Yapı Taşı için haritalandırılması.

• Düzeltme önceliğini belirlemek için önem derecesine göre listelenen bulgular.

CIS CSC

İnternet Güvenliği Merkezi (CIS) kamu sektörü ve özel sektörde siber güvenlik okuması ve müdahalesinin geliştirilmesine odaklanan kar amacı gütmeyen bir kuruluştur. CIS Kritik Güvenlik Denetimleri (CSC) siber savunma için günümüzün en yaygın ve tehlikeli saldırılarını durdurmanın bazı ve eyleme geçirilebilir yollarını sunan önerilen bir eylemler dizisidir. Denetimlerin temel avantajı oldukça faydalı sonuçlar barındıran daha küçük sayıdaki eylemleri önceliklendirmeleri ve bu eylemlere odaklanmalarıdır. CIS Güvenlik Standartları olarak da bilinen CIS Kriterleri günümüzün gelişen siber tehditlerine karşı koruma sistemlerine yönelik birçok teknoloji grubu için 140+ yapılandırma kılavuzundan oluşmaktadır.
AWS ve VMware ortamlarınızın güvenliğine yönelik denetim süreci meşakkatli ve maliyetli olabilir ve manuel kontrollerin tümü insan hatasına tabidir.
Sorunlar
Kurumlar ve adminler oldukça fazla DIY çalışmalarıyla CIS Güvenlik Kriterleri için manuel denetim yapabilmektedir, ancak bu süreç zor, uzun süren bir işlemdir ve insan hatasına yatkındır.
Ayrıca, kurumların gelecek yıl için uygun olarak değerlendirilebilmesi adına yıl içerisinde geçmiş dönemlere dair üç ayda bir CIS uygunluğunu gösterebiliyor olması gerekir.
Otomatik CIS uygunluğu için gereklilikler

- Otomatik CIS Kriter kontrolleri.
- Hem yerinde, hem de bulut tabanlı servislerin kapsam dahilinde olması.
- Hiçbir veriyi alan dışına çıkarmaksızın yerinde analiz.
- Resmi olarak onaylı CIS şiddet düzeylerine göre sorunların gruplandırılması.
- Geçmişteki otomatik taramalara ilişkin bulguların ayrıntılı geçmişi.

• Hiçbir veriyi alan dışına çıkarmaksızın yerinde analiz.
• Resmi olarak onaylı CIS şiddet düzeylerine göre sorunların gruplandırılması.
• Geçmişteki otomatik taramalara ilişkin bulguların ayrıntılı geçmişi.

DISA STIG

Amerika Birleşik Devletleri Savunma Bakanlığı (DoD) tüm ortamlarda tutarlı ve güvenli yapılandırmaların sağlanması için bu standartları tasarlamıştır. DISA STIG kılavuzları diğer sektörlerde veya segmentlerde genellikle standartlara uygunluğu ve DoD ağlarına erişimi sağlamak için bir taban olarak kullanılır. Tüm kurumlar DoD ağlarına erişmeden ve bu ağlar üzerinde çalışmadan önce DISA STIG güvenlik standartlarını karşılamalıdır. Bu standartlar aşağıdaki gibi tanımlanmaktadır:
DISA Savunma Bilgi Sistemleri Ajansı (savunma ajanslarına ve federal ajanslara, hükümete ve koalisyon ortaklarına BT ve iletişim desteği sağlar).
STIG Güvenlik Teknik Uygulama Kılavuzları (ağlarda, sunucularda, bilgisayarlarda ve mantıksal tasarımlarda genel güvenliğin güçlendirilmesi için güvenlik protokollerinin standartlaştırılmasına yönelik siber güvenlik metodolojisine dayanarak oluşturulan ve uygulanan bir kurallar dizisidir. Bu kılavuzlar uygulandığında güvenlik açıklarının iyice azaltılması adına yazılım, donanım, fiziksel e mantıksal mimarilere yönelik güvenliğin güçlendirilmesini sağlar).
Güvenlik Kontrollerinin Üç Düzeyi
DISA STIG, bilgi güvenliği perspektifinden CIA üçlüsü adına konuşur. Söz konusu bir sistem olduğunda, Gizlilik, Bütünlük ve Uygunluk hep birlikte önemlidir. Bu üç hususta hata olması halinde güvenlikten ödün verilmiş sayılabilir. Güvenlik açıkları şiddeti bakımından sınıflandırılır.
Düşük Şiddetli: Varlığı Gizlilik, Bütünlük veya Uygunluk hususlarında kayıpların önlenmesi için alınan önlemleri etkisiz hale getirebilecek her türlü güvenlik açığı.
Orta Şiddetli Kullanımı Gizlilik, Bütünlük veya Uygunluk hususlarında kayıplara yol açma potansiyeli taşıyan her türlü güvenlik açığı.
Yüksek Şiddetli Kullanımı doğrudan ve hemen Gizlilik, Bütünlük veya Uygunluk hususlarında kayıplara yol açacak her türlü güvenlik açığı.
Sorunlar
Uygunsuzluk, sistemlerin DoD ağlarını işletme erişimini ve yetkisini kaybetmesi demektir. Politika karmaşıklığı altyapı yapılandırma ayarlarının kontrolünden manuel kullanıcı doğrulamalarının onaylanmasına kadar (örn doğrulanmış ESXi kurulum ortamının kullanılması) büyük ölçüde değişkenlik gösterir.
Otomatik DISA uygunluğu için gereklilikler
• Mevcut DISA yapılandırma sorunlarının ve trendlerinin bir özeti.
• DISA STIG'e karşı ortamın (ortamların) düzenli bir şekilde otomatik olarak taranması.
• Karşılıklı bağımlılık haritalandırması da dahil olmak üzere ortamın tüm önemli bileşenlerinin kapsam dahiline alınması.
• Manuel olarak nasıl denetlenebileceği ve rapor edilen sorunların nasıl düzeltilebileceği ile ilgili detaylar da dahil olmak üzere her bulgunun ayrıntılı açıklamaları.
• DISA STIG'de detaylı olarak verilen bazı Güvenlik Açığı ID'sine yönelik her türlü bulgunun haritalandırılması.
• Her bulguda düzeltme çalışmalarının önceliklendirilmesini sağlamak üzere Etki, Önem ve Risk Derecelendirmesini içermesi gerekmektedir.

HIPAA

1996 yılında çıkarılan Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA), ABD Sağlık ve Sosyal Hizmetler Bakanlığı (HHS) Sekreterliğinin bazı sağlık bilgilerinin gizliliğini ve güvenliğini koruyan düzenlemeler yapmasını zorunlu kılmıştır. HHS bu gerekliliği yerine getirmek adına herkesçe HIPAA Gizlilik Kuralı ve HIPAA Güvenlik Kuralı olarak bilinen Kuralları yayınlamıştır.

Sorunlar

HIPAA güvenlik denetimleri sanal ortamı analiz ederken başka bir karmaşıklık katmanı ekler. Kurallar ve düzenlemeler sağlık hizmetinin üç önemli yönünü kapsar: elektronik veri değişimi (EDI), güvenlik ve gizlilik.

Sağlık planları EDI formatındaki tüm işlemleri kabul etmeli ve bu işlemlere yanıt vermelidir. Bilgilerin doğruluğunu ve bütünlüğünü koruyan ve erişimi kısıtlayan güvenlik politikaları ve prosedürleri uygulanmalıdır. Bilginin nasıl kullanıldığı ve paylaşıldığı ile ilgili olarak gizlilik esas alınmalıdır. Güvenlik ve gizlilik düzenlemeleri sistem adminlerinin sorunları anlaması ve düzeltmesi için karmaşık olabilecek idari, fiziksel ve teknik tedbirler gerektirir.

Otomatik HIPAA uygunluğu için gereklilikler

• Mevcut HIPAA yapılandırma sorunlarının ve trendlerinin bir özeti.

• Eski ve yeni HIPAA gizlilik ve güvenlik ihlallerine yönelik sürekli izleme.

• VMware ortamlarındaki etkilenen nesnelerin Ve VMware ürünlerinin sayısı da dahil olmak üzere tüm sorunların detaylı listesi.

Her bir kontrolün düzeltme işlemleri için teknik detayların tamamını içeren detaylı açıklamaları.

• HIPAA'ya uygun bir ortama yönelik otomatik düzeltme.

• HIPAA standardında detaylı olarak verilen Kural ID'si için her bir bulgunun haritalandırılması.

• Düzeltme önceliğini belirlemek için önem derecesine göre listelenen bulgular.

NIST

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), federal bilgi sistemleri ve kuruluşlarına yönelik güvenlik ve gizlilik kontrolleri sağlayan NIST özel yayını 800-53'ü (SP) yayınlamıştır. Yönetim ve Bütçe Ofisine (OMB) göre, NIST standartları ve politikaları ABD'deki federal kurumlarca işletilen tüm ulusal olmayan güvenlik sistemleri için zorunludur.

Sorunlar

Hem verileri, hem de bilgi sistemlerini korumak için, federal kurumların Federal Bilgi Güvenliği Yönetim Kanununun (FISMA) gerekliliklerini karşılamaları gerekir. SP 800-53 vasıtasıyla, NIST bu federal kurumların yaygın en iyi uygulamalar ve FIPS 200 gibi diğer standartların yanı sıra FISMA'ya uygun hareket etmelerine yardımcı olmak adına güvenlik kontrolleri sağlar.

Yayınlanan tüm güncel NIST kontrollerine dayanarak sanal ortamınızın tamamını doğrulamak zahmetli ve uzun ve süreklilik arz eden bir süreç olabilir. Tüm uygulanabilir NIST kontrollerine uygun olarak sürekli izleme ve hızlı yönlendirilen düzeltme işleri olmadan denetimle keşfedilene kadar risklerin tespiti yapılamaz veya tespit edilen riskler hafifletilemez.

Sonuç olarak, iş yükleri denetimin hızlandırılması için hızlıca artar ve bu nedenle diğer görevler geciktirilebilir. Kontrolü geri kazanmak ve "panikten doğan" denetim öncesi senaryolarını önlemek için, denetim hazırlıklarını günlük rutininizin bir parçası haline getirmek önemlidir. Bu tür bir devamlı çalışma hali nedeniyle günlük işlerinizin yavaşlamasını önlemek için, güvenlik döngünüzdeki tekrar eden adımları otomatikleştirmeye harcadığınız para ve zamanı büyük ölçüde azaltmanız gerekir

Otomatik NIST uygunluğu için gereklilikler

- Mevcut HIPAA yapılandırma sorunlarının ve trendlerinin bir özeti.
- Düzeltilecek NIST 800-53 kontrollerinin detayları.
- Hem yerinde, hem de bulut tabanlı servislerin kapsam dahilinde olması.
- Tespit edilen açıkların nasıl ortadan kaldırılabileceğini tam olarak gösteren kılavuzlu düzeltme işlemi.
- Belge sorumluluğu ve değişikliklerin izlenebilirliği.
- Ayrıntılı NIST uygunluk geçmişi.
- Düzeltme önceliğini belirlemek için önem derecesine göre listelenen bulgular ile birlikte kapsamlı raporlama.

PCI DSS

Ödeme Kartı Endüstrisi Veri Güvenliği Standardı (PCI DSS) kredi kartı ve kredi kartına ilişkin verileri kullanan kurumlara yönelik bir BT güvenlik standardıdır. Ödeme Kartı Endüstrisi Güvenlik Standartları Konseyi tarafından idare edilen PCI Standardı, kart sahibi verilerine yönelik kontrolleri sıkılaştırmak ve kredi kartı dolandırıcılığını azaltmak amacıyla kart markaları tarafından yönetilir.

Sorunlar

Özellikle finans sektöründe olmak üzere büyük ölçüde PCI DSS yönetmeliklerine tabi olan birçok BT departmanı için güvenlik denetimi ve uygunluk gerekliliklerin karmaşıklığı nedeniyle devam eden bir problemdir. PCI DSS güvenli bir ağ oluşturmaya ve işletmeye yönelik 12 uygunluk koşulundan oluşur. Güvenlik doğrulaması düzenli aralıklarla onaylı bir bilirkişi tarafından yapılır.

Bu 12 koşul daha sonra iş sürekliliği ve tüketicinin korunmasına yönelik geniş kapsamlı güvenlik süreçlerini kapsayan kontrol hedefleri olarak bilinen ek gruplara ayrılır.

Otomatik PCI DSS uygunluğu için gereklilikler

- Uygunsuzlukların ve açıkların tespiti.
- Kurumdaki risk durumunun taban gerekliliklerden daha yüksek standartlar gerektirdiği durumlarda denetimleri özelleştirebilme işlevi.
- Hem yerinde, hem de bulut tabanlı servislerin kapsam dahilinde olması.
- PCI-DSS ihlallerine karşı sürekli izleme.
- Adres Kontrol ID'si ve standardın dönüm noktası hususları.
- Tam raporlama işlevleri ile geçmişe yönelik analiz sağlar.
- PCI DSS kontrollerine karşı düzeltme işlemlerine yönelik otomasyon sağlar.
- Güvenlik açığı yönetimi ve risk değerlendirmesi kapsamı.
- Standardın en güncel revizyonuna yönelik destek (3.2.1, Mayıs 2018'de yayınlanmıştır).
- Tüm uygunsuzluk kontrolleri için ilgili gerekliliklerin alanından alınan ilgili kontrol ve bağlamın belirli ve tam içeriğini görüntüleme.
- PCI DSS güvenlik dönüm noktalarına göre düzeltme işlemlerinin önceliklendirilmesi.
- Bir otomatik kontrolün standarttaki belli bir kontrolle nasıl ilişkili olduğuna ve (uygulanabilir olduğu durumda) kontrolün belirli alt bölümler ile nasıl ilişki kurduğuna dair tamamen haklı gerekçelere dayanan bir görüntüleme sağlar.
- Manuel denetleme ve düzeltmeye yönelik detaylar da dahil olmak üzere PCI standardını bazı ortamlar için haritalandıran ayrıntılı teknik açıklamalar.

VMware Güvenlik Yapılandırma Kılavuzu

VMware Güvenlik Yapılandırma Kılavuzu Güvenlik güçlendirme kılavuzları müşterilere VMware ürünlerinin güvenli bir şekilde nasıl dağıtılacağı ve işletileceği ile ilgili kuralcı bir kılavuz sunar.

Bazı kurumlar güvenlik uygunluk standartlarının tamamına uygun olmak ve uygunluğu sürdürmek mecburiyetinde değildir. Aynı zamanda, tüm bunlara rağmen sağlayıcının güvenlik standartlarının bir başlangıç noktası olarak kullanıldığı bir şirket içi güvenlik politikası oluşturmaları gerekir.

Sorunlar

Bütün Sistem Adminleri VMware güvenlik uzmanları değildir ve güvenlik açıklarına ilişkin gündemi takip etmek hem zaman alan, hem de maliyetli bir süreçtir. Sorunun nerede olduğunu bulmak için VMware Güvenlik Yapılandırması Kılavuzunun tamamının taranması, Sistem Adminlerinin çalışmalarının diğer alanlarındaki proaktif olabilme kabiliyetini ortadan kaldırır.

Potansiyel sorunların üretim ortamınızı etkilemeden önce düzeltilmesi de zaman alan bir süreçtir ve sorunlar ortaya çıktıktan sonra yapılan reaktif bir düzeltme işlemi veri ihlallerine ve aksaklığa sebep olabilir. Sorunların keşfine harcanan zamanın Sistem Adminlerinin vakitlerini proaktif düzeltmeye harcamalarını ve güvenlik sorunları eğirisinin ötesinde kalmalarını sağlamak amacıyla anında yanıt verebilecek otomatik bir sistem ile büyük oranda azaltılması gerekir.

Otomatik VMware güvenliği için gereklilikler

- VMware Güvenlik Yapılandırma Kılavuzuna karşı otomatik kontroller.
- Kurumunuzun Güvenlik Politikalarına dayanarak analiz ve raporlama işlemlerini özelleştirmek için granüler filtreleme fonksiyonelliği.
- Güvenlik açıklarının açıklanması ve denetim ve düzeltme işlemleri için anında yanıt verilmesi gerekir.
- Uygunluğa yönelik zamanın minimuma indirilmesi için düzeltme otomasyonu gereklidir.
- Tam raporlama işlevleri ile birlikte bazı güvenlik uygunluk tabanlarına karşı güvenlik uygunluk durumunun geçmiş görüntülemeleri sağlanmalıdır.
- Düzeltme önceliğini belirlemek için önem derecesine göre listelenen bulgular.

Özet: Uygunluğun Sağlanması

Güvenlik standartlarına uygunluğu sürdürmek ve en yeni değişiklikleri ve güncellemeleri takip etmek oldukça vakit alan süreçlerdir. Standartların dokümantasyonu genellikle yeni teknolojiyle geçişlerden etkilenmeyen bir bakış açısıyla yazıldıkları için Sistem Adminleri için anlaması zor olabilir. Reaktif olarak cevap ararken harcanan zaman aslında proaktif olarak iş değeri sunabilmek için daha iyi harcanabilecek bir zamandır.

Sistem Adminlerinin bir yangın söndürme paradigmasında kilitli kalmaktan ziyade eğrinin ötesine geçmesi sağlanarak güvenlik uygunluğunun proaktif bir şekilde sağlanması oldukça önemlidir. Ortamların en yeni boşluklara ve güvenlik açıklarına karşı güvenli hale getirilmesi veri güvenliğini sağlar ve hizmet devamlılığı ve müşterilerin güvenebileceği bir marka güvencesi sunar.

Yöneticiler, güvenlik güçlendirme kılavuzları ve uygunluk belgeleri ile kontrol etmeye zaman harcama gereksinimini ortadan kaldıran bir çözüme ihtiyaç duyar. Olaydan sonra bu sorunların düzeltilmesinden ziyade önlenmesiyle sayısız iş saatleri kurtarılabilir. Sistem Adminlerine yönelik tahmini ve eyleme geçirilebilir bir zeka, risklere ve güvenlik uygunsuzluklarına ilişkin %100 şeffaflık sağlayıp adminlerin sorun giderme ihtiyacını ortadan kaldırarak ortamların geçmişine, şu anki durumuna ve geleceğine tek bir yerden ayrıntılı bir şekilde bakılmasını sağlamalıdır.

Güvenliğin geleceği proaktif analiz, anında çözüm yanıtları, açık bir dil, granüler raporlama ve anlayış derinliği sunan bir çözümdür.

Çözüm, sınırlı ve reaktif bir kapasitede karmaşık sorunların giderilmesi nedeniyle kaybedilen zamanı ve ortaya çıkan ilgili maliyetleri azaltmalıdır. Daha proaktif bir modele geçerek, potansiyel riskleri keşfedebilir ve adminlere sorunlar büyük sistem kesintisi veya güvenlik ihlaline dönüşmeden önce düzeltme çözümleri sağlayabilirsiniz.

Sistem Adminleri işe ilişkin riskleri hafifletmeye zorlandığı için, yenilikçi çalışmalar için zamanı boşa çıkarmak amacıyla daha büyük iş değeri yaratacak otomasyonun kullanılması gerekir. Parmak izlerine yönelik yanıtların tümünü ileten bir çözümle, tecrübesiz bir teknisyenin dahi tecrübeli bir uzman gibi olması sağlanabilir.

Runecast Analyzer gibi bir platformun kullanılması, hizmet devamlılığı ve müşteri güvenini sağlayarak Veri Merkezlerinin daha güvenli olmasını, işe ilişkin zaman ve paradan tasarruf edilmesini ve marka beklentisinin yükselmesini sağlar.

Aynı zamanda yukarıda ayrıntılı olarak bahsedilen otomatik güvenlik uygunluğu koşullarının tamamını ele alan pazardaki (bu yayının tarihinde) tek çözümdür.

Runecast Hakkında

Runecast Solutions Ltd., dünya genelinde birçok ofisi bulunan ve VMware ve AWS ortamları için patentli ve eyleme geçirilebilir tahmini zekaya dair önde gelen bir hibrit bulut çözümleri sağlayıcısı olan Londra, İngiltere merkezli bir şirkettir.

Sanallaştırma uzmanlarının yücelttiği ödüllü Runecast Analyzer yazılımı her ölçekten şirketler için gerçek zamanlı, otomatik yapılandırma ve güvenlik uygunluk analizi sağlamaktadır.

IDG Connect, Runecast'ı "2019 B2B Tech'te Yer Alacak 20 Yükselen Halka Arz Öncesi Şirket" arasında görmüştür ve Runecast 2020 Bulut Tabanlı Mimarilere ilişkin 2020 Performans Analizi raporunda Gartner tarafından Cool Vendor ödülüne layık görülmüştür.

Daha fazla bilgi için,
www.runecast.com adresini ziyaret edin.