Kaspersky® Endpoint Security

PCI DSS v3.2 Eşleştirme

PCI DSS 3.2, kredi kartı verileriyle çalışan sistemler için birçok teknik güvenlik gerekliliğini ve ayarını düzenler. PCI DSS v3.2 standardının 1.4, 2.4a, 3.4.1, 5.1, 5.1.1, 5.2, 5.3, 6.1, 6.2, 10.5.5, 11.5 alt maddeleri, Kart Sahibi Verileri ile çalışan uç noktalarla ilgili virüsten koruma yazılımı korumasının sıkı bir şekilde düzenlemesini sağlar. Resmi bir kural olmamasına rağmen, Cihaz Kontrolü + Uygulama Kontrolü işlevlerinin PCI DSS virüsten koruma yazılımı denetimi kapsamında değerlendirilmesi yaygın bir uygulamadır.

1.4

PCI DSS GEREKLILIKLERI:

Ağ dışındayken internete bağlanan ve aynı zamanda CDE'ye (Kart Verileri Ortamı) erişim için kullanılan taşınabilir bilgi işlem cihazlarına kişisel güvenlik duvarı yazılımı veya eşdeğer işlevselliğe sahip bir yazılım yükleyin. Güvenlik duvarı (veya eşdeğer yazılım) yapılandırmaları aşağıdakileri içerir:

- Belirli yapılandırma ayarları tanımlanır.
- Kişisel güvenlik duvarı (veya eşdeğer yazılım) etkin bir biçimde çalışır.
- Kişisel güvenlik duvarı (veya eşdeğer yazılım), taşınabilir bilgi işlem cihazlarının kullanıcıları tarafından değiştirilemez.

TEST PROSEDÜRLERI:

1.4.a Aşağıdakileri doğrulamak için ilkeleri ve yapılandırma standartlarını inceleyin:

- Ağ dışındayken internete bağlanan ve aynı zamanda CDE'ye erişim için kullanılan tüm taşınabilir bilgi işlem cihazları için kişisel güvenlik duvarı yazılımı veya eşdeğer işlevselliğe sahip bir yazılım gereklidir.
- Kişisel güvenlik duvarı (veya eşdeğer yazılım) için belirli yapılandırma ayarları tanımlanır.
- Kişisel güvenlik duvarı (veya eşdeğer yazılım) etkin bir biçimde çalışmak üzere yapılandırılır.
- Kişisel güvenlik duvarı (veya eşdeğer yazılım), taşınabilir bilgi işlem cihazlarının kullanıcıları tarafından değiştirilemeyecek şekilde yapılandırılır.

1.4.b Aşağıdakileri doğrulamak için şirket cihazlarının bir örneğini inceleyin:

- Kişisel güvenlik duvarı (veya eşdeğer yazılım) yüklüdür ve kuruluşun özel yapılandırma ayarlarına göre yapılandırılmıştır.
- Kişisel güvenlik duvarı (veya eşdeğer yazılım) etkin bir biçimde çalışır.
- Kişisel güvenlik duvarı (veya eşdeğer yazılım), taşınabilir bilgi işlem cihazlarının kullanıcıları tarafından değiştirilemez.

KILAVUZ:

Kurumsal güvenlik duvarının dışında internete bağlanmasına izin verilen taşınabilir bilgi işlem cihazları, internet tabanlı tehditlere karşı daha savunmasızdır. Kişisel güvenlik duvarı işlevinin kullanımı (ör. kişisel güvenlik duvarı yazılımı veya donanımı), cihaz ağa tekrar bağlandığında kuruluşun sistemlerine ve verilerine erişim sağlamak için cihazı kullanabilecek internet tabanlı saldırılara karşı cihazları korumaya yardımcı olur.

Özel güvenlik duvarı yapılandırma ayarları kuruluş tarafından belirlenir.

2.4a

PCI DSS GEREKLILIKLERI	PCI DSS kapsamındaki sistem bileşenlerinin bir envanterini tutun.
TEST PROSEDÜRLERI	**2.4.a** Donanım ve yazılım bileşenlerinin bir listesinin tutulduğunu ve listede her bir bileşen için işlev/kullanım açıklamasının bulunduğunu doğrulamak için sistem envanterini inceleyin.
KILAVUZ	Tüm sistem bileşenlerinin geçerli bir listesini tutmak, bir kuruluşun, PCI DSS kontrollerini uygulamak için ortam kapsamını doğru ve etkin bir şekilde tanımlamasını sağlar. Envanter olmadan bazı sistem bileşenleri unutulabilir ve yanlışlıkla kuruluşun yapılandırma standartlarından hariç tutulabilir.

3.4.1

PCI DSS GEREKLILIKLERI	Disk şifreleme kullanılıyorsa (dosya ya da sütun düzeyi veritabanı şifrelemesi yerine), mantıksal erişim, yerel işletim sistemi kimlik doğrulama ve erişim kontrolü mekanizmalarından ayrı ve bağımsız olarak yönetilmelidir (örneğin, yerel kullanıcı hesabı veritabanları veya genel ağ oturum açma kimlik bilgileri kullanılmayarak). Şifre çözme anahtarları, kullanıcı hesaplarıyla ilişkilendirilmemelidir.
TEST PROSEDÜRLERI	**3.4.1.a** Disk şifreleme kullanılıyorsa şifrelenmiş dosya sistemlerine mantıksal erişimin, yerel işletim sisteminin kimlik doğrulama mekanizmasından ayrı olan bir mekanizma aracılığıyla uygulandığını (örneğin, yerel kullanıcı hesabı veritabanları veya genel ağ oturum açma kimlik bilgileri kullanılmayarak) doğrulamak için yapılandırmayı inceleyin ve kimlik doğrulama sürecini gözlemleyin. **3.4.1.b** Şifreleyici anahtarların güvenli bir şekilde saklandığını (örneğin, güçlü erişim kontrolleriyle yeterince korunan çıkarılabilir ortamda depolama) doğrulamak için süreçleri gözlemleyin ve personelle görüşün. **3.4.1.c** Çıkarılabilir ortamdaki kart sahibi verilerinin saklandığı yerlerde şifrelendiğini doğrulamak için yapılandırmaları inceleyin ve süreçleri gözlemleyin.
KILAVUZ	Bu gerekliliğin amacı, kart sahibi verilerini okunamaz hale getirmek için disk düzeyinde şifrelemenin kabul edilebilirliğini incelemektir. Disk düzeyinde şifreleme, bir bilgisayardaki tüm diski/bölümü şifreler ve yetkili bir kullanıcı istediğinde bilgilerin şifresini otomatik olarak çözer. Birçok disk şifreleme çözümü, işletim sistemi okuma/yazma işlemlerini engeller ve sistemin başlaması üzerine veya bir oturumun başlangıcında kullanıcının bir şifre ya da parola sağlamanın dışında herhangi bir özel eylem yapmasına gerek olmadan uygun kriptografik dönüştürmeleri gerçekleştirir. Disk düzeyinde şifrelemenin bu özellikleri temelinde yöntem, bu gereklilikle uyumlu olmak için: • İşletim sistemiyle aynı kullanıcı hesabı kimlik doğrulayıcıyı kullanamaz veya • Sistemin yerel kullanıcı hesabı veritabanı veya genel ağ oturum açma kimlik bilgileriyle ilişkilendirilen ya da bunlardan türetilen bir şifre çözme anahtarı kullanamaz. Tam disk şifreleme, bir diskin fiziksel olarak kaybedilmesi durumunda verilerin korunmasına yardımcı olur ve bu nedenle kart sahibi verilerinin saklandığı taşınabilir cihazlar için uygun olabilir.

5.1

PCI DSS GEREKLILIKLERI:	Virüsten koruma yazılımını, kötü amaçlı yazılımlardan yaygın olarak etkilenen tüm sistemlere (özellikle kişisel bilgisayarlara ve sunuculara) dağıtın.

TEST PROSEDÜRLERI: Kötü amaçlı yazılımlardan yaygın olarak etkilenen tüm işletim sistemi türleri dahil olmak üzere, sistem bileşenlerinin bir örneği için uygulanabilir virüsten koruma teknolojisi mevcutsa virüsten koruma yazılımının dağıtıldığını doğrulayın.

KILAVUZ: Başka şekilde güvenli kılınmamış sistemlere karşı sıklıkla "sıfır gün" adı verilen (daha önce bilinmeyen bir güvenlik açığını kullanan saldırı), yaygın biçimde yayınlanmış açıklardan yararlanan yazılımları kullanan sabit bir saldırı akışı vardır. Düzenli olarak güncellenen bir virüsten koruma çözümü olmadan, kötü amaçlı yazılımların bu yeni biçimleri sistemlere saldırabilir, bir ağı devre dışı bırakabilir veya verilerin tehlikeye düşmesine neden olabilir.

5.1.1

PCI DSS GEREKLILIKLERI: Virüsten koruma programlarının, bilinen tüm kötü amaçlı yazılım türlerini tespit etme, kaldırma ve koruma sağlama becerisine sahip olduğundan emin olun.

TEST PROSEDÜRLERI: Virüsten koruma programlarının kötü amaçlı yazılımların tüm bilinen türlerini tespit ettiği, kötü amaçlı yazılımların tüm bilinen türlerini kaldırdığını ve kötü amaçlı yazılımların tüm bilinen türlerine karşı koruma sağladığını doğrulamak için satıcı belgelerini gözden geçirin ve virüsten koruma yapılandırmalarını inceleyin.

KILAVUZ: Kötü amaçlı yazılımların TÜM türlerine ve biçimlerine karşı koruma sağlamak önemlidir.

5.2

PCI DSS GEREKLILIKLERI: Tüm virüsten koruma mekanizmalarının güncel tutulduğundan, düzenli taramalar gerçekleştirdiğinden ve PCI DSS 10.7 sayılı gerekliliğe göre tutulan denetim günlükleri oluşturduğundan emin olun.

TEST PROSEDÜRLERI: **5.2.a** Virüsten koruma yazılımı ve tanımlarının güncel tutulması gerektirildiğini doğrulamak için ilkeleri ve prosedürleri inceleyin.

5.2.b Virüsten koruma mekanizmalarının otomatik güncellemeler ve düzenli taramalar gerçekleştirmek için yapılandırıldığını doğrulamak için yazılımın ana kurulumu dahil olmak üzere virüsten koruma yapılandırmalarını inceleyin.

5.2.c Virüsten koruma yazılımının ve tanımlarının güncel olduğunu ve düzenli taramaların gerçekleştirildiğini doğrulamak için kötü amaçlı yazılımlardan yaygın olarak etkilenen tüm işletim sistemi türleri dahil olmak üzere sistem bileşenlerinin bir örneğini inceleyin.

5.2.d Virüsten koruma yazılımı günlük oluşturma özelliğinin etkin olduğunu ve günlüklerin, PCI DSS 10.7 sayılı gerekliliğe göre tutulduğunu doğrulamak için yazılımın ana kurulumu ve sistem bileşenlerinin bir örneği dahil olmak üzere virüsten koruma yapılandırmalarını inceleyin.

KILAVUZ: En iyi virüsten koruma çözümleri bile en son güvenlik güncellemeleri, imza dosyaları ve kötü amaçlı yazılım korumaları ile sürdürülmez ve güncel tutulmazsa sınırlı etkinlik gösterir. Denetim günlükleri, virüs ve kötü amaçlı yazılım etkinliğini ve kötü amaçlı yazılımlarda koruma tepkilerini izleme becerisi sağlar. Dolayısıyla kötü amaçlı yazılımlardan koruma çözümlerinin denetim günlükleri oluşturmak üzere yapılandırılması ve bu günlüklerin Gereklilik 10 uyarınca yönetilmesi zorunludur.

5.3

PCI DSS GEREKLILIKLERI:

Virüsten koruma mekanizmalarının etkin bir biçimde çalıştığından ve sınırlı **bir zaman dilimi için olay temelinde özel olarak yönetim tarafından yetkilendirilmediği sürece kullanıcılarca devre dışı bırakılamadığı ya da değiştirilemediğinden emin olun.**

TEST PROSEDÜRLERI:

5.3.a Virüsten koruma yazılımının etkin biçimde çalıştığını doğrulamak için yazılımın ana kurulumu ve sistem bileşenlerinin bir örneği dahil olmak üzere virüsten koruma yapılandırmalarını inceleyin.

5.3.b Virüsten koruma yazılımının kullanıcılar tarafından devre dışı bırakılamadığını ya da değiştirilemediğini doğrulamak için yazılımın ana kurulumu ve sistem bileşenlerinin bir örneği dahil olmak üzere virüsten koruma yapılandırmalarını inceleyin.

5.3.c Sınırlı bir zaman dilimi için olay temelinde yönetimce özel olarak yetkilendirilmediği sürece, virüsten koruma yazılımının kullanıcılar tarafından devre dışı bırakılamadığını ya da değiştirilemediğini doğrulamak için sorumlu personelle görüşün ve süreçleri gözlemleyin.

KILAVUZ:

Sürekli çalışan ve değiştirilemez olan virüsten koruma yazılımı, kötü amaçlı yazılımlara karşı devamlı koruma sağlar.

Kötü amaçlı yazılımlardan koruma yazılımlarının değiştirilemediğinden ya da devre dışı bırakılamadığından emin olmak için tüm sistemlerde ilke tabanlı kontrollerin kullanımı, kötü amaçlı yazılımın sistemin zayıflığından yararlanmasını önlemeye yardımcı olur.

Virüsten korumanın etkin olmadığı zaman dilimi için ek güvenlik önlemlerinin uygulanması da gerekebilir; örneğin, virüsten koruma devre dışı bırakıldığında korunmayan sistemin internet bağlantısını kesme ve tekrar etkinleştirildikten sonra tam bir tarama çalıştırma uygulanabilir.

6.1

PCI DSS GEREKLILIKLERI:

Güvenlik açığı bilgisi için tanınmış dış kaynaklar kullanarak, güvenlik açıklarını belirlemeye yönelik bir süreç oluşturun ve yeni keşfedilen güvenlik açıklarına bir risk derecelendirmesi (örneğin "yüksek", "orta" ya da "düşük" olarak) atayın.

TEST PROSEDÜRLERI:

6.1.a Aşağıdakilere yönelik süreçler tanımlandığını doğrulamak için ilkeleri ve prosedürleri inceleyin:

- Yeni güvenlik açıklarını belirleme
- Güvenlik açıklarına, tüm "yüksek" riskli ve "önemli" güvenlik açıklarının tanımlanmasını içeren bir risk derecelendirmesi atama.
- Güvenlik açığı bilgileri için güvenilir dış kaynaklar kullanma.

6.1.b Aşağıdakileri doğrulamak için personelle görüşün ve süreçleri gözlemleyin:

- Yeni güvenlik açıkları belirlenir.
- Güvenlik açıklarına, tüm "yüksek" riskli ve "önemli" güvenlik açıklarının tanımlanmasını içeren bir risk derecelendirmesi atanır.
- Yeni güvenlik açıklarını belirleme amaçlı süreçler, güvenlik açığı bilgilerine yönelik tanınmış dış kaynakları kullanmayı içerir.

KILAVUZ:

Bu gerekliliğin amacı, kuruluşların, ortamlarını etkileyebilecek yeni güvenlik açıklarına karşı güncel olmalarıdır.

Güvenlik açığı bilgilerinin kaynakları güvenilir olmalıdır ve çoğunlukla satıcı web sitelerini, endüstri haber gruplarını, posta listelerini ya da RSS beslemelerini içermelidir.

Bir kuruluş, ortamını etkileyebilecek bir güvenlik açığı belirlediğinde, güvenlik açığının taşıdığı risk değerlendirilmeli ve derecelendirilmelidir. Bu nedenle kuruluş güvenlik açıklarını sürekli değerlendirmek için yürürlükte olan bir yönteme sahip olmalı ve bu güvenlik açıklarına risk dereceleri atamalıdır. Bu, bir ASV taramasıyla ya da dahili güvenlik açığı taramasıyla gerçekleştirilemez. Bunun yerine, güvenlik açığı bilgileri için endüstri kaynaklarını etkin bir biçimde izleyen bir süreç gerektirir.

Riskleri sınıflandırmak (örneğin "yüksek", "orta" yada "düşük" olarak), kuruluşların, en yüksek risk unsurlarını daha hızlı belirlemesine, önceliklendirmesine, ele almasına ve en büyük riski taşıyan güvenlik açığından yararlanma olasılığını düşürmesine olanak tanır.

6.2

PCI DSS GEREKLILIKLERI:

Tüm sistem bileşenlerinin ve yazılımların, satıcı tarafından sunulan uygulanabilir düzeltme ekleri yüklenerek bilinen güvenlik açıklarına karşı korunduğundan emin olun. Önemli düzeltme eklerini, yayınlanmalarından sonraki bir ay içinde yükleyin

Not: Önemli düzeltme ekleri, Gereklilik 6.1'de tanımlanan risk derecelendirme sürecine göre belirlenmelidir.

TEST PROSEDÜRLERI:

6.2.a Satıcı tarafından sunulan uygulanabilir önemli düzeltme eklerinin, yayınlanmalarından sonraki bir ay içinde yüklendiğini ve satıcı tarafından sunulan tüm uygulanabilir düzeltme eklerinin uygun bir zaman dilimi (örneğin üç ay) içinde yüklendiğini doğrulamak için düzeltme eki yüklenmesiyle ilgili ilkeleri ve prosedürleri inceleyin.

6.2.b Satıcı tarafından sunulan uygulanabilir önemli düzeltme eklerinin, yayınlanmalarından sonraki bir ay içinde yüklendiğini ve satıcı tarafından sunulan tüm uygulanabilir düzeltme eklerinin uygun bir zaman dilimi (örneğin üç ay) içinde yüklendiğini doğrulamak için sistem bileşenleri ve ilgili yazılım örneği için her sistemde kurulu olan sistem düzeltme eklerinin listesini, sağlayıcı tarafından sunulan en son düzeltme eklerinin listesiyle karşılaştırın.

KILAVUZ:

Başka şekilde güvenli kılınmamış sistemlere karşı sıklıkla "sıfır gün" adı verilen (daha önce bilinmeyen bir güvenlik açığını kullanan saldırı), yaygın biçimde yayınlanmış açıklardan yararlanan yazılımları kullanan sabit bir saldırı akışı vardır. En son düzeltme ekleri önemli sistemlerde en kısa sürede uygulanmazsa kötü niyetli bir kişi, bir sisteme saldırmak ya da sistemi devre dışı bırakmak veya hassas verilere erişim elde etmek için bu açıkları kullanabilir.

Önemli altyapılar için düzeltme eklerine öncelik vermek, yüksek öncelikli sistemlerin ve cihazların, düzeltme ekleri yayınlandıktan sonra en kısa zamanda güvenlik açıklarından korunmasını sağlar. Düzeltme eki yüklemelerine, önemli ya da risk altındaki sistemlere yönelik düzeltme ekleri 30 gün, diğer düşük riskli düzeltme ekleri de 2-3 ay içinde kurulacak şekilde öncelik vermeyi düşünün.

Bu gereklilik, tüm yüklü yazılımlara yönelik uygulanabilir düzeltme ekleri için de geçerlidir.

10.5.5 *

PCI DSS GEREKLİLİKLERİ

Mevcut günlük verilerinin uyarılar üretmeden değiştirilememesini sağlamak için (ancak yeni eklenen veriler uyarı üretmemelidir), günlüklerde dosya bütünlüğü izleme ya da değişiklik tespit etme yazılımı kullanın.

TEST PROSEDÜRLERİ:

Günlüklerde dosya bütünlüğü izleme ve değişiklik tespit etme yazılımı kullanımını doğrulamak için sistem ayarlarını, izlenen dosyaları ve izleme etkinliklerden alınan sonuçları inceleyin.

KILAVUZ

Dosya bütünlüğü izleme ya da değişiklik tespit etme sistemleri, önemli dosyalardaki değişiklikleri kontrol eder ve bu tür değişiklikler belirlendiğinde bildirir. Kuruluşlar, genellikle dosya bütünlüğü izleme amaçları için düzenli olarak değişmeyen ama değiştiği zaman olası bir tehlikeyi işaret eden dosyaları izler.

11.5 *

PCI DSS GEREKLİLİKLERİ:

Önemli sistem dosyalarının, yapılandırma dosyalarının ya da içerik dosyalarının yetkisiz değiştirilmesi (değişiklikler, eklemeler ve silmeler dahildir) konusunda personeli uyarmak için bir değişiklik tespit etme mekanizması (örneğin, dosya bütünlüğü izleme araçları) kurun ve yazılımı, önemli dosya karşılaştırmalarını haftada en az bir kez gerçekleştirecek biçimde yapılandırın

TEST PROSEDÜRLERİ:

Sistem ayarları ve izlenen dosyaları gözlemlemenin yanı sıra izleme etkinliklerinden alınan sonuçları gözden geçirerek değişiklik tespit etme mekanizmasının kullanımını doğrulayın.

İzlenmesi gereken dosyaların örnekleri:

- Yürütülebilir sistem dosyaları
- Yürütülebilir uygulama dosyaları
- Yapılandırma ve parametre dosyaları
- Merkezi olarak depolanan, geçmiş veya arşivlenmiş, günlük ve denetim dosyaları
- Kuruluş tarafından belirlenen (örneğin risk değerlendirmesi ya da başka yollarla) ek önemli dosyalar.

KILAVUZ

Dosya bütünlüğü izleme (FIM) gibi değişiklik tespit etme çözümleri, önemli dosyalardaki değişiklikleri, eklemeleri ve silmeleri kontrol eder ve bu tür değişiklikler belirlendiğinde bildirir. Düzgün bir şekilde uygulanmaz ve değişiklik tespit etme çözümünün çıktıları izlenmezse kötü niyetli bir kişi, yapılandırma dosyası içeriklerini, işletim sistemi programlarını ya da yürütülebilir uygulama dosyalarını ekleyebilir, kaldırabilir veya değiştirebilir. Yetkisiz değişiklikler, tespit edilmemeleri durumunda, mevcut güvenlik kontrollerini etkisiz duruma
getirebilir ve/veya normal işlemde hiçbir fark edilebilir etki olmadan kart sahibi verilerinin çalınmasıyla sonuçlanabilir.

*Kaspersky Security for Windows Server için uygulanabilir

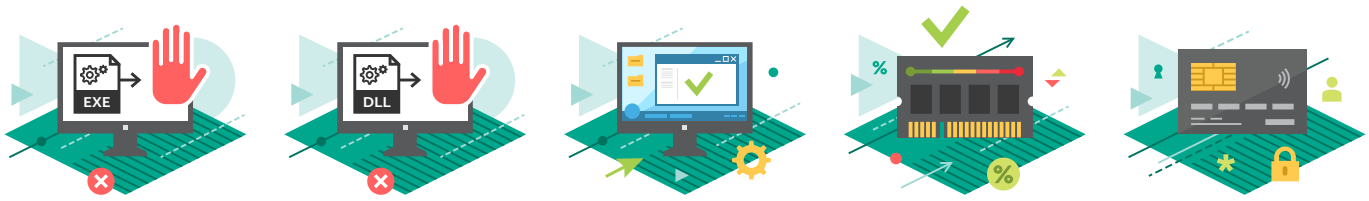
Neredeyse sonsuz ölçeklenebilir olan bu çözüm; envanterlere, lisanslara, uzaktan sorun çözme özelliğine ve ağ kontrollerine tek bir konsoldan (Kaspersky Security Center) erişim sağlar.

BAKIM VE DESTEK

Dünya genelinde 200'den fazla ülkede, 34 ofisimizle hizmet veriyoruz. 24/7/365 global destek anlayışımız Maintenance Service Agreement (MSA) destek paketlerine de yansımıştır.

Profesyonel Hizmetler ekibimiz, Kaspersky Lab güvenlik kurulumunuzdan maksimum düzeyde yararlanmanız için sürekli nöbettedir.

Uç noktalarınızı daha etkili bir şekilde korumakla ilgili daha fazla bilgi edinmek için lütfen Kaspersky Lab Kurumsal Satış Ekibi ile iletişime geçin.



İnternet güvenliği hakkında her şey için: **www.securelist.com**
Size en yakın iş ortağımızı bulun: **www.kaspersky.com.tr/buyoffline**

www.kaspersky.com.tr
#truecybersecurity