KVKK

Kişisel Verilerin Korunması Kanunu (6698)

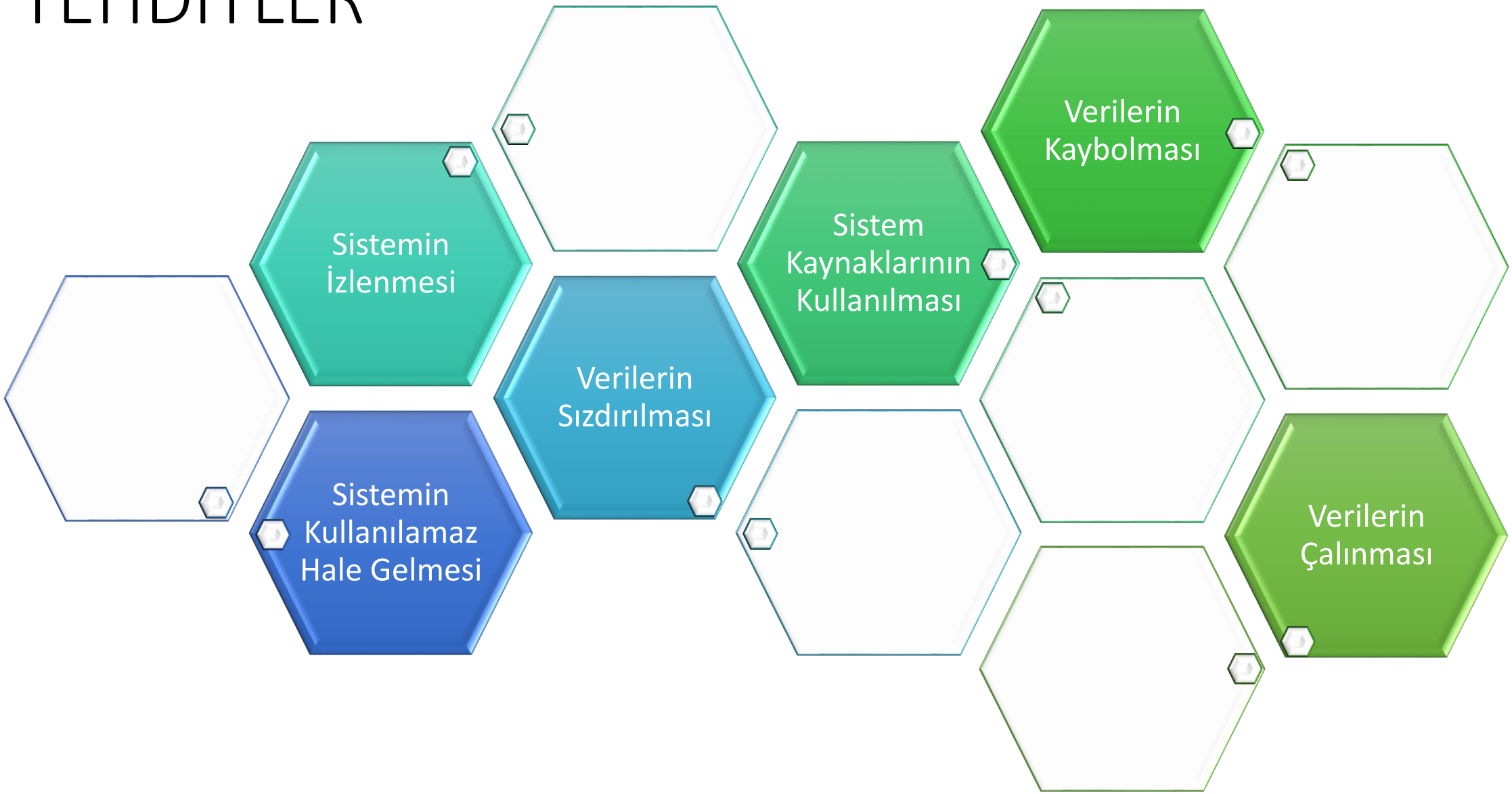
Teknik Tedbirlerde E-Data Teknoloji Ürünleri

www.e-data.com.tr

Kişisel Veri Güvenligi Rehberi

(Teknik ve idari tedbirler)

TEHDİTLER


Sistemin İzlenmesi
Verilerin Sızdırılması
Sistemin Kullanılamaz Hale Gelmesi
Sistem Kaynaklarının Kullanılması
Verilerin Kaybolması
Verilerin Çalınması

ENDPOINT PROTECTOR | by CoSoSys

Tehditler :

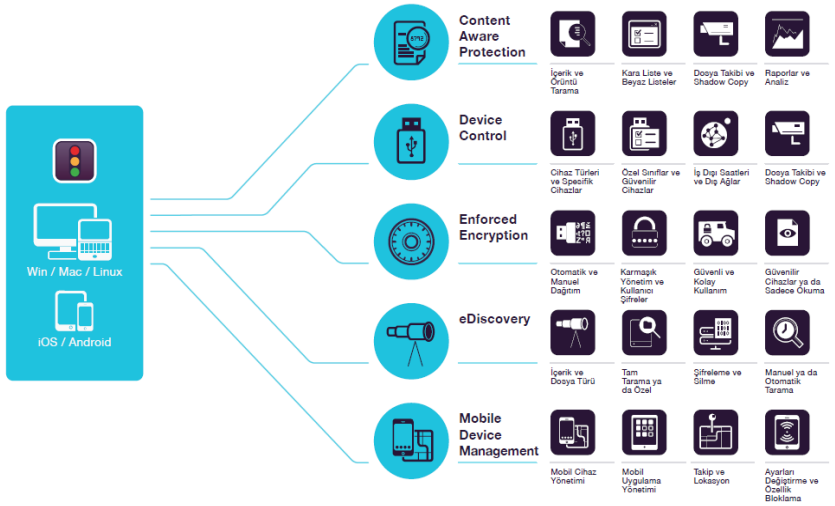
- Bir dosyanın, izinsiz olarak, buluttaki dosya barındırma sistemlerine (Google Drive, Wetransfer, One Drive vb.) kaydedilmesi, şirket veya kişisel E-Posta hesabı ile yetkisiz bir hesaba gönderilmesi, herhangi bir web sayfasına eklenmesi, kes-kopyala-yapıştır yoluyla veri alınması, izinsiz olarak yazdırılması, ekran görüntüsünün alınması, Flash disk, Harici Disk vb. harici ortamlara kaydedilmesi
- Yetki verilmemiş usb diskler yoluyla kötücül yazılımların sisteme girmesi
- Mobil Telefonların ve Bilgisayarların çalınması veya kaybolması

KVKK KİŞİSEL VERİLERİ KORUMA KURUMU

KVGR 1.3 Tanımlar (sayfa 5)
Veri kaybı/sızıntısı önleme (DLP): Kişisel verilerin, yanlışlıkla ya da kötü niyetli kişilerce kurum dışına çıkarılmasına engel olan ya da engel olmadan işlemi raporlamaya yarayan güvenlik yazılımını ifade eder.
KVGR 3.3. Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması (sayfa 21)
Kişisel veri içeren cihazların kaybolması veya çalınması gibi durumlara karşı erişim kontrol yetkilendirmesi ve/veya şifreleme yöntemlerinin kullanılması kişisel veri güvenliğinin sağlanmasına yardımcı olacaktır.

A.6.2.1 Mobil cihaz politikası
Mobil cihazlar riskleri yönetmek için uygun destekleyici güvenlik önlemleri alınmalı ve politika hazırlanmalıdır.
A.8.3.1 Taşınabilir ortam yönetimi
Kurum tarafından adapte edilmiş olan bilgi sınıflandırma sistemine uygun olarak taşınabilir ortam yönetimi için mevcut prosedürler olmalıdır.
A.8.3.3 Fiziksel ortam aktarımı
Bilgi içeren ortam, taşıma sırasında, yetkisiz erişime, kötüye kullanıma ya da bozulmalara karşı korunmalıdır.
A.13.2.1 Bilgi transfer politikaları ve prosedürleri
Tüm iletişim olanağı türlerinin kullanımıyla bilgi transferini korumak için resmi transfer politikaları, prosedürleri ve kontrolleri mevcut olmalıdır.
A.13.2.3 Elektronik mesajlaşma
Elektronik mesajlaşmadaki bilgi uygun şekilde korunmalıdır.

Information Security Management System ISO 27001 Certified



CoSoSys'in misyonu, güvenlikten ödün vermeden, dünyanın her yerindeki işletmelerin ve son kullanıcıların, mobilite ve iletişim çözümlerinin avantajlarından tam olarak faydalanmalarını sağlamaktır. Bunu başarmak için, gittikçe artan sayıda cihaz, uç nokta ve hassas verilere erişen ve depolayan mobil cihazlarda veri kaybını önleyen çözümler geliştirmektedir.

CoSoSys, korumayı Windows'un ötesinde Mac ve Linux kullanıcılarına genişletebilen az sayıdaki BT güvenlik şirketlerinden biridir. Uygulama portföyleri; cihaz kontrolü, mobil cihaz güvenliği, dosya izleme ve gölge kopyalama, hareketli ve durağan veriler için DLP, dosya / hassas veri şifresi güvenliği, veri senkronizasyonu ve ağ güvenliği gibi işlevleri içermektedir.

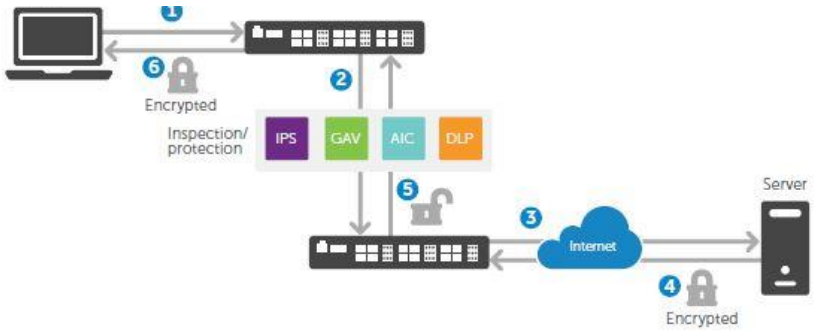
Tehditler :

- Internet üzerinden gelen izinsiz erişimler
  - Kötücül Yazılımlar (Malware)
  - Zero Day saldırıları
  - Virüsler
  - Solucanlar
  - Truva Atı
  - RootKit
  - Yemleme (Pishing)

3.1. Siber Güvenliğin Sağlanması (sayfa 16)
Kişisel veri içeren bilgi teknoloji sistemlerinin internet üzerinden gelen izinsiz erişim tehditlerine karşı korunmasında alınabilecek öncelikli tedbirler, güvenlik duvarı ve ağ geçididir. Bunlar, internet gibi ortamlardan gelen saldırılara karşı ilk savunma hattı olacaktır.
3.1. Siber Güvenliğin Sağlanması (sayfa 18)
Veri sorumluları tarafından, farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecekse, bağlantıların SSL ya da daha güvenli bir yol ile gerçekleştirilmesi de kişisel veri güvenliğinin sağlanması için önemlidir.

A.14.1.2 Halka açık ağlardaki uygulama hizmetlerinin güvenliğinin sağlanması
Halka açık ağlar üzerinden geçen uygulama hizmetlerindeki bilgi, hileli faaliyetlerden, sözleşme ihtilafından ve yetkisiz ifşadan ve değiştirmeden korunmalıdır
A.13.1.2 Ağ hizmetleri güvenliği
Tüm ağ hizmetlerinin güvenlik mekanizmaları, hizmet seviyeleri ve yönetim gereksinimleri tespit edilmeli ve hizmetler kuruluş içinden veya dış kaynak yoluyla sağlanmış olsun olmasın, ağ hizmetleri anlaşmalarında yer almalıdır

SonicWall yeni nesil güvenlik duvarları, IDS – IPS güvenlik servisi, 3700 den fazla imza veri tabanı sayesinde yüksek performans ve düşük gecikme süresini korurken, ağınıza giren ve çıkan her paketin her byte'ını denetler ve ağ içerisine gerçekleşebilecek izinsiz girişleri hem kayıt altına alınmasını hem de önlenmesini sağlar.
Sonicwall Net Extender ve **Mobile Connect** uygulamaları ile iOS, MacOS X, Android, Chrome OS, Kindle Fire ve Windows işletim sistemleri ayırt etmeksizin, Sonicwall güvenlik duvarı aracılığı ile şirketinize uzaktan SSL bağlantısı yapabilir, isterseniz mobil durumda iken tüm ağ trafiğinizi şirket lokasyonunuzdan dışarıya çıkartabilirsiniz.



Tehditler :

- BT Varlıklarının el değiştirmesi veya şirket dışına çıkarılması durumunda barındırdıkları veriler format ve benzeri silme işlemleriyle tamamen yok edilemez,
- Cep telefonlarının da el değiştirmesi durumunda fabrika ayarlarına dönülmesi daha önce kaydedilmiş verileri yok etmez.

2.4. Kişisel Verilerin Mümkün Olduğunca Azaltılması (sayfa 12)
Bunun yanında, yetkisiz erişimin önüne geçilebilmesi için kişisel veri işleme amaçlarına uygun olmasına rağmen, veri sorumlularının sıklıkla erişimi gerekmeyen ve arşiv amaçlı tutulan kişisel verilerin, daha güvenli ortamlarda muhafaza edilmesi tavsiye edilmekte ve ihtiyaç duyulmayan kişisel verilerin ise kişisel veri saklama ve imha politikası ile kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yönetmeliğine uygun ve **güvenli bir şekilde imha edilmesi** gerekmektedir.
1.3 Tanımlar (sayfa 4)
Kişisel veri saklama ve imha politikası: Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikayı ifade eder.

A.8.1.4 Varlıkların iadesi
Tüm çalışanlar ve dış tarafların kullanıcıları, istihdamlarının, Sözleşme veya anlaşmalarının sonlandırılmasının ardından ellerinde olan tüm kurumsal varlıkları iade etmelidirler.
A.8.3.2 Ortamın yok edilmesi
Ortam artık ihtiyaç kalmadığında resmi prosedürler kullanılarak güvenli bir şekilde yok edilmelidir.
A.11.2.7 Teçhizatın güvenli yok edilmesi ve tekrar kullanımı
Depolama ortamı içeren teçhizatların tüm parçaları, yok etme veya tekrar kullanımdan önce tüm hassas verilerin ve lisanslı yazılımların kaldırılmasını veya güvenli bir şekilde üzerine yazılmasını temin etmek amacıyla doğrulanmalıdır.

Blancco PC, Laptop, Sunucu, LUN, Flash Bellek, Mobil cihaz, dosya, klasör gibi çeşitli veri ortamlarıyla ilgili veri imha çözümü sağlamaktadır.
Veriler geri dönüşü olmayacak şekilde silinir. HDD, SATA, SCSI ve SSD diskler için veri silme işlemi gerçekleştirilebilmektedir.
Veri silme işlemi sonrası pdf, xml, csv formatlarında raporlanmaktadır. Bu raporlar dijital imzaya sahiptir. msi ve pxe boot metodlarıyla da uzaktan silme işlemi gerçekleştirilebilmektedir.
Blancco 22 adet silme standardına sahiptir.

Tehditler :

- Güncellenmemiş işletim sistemleri ve uygulamalar, güncellenmediği sürece açık oluştururlar,

3.1. Siber Güvenliğin Sağlanması (sayfa 17)
Diğer önemli unsurlardan biri de yama yönetimi ve yazılım güncellemeleri olup yazılım ve donanımların düzgün bir şekilde çalışması ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli olarak kontrol edilmesi de olası güvenlik açıklarının kapatılması için gereklidir.

A.12.6.2 Yazılım kurulumu kısıtlamaları
Kullanıcılar tarafından yazılım kurulumuna dair kurallar oluşturulmalı ve uygulanmalıdır
A.12.5.1 İşletim sistemleri üzerine yazılım kurulumu
Operasyonel sistemler üzerine yazılım kurulmasını kontrol eden prosedürler hazırlanmalı ve uygulanmalıdır.
A.14.2.9 Sistem Kabul Testleri
Kabul test programları ve ilgili kriterler, yeni bilgi sistemleri, **yükseltmeleri** ve yeni versiyonları için belirlenmelidir

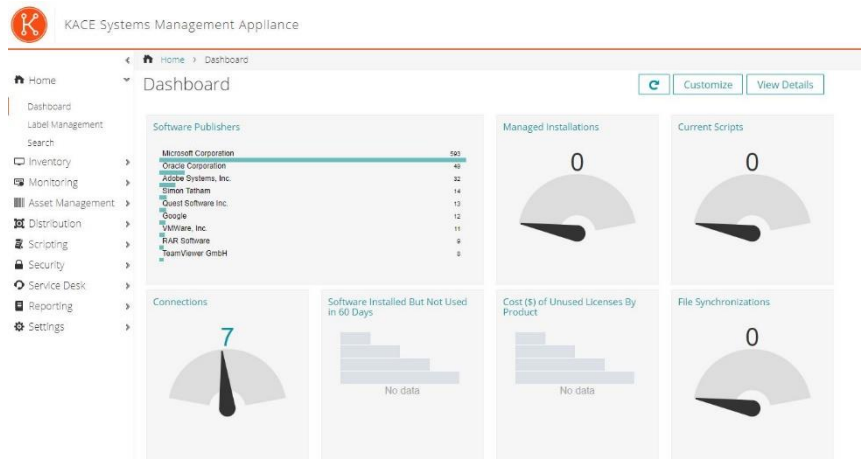
Ivanti (Patch for Windows ve Patch for SCCM) ürünleri ile güncel olmayan yazılımları tespit edip güncellemelerini otomatize edebilirsiniz. İşletim sistemlerinin ve üçüncü parti uygulamaların yamalarını otomatik olarak dağıtabilirsiniz. Ürünün ajanlı ya da ajansız olarak çalışabilme seçenekleri mevcuttur.
Windows yama yönetimi, sanal sunucular, fiziksel sunucular yada uçnoktalarda merkezileştirilmiş, ajansız yama yönetimi sağlar. Yama eksikleri yada 3.parti yazılımların yama ve güncelleştirme işlemlerini merkezi ve otomatize hale getirir. Shavlik ve Patchlink ürün ailesi, Microsoft SCCM ürünlerine entegre olarak, kurumsal altyapılarda SCCM için 3.parti yama yönetimi yapar. Adobe, Apple, Google, Mozilla ve Oracle gibi kurumsal altyapilarda kullanilan ve SCCM tarafından destelenmeyen yamalama özelliklerini SCCM e kazandırarak tek bir konsoldan yönetim kolaylığı sağlar.

Tehditler :

- Güncellenmemiş işletim sistemleri, uygulama ve BIOS v.b. üretici tarafından gömülü gelen yazılımlar,
- Sisteme izinsiz bir donanım eklenmesi,
- Donanım kapasite kontrollerinin yapılmaması nedeniyle yaşanacak kesintiler,
- Lisanssız ürün kullanımından doğan açıklar

3.1. Siber Güvenliğin Sağlanması (sayfa 16)
Bununla birlikte hemen hemen her yazılım ve donanımın bir takım kurulum ve yapılandırma işlemlerine tabi tutulması gerekmektedir. Ancak yaygın şekilde kullanılan bazı yazılımların özellikle eski sürümlerinin belgelenmiş güvenlik açıkları bulunmakta olup, kullanılmayan yazılım ve servislerin cihazlardan kaldırılması potansiyel güvenlik açıklarının azalmasını sağlamaya yardımcı olacaktır. Bu nedenle, kullanılmayan yazılım ve servislerin güncel tutulması yerine silinmesi, kolaylığı nedeniyle öncelikle tercih edilebilecek bir yöntemdir.
3.1. Siber Güvenliğin Sağlanması (sayfa 17)
Diğer önemli unsurlardan biri de yama yönetimi ve yazılım güncellemeleri olup yazılım ve donanımların düzgün bir şekilde çalışması ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli olarak kontrol edilmesi de olası güvenlik açıklarının kapatılması için gereklidir.

A.8.1.1 Varlıkların envanteri
Bilgi ve bilgi işleme olanakları ile ilgili varlıklar belirlenmeli ve bu varlıkların bir envanteri çıkarılmalı ve idame ettirilmelidir
A.12.5.1 İşletim sistemleri üzerine yazılım kurulumu
Operasyonel sistemler üzerine yazılım kurulmasını kontrol eden prosedürler hazırlanmalı ve uygulanmalıdır.



Quest KACE ile envanterde bulunan makinelerdeki yazılımların kullanım oranları takip edilebilir. Bir gün, bir hafta veya son 90 gün içerisinde bir yazılımın kaç kullanıcı tarafından kaç kez kullanıldığı bilgisine erişilebilir ve raporlanabilir. Böylelikle kullanılmayan yazılımların tespiti ve envanterden kaldırılması gerçekleştirilebilir.
Quest KACE ile envanterde bulunan makineler için güncelleme planları oluşturulabilir. Envanterdeki makinelerde bulunan KACE agent'ı aracılığıyla eksik güncellemeler ve yamalar tespit edilip, yazılımlar son sürümlerine yükseltilebilir. Bunun yanı sıra rollback özelliği sayesinde memnun kalınmayan sürümlerden, bir önceki problemsiz sürüme geri dönüş de gerçekleştirilebilir. Eğer istenirse son kullanıcının bu işlemlerden haberi dahi olmayabilir. Tercihen son kullanıcıya paket yüklenmesi işlemini ertelemesi seçeneği de sunulabilir. Böylelikle tüm envanter için güvenlik açığı oluşturabilecek güncelleme eksikliklerinin önüne geçilmiş olur.

Tehditler :

- Ayrıcalıklı erişim yönetiminin yeterli seviyede yapılamaması,
- Kullanıcı şifrelerinin güvenliğinin sağlanamaması,
- Sisteme eklenen yeni donanımların şifrelerinin değiştirilmesinin unutulması,

A.6.2.2 Mobil Cihazlar ve Uzaktan Çalışma
Uzaktan çalışma alanlarında erişilen, işlenen veya depolanan bilgiyi korumak amacı ile bir politika ve destekleyici güvenlik önlemleri uygulanmalıdır.

A.9.1.2 Ağlara ve Ağ Hizmetlerine Erişim
Kullanıcılara sadece özellikle kullanımı için yetkilendirildikleri ağ ve ağ hizmetlerine erişim verilmelidir.

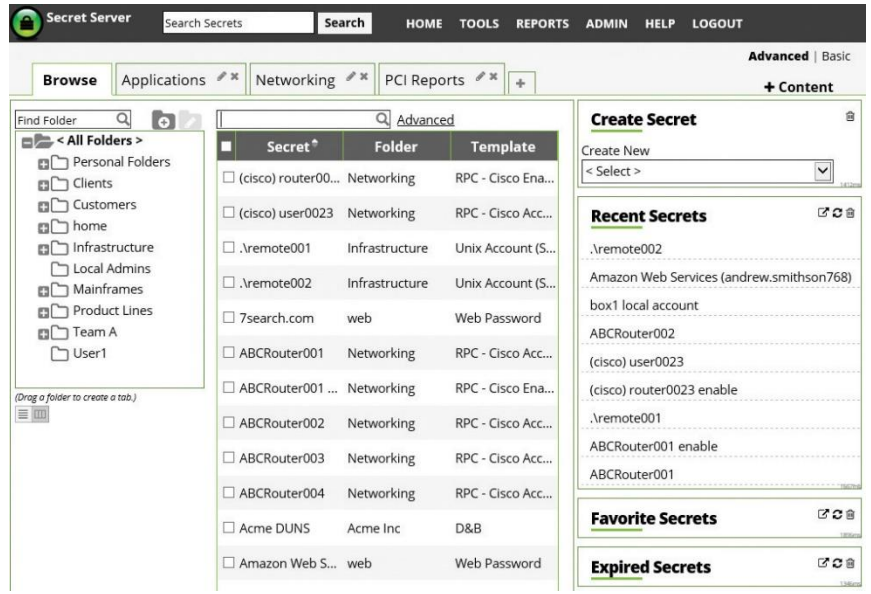
A.9.2.2 Kullanıcı erişimine izin verme
Tüm kullanıcı türlerine tüm sistemler ve hizmetlere erişim haklarının atanması veya iptal edilmesi için resmi bir kullanıcı erişim izin prosesi uygulanmalıdır.

A.9.2.3 Ayrıcalıklı erişim haklarının yönetimi
Ayrıcalıklı erişim haklarının tahsis edilmesi ve kullanımı kısıtlanmalı ve kontrol edilmelidir

A.9.2.5 Kullanıcı erişim haklarının gözden geçirilmesi
Varlık sahipleri kullanıcıların erişim haklarını düzenli aralıklarla gözden geçirmelidir.

A.9.2.6 Erişim haklarının kaldırılması veya düzenlenmesi
Tüm çalışanların ve dış taraf kullanıcılarının bilgi ve bilgi işleme olanaklarına erişim yetkileri, istihdamları, sözleşmeleri veya anlaşmaları sona erdirildiğinde kaldırılmalı veya bunlardaki değişiklik üzerine düzenlenmelidir

A.9.4.3 Parola yönetim sistemi
Parola yönetim sistemleri etkileşimli olmalı ve yeterli güvenlik sevi esine sahi ardaları temin etmelidir



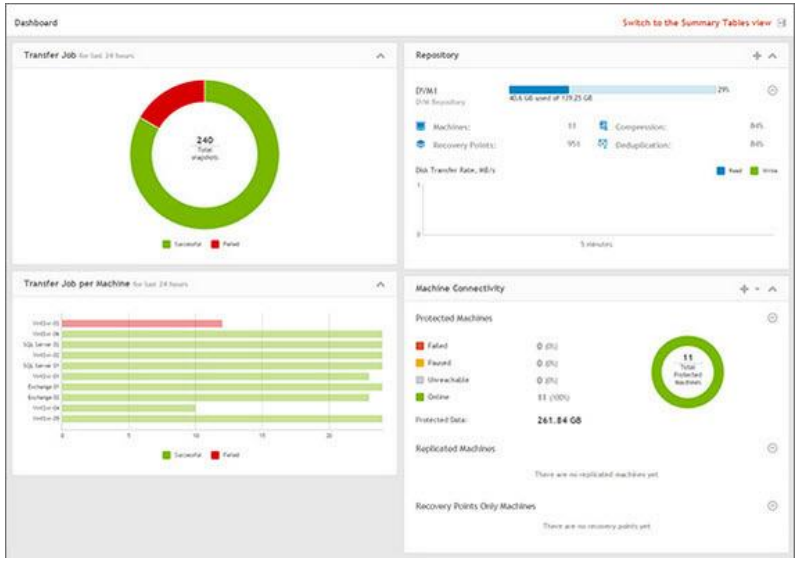
Thycotic Kullanıcı Şifrelerini güvenlik altına almak, uç noktaları korumak ve erişimi kontrol altına almak suretiyle siber saldırıları engeller.
Thycotic Secret Server ile kritik cihazların şifre yönetimini tek merkezden yapıp bu cihazlardaki erişimi onay mekanizmasından geçirip, gerçekleşen oturumları kayıt ederek (session monitoring) izleyip müdahale edebilirsiniz. Ayrıca şifrelerin düzenli aralıklarla değişimini de Secret Server ile yapabilirsiniz. Oluşturulan şifreler kolayca tahmin edilemeyecek standartlarda oluşturulur.

Tehditler :

- Herhangi bir ihlal veya saldırı sonrasında sistem en kısa zamanda en az veri kaybıyla işene devam etmelidir.
- Veri kaybını önlemek için bulutta tutulan verilere izinsiz erişim olması durumu

3.6. Kişisel Verilerin Yedeklenmesi (sayfa 24)
Kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde veri sorumlularının yedeklenen verileri kullanarak en kısa sürede faaliyete geçmesi gerekmektedir.
3.4. Kişisel Verilerin Bulutta Depolanması (sayfa 22)
Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi, bulut ortamlarına şifrelenerek atılması, kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir.

A.12.3.1 Bilgi yedekleme
Bilgi, yazılım ve sistem imajlarının yedekleme kopyalan alınmalı ve üzerinde anlaşılmış bir yedekleme politikası doğrultusunda düzenli olarak test edilmelidir
A.13.2.1 Bilgi transfer politikaları ve prosedürleri
Tüm iletişim olanağı türlerinin kullanımıyla bilgi transferini korumak için resmi transfer politikaları, prosedürleri ve kontrolleri mevcut olmalıdır



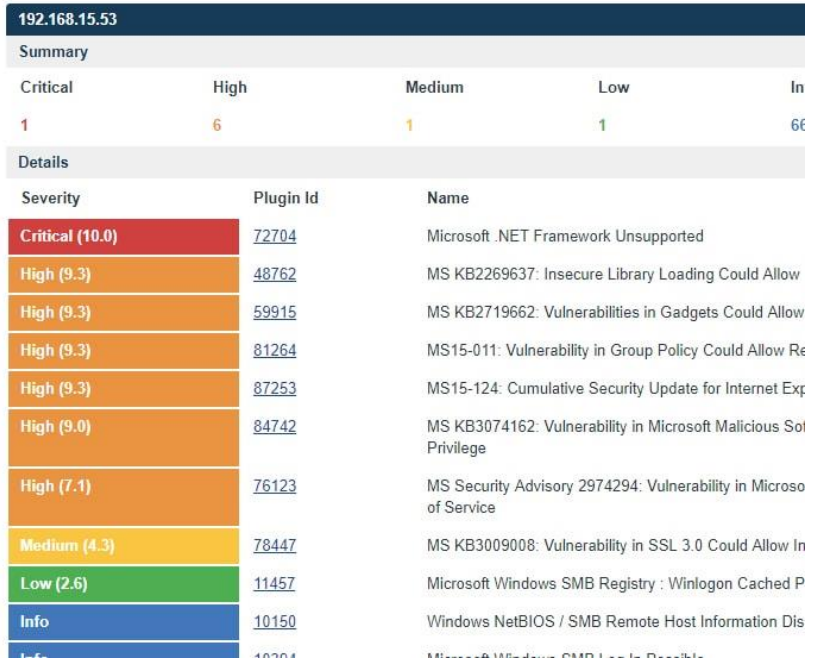
Quest Rapid Recovery ile sanal veya Fiziksel sunucuların yedeklenmesi, yedekten geri dönülmesi ve replikasyonu işlemleri gerçekleştirilebilir. Quest yedekleme yazılımları Client yedekleme için kullanılmamaktadır. Bunun sebebi Fiziksel cihazların yedeklenmesi işleminin Agent aracılığıyla gerçekleştirilmesidir. Sunucular için çok büyük bir yük sayılmayacak kaynak kullanımları, client makinelerde zaman zaman kaynak kullanımına bağlı olarak ağırlık hissettirebilmektedir. Yedeklenmesi gereken veriler sunucularda ise hem Rapid Recovery hem vRanger hem de Netvault isteneni gerçekleştirebilmektedir. File server'lar, uygulama server'ları, web server'ları gibi makinelerin veri yedekliliği konusunda kendilerini kanıtlamış, başarılı yedekleme çözümleridir.

Tehditler :

- Sistemde klasik yollardan tespit edilemeyen tehditler

3.2. Kişisel Veri Güvenliğinin Takibi (sayfa 18)
b) Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi,
ç) Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması,
d) Çalışanların sistem ve servislerdeki güvenlik zaafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması,
gerekmektedir.
3.2. Kişisel Veri Güvenliğinin Takibi (sayfa 19)
Bilişim sistemlerinin bilinen zaafiyetlere karşı korunması için düzenli olarak zaafiyet taramaları ve sızma testlerinin yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılması gerekmektedir.

A.12.6.2 Teknik açıklıkların yönetimi
Kullanılmakta olan bilgi sistemlerinin teknik açıklıklarına dair bilgi, zamanında elde edilmeli kuruluşun bu tür açıklıklara karşı zafiyeti değerlendirilmeli ve ilgili riskin ele alınması için uygun tedbirler alınmalıdır
A.12.7.1 Bilgi sistemleri tetkik kontrolleri
İşletimsel sistemlerin doğrulanmasını kapsayan tetkik gereksinimleri ve faaliyetleri, iş proseslerindeki kesintileri asgariye indirmek için dikkatlice planlanmalı ve üzerinde anlaşılmalıdır.



192.168.15.53

Summary

Critical	High	Medium	Low	In
1	6	1	1	66

Details

Severity	Plugin Id	Name
Critical (10.0)	72704	Microsoft .NET Framework Unsupported
High (9.3)	48762	MS KB2269637: Insecure Library Loading Could Allow
High (9.3)	59915	MS KB2719662: Vulnerabilities in Gadgets Could Allow
High (9.3)	81264	MS15-011: Vulnerability in Group Policy Could Allow Re
High (9.3)	87253	MS15-124: Cumulative Security Update for Internet Exp
High (9.0)	84742	MS KB3074162: Vulnerability in Microsoft Malicious Sof Privilege
High (7.1)	76123	MS Security Advisory 2974294: Vulnerability in Microso of Service
Medium (4.3)	78447	MS KB3009008: Vulnerability in SSL 3.0 Could Allow In
Low (2.6)	11457	Microsoft Windows SMB Registry : Winlogon Cached P
Info	10150	Windows NetBIOS / SMB Remote Host Information Dis

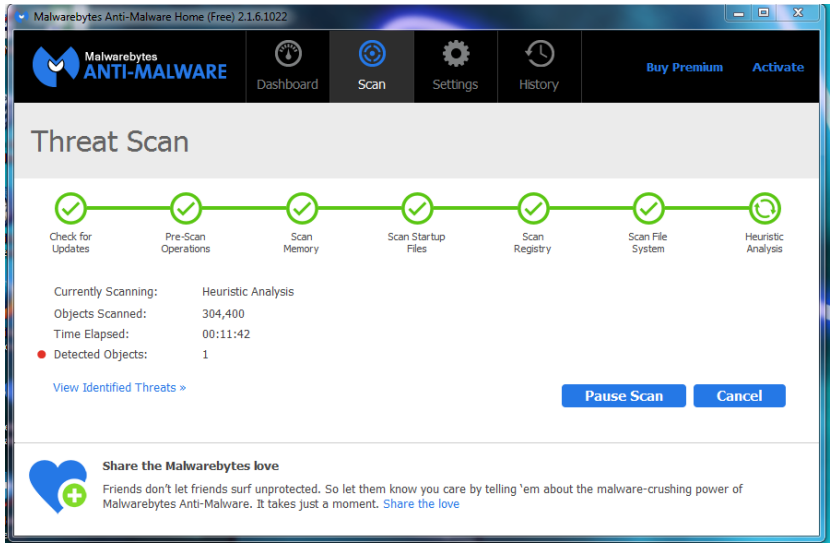
Tenable Zafiyet yönetimi ürünü, riskleri ve zayıf noktaları algılayıp, derecelendirir. Ayrıca, riskin niteliğine ve bunları hafifletmek için yapılacak tavsiyelere ilişkin ayrıntılı bilgi sağlar, sanallaştırma platformlarını (VmWare ESX, NSX, vCenter) Microsoft işletim sistemleri ve uygulamaları, Linux ve Unix, bilinen ağ servisleri, ağ aktif cihazları, güvenlik sistemleri, veri tabanları, web uygulamaları, Amazon Web Servisleri ve Amazon Machine Images ve üçüncü parti uygulamaları için zafiyet taraması yapabilmektedir.

Tehditler :

- Çeşitli güvenlik açıkları nedeniyle sisteme giren (hemen veya bir süre bekledikten sonra aktive olan) kötücül yazılımlar, veri kaybına ve sistem kaynaklarının başkaları tarafından kullanılmasına sebep olmaktadırlar.
- Fidye yazılımlarının sisteme bulaşması

3.1. Siber Güvenliğin Sağlanması (sayfa 18)
Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılması gerekmektedir. Ancak bu ürünlerin sadece kurulumu yeterli olmayıp güncel tutularak gereken dosyaların düzenli olarak tarandığından emin olunmalıdır.
3.6. Kişisel Verilerin Yedeklenmesi (sayfa 24)
Ayrıca kötü amaçlı yazılımlar da halihazırdaki verilere erişime engel olabilmektedir. Örneğin elektronik cihazlardaki kişisel verileri içeren dosyaları kilitleyen ve bunların açılabilmesi için veri sorumlusunu fidye ödemeye zorlayan kötü amaçlı yazılımlar olabilir. Bu tür kötü amaçlı yazılımlara karşı kişisel veri güvenliğini sağlamak için veri yedekleme stratejilerinin geliştirilmesi önerilmektedir.

A.12.2.1 Kötücül yazılımlara karşı kontroller
Kötücül yazılımlardan korunmak için tespit etme, engelleme ve kurtarma kontrolleri uygun kullanıcı farkındalığı ile birlikte u ulanmalıdır.



Malwarebytes; imza kontrolü tekniği kullanarak, klasik güvenlik önleminin yanı sıra, Zero-Day başta olmak üzere bir çok zararlı yazılım veya kod parçalarını Anti-Malware Linking Engine teknolojisi ile tespit ve temizleme işlemini yapar. Anti-Malware, trojen, ransomware gibi kötücül yazılımların tespit edilmesi ile ilgili bir çok patentli yazılım teknolojileri geliştiren ve bu alandaki veri tabanı en geniş olan çözümdür.
Proaktif savunma kapsamında yer alan bu ilk savunma hattı, herhangi bir imza olmaksızın, jenerik yaklaşımla uç noktaların korunmasına olanak tanımakta ve saldırı zincirinin erken aşamalarında dahi bulaşmayı engellemektedir. Kullandığımız teknolojilerin yanı sıra, araştırma çalışmalarımızın da %100 odağı, zero-day kötü niyetli yazılımı ve zero-day exploit'lerinin üstesinden gelmektir.

Tehditler :

- Çeşitli güvenlik açıkları nedeniyle sisteme giren (hemen veya bir süre bekledikten sonra aktive olan) kötücül yazılımlar, veri kaybına ve sistem kaynaklarının başkaları tarafından kullanılmasına sebep olmaktadırlar.
- Fidye yazılımlarının sisteme bulaşması

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

3.1. Siber Güvenliğin Sağlanması (sayfa 18)
Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılması gerekmektedir. Ancak bu ürünlerin sadece kurulumu yeterli olmayıp güncel tutularak gereken dosyaların düzenli olarak tarandığından emin olunmalıdır.
3.2. Kişisel Veri Güvenliğinin Takibi (sayfa 18)
Veri sorumlularının sistemleri çoğunlukla hem içeriden hem de dışarıdan gelen saldırılar ve siber suçlara veya kötü amaçlı yazılımlara maruz kalmakta olup çeşitli belirtilere rağmen bu durum uzun süre fark edilememekte ve müdahale için geç kalınabilmektedir.
3.2. Kişisel Veri Güvenliğinin Takibi (sayfa 19)
Bilişim sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilişim sisteminin kötüye kullanılması gibi istenmeyen olaylarda deliller toplanmalı ve güvenli bir şekilde saklanmalıdır.

A.12.2.1 Kötücül yazılımlara karşı kontroller
Kötücül yazılımlardan korunmak için tespit etme, engelleme ve kurtarma kontrolleri uygun kullanıcı farkındalığı ile birlikte u ulanmalıdır.
A.16.1.2 Bilgi güvenliği olaylarının raporlanması
Bilgi güvenliği olayları uygun yönetim kanalları aracılığı ile olabildiğince hızlı bir şekilde raporlanmalıdır
A.16.1.7 Kanıt toplama
Kuruluş kanıt olarak kullanılabilecek bilginin teşhisi, toplanması, edinimi ve korunması için prosedürler tanımlamalı ve uygulamalıdır.

Günümüzün gelişmiş siber tehditleri geleneksel savunma noktalarını kolaylıkla bypass etmektedir. Kurum ve devlet dairelerinin, düzenleme altındaki veriler ve uç noktalara yönelik daha güçlü politikalar ve imzaya dayalı önlemleri uygulamaya koymasından bu yana, gelişmiş suç örgütleri de taktiklerini değiştirmiş ve yeni nesil siber saldırılar kullanarak fikri mülkiyet ve diğer ağ bağlantılı varlıkları hedef almışlardır. Kitlesel kötü niyetli yazılımın yerini alan günümüzün siber saldırıları kişiselleştirilmiş olup oldukça dirençlidirler. Tehditler gitgide biçim değiştiren, dinamik ve zero day bir hal almışlardır. Bu çok-kademeli saldırılar, geleneksel ve yeni nesil güvenlik duvarları, IPS, AV nezdinde ve imzaya, bilinen uygunsuz davranış kalıplarına veya itibara dayalı olarak oluşturulan ağ geçitleri nezdinde tamamen masum olarak algılanabilmektedir. Bugün gelinen noktada güvenlik bilinci yüksek kurumlar ve devlet daireleri, gelişmiş kötü niyetli yazılım, zero-day ve hedeflenmiş APT saldırıları gibi günümüzün gelişmiş siber saldırılarına karşı sektörde öncü bir koruma sağlayan FireEye platformlarını seçmektedirler.

KVGR Teknik Tedbirler Tablosu

Yetki Matrisi	
Yetki Kontrol	THYCOTIC
Erişim Logları	THYCOTIC
Kullanıcı Hesap Yönetimi	THYCOTIC
Ağ Güvenliği	FIREEYE / SONICWALL / TENABLE
Uygulama Güvenliği	THYCOTIC
Şifreleme	COSOSYS
Sızma Testi	
Saldırı Tespit ve Önleme Sistemleri	FIREEYE / MALWAREBYTES / SONICWALL
Log Kayıtları	
Veri Maskeleme	
Veri Kaybı Önleme Yazılımları	COSOSYS
Yedekleme	QUEST
Güvenlik Duvarları	SONICWALL
Güncel Anti-Virüs Sistemleri	SONICWALL / MALWAREBYTES
Silme, Yok Etme veya Anonim Hale Getirme	BLANCCO
Anahtar Yönetimi	THYCOTIC

Teşekkürler…