KVKK

Kişisel Verilerin Korunması Kanunu (6698)

FARKINDALIK EĞİTİMİ

e-data TEKNOLOJİ

www.e-data.com.tr

AMAÇ / KAPSAM

- **AMAÇ**
- **MADDE 1-** Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.
- **KAPSAM**
- **MADDE 2-** Bu Kanun hükümleri, **kişisel verileri işlenen gerçek kişiler** ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla **işleyen gerçek ve tüzel kişiler** hakkında uygulanır.

TARİHÇE

28 Ocak 1981 Strasbourg / Avrupa Konseyi 108 nolu sözleşme

- Kişisel verilerin otomatik işleme tabi tutulması karşısında bireylerin korunması sözleşmesi

17 Şubat 2016 Uygun Bulunma Kanunu

- 108 nolu sözleşme Resmi Gazetede yayınlandı

24 Mart 2016 6698 KVKK

- Kanun TBMM'de kabul edildi.

7 Nisan 2016 6698 KVKK

- Kanun Resmi gazetede yayınlanarak yürürlüğe girdi.

TERİMLER

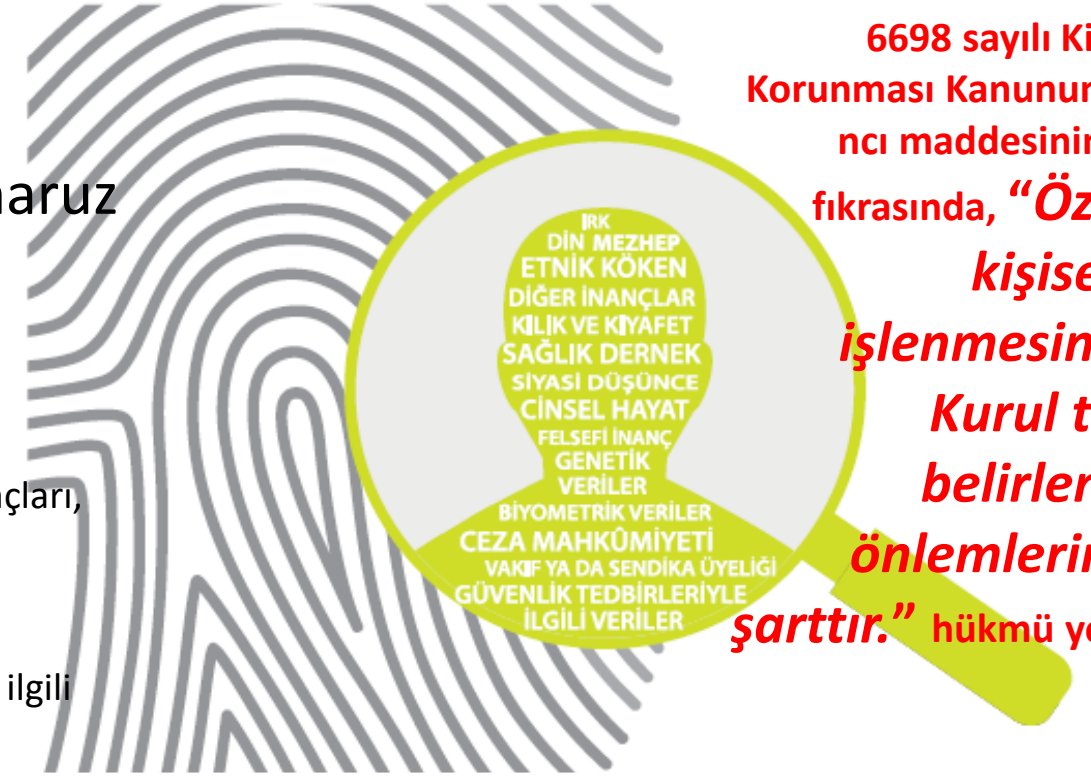
- **Kişisel Veri:**
  - **Gerçek kişiye ilişkin olma:** Kişisel veri, gerçek kişiye ilişkin olup, tüzel kişilere ilişkin veriler kişisel verinin tanımının dışındadır
  - **Kişiyi belirli veya belirlenebilir kılması:** Kişisel veri, ilgili kişinin doğrudan kimliğini gösterebileceği gibi, o kişinin kimliğini doğrudan göstermemekle birlikte, herhangi bir kayıtla ilişkilendirilmesi sonucunda kişinin belirlenmesini sağlayan tüm bilgileri de kapsar
  - **Her türlü bilgi:** Bu ifade son derece geniş olup, bir gerçek kişinin; adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgiler değil; telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, özgeçmiş, resim, görüntü ve ses kayıtları, parmak izleri, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri, sağlık bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm veriler kişisel veri olarak kabul edilmektedir.

TERİMLER

Özel Nitelikli Kişisel veri:

Başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikteki verilerdir.

- Kişilerin ırkı,
  Etnik kökeni,
  Siyasi düşüncesi,
  Felsefi inancı, dini, mezhebi veya diğer inançları,
  Kılık ve kıyafeti,
  Dernek, vakıf ya da sendika üyeliği,
  Sağlığı,
  Cinsel hayatı,
  Ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri
  Biyometrik ve genetik verileri



6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 6 ncı maddesinin (4) numaralı fıkrasında, *"Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır."* hükmü yer almaktadır.

TERİMLER

- **İlgili kişi:** Kişisel verisi işlenen gerçek kişiyi,
- **Veri sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi,
- **Kişisel verilerin işlenmesi:** Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,
- **Veri işleyen:** Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

TERİMLER

- **Açık rıza:** Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,
- **Aydınlatma Metni:** Kişisel verilerin elde edilmesi, kaydedilmesi, saklanması, güncellenmesi, sınıflandırılması, mevzuatın izin verdiği üçüncü kişilerle paylaşılması veya onlara devredilmesi gibi konularda mevzuata uygun şekilde yapılan açıkladır.
- **Anonim hâle getirme:** Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini,
- **VERBİS:** Veri sorumlularının kayıt olmak zorunda oldukları ve veri işleme faaliyetleri ile ilgili bilgileri beyan ettikleri bir kayıt sistemidir. Veri sorumlularının, Kurulun gözetiminde Başkanlık tarafından tutulmakta olan Veri Sorumluları Siciline kaydolmaları zorunludur.

KVKK UYGULAMA DIŞI ALANLAR

- Kişisel verilerin kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi
- Resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi
- Millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi

KVKK UYGULAMA DIŞI ALANLAR

- Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi
- Soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi

VERBİS İSTİSNALAR

- Herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler.
- 18/01/1972 tarihli ve 1512 sayılı **Noter**lik Kanunu uyarınca faaliyet gösteren noterler.
- 04/11/2004 tarihli ve 5253 sayılı **Dernekler** Kanununa göre kurulmuş derneklerden,
  20/02/2008 tarihli ve 5737 sayılı **Vakıflar** Kanununa göre kurulmuş vakıflardan ve 18/10/2012 tarihli 6356 sayılı **Sendikalar** ve Toplu İş Sözleşmesi Kanununa göre kurulmuş sendikalardan yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik kişisel veri işleyenler.

VERBİS İSTİSNALAR

- 22/04/1983 tarihli ve 2820 sayılı **Siyasi Partiler** Kanununa göre kurulmuş siyasi partiler.
- 19/3/1969 tarihli ve 1136 sayılı **Avukat**lık Kanunu uyarınca faaliyet gösteren avukatlar.
- 1/6/1989 tarihli ve 3568 sayılı Serbest Muhasebeci Mali Müşavirlik ve Yeminli Mali Müşavirlik Kanunu uyarınca faaliyet gösteren **Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler**.

KVKK Maddeler

Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesi

MADDE 7- (1) Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

(2) Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.

(3) Kişisel verilerin silinmesine, yok edilmesine veya anonim hâle getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir.

Veri güvenliğine ilişkin yükümlülükler

MADDE 12- (1) Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

VERBİS'e Kayıt

- Yıllık çalışan sayısı 50'den veya yıllık mali bilançosu 25 milyon TL'den çok olan gerçek veya tüzel kişi veri sorumluları için kayıt zorunluluğu 01.10.2018 ila **30.06.2020** arası olarak belirlendi. Yurt dışında yerleşik gerçek veya tüzel kişi veri sorumluları için de aynı tarihler geçerli.
- Yıllık çalışan sayısı 50'den ve yıllık mali bilançosu 25 milyon TL'den az olan ancak ana faaliyet konusu özel nitelikli veri işleme olan gerçek ve tüzel kişi veri sorumluları için bu tarihler 01.01.2019 ila **30.09.2020** olarak belirlendi.

Şirketler için KVKK süreçleri

- Kişisel veri işleme envanterinin hazırlanması
- Kişisel Veri Saklama ve İmha Politikası'nın hazırlanması
- Veri Sorumluları Sicili'ne (VERBİS) kayıt
- Aydınlatma yükümlülüğünün yerine getirilmesi
- Açık rızaların alınması
- Kişisel verilerin toplanması
- Kişisel verilerin güvenliğinin sağlanması
- İşlenme şartları ortadan kalkan kişisel verilerin silinmesi
- Üçüncü kişilerle kişisel verilerin paylaşılması
- İlgili kişilerin şikayetlerinin değerlendirilmesi

KVKK 6698 Uyum Danışmanlık Projesi

e-data TEKNOLOJİ

Başlama Toplantısı

- KVKK Uyum Ekibinin oluşturulması
- Kanun hakkında bilgilendirme
- Çalışma takviminin gözden geçirilmesi
- KVKK Uyum Çalışması Duyurusunun hazırlanması
- Envanterin dağıtımı ve envanter eğitimi

Kişisel Veri Envanteri

Kişisel Veri Envanteri Özeti (VERBİS Kaydı)

Tarih
13.01.2020
Sayfa
1/2

Veri Kategorisi	Veri Konusu Kişi Grubu	İşleme Amacı	Saklama Süresi	Yurt İçi Alıcı Grupları	Yurt Dışı Alıcı Grupları	Tedbirler
Özlük	Çalışan	Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi	10 Yıl	Yetkili Kamu Kurum ve Kuruluşları	Veri Aktarılmamaktadır	Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
Finans	Çalışan	Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi	10 Yıl	Yetkili Kamu Kurum ve Kuruluşları	Veri Aktarılmamaktadır	Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
Kimlik	Çalışan Yakınları	Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi	10 Yıl	Yetkili Kamu Kurum ve Kuruluşları	Veri Aktarılmamaktadır	Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
İletişim	Çalışan	Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi	10 Yıl	Veri Aktarılmamaktadır	Veri Aktarılmamaktadır	Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
Kimlik	Çalışan	Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi	10 Yıl	Yetkili Kamu Kurum ve Kuruluşları	Veri Aktarılmamaktadır	Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
Kimlik	Ürün veya Hizmet Alan Kişi	Sözleşme Süreçlerinin Yürütülmesi , Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi	2 Yıl	Veri Aktarılmamaktadır	Veri Aktarılmamaktadır	Veri kaybı önleme yazılımları kullanılmaktadır.
İletişim	Ürün veya Hizmet Alan Kişi	Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi	2 Yıl	Veri Aktarılmamaktadır	Veri Aktarılmamaktadır	Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir. ,

Neler uyumlu? (uyumsuz)

KVKK Politikası

- Politika Kapsamı ve amacı
- Tanımlar
- Görev ve Sorumluluklar
- Risk Değerlendirme
- Veri Koruma İlkeleri
- Veri Sahiplerinin Hakları
- Açık Rıza Alınması
- Veri Güvenliği
- Veri Paylaşımı
- Kayıtların yönetimi
- Denetim
- Politikanın Güncel Tutulması

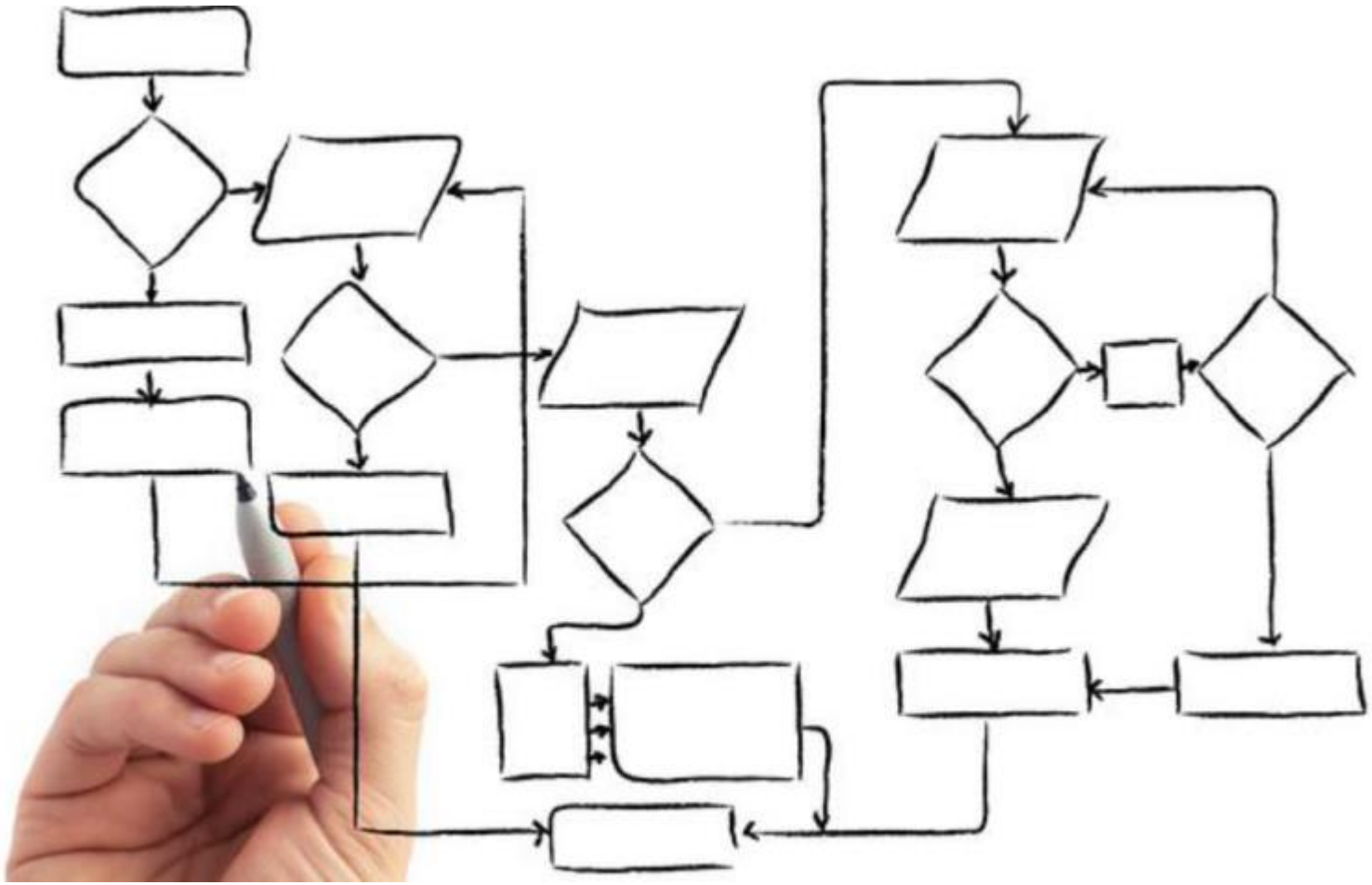
Veri Saklama ve İmha Politikası

Taahhütname ve Sözleşmeler

- Çalışan KVKK taahhütnameleri
- Tedarikçi ve müşteri taahhütnameleri
- Veri işleyen taahhütnameleri

Prosedürler

- Olay (ihlal) yönetim prosedürü
- Kayıt yönetim prosedürü
- Veri aktarım politikası
- Talep yönetim prosedürü
- Disiplin prosedürü



VERBİS


Kullanıcı Adı
Parola
Giriş Yap
Parolamı unuttum
Bir hesabınız yok mu?
Kayıt Olun
KVKK
Değerli Kullanıcımız;
Kişisel Verileri Koruma Kurumu Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) hoşgeldiniz.
Sisteme giriş yapabilmek için;
Eğer daha önce başvuru formu doldurarak göndermiş ve akabinde de Kurumumuzca tarafınıza "kullanıcı adı" ve "parola" iletilmişse, öncelikle sol taraftaki alanlara bu kullanıcı adı ve parolayı yazmanız ve "Giriş Yap" butonuna tıklamanız gerekmektedir.
Eğer daha önce başvuru formu doldurarak göndermemişseniz en alttaki "Kayıt Olun" butonuna tıklamanız ve gelen ekranda ilgili alanları doldurarak başvuru formu oluşturmanız gerekmektedir.
Daha önce başvuru yaptıysanız, başvuru durumunuz ile başvuru formunuzun örneğini Başvuru Kontrol sayfasından giriş yaparak görebilirsiniz.

KVKK

Kişisel Verilerin Korunması Kanunu (6698)

Teknik Gereklilikler ve Çözümler

www.e-data.com.tr

Kişisel Veri Güvenligi Rehberi

(Teknik ve idari tedbirler)

ENDPOINT PROTECTOR by CoSoSys

Tehditler :

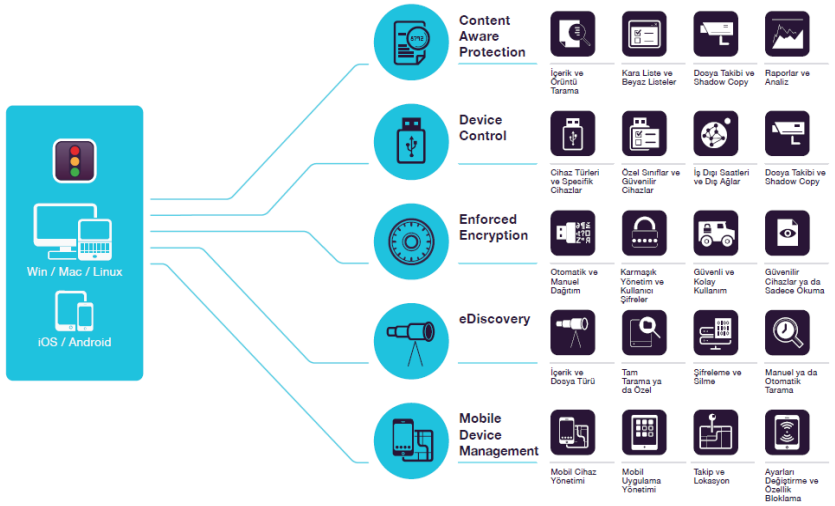
- Bir dosyanın, izinsiz olarak, buluttaki dosya barındırma sistemlerine (Google Drive, Wetransfer, One Drive vb.) kaydedilmesi, şirket veya kişisel E-Posta hesabı ile yetkisiz bir hesaba gönderilmesi, herhangi bir web sayfasına eklenmesi, kes-kopyala-yapıştır yoluyla veri alınması, izinsiz olarak yazdırılması, 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 :

- Bir dosyanın, izinsiz olarak Flash disk, Harici Disk vb. harici ortamlara kaydedilmesi
- Yetki verilmemiş usb diskler yoluyla kötücül yazılımların sisteme girmesi

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.

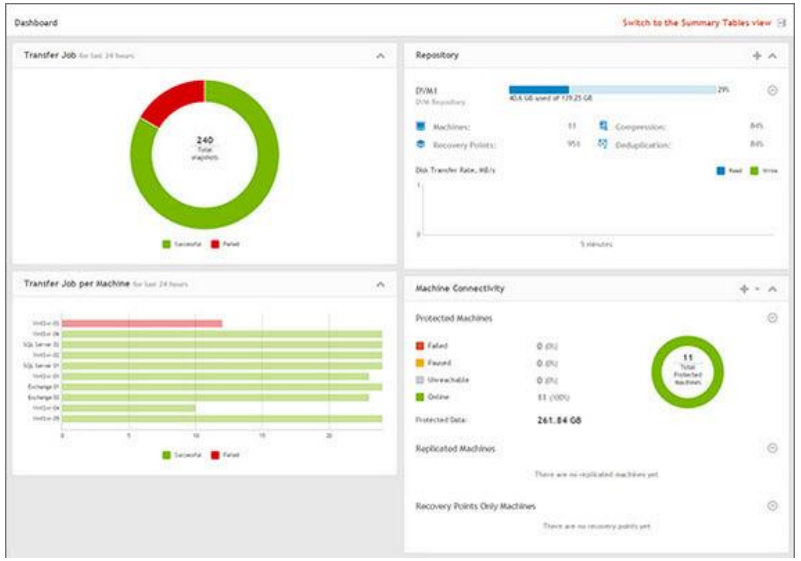
Apricorn'un 256-bit dahili ve taşınabilir HDD şifreleme kullanmasına yönelik benzersiz yaklaşımı, tamamı ile otonom çalışarak, AES256-XT kriptolama ve bağımsız anahtar üretimini işletim sistemi bağımsız olarak yapmaktadır. Toplu yönetim desteği ile şifre uzunluğunu tanımlayabilir, akıllı şifre zorlama, otomatik kilitlenme, salt okunur çalışma ve kendini imha özellikleri ekleyebilirsiniz. Aluminyum gövde (belirli modellerde) ve şok ve titreşim koruma ile dış etkenlere epoksi dolgu koruma ile iç müdahalelere karşı koruma sağlarsınız.

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.

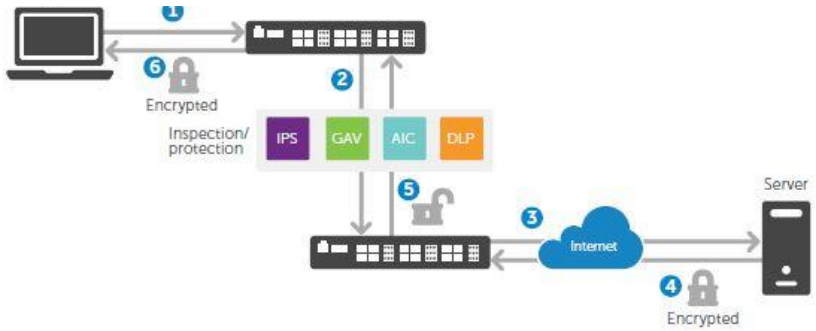
Tehditler :

- 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.

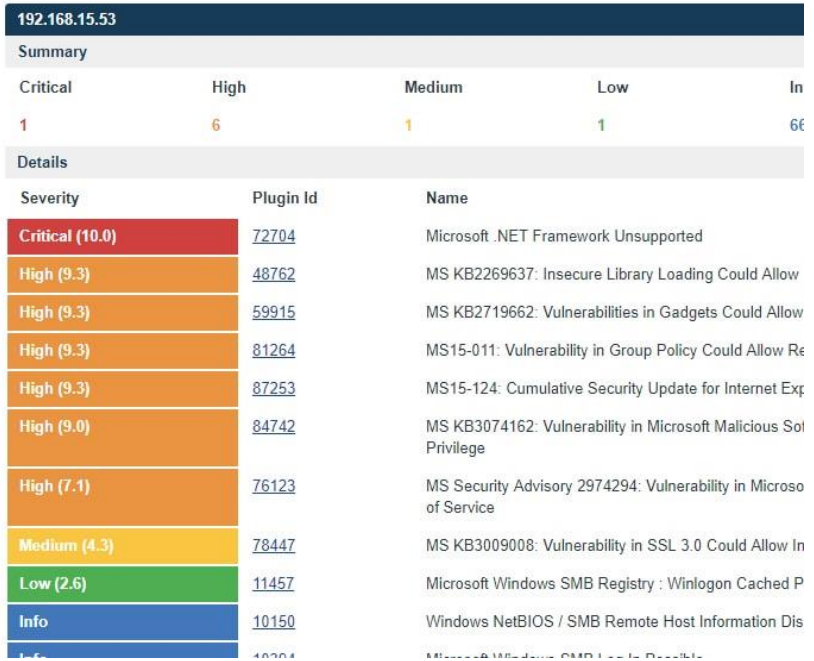
Blancco PC, Laptop, Sunucu, LUN, Flash Bellek, Mobil cihaz, dosya, klasör gibi çeşitli veri ortamlarıyla ilgili veri imha çözümü sağlamaktadır.
Veriler geri dönüşü olmayacak şekilde silinir. HDD, SATA, SCSI ve SSD diskler için veri silme işlemi gerçekleştirilebilmektedir. Veri silme işlemi sonrası pdf, 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 :

- 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 :

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

3.1. Siber Güvenliğin Sağlanması (sayfa 17)
Ayrıca, kişisel veri içeren sistemlere erişimin de sınırlı olması gerekmektedir. Bu kapsamda çalışanlara, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanınmalı ve kullanıcı adı ve şifre kullanılmak suretiyle ilgili sistemlere erişim sağlanmalıdır. Söz konusu şifre ve parolalar oluşturulurken, kişisel bilgilerle ilişkili ve kolay tahmin edilecek rakam ya da harf dizileri yerine büyük küçük harf, rakam ve sembollerden oluşacak kombinasyonların tercih edilmesi sağlanmalıdır.

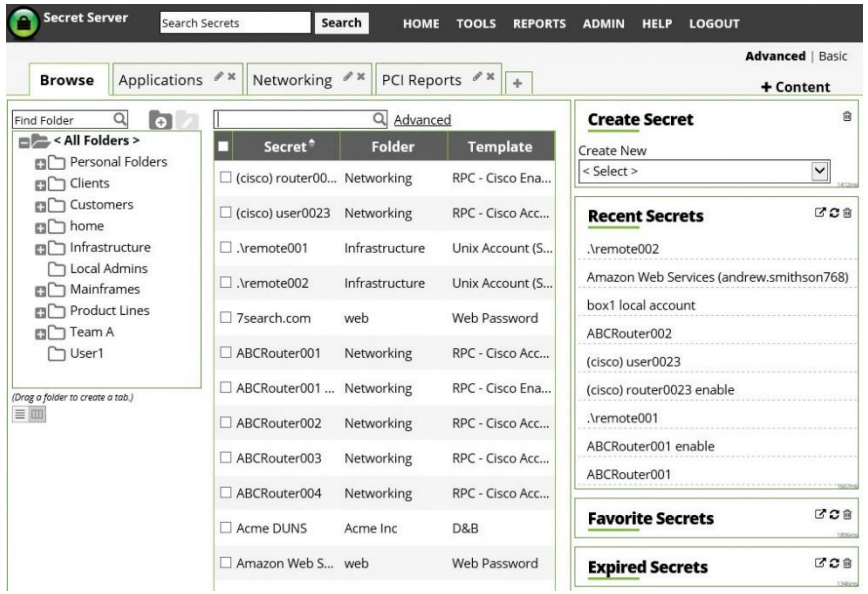
A.9.2.2 Kullanıcı erişimine izin verme
Tüm kullanıcı türlerine tüm sistemler ve hizmetlere erişim haklarının atanması veya iptal edilmesi için resmi bir kullanıcı erişim izin prosesi uygulanmalıdır.

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 :

- 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.

Teşekkürler

www.e-data.com.tr