TÜBİTAK
BİLGEM

BİLİŞİM VE BİLGİ GÜVENLİĞİ İLERİ TEKNOLOJİLER ARAŞTIRMA MERKEZİ

SİBER GÜVENLİK TEKNOLOJİ VE ÜRÜN TAKSONOMİSİ

(TASLAK)

Rev: 0.1

25 Eylül 2017

P.K. 74, 41470 Gebze / KOCAELİ
Tel: (0262) 648 10 00, Faks: (0262) 648 11 00
www.bilgem.tubitak.gov.tr/

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

TANIMLAR

BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BYOD	Bring Your Own Device
BYOK	Bring Your Own Key
CSP	Cloud Service Provider
DDoS	Distributed Denial of Service
FwaaS	Firewall as a Service
IAM	Identity and Access Management
IDaaS	Identity as a Service
IGA	Identity Governance and Administration
IoT	Internet of Things
IPS	Intrusion Prevention System
IT	Information Technology
JSON	JavaScript Object Notation
KOBİ	Küçük ve Orta Büyüklükteki İşletmeler
NAC	Network Access Control
NFV	Network Functions Virtualization
NGFW	Next-Generation Firewall
NIST	National Institute of Standards and Technology
OOB	Out-of-Band
OTP	One Time Password
OTT	Over-the-Top
PC	Personal Computer
PKI	Public Key Infrastructure
SCIM	System for Cross-Domain Identity Management
SDN	Software-Defined Networking
SGE	Siber Güvenlik Enstitüsü
SMS	Short Message Service
SSO	Single Sign On
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UTM	Unified Threat Management
VPN	Virtual Private Network

1. GİRİŞ

Bu doküman, 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda TÜBİTAK sorumluluğunda olan "Siber Güvenlik Teknoloji Yol Haritasının ve Araştırma Gruplarının Oluşturulması" (Eylem No 4.2) eylemi ve T.C Kalkınma Bakanlığı desteği ile yürütülen Siber Güvenlik Eğitim ve Araştırma Projesi hedefleri doğrultusunda TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsü (SGE) tarafından hazırlanmıştır. Dokümanda ülkemizin siber güvenlik teknoloji yol haritası çalışmalarına girdi olacak siber güvenlik teknoloji taksonomisi tanımlanlanmıştır.

Siber güvenlik teknoloji ve ürün taksonomisi dokümanı, iki bölümden oluşmaktadır. Birinci Bölümde dokümanın genel içeriği, dokümanın amacı ve kapsamı tanımlanmaktadır. İkinci Bölümde siber güvenlik teknoloji yol haritasına girdi sağlayacak siber güvenlik teknoloji taksonomisi ile siber güvenlik teknoloji ve ürün taksonomisinin açıklamalarını içeren sözlük yer almaktadır.

1.1 Amaç ve Kapsam

Bu dokümanın amacı, siber güvenlik ekosistemindeki teknoloji geliştirme faaliyetlerinin ulusal ihtiyaçlar ve ulusal siber güvenlik vizyonu ile uyumlu olarak yürütülmesine katkı sağlamak için gerekli altyapıları hazırlamak, paydaşlar arasında ortak dil kullanılmasını sağlamak, teknoloji önceliklerinin belirlenmesi için bir çatı oluşturmaktadır.

Dokümanın içeriği, 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nda TÜBİTAK sorumluluğunda olan "Siber Güvenlik Teknoloji Yol Haritasının ve Araştırma Gruplarının Oluşturulması" (Eylem No 4.2) eylemi ve T.C Kalkınma Bakanlığı desteği ile yürütülen Siber Güvenlik Eğitim ve Araştırma Projesi hedefleri doğrultusunda yürütülen ve aşağıda belirtilen çalışmaların sonuçlarından faydalanılarak hazırlanmıştır.

- Siber güvenlik teknolojisi geliştiren paydaşlarla gerçekleştirilen toplantılar
- Uluslararası bakış açısı ile siber güvenlik teknolojilerinin ve eğilimlerinin değerlendirilmesi

2. SİBER GÜVENLİK TEKNOLOJİ VE ÜRÜN TAKSONOMİSİ

Siber güvenlik teknoloji yol haritasının belirlenmesi için öncelikle siber güvenlik teknoloji ve ürün taksonomisinin uluslararası siber güvenlik teknolojileri ve eğilimleri dikkate alınarak tanımlanması gerekmektedir. Bu kapsamda hazırlanan taksonomi Şekil 1'de sunulmuştur. Şekil 1'de sunulan taksonominin her bir öğesi numaralandırılmıştır. Sonraki bölümde taksonomide yer alan her bir öğenin açıklaması yer almakta olup, tanımlanan taksonominin en alt öğeleri için örnek siber güvenlik teknolojileri için özet bilgi sunulmuştur.

Şekil 1. Siber Güvenlik Teknoloji ve Ürün Taksonomisi

3. SİBER GÜVENLİK TEKNOLOJİ VE ÜRÜNLERİ TAKSONOMİ SÖZLÜĞÜ

1 Kullanım Alanına Göre

1.1 Ağ Güvenliği

Ağ Güvenliği, ağ altyapısını yetkisiz erişime, yanlış kullanıma, arıza, değişiklik, imha veya yanlış bilgilendirmeye karşı korumak için gerek donanım gerek yazılım olarak önleyici önlemlerin alınması işlemidir. Güvenli bir platform oluşturularak, bilgisayarlar, kullanıcılar ve programlar için izin verilen kritik işlevlerin güvenli bir ortamda gerçekleştirilmesi sağlanır. Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde sıralayabiliriz: Ağ Politika Yönetimi, Güvenlik Duvarı, Ağ İzleme, Saldırı Önleme Sistemleri, Toplu Saldırı Yönetimi vb.

Ağ Politika Yönetimi (Network Policy Management)

Ağ Güvenlik İlke Yönetimi (Network Security Policy Management)

Ağ Güvenlik İlke Yönetimi sağlayıcıları, kural performansını optimize etmek ve yönetim iş akışını değiştirmek, uyumluluk için kuralları kontrol etmek ve birden çok ağ yolu üzerinde dağıtılan bir ağ haritasını görselleştirmek için analitik araçlar sağlar.

Ağ Erişim Denetimi (Network Access Control)

Bir ağ erişim denetimi (NAC) işlemi, tüm aygıtların ve kullanıcıların erişimini denetlemek için ağa politikalar ekler. Politikalar, cihaz ve / veya kullanıcı kimlik doğrulamasına ve uç nokta yapılandırmasına bağlı olabilir.

Yazılım Tanımlı Güvenlik (Software-Defined Security)

Yazılım Tanımlı Güvenlik bir çatı terimdir. Güvenlik politika yönetiminin soyutlaştırılmasından fayda sağlayan teknolojilerin birleşiminden oluşmaktadır. Lokasyondan bağımsız olarak iş yükü ve bilgi korunması, güvenlik kontrollerinin risk profiline göre ayarlanması gibi özellikleri mevcuttur.

Ağ İzleme ve Adli Bilişim (Network Monitoring and Forensics)

Ağ izleme, bir bilgisayar ağını ve bileşenlerini sürekli olarak izleyen ve ağ yöneticisine (e-posta, SMS veya diğer alarmlar aracılığıyla) kesinti veya başka bir sorun olması durumunda bunu bildiren bir sistemin kullanılmasıdır. Ağ adli bilişimi, güvenlik saldırılarının veya diğer sorunlu olayların kaynağını keşfetmek için ağ olaylarının yakalanması, kaydedilmesi ve analiz edilmesidir.

Ağ Güvenlik Duvarı (Network Firewall)

Hizmet Olarak Güvenlik Duvarı (Firewall as a Service)

Hizmet Olarak Güvenlik Duvarı (FwaaS) bulut bazlı servis veya hibrit çözüm (bulut&geliştirme uygulamaları) olarak servis veren güvenlik duvarıdır. FwaaS'in vaatleri; merkezcil yönetim biçimini öne çıkararak, daha çok kurumsal güvenlik duvarı özellikleri kullanmak ve güvenlik incelemelerini bir bulut altyapısına kısmen ya da tamamen aktararak, daha basit ve daha esnek mimari sağlamaktır.

Yeni Nesil Güvenlik Duvarları (Next-Generation Firewalls)

Yeni Nesil Güvenlik Duvarları (NGFW), port/protokol incelemesinin ötesinde, uygulama ekleme seviyesindeki incelemeyi durdurma ve güvenlik açığının önlemesi gibi güvenlik duvarı dışından da bilgi getirebilen, derin paket inceleyici güvenlik duvarlarıdır. Bu ekstra güvenlik duvarı bilgi servisleri bulut bazlı gelişmiş tehdit tespiti ve tehdit bilgisini içerir. NGFW, bağımsız tehdit önleme sistemleri veya birleşik tehdit yönetimi ile karıştırılmamalıdır.

Durum Denetlemeli Güvenlik Duvarları (Stateful Firewalls)

Durum Denetlemeli Güvenlik Duvarı: "Durum" kullanımı bağlantının nasıl kullanıldığı hakkında daha güvenli bilgi verirken; eski güvenlik duvarları sadece internet protokol (IP) adres kaynağı, varış noktası ve portlarını kullanmaktaydı. Durumsal güvenlik duvarları; kaynak IP, varış IP, kullanılan portlar ve kaynak ile hedefin arasındaki geçmiş etkileşimlere dayalı paket filtreleme ve kontroller bulundurur. Durum denetlemeli güvenlik duvarları; yönlendirici ve servis sağlayıcı bulut altyapısı (IaaS) dahil pek çok teknolojide yer alabilir

Saldırı Önleme Sistemi (IPS)

Ağ Saldırı Önleme Sistemi (Network IPS)

Bir ağ saldırı önleme sistemi (IPS) sıralı, derin paket inceleme gereçleri ile teknolojik gelişmeleri kullanarak saldırıları ve istenmeyen trafiği belirler, engeller ve bunlara karşı koruma sağlar. Ağ IPS'leri gelecek nesil IPS'leri (NGIPS) gibi kullanıcı veya uygulama içeriklerine yaptırım uygulamaz.

Yeni Nesil Saldırı Önleme Sistemi (Next-Generation IPS)

Yeni nesil saldırı önleme sistemleri, birinci nesil saldırı önleme sistemi (IPS) yeteneklerine ek olarak, uygulama bilinci ve tam yığın görünürlük, içerik ve bağlam farkındalığı, yeni bilgi kaynaklarını entegre etmek için yolar sağlar.

Dağıtık Hizmet Dışı Bırakma Savunması (DDoS Defense)

Dağıtık Hizmet Dışı Bırakma saldırılarında, internetin iş amaçlı kullanımına engel olmak veya şirketlerden para koparmaya çalışmak için pek çok teknik kullanılır. Hackerlık, siyasal veya sosyal amaçlı olarak düşünüldüğünde, DDOS saldırganları için motivasyon kaynaklarından biridir. DDoS savunma ürünleri ve servisleri, bu tip saldırıları tespit eder ve azaltır.

Birleşik Tehdit Yönetimi (UTM)

Birleşik tehdit yönetimi platformları, özellikle küçük veya orta ölçekli işletmelerde kullanılan, çok fonksiyonlu ağ güvenlik uygulamalarıdır. Özellik kullanılabilirliği büyümekte olup, diğer ağ güvenlik teknolojilerinin yeni özelliklerini alabilir; fakat daha fazla özellik geçerli kılındığında performası yavaşlamaktadır. Bu yüzden başlıca UTM kullanılan durumlar, personel üretkenliği ve internet güvenliğidir. Fonksiyonların hiçbiri türünün en iyisi olamazken, UTM ürünleri düşük maliyet ihtiyacını karşılar.

Yazılım Tanımlı Ağlar ve Ağ Fonksiyonu Sanallaştırma (SDN and NFV Security)

Yazılım Tanımlı Çevre (Software-Defined Perimeter)

Yazılım Tanımlı Çevre (YTÇ), güvenli bölgede yer alan, farklı şeylerden oluşan, ağ bağlantılı katılımcıların mantıksal setini tanımlar. Kaynaklar genellikle açık erişime gizlidir, güvenlik aracıları aracılığıyla erişim sınırlıdır ve saldırılabilir alanı azaltır.

Ağ Anahtarı Güvenliği (Security in the Switch)

Ağ Anahtarı Güvenliği, mevcut ağ güvenlik kontrollerini, ağ ve diğer altyapı ürünlerinin içerisine dahil eder. Bu da ağ güvenlik sınıflandırması ve iç ağ güvenlik fonksiyonlarını ayrık gereçlerden ziyade ağ yapısının parçası olarak uygulayarak, maliyet düşürülmesini sağlar. Bu teknoloji sanallaştırma, ağ fonksiyon sanallaştırması (NFV) ve uygulama tanımlı ağ kurma (SDN) sayesinde geliştmiştir.

1.2 Son Kullanıcı Güvenlik Tespiti ve Koruma

Son Kullanıcı Güvenlik Tespiti ve Koruma, mobil aygıtlar, dizüstü bilgisayarlar ve masaüstü bilgisayarlar gibi son kullanıcı aygıtları olarak tanımlanan çeşitli uç noktaları bir ağda güvence

altına alma işlemidir. Bir veri merkezinde donanım olarak bulunan sunucular da uç nokta olarak kabul edilmektedir.Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde sıralayabiliriz: Güvenli Ağ Geçidi, Kötü Amaçlı Yazılım Analizi, Korunmuş Mobil Tarayıcılar, Mobil Uygulama Sıkılaştırma vb.

Güvenli Ağ Geçitleri (Secure Web Gateways)

Güvenli Ağ Geçitleri (GAG) URL filtreleme, gelişmiş tehdit koruması (GTK), kötü amaçlı yazılım bulunması ve uygulama kontrol teknolojisinden faydalanarak; organizasyonları korur ve politika uyumluluğunu devam ettirir. GAG'ler geliştirme uygulamaları (donanım ve sanal), bulut bazlı servisler veya hibrit çözümler (bulut&geliştirme) olarak servis edilir.

Uygulama Kontrol (Application Control)

Uygulama beyaz listeleri olarak da adlandırılan uygulama kontrol çözümleri, genellikle uç noktası ve bulut işyükü koruma platformlarıyla birlikte kullanılabilen bir uç nokta koruması (masaüstü ve sunucu) türüdür.

- Basit çözümler: kodun çalışıp çalışmaması gerektiğinin kontrolünü sağlar
- Detaylı çözümler: uygulamanın çalıştığı anda ne yaptığı ve hangi sistem kaynakları ile entegre olduğunun kontrolünü sağlar

Ağ Koruması (Network Sandboxing)

Network sandbox ları, ağ trafiğini izleyerek şüpheli gördükleri nesneleri (çalıştırılabilir kodlar, Microsoft Office dosyaları, Javascript kodları vb.) sanal ortama taşıyarak izole edilmelerini sağlar. Sanal ortamdaki nesneler analiz edilir ve önem derecelerine göre puanlandırılır.

İmza Tabanlı Olmayan Zararlı Yazılım Analizi (Non-Signature Malware Analysis)

[Daha sonra tanımlanacak]

1.3 Kimlik ve Erişim Yönetimi

Kimlik ve Erişim Yönetimi, yetkili kişilerin doğru zamanda kendilerine ait kaynaklara erişebilmelerini sağlayan güvenlik disiplinidir. Uyum Gereksinimlerini karşılamak için kritik gereksinimleri ele alır. KEY yeteneklerini geliştiren şirketler, kimlik yönetimi maliyetlerini azaltabilir. Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde sıralayabiliriz: Kurumsal Anahtar Yönetimi, KEY için Blockchain, Ortak Erişim Kartları, Elektronik İmza vb.

Kurumsal Anahtar Yönetimi (Enterprise Key Management)

Kurumsal anahtar yönetimi (EKM), çoklu simetrik şifreleme veya tokenization ürünleri için tek, merkezi bir yazılım veya ağ cihazı sağlar. Kritik olarak, şifreleme ve tokenization yönetimi ile tutarlı veri erişim ilkeleri uygular. Ayrıca, anahtar dağıtımını ve güvenli anahtar depolamayı kolaylaştırır ve tutarlı anahtar yaşam döngüsü yönetimini sürdürür.

Hizmet Olarak Anahtar Yönetimi (Key Management as a Service)

Hizmet Olarak Anahtar yönetimi çözümleri, işletmelerin kendi anahtarınızı (BYOK) getirmesini sağlamak için genel bulut altyapısında bir hizmet olarak dağıtılır.Bunlar yazılım uygulamaları veya donanım güvenlik modülleri olabilir.Üçüncü şahıslar tarafından veya doğal olarak bulut hizmeti sağlayıcısı (CSP) tarafından sağlanabilirler.

Kimlik Yönetimi ve İdaresi (Identity Governance and Administration)

Kimlik Yönetimi ve İdaresi çözümleri, farklı kimlikleri toplayarak ve kontrolü sağlamak için kullanım hakları verilerine erişerek kimliği yönetir ve çoklu sistemler arasındaki hayat döngüsüne erişimi

sağlar. Bu veri yığını; rol ve davranış yönetimi, şifre yönetimi ve denetimi gibi yardımcı fonksiyonlar kadar; kimlik hayat döngüsü ve yetki verme yönetimi, erişim talebinde bulunma, iş akışı düzenlemesi, erişim doğrulaması, otomatik temin ve raporlama ve analiz gibi asıl IGA fonksiyonları için baz olarak görev görür.

Birleşik Kimlik Yönetimi (Federated Identity Management)

Birleşik kimlik yönetimi, uygulamalara tek seferlik giriş (SSO) sağlar ve kimlik bilgisinin güvenilir nüfus sahasında birkaç varlığa paylaşım olanağı verir. Araçlar ve standartlar kimlik özelliklerinin bir güvenilir tanımlayıcı ve doğrulayıcı varlıktan diğerine doğrulama, yönetim ve diğer amaçlar için iletimine onay verir.

Kimlik Erişim Yönetiminde Blockchain Kullanımı (Blockchain for IAM)

Blockchain, değer değişim işlemlerinin, bloklara sıralı olarak gruplandığı dağıtılmış bir teknolojidir. Blockchain özellikli Kİmlik Erişim Yönetimi uygulamaları, merkezileştirilmiş arbitrallere güvenmeden, güven ve esneklik sağlamak için alternatif yöntemler geliştirerek dijital varlıkları takip etmektedir.

Ortak Erişim Kartı (Common Acccess Cards)

Ortak erişim kartı, bina erişimi için olduğu kadar, PC, ağ ve uygulama oturum açma (kullanıcı kimlik doğrulaması) için de kullanılabilen tek bir kurumsal kart veya token olarak ifade edilir.

Biyometrik Doğrulama Yöntemleri (Biometric Authentication Methods)

Biyometrik kimlik doğrulama yöntemleri, uç noktaya, ağlara veya web uygulamalarına erişirken kullanıcıların kimliklerini doğrulamak için benzersiz yöntemler kullanır. Herhangi bir biyometrik kimlik doğrulama yöntemi, birebir karşılaştırma modunda (belirli bir kimlik için örtülü ya da açık bir talep olduğunda) veya birden-çokluya arama modunda kullanılabilir.

Kimlik Doğrulamada Belirteç olarak Telefon Kullanımı (Phone-as-a-Token Authentication Methods)

Telefonun kimlik doğrulama belirteci olarak kullanılmasına dayanır. Sıklıkla, aşağıdaki yollardan biriyle kullanılır.

- Bant Dışı (OOB) Kimlik Doğrulaması, kullanıcı ve kimlik doğrulama sunucuları telefon aracılığı ile kimlik bilgisini (uç nokta ve sunucu arasındaki kanalın dışında) değişir.
- Otomatik sesli aramaları, SMS yazışmaları, aşan/aşırı (OTT) mesajlaşma veya push bildirimi kullanır.
- Tek Kullanımlık Şifre (OTP) akıllı telefonlardaki uygulamalar, telefonların OTP donanım belirteçleri gibi kullanılmasını sağlar.

Mobil Tek Oturum (Mobile Single Sign-On)

Mobil tek oturum (SSO), mobil cihaz kullanıcısının kimlik doğrulamasını sadece bir kere yapmasını ve daha sonraki oturumda hedef sistemler setinde otomatik olarak kimliğinin doğrulanacağını belirtir.

Kimlik Doğrulaması için X.509 Kullanımı (X.509 Tokens for User Authentication)

Kimlik doğrulaması için X.509 akıllı belirteçler, öncelikle kullanıcı kimlik doğrulamasında kullanılan, X.509 açık anahtar altyapısı (PKI) güven belgesi taşıyan açık anahtar donanım belirteçleridir.

Akıllı kartlar, benzer türde çipleri gömen USB belirteçleri ve temassız akıllı kartlar bazı form faktörleridir.

Çok faktörlü X.509 akıllı belirteçler - PIN korumalı veya (çok nadiren) biyometrik - yüksek güven sağlar (NIST Elektronik Kimlik Doğrulama Yönetmeliği'nde Seviye 4)

Hizmet olarak Kimlik ve Erişim Yönetimi (IDaaS)

Hizmet Olarak Kimlik ve Erişim yönetimi (IDaaS) daha çok, çok kullanıcılı veya adanmış gönderim modeli olan bulut bazlı servistir. IDaaS aracılarının amacı, kullanıcı cihazlarında ve bulutta yer alan hedef sistemlere erişim sağlamak ve analiz etmektir.

Kurumsal Erişim İçin Güçlü Kimlik Doğrulaması (Strong Authentication for Enterprise Access)

Kurumsal Erişim için Güçlü Kimlik Doğrulaması, kurum güvenlik duvarının içinde ve dışındaki IT kaynaklarına erişiminde kullanılan çeşitli kimlik doğrulama faktörlerini ifade eder.

Güçlü kimlik doğrulaması, 3 kimlik doğrulaması faktöründen en az 2 sine dayalıdır - (yalnızca kullanıcının bildiği bir şey, yalnızca kullanıcının sahip olduğu bir şey ve yalnızca kullanıcıya özgü bir şey.)

Elektronik İmza (Electronic Signature)

Elektronik imza, imza atma niyetini göstermek ve çeşitli derecelerde belge bütünlüğünü ve özgünlük özelliklerini sunmak için elektronik bir belgeye uygulanabilen geniş bir imza sınıfıdır. Elektronik İmza için kabul edilen teknoloji türü uluslararası geçerliliğe sahip, hukuki gereklilikler ve belirli endüstri segmenti kullanım durumlarına bağlı olarak değişmektedir.

İmtiyazlı Erişim Yönetimi (Privileged Access Management)

İmtiyazlı Erişim Yönetimi araçları aşağıdaki özelliklerden bir veya daha fazlasını barındırabilir:

- Paylaşılan hesaplarda, firecall (acil durum erişimi) içeren hesaplarda kontrol erişimi.
- Yönetim, hizmet ve uygulama hesapları için kimlik bilgilerini otomatik olarak randomize etme ve yönetme.
- İmtiyazlı erişim için tek seferlik oturum açma sağlamak. Böylece kimlik bilgileri açığa çıkmaz.
- Yöneticinin çalıştırabileceği kontrol etmek veya filtrelemek.
- Sabit kodlu şifreleri, uygulamalarda erişilebilir yaparak, elimine etmek.
- İmtiyazlı erişimleri, komutları ve olayları denetlemek, kayda almak ve görüntülemek.

Harici Yetkilendirme Yönetimi (Externalized Authorization Management)

Harici yetkilendirme yönetimi (HYY), uygulamaların, sistemlerin ve verilerin bileşenlerine erişimi belirlemek için kullanılan bir çalışma zamanı yetkilendirme politikası yönetimi, karar verme ve uygulama teknolojisidir.

Mobil-Apt Kullanıcı Kimlik Doğrulama Yöntemleri (Mobile-Apt User Authentication Methods)

Mobil kullanıcı elverişlilik kimlik doğrulama yöntemleri, bir mobil aygıttan ana sistemden uç birime veri akışı sağlayan bir uygulamaya veya hizmete erişimi destekleyen yöntemlerdir ve kuruluşların, bu kullanım örneklerinde güven ve kullanıcı deneyimini dengelemek için ihtiyaçlarını en iyi şekilde karşılayabilir.

Etki Alanları Arası Kimlik Yönetimi (SCIM)

Etki Alanları Arası Kimlik Yönetimi özellikleri, web üzerinde kimlik verilerini hazırlama ve yönetme için bir uygulama düzeyi, REST / JavaScript Nesne Tabelası (JSON) protokolü ve şeması sağlar. Başlangıçta Basit Bulut Kimliği Yönetimi olarak adlandırılan protokol, kullanıcılar, nesneler ve

gruplar ile özel kaynak uzantıları gibi temel kimlik kaynaklarının oluşturulması, değiştirilmesi, alınması ve keşfedilmesini desteklemektedir.

1.4 Mesajlaşma ve İletişim Güvenliği

Mesaj güvenliği cihazınızdaki mesajların şifrelenmesi ve böylece yalnızca alıcı tarafından okunabilmesi için uygulanır. İletişim güvenliği, yetkili olmayan önlemcilerin, telekomünikasyona anlaşılır bir biçimde erişmelerini önleme disiplinidir.

Mobil Ses Koruması (Mobile Voice Protection)

Mobil ses koruması teknolojileri, mobil ve kablosuz ağlarda iletilen, mobil araçlarda başlayan ve sonlanan sesli haberleşmelerin gizliliğini ve bütünlüğünü sağlar. Mobil ses koruması içeren araçlar genellikle mobil cihazlarda bulunan bağımsız uygulama şeklinde gelmektedir.

Güvenli Mesajlaşma (Secure Texting)

Güvenli mesajlaşma teknolojileri, mobil cihazlardan gönderilen veya alınan ve kablosuz veya mobil şebekelerde iletilen anında mesajlaşma ve SMS'in gizliliğini ve bütünlüğünü sağlar. Mobil metin koruması sağlayan araçlar genellikle bir taşınabilir aygıtta bulunan bağımsız bir uygulama biçimindedir.

Mobil Sanal Özel Ağlar (Mobile Virtual Private Networks)

Mobil sanal özel ağlar (VPN'ler) istemci ağ geçitleri ve araç setlerinden oluşur ve son derece güvenilmez uzak bağlantılarda ve akıllı telefonlar ve tabletler içeren mobil kullanım durumlarıyla çalışacak şekilde optimize edilmiştir. Mobil VPN'ler, SSL ve IPsec'in halefi olan Aktarım Katmanı Güvenliği (TLS) çevresinde oluşturulabilir. İstemcide, tarayıcı aracılığıyla çağrılan veya platform API'ları aracılığıyla çağrılan uygulamaları ve kapsayıcıları içine gömülebilirler.

1.5 Veri Güvenliği

Veri güvenliği, bilgisayarlara, veritabanlarına ve web sitelerine yetkisiz erişimi önlemek için uygulanan koruyucu dijital gizlilik önlemlerini ifade eder. Veri güvenliği ayrıca verileri bozulmalardan korur. Veri Güvenliği, Veri Tabanı Güvenliği, Verileri Ortadan Kaldırma, Veri Kaçakçılığını Önleme gibi alt alanlara ayrılabilir. Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde sıralayabiliriz: Statik/Dinamik Veri Maskeleme, Veri Dağılım Algoritmaları, Veri Temizleme, Veritabanı Şifreleme vb.

Veri Güvenliği (Data Security)

Statik Veri Maskeleme (Static Data Masking)

Veri maskeleme, yazılım testleri ve kullanıcı eğitimleri gibi amaçlar için kullanılabilen, bir kuruluşun verisinin yapısal olarak benzer ancak özgün olmayan versiyonunun oluşturulması için bir yöntemdir. Amaç, gerçek veriler gerekli olmadığı zaman, benzer verilerle işlem yaparak gerçek verileri korumaktır. Statik Veri Maskeleme, durağan verilerin korunmasını sağlar.

Dinamik Veri Maskeleme (Dynamic Data Masking)

Veri maskeleme, yazılım testleri ve kullanıcı eğitimleri gibi amaçlar için kullanılabilen, bir kuruluşun verisinin yapısal olarak benzer ancak özgün olmayan versiyonunun oluşturulması için bir yöntemdir. Amaç, gerçek veriler gerekli olmadığı zaman, benzer verilerle işlem yaparak gerçek verileri korumaktır.

Dinamik veri maskeleme (DVM), üretilen verinin gerçek zamanlı maskelenmesini amaçlayan bir teknolojidir. DVM, istemcinin hassas verilere erişememesi için veri akışını değiştirir; orijinal üretim verilerinde herhangi bir değişiklik yapılmaz.

Biçim Koruma Şifreleme (Format Preserving Encryption)

Biçim koruma şifrelemesi (FPE) araçları, durağan verileri, ilişkisel veritabanı yönetim sistemleri (RDBMS'ler), veri ambarları, büyük veriler ve Hadoop, Cassandra ve MongoDB gibi NoSQL veritabanlarında kullanılan alanlardaki verileri korumak için kullanılır

Bilgi Dağıtma Algoriatmaları (Information Dispersal Algorithms)

Bilgi dağıtma algoritmaları, bilgiyi parçalı olarak (yani dağınık) birden çok yerde depolamak için bir metodoloji sağlar, böylece lokal kesinti durumunda bilgi korunur ve tek bir yerde yetkisiz veri erişiminin olması erişimi yapana kişiye kullanışlı bilgi sağlamaz.

Belirtkeleme (Tokenization)

Belirtkeleme, bir ödeme kartı numarası gibi bir hassas verinin bir parçasının, belirteç olarak bilinen yedek değeri değiştirdiği bir işlemi ifade eder. "Vaultless" simgeleşme kullanılmadığı sürece, hassas verilerin merkezi bir konumda güvenli bir şekilde depolanması ve korunması gerekir.

Birlikte Çalışabilir Depolama Şİfreleme (Interoperable Storage Encryption)

Endüstri standartlarına dayanan ve sürücü denetleyicilerine yerleştirilen birlikte çalışabilir depolama şifrelemesi, güvenli yığın depolama sürücülerinin performansını önemli ölçüde artırabilir. Standart şifreli sürücüler (SED'ler) için vitrin teknolojisi Opal Güvenlik Alt Sınıf Sistemi (SSC) 'dir.

Güvenilir Taşınabilir Depolama Güvenliği (Trusted Portable Storage Security)

Güvenilir taşınabilir depolama güvenlik aygıtları, genelde USB konektörlü bir flash bellek cihazında sunulan sağlam güvenlik politikalarını uygulamak üzere tasarlanmış yerleşik erişim denetimleri ve şifrelemeye sahip, bağımsız bir ortam sistemidir.

Veri Güvenliği İçin Blockchain (Blockchain for Data Security)

Blockchain, değer değişim işlemlerinin, bloklara sıralı olarak gruplandığı dağıtılmış bir teknolojidir. Blockchain özellikli veri güvenliği uygulamaları, merkezileştirilmiş arbitrallere güvenmeden, güven ve esneklik sağlamak için alternatif yöntemler sunar ve dijital varlıkları takip eder.

Gizlilik Yönetim Araçları (Privacy Management Tools)

Gizlilik yönetim araçları, kuruluşların gizlilik etkisi değerlendirmelerini yürütmesine ve gizlilik düzenlemelerinin gereklerine karşı işleme faaliyetlerini kontrol etmesine yardımcı olur. Kişisel bilgilerin veri akışlarını analiz ve dokumante etmekte, gizlilik politikalarının dağıtımını desteklemekte ve kullanıcı farkındalığını izlemektedir.

Veri İmha (Data Disposal)

Veri Temizleme (Data Sanitization)

Veri temizleme, tüm verileri bir okuma / yazma ortamından güvenilir bir şekilde ve tamamen çıkararak, artık okunamayan veya kurtarılamaz hale getirmek için sürekli uygulanan bir işlemdir.

Mobil Cihazlar İçin Veri Elden Çıkarma Araçları (Data Disposal Tools for Mobile Devices)

Mobil cihazlar için veri elden çıkarma araçları, mobil aygıtların güvenli bir şekilde hizmet dışı kalmasını sağlayan ve veri silinmesini sağlayan silme teknolojilerini kullanır

Veritabanı Güvenliği (Database Security)

Veritabanı Denetim ve Koruma (Database Audit and Protection)

Veritabanı denetim ve koruma (DAP) araçları, ilişkisel veritabanı yönetim sistemleri (RDBMS'ler) için veri güvenliği ilkeleri, kullanıcı etkinliği izleme ve veri korumasının merkezi yönetimini sağlar.

Veritabanı Şifreleme (Database Encryption)

Veritabanı şifreleme araçları ilişkisel veritabanı yönetim sistemlerini (RDBMS) korumak için kullanılır. Şifreleme, saldırı veya içeriden istismar riskini en aza indirmeye yardımcı olmak ve yöneticilerin ve yetkisiz kullanıcıların erişimini engelleyerek uyumluluk sorunlarını ortadan kaldırmayı sağlar. Operasyonel olarak şifreleme, durağan bir tabloyu veya veritabanı örneğini koruyabilir.

Veri Kaçağı Önleme / İç Tehdit Savunma (DLP / Inside Threat Protection)

Veri Kaybını Önleme (Data Loss Preventation)

Veri kaybını önleme bir işlemin yapıldığı andaki içeriğe ve bağlama dayalı bir politikanın dinamik uygulamasıdır. DLP, yanlışlıkla veya kazara veri kaybı riskini ve izleme, filtreleme, engelleme ve iyileştirme özelliklerini kullanarak hassas verilere maruz kalma riskini ele alır.

E-posta için İçerik Tanıyan Veri Kaybını Önleme (Content-Aware DLP for Email)

E-posta için içerik tanıyan veri kaybını önleme (VKÖ), tüm kurumda değil sadece bir e-posta sisteminde kullanılmak üzere VKÖ politikaları oluşturma amacıyla kullanıldığı için entegre bir VKÖ dağıtımı olarak düşünülür.

İçerik Tanıyan Mobil Veri Kaybını Önleme (Content-Aware Mobile DLP)

İçerik tanıyan mobil veri kaybını önleme, yasal uyumluluk, fikri mülkiyet gibi hassas verileri koruyan mevcut DLP ürünlerinin mobil için genişletilmiş halidir.hassas içerikler mobil cihaza kaydedilir, mobil cihaz tarafından buluta yüklenir veya web mail vb. uygulamalar ile gönderilir.

1.6 Bulut Güvenliği

Bulut güvenliği, çevrimiçi depolanan verilerin hırsızlığa, kaçağa ve silinmesine karşı korunmasıdır. Bulut güvenlik sağlama yöntemleri, güvenlik duvarları, penetrasyon testleri, şaşırtma, sanal özel ağların (VPN) kullanımı ve genel İnternet bağlantılarını kullanmaktan kaçınmayı içerir. Bulut güvenliği hem fiziksel hem de mantıksal güvenliği ele alır ve farklı hizmet modellerinin nasıl yerine getirildiğini (genel-özel-hybrid) belirtir. Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde sıralayabiliriz: Bulut Erişim Güvenlik Aracısı, Yüksek Güvenceli Arakatmanlar, Saas Güvenlik Yönetimi , IaaS Container Şifreleme vb.

Bulut Erişim Güvenlik Aracıları (Cloud Access Security Brokers)

Bulut erişim güvenlik aracıları, kurum güvenlik denetimlerine müdahale etmek ve ilkeleri uygulamak için bulut hizmeti tüketicileri ile bulut hizmeti sağlayıcıları arasında aracılık yapan kurum içi veya bulut tabanlı güvenlik ilkesi uygulama noktalarıdır. Bulut Erişim Güvenlik Aracı platformları, bulut hizmeti bulma, bulut sağlayıcı risk derecelendirmeleri, tek oturum açma, yetkilendirme, aygıt profillemesi, şifreleme, tokenization, hassas veri izleme, kullanıcı davranışı izleme gibi birden çok güvenlik ilkesini birleştirir.

Yüksek Güvenilirlikli Hypervisor (High-Assurance Hypervisors)

Yüksek güvenilirlikli bir hypervisor, müdahale edilmemiş veya ele geçirilmemiş yüksek bir güven seviyesi oluşturulmasını sağlayan hypervisor dur. Yüksek güvence sağlandıktan sonra kritik öneme sahip iş yükleri ve hassas veriler güvence altına alınır.

Bulut Veri Koruma Ağ Geçitleri (Cloud Data Protection Gateways)

Bulut veri koruma ağ geçitleri, proxy vasıtasıyla bulut SaaS sağlayıcısına akarken yapılandırılmış ve yapılandırılmamış verilere şifreleme, maskeleme veya tokenization uygulayarak bir vekil kurabilir. Bulut veri koruma ağ geçidi işlevi, birkaç bulut erişim güvenlik aracısı çözümüne eklenmektedir. Uygulama kullanıcıları, diğer bulut kiracıları, SaaS yöneticileri ve bilgisayar korsanlarının bulut hizmetine yetkisiz erişimi önler ve SaaS kullanırken veri ikameti gereksinimlerini karşılamaya yardımcı olur.

SaaS Platform Güvenlik Yönetimi (SaaS Platform Security Management)

SaaS platform güvenlik yönetimi araçları, bir veya daha fazla SaaS hizmeti içinde veri erişimi ve kullanıcı etkinliği üzerinde kontrol sağlayan bir yönetişim gösterge tablosunu uygulamak için SaaS sağlayıcılarının API'lerini kullanır.

Bu tür mekanizmalar tipik olarak bulut erişim güvenlik aracısı ürünlerinin bir bileşeni olarak sağlanır ancak birkaç niş SPSM satıcısı, bir veya az sayıdaki SaaS uygulamasını hedef alan ürünler sunmaya devam etmektedir.

Hizmet Olarak Altyapı Konteyner Şifrelemesi (IaaS Container Encryption)

Hizmet olarak altyapı konteyner şifrelemesi, IaaS sağlayıcılarının barındırdığı iş yüklerinde, uygulama tarafında olmayan bir şekilde IaaS sağlayıcı altyapısında bulunan iş yükü tarafından depolanan verileri şifrelemek için kullanılan şifreleme teknolojisinin kullanılmasıdır.

Kurumlar, şifre çözme anahtarlarına erişimi kontrol ederek, IaaS iş yükleri tarafından kullanılan ve oluşturulan verileri, komşu kiracılardan, bulut hizmeti sağlayıcısı yöneticilerinden ve IaaS sağlayıcının olası bilgisayar korsanlarından koruyabilirler.

1.7 Güvenlik Analizleri ve İstihbarat

Güvenlik Analizi, büyük risk teşkil eden olayları anlamak için güvenlik olaylarını toplamak ve analiiz etmek amaçlı bilgi teknolojisi kullanımıdır. Çoğunlukla büyük miktarda veri toplayarak çalışır ve önleyici tedbirlerin zamanında alınabilmesi için tehdit kalıpları yaratmada kullanır. Düzgün bir analiz, tehditin kök nedenleri hakkında derinlemesine bilgi sağlar. Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde sıralayabiliriz: Kullanıcı ve Davranış Analizi, Ağ Trafik Analizi, Sahtecilik Tespiti vb.

Kullanıcı ve Varlık Davranış Analizi (User and Entity Behavior Analytics)

Kullanıcı ve varlık davranış analizi olarak bilinen UEBA aslında kullanıcı ve kimliklerin kullanım modellerini profil analizi ile öğrenip daha sonra anormal davranışların sergilenmesinde durumunda bunların raporlanmasını sağlar. Örnek vermek gerekir ise, bir banka kartı ile sürekli Türkiye'de alış veriş yapılıyor iken, aynı kart Amerika kökenli amazon.com sitesinde kullanılırsa banka bunun normal bir davranış olmadığını tespit eder ve hemen kart sahibini arayarak bu alış verişin kart sahibinin bilgisi dahilinde olup olmadığını doğrular.

Ağ Trafik Analizi (Network Traffic Analysis)

Ağ trafiği analizi teknolojisi, kurumsal ağdaki şüpheli etkinlikleri tespit etmek için istatistiksel analiz, makine öğrenmesi, meta veri ve içerik denetimi yöntemlerini kullanır. Genellikle ihlal olayları sonrası yapılır. Birçok NTA satıcısı, tüm ağın izlenmesi yerine LAN segmenti izleme konusunda uzmanlaşmaktadır.

Tehdit İstihbarat Platformları (Threat Intelligence Platforms)

Tehdit İstihbarat Platformları (TIP), savunma eylemlerinin önceliklendirilmesini desteklemek ve saldırı önleme, tespit ve yanıt vermeye yardımcı olmak için gerçek zamanlı olarak güvenlik tehdidi verilerini toplamak, ilişkilendirmek, kategorilere ayırmak, paylaşmak ve bütünleştirmek için kullanılır. Ayrıca bu platformlar SIEM, EDR, IPS ve güvenlik duvarı gibi mevcut güvenlik teknolojileri ve süreçleri ile entegre olabilirler.

Dolandırıcılık Tespiti ve İşlem Güvenliği (Fraud Detection and Transaction Security)

Fraud Detection (Dolandırıcılık Tespiti), müşterilerin ve kurumun bilgilerini, varlıklarını, hesaplarını ve (hesap) işlemlerini gerçek zamanlı, gerçeğe yakın zamanlı veya kullanıcı aktivitelerini toplu analiz etme yöntemiyle tespitini sağlar. Kullanıcı aktivitesi şüpheli olmadığı sürece müdahale edilemez.

Aldatma Teknolojisi (Deception Technology)

Aldatma teknolojisi, ağa sızmış olan bir saldırganın ağa zarar vermesini önlemek için tasarlanmış güvenlik araçları ve teknikleri kategorisidir.Bu teknoloji saldırganın yönünü şaşırtmak için tuzak kullanmakta, saldırganın hedefine ulaşmasını geciktirmekte veya önlemektedir.

1.8 Güvenlik Operasyonları, Olay Yönetimi ve Adli Bilişim

Bir güvenlik operasyon merkezi (SOC), örgütsel ve teknik düzeyde güvenlik konularını ele alan merkezi bir birimdir. Bir bina veya tesis içindeki bir SOC, personelin veri işleme teknolojisini kullanarak siteyi denetlediği merkezi bir konumdur. Olay yönetimi (ICM), bir organizasyonun gelecekte yeniden oluşumunu önlemek için tehlikeleri tanımlama, analiz etme ve düzeltme faaliyetlerini tanımlayan bir terimdir. Yapısal bir organizasyon içindeki bu olaylar normalde olayla mücadele ekibi (IRT) veya bir olay yönetimi ekibi (IMT) tarafından ele alınır. Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde sıralayabiliriz: SIEM (Bilgi Güvenliği Olay Yönetimi) ,Kriz Yönetim Platformları vb.

Bilgi Güvenliği ve Olay Yönetimi (SIEM)

Bilgi Güvenliği ve Olay Yönetimi, olay yönetimi güvenlik olaylarının anında tespit edilerek güvenlik ihlâllerine zamanında cevaplar verilmesini sağlar. Daha önce denenen ve başarılı olan güvenlik kırılmaları, güvenlik yöneticisinin güvenlik faaliyetlerinin beklenen biçimde çalışıp çalışmadığının belirlenebilmesi, güvenlik önlemlerinin alınarak güvenlik ihlallerinin önlenmesi, bir güvenlik kırılmasını önlemek için alınan önlemlerin etkili olup olmadığına karar verilir.

Kriz/Olay Yönetimi Platformları (Crisis/Incident Management Platforms)

Kriz/Olay yönetimi platformları, iş kesintileri, hizmette aksama gibi olaylara karşı müdahale ve iyileştirme gibi tedbirleri yönetmek için kullanılır. Kriz halinde iletişim, kurtarma planı veri havuzu, iş gücü planlama, devlet kurumu raporlaması gibi fonksiyonaliteleri içerir.

Adli Bilişim

Adli Bilişim, kanun önünde sunmak amacıyla, belirli bir bilgi işlem cihazından elde edilen kanıtları toplamak ve muhafaza etmek için soruşturma ve analiz tekniklerinin uygulanmasıdır. Adli Bilişimin amacı, bir bilgi işlem aygıtında tam olarak neler olduğunu ve kimin sorumlu olduğunu bulmak için gerekli kanıtları toplamak ve bunları belgelendirmektir.

1.9 Güvenlik Risk ve Uyum Yönetimi

Uyum riski, bir kurumun, kanun ve yönetmeliklere, iç politika veya öngörülen en iyi uygulamaları uyarınca hareket etmemesi durumunda karşı karşıya kaldıkları yasal cezalar, istihkak kaybı ve maddi kayıplara maruz kalmasıdır. Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde

sıralayabiliriz: Konfigürasyon Denetimi, Yazılım Bileşim Analizi, BT Risk Yönetimi, Sosyal Risk Yönetimi vb.

Yapılandırma Denetleme (Configuration Auditing)

Yapılandırma denetleme araçları, sunucular, uygulamalar, veritabanları ve ağ aygıtları arasında, iç ve genel bulut altyapısında değişiklik algılama ve yapılandırma değerlendirmesi sağlar. Şirkete özgü ilkeler veya endüstri tarafından tanınan güvenlik yapılandırma değerlendirme şablonları (örneğin, NIST), sistemin denetim, sıkılaştırma veya kullanılabilirlik açısından doğruluğunu korur. Bazıları iyileştirme için yapılandırma yönetimi araçları ile çalışırken bazıları istenilen bir duruma dönüştürülebilir.

Yazılım Bileşimi Analizi (Software Composition Analysis)

Yazılım bileşimi analizi aşağıdaki görevleri gerçekleştirir:

- Güvenlik ve / veya işlevsellik açığı olan veya uygun lisanslamayı gerektiren bileşenleri algılamak için uygulama bileşimini analiz eder.
- Kurumsal yazılım tedarik zincirinin yalnızca güvenli bileşenleri içerdiğinden ve bu nedenle güvenli uygulama geliştirme ve kurma işlemini desteklediğinden emin olmaya yardımcı olur.

Risk Yönetimi Risk Management)

BT Risk Yönetimi Çözümleri (IT Risk Management Solutions)

BT risk yönetimi çözümleri, BT riskinin ve güvenlik ekiplerinin riske dayalı karar vermeyi desteklemek için kullandığı işlevleri ve iş akışlarını desteklemektedir. Bu çözümlerin beş kritik özelliği şunlardır:

- Politika Yönetimi
- Kontrol Eşleme ve Raporlama
- Güvenlik İşlemleri Analizi ve Raporlaması
- BT Risk Değerlendirmesi
- Olay Yönetimi

Dijital Risk Yönetimi (Digital Risk Management)

Dijital risk yönetimi (DRY), bulut, mobil, sosyal, büyük veriler, üçüncü parti teknoloji sağlayıcıları, operasyonel teknoloji (OT) ve Nesnelerin İnterneti (IoT) gibi dijital iş bileşenleri ile ilişkili risklerin yönetimini kolaylaştırır

BT Tedarikçi Risk Yönetimi (IT Vendor Risk Management)

BT tedarikçi risk yönetimi, BT sağlayıcılarının ve servis sağlayıcıların kullanılmasının iş kesintisi veya iş performansı üzerinde olumsuz bir etki için kabul edilemez bir potansiyel yaratmamasını sağlayan bir yöntemdir. BT tedarikçi risk yönetimi teknolojisi, satıcılarla ilgili riske maruziyeti değerlendiren, izleyen ve yöneten kuruluşları destekler.

Operasyonel Risk Yönetimi (Operational Risk Management)

Operasyonel risk yönetimi çözümleri daha kapsamlı bir kurumsal risk yönetimi (ERM) programı kapsamında desteklemektedir. Operasyonel riskler, Gartner tarafından "günlük taktik ticari faaliyetlerin belirsizliğinin yanı sıra yetersiz veya başarısız iç süreçler, insanlar veya sistemler veya dış olaylardan kaynaklanan risk olaylarıyla ilgili" riskler olarak tanımlanır.

Endüstriyel Operasyonel Risk Yönetimi (Industrial Operational Risk Management)

Endüstriyel operasyonel risk yönetimi uygulamaları, yetersiz veya başarısız iç süreçler ve sistemler, insan faktörleri veya dış olaylardan kaynaklanan zarar riski dahil olmak üzere operasyonel riskin belirlenmesi, değerlendirilmesi, hafifletilmesi, izlenmesi ve kontrol edilmesi süreçlerini desteklemek üzere tasarlanmıştır.

Yönetilen Entegre Risk Yönetimi Çözümü (Managed Integrated Risk Management) Solution

Yönetilen entegre risk yönetimi çözümü , bir kuruluştaki risk bileşenlerini bütünleştirir ve yönetir. Bu, sağlayıcının tek bir harici sistem ve süreç grubu aracılığıyla alıcının kurumsal boyuttaki teknolojisi ve iş süreçleri (uygulamalar, mimari, güvenceler ve risk kontrolleri) hakkında bilgi toplamak ve daha sonra yönetilen YERY hizmetlerini müşterilere sunmak için yönetilen hizmetleri kullanmayı içerir.

Sosyal Medya Risk Yönetimi (Social Risk Management)

Sosyal medya riski yönetimi (SMRY) uygulamaları, sosyal medyanın iş süreçlerine dahil edilmesiyle ilgili belirsizliğin etkilerini, düzenlemelere ve politikalara uyumu, sosyal medyanın ve diğer dinamik içeriğin düzenleyici uyumluluk, yasal gereksinimler ve iş hedeflerine yönelik riskler açısından analizi için gerekli süreçleri sağlamaktadır.

1.10 Uygulama ve İnternet Güvenliği

Uygulama güvenliği, güvenlik açıklarını tespit ederek ve önleyerek bir uygulamanın güvenliğini artırmak için alınan önlemleri kapsar. Web uygulaması güvenliği, özellikle web sitelerinin, web uygulamalarının ve web servislerinin güvenliğini sağlayan Bilgi Güvenliği'nin bir dalıdır. Web uygulaması güvenliği, yüksek düzeyde, uygulama güvenliği ilkelerini benimser, ancak bunları özellikle İnternet ve Web sistemlerine uygular.

Web Uygulama Güvenlik Duvarı ve Uygulama Güvenliği (WAF and Application Security)

RASP (Runtime Application Self-Protection)

Çalışma zamanı uygulama özkaynağı koruması (RASP), bir uygulama çalışma zamanı ortamında yerleşik olan veya daha sonra eklenen bir güvenlik teknolojisidir. Uygulama davranışlarını izleyebilir, uygulama yürütmeyi denetleyebilir, ayrıca gerçek zamanlı saldırıları tespit edebilir ve önleyebilir.

Uygulama Koruması (Application Shielding)

Uygulama koruması, uygulama düzeyindeki saldırıların etkin bir şekilde önlenmesi ve tespit edilmesi için doğrudan güvenlik işlevselliği eklemek için kullanılan bir dizi teknolojiyi belirtir. Özellikle mobil uygulamaları korumak için tercih edilmektedir.

Web Uygulama Güvenlik Duvarı (Web Application Firewalls)

Bir web uygulama güvenlik duvarı (WAF), web uygulamaları ve web API'lerini korumak için web sunucularının önünde konumlandırılmış bir tespit ve önleme teknolojisidir. Birçok WGD, daha doğru koruma için olumsuz ("imzalar") ve pozitif ("beyaz liste") güvenlik modellerinin bir kombinasyonunu içerir.

Aracı API (Mediated APIs)

Aracı API, bir API'nin sanallaştırılmış, yönetilen, korunan ve bir ara katmanı tarafından zenginleştirilmiş bir tasarım modelidir. Bu katman, artan çeviklik, kullanılabilirlik, performans, güvenlik ve kontrol için ilkeyi uygulayabilir ve API etkileşimine yetenekler katabilir. Aracı API, bir

hizmetin, alan modelini doğrudan yansıtan "iç API" yi ve belirli istemci gereksinimlerini desteklemek üzere uyarlanmış bir veya daha fazla "dış API" yi ortaya koymasını sağlar.

Hizmet Olarak Uygulama Güvenliği (Application Security as a Service)

Test hizmetlerinin, genellikle internet üzerinden aboneliğe dayalı fiyatlandırma modeliyle uzaktan çalışan üçüncü parti profesyonel güvenlik sağlayıcılarına devredildiği bir teslimat modelidir.

Uygulama Gizleme (Application Obfuscation)

Uygulama gizleme, uygulamayı ve içinde bulunan fikri mülkiyeti sızma, ters mühendislik ve hack işlemlerinden koruma amaçlı teknolojileri içermektedir.

Gömülü Yazılım ve Sistem Güvenliği (Embedded Software and Systems Security)

Gömülü yazılım ve sistemler güvenliği, donanım ve gömülü yazılımı tehlikeye atılmış saldırılardan korumak ve bu sistemlerin işlediği verilerin bütünlüğünü ve gizliliğini sağlamak için mühendisler ve geliştiriciler için tasarlanmış teknoloji ve uygulamaları sunar. Bu sistemler hem fiziksel hem de dijital saldırılara maruz kalabilirler.

Zafiyet Denetimi (Vulnerability Assesment)

Açıklık Değerlendirme (Vulnerability Assessment)

Güvenlik açığı değerlendirmesi ürünleri ve hizmetleri kurumsal BT ortamlarını değerlendirir

ve aşağıdaki özellikleri gerçekleştirir:

- Aygıt, işletim sistemi ve yazılım güvenlik açıklarının keşfedilmesi ve tanımlanması
- Güvenlik açığı koşullarının temelini oluşturmak ve eğilim oluşturmak
- BT varlıklarının güvenlik konfigürasyonunu belirleme ve raporlama
- Ağa bağlı BT ve OT varlıklarının keşfedilmesi ve raporlanması
- Özel uygunluk raporlaması ve kontrol çerçevelerini destekleme
- Risk değerlendirme
- BT operasyon grupları tarafından iyileştirmenin desteklenmesi

Uygulama Güvenlik Açığı Korelasyon (Application Vulnerability Correlation)

Uygulama Güvenlik Açığı Korelasyon araçları, Statik ve Dinamik test araçlarından gelen iyileştirmelerin analizi ve önceliklendirilmesi sonrası merkezi bir uygulamaya girdi sağlanmasını sağlar.

Penetrasyon Testi (Network Penetration Testing Tools)

Penetrasyon testi, güvenlik açıklarını bulmak ve onları, aygıt rollerini, güven ilişkilerini, erişilebilir ağ hizmetlerini ve olası güvenlik açıklarını eşleştirmek ve onları hedef sistemlere erişmek için kullanmak için çok aşamalı saldırı senaryolarını kullanır. Penetrasyon test araçları, yüksek riskli güvenlik açıklarının önceliklendirilmesi ve mevcut savunmaların savunmasızlığını göstermek için yol gösterici bir etkiye sahiptir.

Kİtle Kaynak Güvenlik Test Platofmrları (Crowdsourced Security Testing Platforms)

Kitlekaynak güvenlik test platformları, güvenlik açıklarını belirlemek için geniş güvenlik testi uygulayıcılarından yararlanarak penetrasyon testi ve / veya uygulama güvenlik testinin kitlelere yönlendirilmesine olanak tanıyan bir SaaS platformu sağlar. CSSTP'ler sıklıkla, platformlarının bir parçası olarak ödül programı yönetim hizmetleri sunar.

İnteraktif Uygulama Güvenlik Testi (Interactive Application Security Testing)

İnteraktif uygulama güvenlik testi, uygulama güvenliği testinin doğruluğunu arttırmak için dinamik uygulama güvenlik testi ve statik analiz güvenlik test tekniklerini birleştiren teknolojidir.

Mobil Uygulama Güvenliği Testi (Mobile Application Security Testing)

Mobil uygulama güvenliği testi (MAST), güvenlik açıklarını tanımlamak için kodlama, tasarım, paketleme, dağıtım ve çalışma zamanı koşulları için mobil uygulamaları analiz eder. Mobil Uygulama Onaylama Çözümü (MARS) olarak kullanıldığında, MAST, bir kuruluşun güvenlik ilkeleriyle çakışan uygulama işlevlerine de işaret edebilir.

Statik Uygulama Güvenliği Testi (Static Application Security Testing)

Statik Uygulama Güvenlik Testi, uygulama kaynak kodu, bayt kodu ve binary dosyaları analiz etmek üzere tasarlanmış bir dizi teknolojidir.

Dinamik Uygulama Güvenliği Testi (Dynamic Application Security Testing)

Dinamik uygulama güvenliği testi (DUGT) teknolojileri, bir uygulamadaki güvenlik açığına işaret eden koşulları çalışma durumunda algılamak için tasarlanmıştır. Bazı dinamik test çözümleri özellikle web dışı protokol ve veri hataları için tasarlanmıştır

Software Development Life Cycle Security

Yazılım Geliştirme Yaşam Döngüsü (SDLC), ilk fizibilite çalışmasından tamamlanan başvurunun sürdürülmesine kadar bir bilgi sistemi geliştirme projesinde yer alan aşamaları tanımlayan, proje yönetiminde kullanılan kavramsal bir modeldir.

DevSecOps (DevSecOps)

DevSecOps, geliştiricileri, operasyon ekibini ve işletme ekiplerini birlikte çalışmaya teşvik eden yazılım geliştirmeye yönelik bir yaklaşımdır; böylece, kuruluş yazılımları daha hızlı geliştirir, kullanıcı talebine daha duyarlı olur ve sonuç olarak gelirini en üst düzeye çıkarabilir.

1.11 Mobil ve Taşınabilir Cihaz Yönetimi Güvenliği

Mobil güvenlik, akıllı telefonların, tabletlerin, dizüstü bilgisayarların ve diğer taşınabilir bilgi işlem cihazlarının ve bunlarun bağlandığı ağların, tehdit ve zayıf noktalardan korunmasıdır. Cihazın kaybedilmesi, cihazdan dışarıya izinsiz veri transferi, zararlı yazılım atakları gibi konular mobil güvenlik kapsamında değerlendirilir.

Kurumsal Mobilite Yönetim Sistemleri (Enterprise Mobility Management Suites)

Kurumsal Mobilite Yönetim Sistemleri, mobil aygıtların işletmelerin sistemlerine güvenli bir şekilde entegre edilmesini sağlar. Bu sistemler aygıtları kuruluşların politikalarına uymak, uygulamaları güvenli hale getirmek ve dağıtmak, kuruluş verilerini korumak ve isteğe bağlı olarak bağlamsal güven sağlamak için yapılandırır.

Kurumsal Mobil Yönetimi Güvenliği (EMM Security)

Kurumsal mobil yönetimi (EMM) ürünleri ve hizmetleri, mobil cihazları kurumsal BT uç nokta sistemi yaşam döngüsüne entegre eder. EMM araçları mobil politikaların merkezi olarak uygulanmasını sağlar. Örnek olarak, jailbreak algılama ve uzaktan silme gibi cihaz politikalarının yanı sıra veri erişimi, uygulama yönetimi ve mobil kimlik için daha geniş politikalar verilebilir.

Kendi Cihazınızı Getirin (BYOD)

Kendi cihazınızı getirin (BYOD), çalışanların, iş ortaklarının ve diğer kullanıcıların, kurumsal uygulamaların yürütülmesi ve verilere erişmek için kişisel olarak seçilmiş ve satın alınmış bir

istemci cihazı kullanmalarını sağlayan son nokta dağıtım stratejisidir. Genellikle akıllı telefonları ve tabletleri kapsar, ancak strateji PC'ler için de kullanılabilir. Çalışanın cihazına, yerel vergi düzenlemelerine, işgücü gereksinimlerine ve şirket politikasına bağlı olarak, bir sübvansiyon içerebilir.

Mobil Cihazlar İçin Kullanıcı Kimlik Doğrulaması (User Authentication to Mobile Devices)

Mobil cihazlar için kullanıcı kimlik doğrulaması, cihazın kendisine erişen kullanıcının kimliğini doğrulayan çeşitli yöntemleri kapsar. Kısa sayısal PIN'ler ve alfa sayısal şifreler sıradanlaşmakta; grafik desenler ve biyometrik yöntemler daha yaygın hale gelmektedir

Mobil Tehdit Savunma (Mobile Threat Defense)

Mobil tehdit savunma araçları (MTS), işletmeleri mobil platformlardaki tehditlerden korur. MTDS çözümleri, aygıt (davranışsal anomali algılama ve güvenlik açığı değerlendirmeleri aracılığıyla), uygulama (kod analizi yoluyla) ve ağ (ağ trafiğini izleyerek ve şüpheli ağları otomatik olarak mobil aygıtlardan devre dışı bırakarak) üç düzeyde güvenlik sağlar.

Mobil Uygulama Sıkılaştırma (Mobile Application Hardening)

Mobil Uygulama Sıkılaştırma teknolojileri, mobil uygulamaları tersine mühendislik ve yeniden paketleme saldırılarına karşı korur.

Yeniden Paketleme: Android cihazlarda çok yaygın bir saldırı türüdür. Böyle bir saldırıda, saldırganlar uygulama pazarlarından indirilen popüler bir uygulamayı değiştirir, uygulama kodlarına ters mühendislik yaparlar, bazı kötü amaçlı yazılım (payload) ekler ve sonra değiştirilen uygulamayı uygulama pazarlarına yüklerler.

Korumalı Mobil Tarayıcılar (Protected Mobile Browsers)

Korumalı mobil tarayıcılar, tüketici ve kurumsal portallar gibi web tabanlı kaynaklara erişmek için veri güvenliği ve katman koruma katmanları ekleyerek veri kaybını önlemeye ve varsayılan tarayıcıların ötesinde yeteneklerle güvenlik ilkelerini uygulamaya yardımcı olur.

Mobil Platform Sağlık Kontrolü (Mobile Platform Health Checks)

Mobil platform sağlık kontrolü, bir aygıtın güvenlik durumunu doğrulamak ve muhtemel tehlikeleri belirlemek için kullanılan yöntemlerdir. Mobil platform sağlık kontrolleri, uygulamalarda gömülü olabilecek yazılım geliştirme kitleri şeklinde gelir.

Güvenilir Mobil Ortam (Trusted Mobile Environments)

Güvenilir mobil ortamlar, güvenlik özelliklerini yazılım temelli güvenlik mekanizmalarından daha yüksek düzeyde güven altına almak için bir mobil cihaza (akıllı telefon veya tablet) gömülü veya bağlı bir özel donanıma dayanır.

Mobil Açıklık Yönetim Araçları (Mobile Vulnerability Management Tools)

Mobil açıklık yönetim araçları aşağıdaki yetenkleri sağlar:

- Mobil işletim sistemlerinde (işletim sistemleri), yazılım ve uygulamalarda bulunan güvenlik açıklarının tanımlanması, sınıflandırılması ve düzeltilmesine yardımcı olmak
- Mobil varlıkların riskinin değerlendirilmesi ve raporlanmasına izin verilmesini sağlamak

Tüketici Mobil Güvenlik Uygulamaları (Consumer Mobile Security Apps)

Tüketici mobil güvenlik uygulamaları, mobil cihazları güvenlik tehditlerine karşı korur ve kullanıcıların gizlilik ve cihaz performansını yönetmesine yardımcı olur. Antivirüs taramaları, gizlilik yönetimi, aygıt performans optimizasyonu ve hırsızlığa karşı koruma gibi özellikler içerir.

1.12 Endüstriyel / IoT Sistemleri Güvenliği

Endüstriyel güvenlik, endüstriyel kontrol sistemlerinin korunması, endüstri ortamlarında makine ve ilgili cihazların çalışmasını izlemek ve kontrol etmek için tasarlanmış entegre donanım ve yazılım içeren bir çalışma alanıdır. IoT güvenliği, nesnelerin internette bağlı cihazların ve ağların korunması ile ilgili çalışma alanıdır

IoT Security

Nesnelerin İnterneti Kimlik Doğrulaması (Internet of Things Authentication)

Nesnelerin kimlik doğrulaması, bir IoT ortamında çalışan aygıtlar, uygulamalar, bulut hizmetleri veya ağ geçitleri gibi diğer varlıklarla etkileşime giren bir nesnenin kimliğine güven oluşturmanın mekanizmasıdır. IoT'deki "nesneler" için kimlik doğrulama, IoT aygıtlarının potansiyel kaynak kısıtlamaları, içinde faaliyet gösterdikleri ağların bant genişliği sınırlamaları ve çeşitli IoT varlıkları arasındaki etkileşimin mekanize olması nedeniyle günümüzde yaygın olan kullanıcı kimlik doğrulama yöntemlerinden farklı ve daha karmaşıktır.

Operasyonel Teknoloji Güvenliği (Operational Technology Security)

Operasyonel teknoloji (OT) güvenliği, endüstriyel otomasyon ve kontrol sistemleri, süreçleri ve organizasyonları için sayısal ve fiziksel güvenliğin yönetilmesi, geliştirilmesi, yönetimi ve işletilmesidir.

2 Entegre Olduğu Teknolojilere Göre

2.1 Bulut Bilişim Güvenliği

Bulut Erişim Güvenlik Aracıları (Cloud Access Security Brokers)

Bulut erişim güvenlik aracıları, kurum güvenlik denetimlerine müdahale etmek ve ilkeleri uygulamak için bulut hizmeti tüketicileri ile bulut hizmeti sağlayıcıları arasında aracılık yapan kurum içi veya bulut tabanlı güvenlik ilkesi uygulama noktalarıdır. Bulut Erişim Güvenlik Aracı platformları, bulut hizmeti bulma, bulut sağlayıcı risk derecelendirmeleri, tek oturum açma, yetkilendirme, aygıt profillemesi, şifreleme, tokenization, hassas veri izleme, kullanıcı davranışı izleme gibi birden çok güvenlik ilkesini birleştirir.

Yüksek Güvenilirlikli Hypervisor (High-Assurance Hypervisors)

Yüksek güvenilirlikli bir hypervisor, müdahale edilmemiş veya ele geçirilmemiş yüksek bir güven seviyesi oluşturulmasını sağlayan hypervisor dur. Yüksek güvence sağlandıktan sonra kritik öneme sahip iş yükleri ve hassas veriler güvence altına alınır.

Bulut Veri Koruma Ağ Geçitleri (Cloud Data Protection Gateways)

Bulut veri koruma ağ geçitleri, proxy vasıtasıyla bulut SaaS sağlayıcısına akarken yapılandırılmış ve yapılandırılmamış verilere şifreleme, maskeleme veya tokenization uygulayarak bir vekil kurabilir. Bulut veri koruma ağ geçidi işlevi, birkaç bulut erişim güvenlik aracısı çözümüne eklenmektedir. Uygulama kullanıcıları, diğer bulut kiracıları, SaaS yöneticileri ve bilgisayar korsanlarının bulut hizmetine yetkisiz erişimi önler ve SaaS kullanırken veri ikameti gereksinimlerini karşılamaya yardımcı olur.

SaaS Platform Güvenlik Yönetimi (SaaS Platform Security Management)

SaaS platform güvenlik yönetimi araçları, bir veya daha fazla SaaS hizmeti içinde veri erişimi ve kullanıcı etkinliği üzerinde kontrol sağlayan bir yönetişim gösterge tablosunu uygulamak için SaaS sağlayıcılarının API'lerini kullanır.

Bu tür mekanizmalar tipik olarak bulut erişim güvenlik aracısı ürünlerinin bir bileşeni olarak sağlanır ancak birkaç niş SPSM satıcısı, bir veya az sayıdaki SaaS uygulamasını hedef alan ürünler sunmaya devam etmektedir.

Hizmet Olarak Altyapı Konteyner Şifrelemesi (IaaS Container Encryption)

Hizmet olarak altyapı konteyner şifrelemesi, IaaS sağlayıcılarının barındırdığı iş yüklerinde, uygulama tarafında olmayan bir şekilde IaaS sağlayıcı altyapısında bulunan iş yükü tarafından depolanan verileri şifrelemek için kullanılan şifreleme teknolojisinin kullanılmasıdır.

Kurumlar, şifre çözme anahtarlarına erişimi kontrol ederek, IaaS iş yükleri tarafından kullanılan ve oluşturulan verileri, komşu kiracılardan, bulut hizmeti sağlayıcısı yöneticilerinden ve IaaS sağlayıcının olası bilgisayar korsanlarından koruyabilirler.

2.2 IoT Güvenliği

Nesnelerin İnterneti Kimlik Doğrulaması (Internet of Things Authentication)

Nesnelerin kimlik doğrulaması, bir IoT ortamında çalışan aygıtlar, uygulamalar, bulut hizmetleri veya ağ geçitleri gibi diğer varlıklarla etkileşime giren bir nesnenin kimliğine güven oluşturmanın mekanizmasıdır. IoT'deki "nesneler" için kimlik doğrulama, IoT aygıtlarının potansiyel kaynak kısıtlamaları, içinde faaliyet gösterdikleri ağların bant genişliği sınırlamaları ve çeşitli IoT varlıkları arasındaki etkileşimin mekanize olması nedeniyle günümüzde yaygın olan kullanıcı kimlik doğrulama yöntemlerinden farklı ve daha karmaşıktır.

2.3 Büyük Veri Güvenliği

Büyük veri, veri madenciliği potansiyeline sahip, çok miktarda yapılandırılmış, yarı yapılandırılmış ve yapılandırılmamış verileri açıklayan bir terimdir. Yerleşik Hadoop ve NoSQL uygulamalarına dayanan büyük veri ortamları, güvenlik durumunu belirlemek, potansiyel saldırıları tespit etmek, ve bilişimin güvenli kullanılmayan taraflarını (bulut bilişim, IoT) tespit etmek için yeni veri türlerini aramaya çalışır.

2.4 İşletim Sistemleri ve Taşıyıcı Güvenliği

[Daha sonra tanımlanacak]

2.5 Sanallaştırma Ortamı Güvenliği

[Daha sonra tanımlanacak]

2.6 Mobil Güvenliği

Mobil Cihazlar İçin Kullanıcı Kimlik Doğrulaması (User Authentication to Mobile Devices)

Mobil cihazlar için kullanıcı kimlik doğrulaması, cihazın kendisine erişen kullanıcının kimliğini doğrulayan çeşitli yöntemleri kapsar. Kısa sayısal PIN'ler ve alfa sayısal şifreler sıradanlaşmakta; grafik desenler ve biyometrik yöntemler daha yaygın hale gelmektedir

Mobil Tehdit Savunma (Mobile Threat Defense)

Mobil tehdit savunma araçları (MTS), işletmeleri mobil platformlardaki tehditlerden korur. MTDS çözümleri, aygıt (davranışsal anomali algılama ve güvenlik açığı değerlendirmeleri aracılığıyla), uygulama (kod analizi yoluyla) ve ağ (ağ trafiğini izleyerek ve şüpheli ağları otomatik olarak mobil aygıtlardan devre dışı bırakarak) üç düzeyde güvenlik sağlar.

Mobil Uygulama Sıkılaştırma (Mobile Application Hardening)

Mobil Uygulama Sıkılaştırma teknolojileri, mobil uygulamaları tersine mühendislik ve yeniden paketleme saldırılarına karşı korur.

Yeniden Paketleme: Android cihazlarda çok yaygın bir saldırı türüdür. Böyle bir saldırıda, saldırganlar uygulama pazarlarından indirilen popüler bir uygulamayı değiştirir, uygulama kodlarına ters mühendislik yaparlar, bazı kötü amaçlı yazılım (payload) ekler ve sonra değiştirilen uygulamayı uygulama pazarlarına yüklerler.

Korumalı Mobil Tarayıcılar (Protected Mobile Browsers)

Korumalı mobil tarayıcılar, tüketici ve kurumsal portallar gibi web tabanlı kaynaklara erişmek için veri güvenliği ve katman koruma katmanları ekleyerek veri kaybını önlemeye ve varsayılan tarayıcıların ötesinde yeteneklerle güvenlik ilkelerini uygulamaya yardımcı olur.

Mobil Platform Sağlık Kontrolü (Mobile Platform Health Checks)

Mobil platform sağlık kontrolü, bir aygıtın güvenlik durumunu doğrulamak ve muhtemel tehlikeleri belirlemek için kullanılan yöntemlerdir. Mobil platform sağlık kontrolleri, uygulamalarda gömülü olabilecek yazılım geliştirme kitleri şeklinde gelir.

Güvenilir Mobil Ortam (Trusted Mobile Environments)

Güvenilir mobil ortamlar, güvenlik özelliklerini yazılım temelli güvenlik mekanizmalarından daha yüksek düzeyde güven altına almak için bir mobil cihaza (akıllı telefon veya tablet) gömülü veya bağlı bir özel donanıma dayanır.

Mobil Açıklık Yönetim Araçları (Mobile Vulnerability Management Tools)

Mobil açıklık yönetim araçları aşağıdaki yetenkleri sağlar:

- Mobil işletim sistemlerinde (işletim sistemleri), yazılım ve uygulamalarda bulunan güvenlik açıklarının tanımlanması, sınıflandırılması ve düzeltilmesine yardımcı olmak
- Mobil varlıkların riskinin değerlendirilmesi ve raporlanmasına izin verilmesini sağlamak

Tüketici Mobil Güvenlik Uygulamaları (Consumer Mobile Security Apps)

Tüketici mobil güvenlik uygulamaları, mobil cihazları güvenlik tehditlerine karşı korur ve kullanıcıların gizlilik ve cihaz performansını yönetmesine yardımcı olur. Antivirüs taramaları, gizlilik yönetimi, aygıt performans optimizasyonu ve hırsızlığa karşı koruma gibi özellikler içerir.

2.7 Giyilebilir Teknoloji Güvenliği

Giyilebilir teknoloji güvenliği, akıllı saatler, kulaklıklar, akıllı gözlükler ve spor takipçileri gibi kullanıcının vücudu üzerine giydiği bilgisayar cihazlarındaki sistemin ve verilerin korunması ile ilgilidir.

2.8 Veritabanı Güvenliği

Veritabanı güvenliği, bir veritabanı veya veritabanı yönetim yazılımını gayri meşru kullanım ve kötü niyetli tehditlerden, saldırılardan korumak ve güvence altına almak için kullanılan ortak önlemleri belirtir.

2.9 Donanım ve Gömülü Sistem Güvenliği

Gömülü sistem güvenliği, güvenlik açıklarının azaltılması ve gömülü aygıtlarda çalışan yazılımların tehditlerine karşı korunmasıdır.

Çoğu BT alanındaki güvenlik gibi, gömülü sistem güvenliği de, donanım tasarım ve kodlamanın yanı sıra ek güvenlik yazılımları, vicdani yaklaşımları, en iyi uygulamalara uyumu ve uzmanlarla istişareyi içerir.

2.10 Kriptoloji

Blockchain Güvenliği

Güvenlik, blockchain teknolojisinin en önemli avantajlarından biri olarak kabul edilmektedir. Bir blok zinciri bozmak neredeyse imkansızdır çünkü bilgi, binlerce, hatta milyonlarca bilgisayar tarafından paylaşılmakta ve sürekli doğrulanmaktadır. Bir düğümde yaşanan sorun problem arz etmemektedir çünkü her düğümün bir kopyası bulunmaktadır.

3 Kullanıldığı Yere Göre

3.1 Kurumsal Altyapılar

Teknoloji ve ürünlerin enerji, haberleşme, ulaştırma vb. altyapılar tarafından kullanılmasıdır.

3.2 KOBİ

Teknoloji ve ürünlerin Küçük ve Orta Büyüklükteki İşletmeler tarafından kullanılmasıdır.

3.3 Endüstriyel / IoT Sistemler

Akıllı Şehirler ve Siber Güvenlik

[Daha sonra tanımlanacak]

3.4 Kişisel

Teknoloji ve ürünlerin bir çıkar amacı gözetmeksizin bireysel kullanımını ifade eder.

4 Olgunluk Düzeylerine Göre

4.1 Laboratuvar ortamında

İlgili teknolojiye ait ürünler henüz gelişmemiştir ve satıcıları mevcut değildir.

4.2 Gelişmekte Olan

İlgili teknolojiye ait ürünler gelişmekte olup, genellikle yüksek fiyattan satılmakta, sektör liderleri tarafından pilot uygulamaları yayınlanmaktadır.

4.3 Yarı Olgun

İkinci jenerasyonu ifade eder. Bu teknolojiye ait ürünler daha az özelleştirme gerektirir.

4.4 Kendini İspatlamış

Bu teknolojiye ait ürünler out-of-box ın bir adım daha ilerisinde olup, sektör tarafından benimsenmesi daha hızlıdır.

4.5 Olgun Teknoloji

Sağlam bir teknolojiye sahip olan bu ürünler, pazarda dominant olan satıcılar tarafından satılmaktadır.

4.6 Eski Teknoloji

Artık kullanılmayan teknolojileri ifade etmektedir.

5 Tehditlere Göre

5.1 Oltalama Saldırılarından Korunma

Oltalama, saldırganların, e-posta, sohbet veya diğer iletişim kanallarında saygın bir varlık veya kişi gibi maskelenerek kullanıcının giriş kimlik bilgileri veya hesap bilgileri gibi bilgilerini öğrenmeye çalıştıkları dolandırıcılık biçimidir.

Bir ağ geçidi e-posta filtresi, toplu olarak hedeflenen oltalama e-postalarını yakalayarak kullanıcıların gelen kutularına ulaşan oltalama e-postalarının sayısını azaltır. Web güvenlik ağ geçitleri de kullanıcıların kötü amaçlı bir bağlantı hedefine ulaşmasını engelleyerek bir başka savunma katmanı sağlayabilir Web Güvenlik Ağ Geçitleri, istenilen URL'leri, kötü amaçlı yazılım dağıtımından şüphelenilen ve sürekli güncellenen bir veritabanından kontrol ederek çalışırlar.

5.2 Fidyeci Yazılımlardan Korunma

Fidyeci yazılım, kurbanının bilgisayarındaki verilerin genellikle şifreleme yöntemiyle kilitlendiği ve fidye verilen veriler şifresiz hale getirilmeden önce ödeme talep edilen kötü amaçlı yazılımdır. Fidyeci yazılım saldırılarının nedeni neredeyse her zaman parasaldır ve diğer saldırı türlerinden farklı olarak, kurban genellikle bir istismarın meydana geldiği konusunda bilgilendirilir ve kurbana saldırıdan kurtulma talimatları verilir.

Fidye saldırılarına karşı koruma sağlamak için uzmanlar kullanıcıları bilgisayar aygıtlarını düzenli olarak yedeklemeyi ve düzenli olarak virüsten koruma yazılımını güncellemeyi tavsiye etmektedir.

5.3 Servis Engelleme Saldırılarından Korunma

Servis Engelleme saldırısı, bir saldırgan yasal kullanıcının hedef bilgisayar sistemlerine, aygıtlarına veya diğer ağ kaynaklarına erişmesini engelleyen bir işlem başlatması durumunda ortaya çıkan bir güvenlik olayıdır.

Bir DoS saldırısı yaşandığından şüphelenildiğinde, işletmelerin gerçek bir DoS saldırısı mı yoksa başka bir faktörün neden olduğu performans düşüşü olup olmadığını belirlemek için İnternet servis sağlayıcısına (ISS) başvurmaları gerekir. ISS, kötü amaçlı trafiği yeniden yönlendirerek veya azaltarak saldırının hafifletilmesine yardımcı olabilir ve saldırının etkisini azaltmak için yük dengeleyici kullanabilir.

5.4 Gelişmiş Tehdit Saldırılarından Korunma

Gelişmiş tehdit saldırısı (APT), yetkisiz bir kişinin bir ağa erişmesini ve orada uzun süre tespit edilmeden kalmasını sağlayan bir ağ saldırısıdır. APT saldırısının amacı, ağa veya organizasyona zarar vermek yerine verileri çalmaktır. APT saldırıları, ulusal savunma, imalat ve finans endüstrisi gibi yüksek değerli bilgiye sahip sektörlerdeki kuruluşları hedef almaktadır.

APT saldırılarını tanımlamak zor olsa da, verilerin çalınması hiçbir zaman tamamen görünmez olamaz. Giden verideki anormalliklerin tespit edilmesi belki de ağ yöneticisinin, ağının bir APT saldırısının hedefi olduğunu keşfetmesinin en iyi yoludur.

5.5 Yetki Yükseltme Engelleme

Yetki yükseltme saldırısı, saldırganın ağa ve ilişkili veri/uygulamalara ayrıcalıklı erişimini sağlamak için programlama hatalarından veya tasarım kusurlarından yararlandığı bir tür ağ saldırısıdır.

Dikey yetki yükseltme, saldırganın kendisine daha yüksek ayrıcalıklar tanımasını gerektirir. Bu, genellikle, saldırganın yetkisiz kod çalıştırmasına izin veren çekirdek düzeyinde işlemler gerçekleştirerek elde edilir.

Yatay yetki yükseltme, saldırganın daha önce verilen yetkileri kullanmasını gerektirir, ancak benzer ayrıcalıklara sahip başka bir kullanıcının kimliğinin ele geçirildiğini varsaymaktadır. Örneğin, başka bir kişinin çevrimiçi bankacılık hesabına erişen biri, yatay yetki yükseltmiş olur.

5.6 Truva Atından Korunma

Truva atı zararsız görünen, ancak oldukça zararlı olan bir programdır. Genellikle, kötü niyetli program, masum görünümlü bir e-posta eki veya bir oyun gibi ücretsiz bir programın içine gizlidir. Kullanıcı Truva atını indirdiğinde içeride gizlenmiş zararlı yazılım da indirilir.Kötü niyetli kod, bilgisayar içine girdikten sonra, saldırganın gerçekleştirmek üzere tasarladığı herhangi bir görevi yerine getirebilir.Truva atı yazılımının bulaşmasına engel olmak için, kullanıcılar virüsten koruma yazılımlarını güncel tutmalı, dosyaları veya programları güvenilmeyen kaynaklardan asla indirmemeli ve açmadan önce virüsten koruma yazılımıyla yeni dosyaları taramalıdır.

5.7 İnternet Uygulamalarına Saldırılardan Korunma

[Daha sonra tanımlanacak]

5.8 Casus Yazılımlardan Korunma

Casus yazılım, son kullanıcı bilgisi olmadan bir bilgi işlem cihazına kurulmuş bir yazılımdır. Bu tür yazılımlar, bazen nispeten zararsız nedenlerle kurulmuş olsalar bile, son kullanıcının gizliliğini ihlal edebilir ve istismar edilme potansiyeline sahiptir.

Kullanıcılar, casus yazılımları önlemek için yalnızca güvenilir kaynaklardan yazılım yüklemeli, yazılım yüklerken tüm açıklamaları okumalı, açılır pencerelere tıklanmamalı ve tarayıcı, işletim sistemi ve uygulama yazılımlarını güncel tutmalıdır.

5.9 Solucanlardan Korunma

Bir bilgisayar solucanın amacı, bulaştığı sistemde aktif olarak kalmak ve kendini yeni sistemlere bulaştırmaktır. Solucanlar genellikle bir işletim sisteminin kullanıcıya açık olmayan parçalarını kullanırlar. Solucanlar yalnızca kontrol sistem kaynaklarını fazla tüketmesi, diğer görevleri yavaşlatması veya durdurması durumunda fark edilir.

5.10 Karışık Tehdit Saldırılardan Korunma

Karışık tehdit, birden fazla zararlı yazılım türündeki unsurları birleştiren ve genellikle hasarın şiddetini ve bulaşma hızını artırmak için birden fazla saldırı vektörü kullanan bir istismar saldırısıdır. Nimda, CodeRed, Bugbear ve Conficker birkaç iyi bilinen örnektir. Virüs, solucan veya

Truva atları olarak tanımlanabilmelerine rağmen, günümüzdeki istismar saldırıları karışık tehdit örnekleridir.

Uzmanlar, karışık tehditlerden korunmak için ağ yöneticilerini yama yönetimi konusunda dikkatli olmaya, iyi güvenlik duvarı ürünlerini kullanmaya ve korumaya, ve kullanıcıları doğru e-posta kullanımı ve çevrimiçi davranış konusunda eğitmeye davet etmektedir.

5.11 Mobil Zararlı Yazılımlarından Korunma

Mobil casus zararlı yazılımı, son kullanıcının bilgisi veya izni olmaksızın son kullanıcının eylemleri hakkındaki bilgileri izleyen ve kaydeden yazılım programıdır. Son kullanıcı, izleme yazılımının kurulu olduğunun farkındaysa, yazılım casus yazılım olarak değerlendirilmez. Casus yazılımları bulmak ve kaldırmak için antispyware koruması içeren virüsten koruma yazılımı kullanılmalıdır.

5.12 Ortadaki Adam Saldırısından Korunma

Ortadaki Adam saldırısı, saldırganın, doğrudan birbirleriyle iletişim halinde olduklarını düşünen iki taraf arasındaki mesajları gizlice yakaladığı ve bu durumdan faydalandığı bir saldırı türüdür. Bu saldırılar, hassas bilgilerin gerçek zamanlı olarak değiştirilmesine olanak sağlaması sebebiyle çevrimiçi güvenlik için ciddi bir tehdit oluşturmaktadır. Çevrimiçi bankacılık ve e-ticaret siteleri sıklıkla Ortadaki Adam saldırılarının hedefi olur, böylece saldırgan oturum açma kimlik bilgileri ve diğer hassas verileri ele geçirebilir.

5.13 SSL / TLS Altsürüme Zorlama Engelleme

POODLE açıklığı kullanılarak yapılan SSL / TLS Altsürüme Zorlama saldırıları, şifreleme ve kimlik doğrulama için Güvenli Soket Katmanı (SSL) 3.0 protokolüne dayanan tarayıcı tabanlı iletişimi hedef almaktadır. TLS (Taşıma Katmanı Güvenliği) protokolü, SSL protokülünün yerini alsa da, TLS bağlantısı yapılamayan durumlarda birçok tarayıcı SSL protokolünü kullanmaya devam etmektedir. Bu tarz durumlarda saldırgan POODLE açıklığını kullanarak tarayıcıyı SSL 3.0 kullanmaya zorlar. Bu saldırıdan korunmak için ağ yöneticilerinin sunucu yazılımlarının TLS'in en son sürümünü desteklediğini ve düzgün şekilde yapılandırıldığını kontrol etmeleri gerekir.

5.14 Kontrol Dışı Registry Kayıtlarını Engelleme

Dosyasız kötücül saldırılarda güncel bir trend, Windows kayıt defterine kod enjekte etmektir. Bu saldırıların çoğu, bir e-posta iletisinde bir dosya veya bağlantı olarak gönderilir. Bağlantı veya ek tıklandığında, zararlı yazılım yükünü Windows kayıt defterine yazar ve sonra kaybolur. Bu tür yeni dosyasız saldırılara karşı korunmak için antivirüsün güncellenmesi yeterli değildir.

5.15 Bellek Tabanlı Saldırılardan Korunma

Dosyasız zararlı yazılım, yalnızca bellekte bulunan kötü amaçlı koddur. Zararlı yazılım doğrudan RAM'e yazılır. Kod, daha sonra exploit için kullanılan iexplore.exe veya javaw.exe gibi çalışan bir işleme enjekte edilir. Bu tarz saldırılardan korunmak için işletim sistemi tarafından çalıştırılan tüm yeni süreçlerin doğrulanması, beyaz - kara liste kontrolünün düzenli olarak yapılması gerekmektedir.

5.16 Tuş Kaydedicilerden (klavye, Ekran, Ağ) Korunma

Tuş kaydedici, belirli bir bilgisayarın klavyesinde yazılan her tuş vuruşunu izlemek ve kaydetmek için kullanılan bir gözetleme teknolojisidir. Tuş kaydedici yazılımı iPhone ve Android cihazları gibi akıllı telefonlarda da kullanılabilir. Tuş kaydediciler genellikle siber suçlular tarafından kişisel

olarak tanımlanabilir bilgileri, kimlik bilgilerini ve hassas kurumsal verileri çalmak için bir casus yazılım aracı olarak kullanılır.

Antikeylogger yazılımı, ortak tuş kaydedici özelliklerini bir control listesi ile karşılaştırarak, yazılım tabanlı tuş kaydedicileri tespit etmek için dizayn edilmiştir.

5.17 Polimorfik Zararlı Yazılımlardan Korunma

Polimorfik zararlı yazılımlar, sürekli olarak değişen bir virüs, solucan, trojan veya casus yazılım gibi zararlı, yıkıcı veya müdahaleci bilgisayar yazılımları olup, bu yazılımların anti-malware programları ile tespit edilmesi oldukça zordur. Kötü amaçlı kodun evrimi, dosya adı değişiklikleri, sıkıştırma ve değişken anahtarlarla şifreleme gibi çeşitli şekillerde oluşabilir.

Polimorfik zararlı yazılımlarla mücadelede en iyi yöntem çoklu ve çeşitli engelleme, filtreleme, algılama ve ortadan kaldırma programları kullanmaktır. Bu programlar güncel tutulmalı ve olabildiğince sık çalıştırılmalı, (varsa) otomatik koruma özellikleri etkinleştirilmiş olmalıdır.

5.18 Proses Sömürülmesi Engellenmesi

Prosess Sömürülmesi saldırılarının en çok bilinen türü, tarayıcılarda arabellek aşımı saldırılarıdır. Bir program veya işlem, sabit uzunlukta bir bellek bloğuna veya arabelleğe daha fazla veri yazmaya çalıştığında arabellek taşması oluşur. Bir arabellek taşması kullanmak, bir saldırganın prosesleri kontrol etmesine, kilitlemesine veya değişkenlerini değiştirmesine olanak tanır.

Ürün satıcıları, keşfedilen arabellek taşması güvenlik açıklarını gidermek için yazılım güncellemeleri yayınlarlar, ancak keşfedilen güvenlik açığı ile dağıtılan güncelleme arasındaki süre risk oluşturmaya devam etmektedir.

5.19 Rootkits Korunma

Rootkit, bir bilgisayara veya bilgisayar ağına yönetici düzeyinde erişime izin veren araçlara verilen addır. Genellikle, bir system kırıcı, bilinen güvenlik açığından yararlanarak veya bir parola kırarak kullanıcı düzeyinde erişim elde ettikten sonra bilgisayara bir rootkit yükler. Rootkit kurulduktan sonra, saldırganın saldırıya maruz kalmasını maskeleme ve bilgisayara ve muhtemelen ağdaki diğer makinelere root veya ayrıcalıklı erişim hakkı kazanmasına olanak tanır. Rootkit algılandığı takdirde kurtulmanın tek yolu sabit diski tamemen silmek ve işletim sistemini yeniden kurmaktır.

5.20 Kernel - Mode Saldırılarından Korunma

[Daha sonra tanımlanacak]

5.21 Zincirleme Sömürüleri Engelleme

[Daha sonra tanımlanacak]

5.22 Donanım Sömürülerini Engelleme

[Daha sonra tanımlanacak]

5.23 Gömülü Yazılım Sömürülerini Engelleme

Gömülü sistemler, İnternet ve kablosuz erişim noktaları, IP kameralar, güvenlik sistemleri, hızı ayarlayıcılar, dronlar ve endüstriyel kontrol sistemleri gibi çok çeşitli cihazlarda bulunur. Hack işlemi, ROM çipleri üzerinde veya firmware üzerinde gerçekleştirilebilir.

5.24 Yanlış Kullanım Engelleme

[Daha sonra tanımlanacak]

5.25 Hatalı Konfigürasyon Engelleme

Yanlış Kullanım saldırıları, kablosuz ağ saldırı türlerinden biridir. Birbiri ile uyumlu olmayan donanım ve yazılımın, ağ altyapısını saldırıya karşı savunmasız hale getirme olasılığı vardır. Bu tür saldırıları engellemek için konfigürasyonun doğru yapıldığı kontrol edilmelidir.

5.26 Fiziksel Saldırılardan Korunma

Fiziksel saldırı yüzeyi, hedef ile aynı yerde bulunan bir saldırganın kullanabileceği güvenlik açıklarının toplamıdır. Fiziksel saldırı yüzeyi, kötü niyetli çalışanlar, sosyal mühendislik saldırılarını kullanan kişiler vb. tarafından sömürülebilir.

Fiziksel saldırı yüzeyini azaltmaya yönelik en iyi uygulamalar, güvenli kimlik doğrulamayı zorlamak, sabit sürücüleri ve eski donanımları atmadan önce sıfırlamak ve değerli bilgileri ortada bırakmaktan kaçınmaktır.

5.27 Sosyal Mühendislik Saldırılarından Korunma

Sosyal mühendislik, insan etkileşimine büyük ölçüde dayanan ve genellikle insanları, normal güvenlik prosedürlerini çiğnemeye zorlayan bir saldırı vektörüdür. Birçok sosyal mühendislik sömürüsü, insanların yardımcı olmaya istekli olmalarından kaynaklanmaktadır.

Güvenlik uzmanları, BT departmanlarının sosyal mühendislik tekniklerini kullanan penetrasyon testlerini düzenli olarak gerçekleştirmelerini önerir. Bu testler, yöneticilerin hangi kullanıcı türleri tarafından belirli saldırı türleri için en fazla risk oluşturduğunu öğrenmelerine yardımcı olurken, aynı zamanda hangi çalışanın ek eğitime ihtiyaç duyduğunu da belirlemekte yardımcı olmaktadır.

5.28 Kötü Niyetli Kullanıcılardan Korunma

Kötü niyetli kullanıcılar (dahili saldırganlar), yetkili ve "güvenilir" kullanıcı imajı yaratarak hassas bilgileri ele geçirmeye çalışırlar. Kötü niyetli kullanıcılar, hangi verinin nerede olduğunu bildikleri için ve bu verilere güvenilir olarak erişebildikleri için, IT ve bilgi güvenliği profesyonelleri, kötü niyetli kullanıcıları tespit etmekte zorlanmaktadır.

6 Kurulum Yöntemine Göre

6.1 Sunucuya / İstemciye Kurulum Çözümü

Teknoloji ve ürünlerin istemci veya sunucuya kurularak kullanılmasıdır.

6.2 Donanım – Yazılım Hazır Çözümü

Teknoloji ve ürünlerin hazır donanım üzerine kurulu ve optimize edilmiş olarak sunulması ve kullanılmasıdır.

6.3 Sanal Sunucu / Taşıyıcı Hazır Çözümü

Teknoloji ve ürünlerin, bir donanımsal sunucu üzerinde birbirinden bağımsız ve izole olarak birden fazla işletim sisteminin maksimum performansla barındırılmasına olanak sağlayan sanal sunucular üzerinde kurularak kullanılmasıdır.

6.4 Bulut Çözümü

Teknoloji ve ürünlerin, bellek, vb. kaynaklarını sanal bir kaynak havuzu içerisinden temin eden ve bunların güncellemesini anlık olarak gerçekleştirebilen, veri merkezi bağımlılığı bulunmayan, sanallaştırma teknolojisi kullanarak çalışan sanalsunucularda kurularak kullanılmasıdır.

KAYNAKÇA

[1] Tirosh, A. (2017). *Hype Cycle for Application Security, 2017*. [online] Gartner.com. Available at: https://www.gartner.com/doc/3772095/hype-cycle-application-security- [Accessed 1 Jun. 2017].

[2] Sans.org. (2017). *2017 Threat Landscape Survey: Users on the Front Line*. [online] Available at: https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910 [Accessed 1 Jun. 2017].

[3] Techtarget.com. (2017). [online] Available at: http://www.techtarget.com [Accessed 1 Jun. 2017].