BSM 471-AĞ GÜVENLİĞİ

Hafta10: Katman 7 Saldırıları ve Önleme Teknikleri

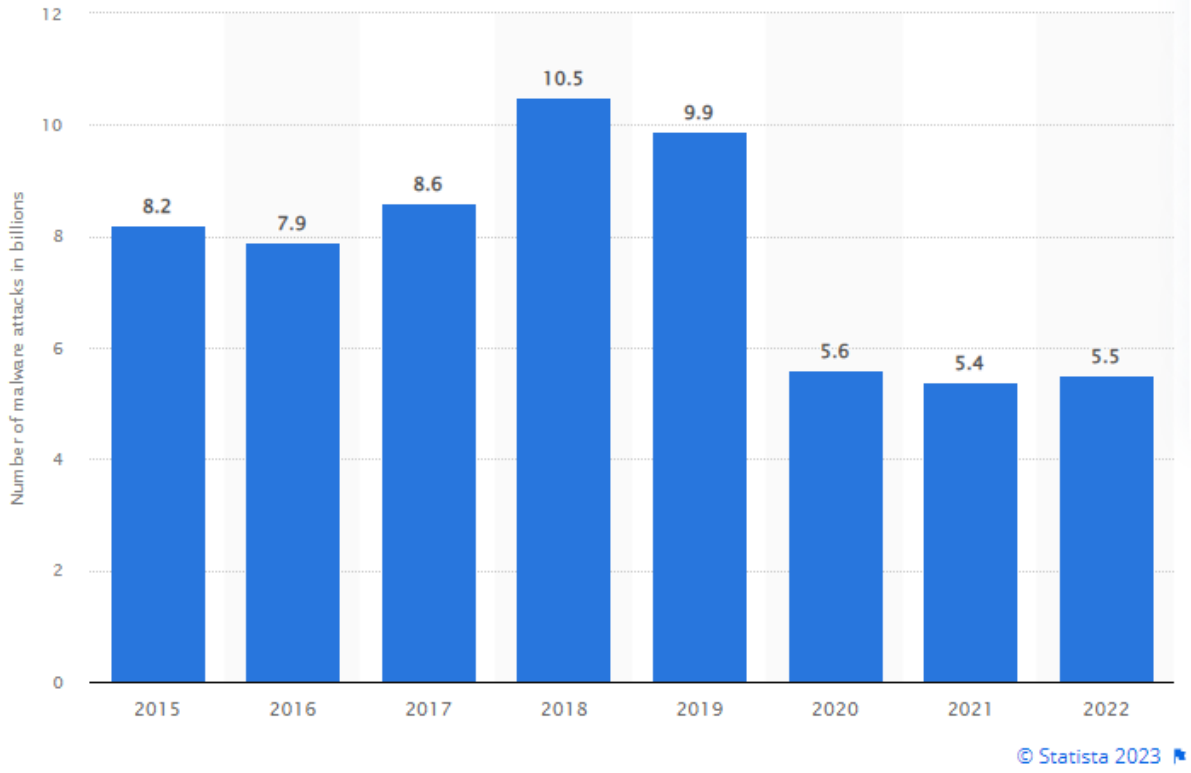
Dr. Öğr. Üyesi Musa BALTA
Bilgisayar Mühendisliği Bölümü
Bilgisayar ve Bilişim Bilimleri Fakültesi

Haftalık İçerik

- ***Zararlı Yazılımlar***
- ***Zararlı Yazılım Analiz Teknikleri***
- ***OWASP Top Ten Saldırıları***
- ***Windows ve Linux Uç Sistemler Üzerinde Sıkılaştırmalar***

Zararlı Yazılım ve Türleri

- Kötü amaçlı yazılım, bir kuruluşa veya bireye zarar vermek için bir tehdit aktörü tarafından dağıtılan yazılımlardır.
- Kötü amaçlı yazılımların genel hedefleri;
  - Kurum içi uç düğümler ve ağlara zarar vermek
  - Kimlik hırsızlığı için kişisel verileri elde etme
  - Diğer ağlara karşı hizmet reddi saldırıları başlatmak için birden fazla bilgisayarın kontrolünün ele geçirilmesi
  - Bilgisayarları enfekte etmek ve bitcoin veya diğer kripto paraları çıkarmak için kullanmaktır.



Zararlı Yazılım Türleri

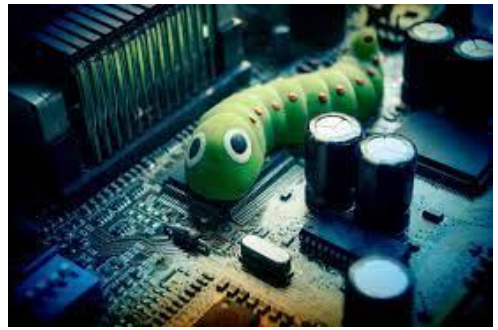
Bulaşma Yöntemleri

- ***E-mail***
- ***Fiziksel medya (usb, disk vb.)***
- ***Pop-up alarmları***
- ***Zaafiyetler***
- ***Arkakapılar***
- ***İndirme işlemleri***
- ***Yetki yükseltme***
- ***Homojenlik***

Zararlı Yazılım Türleri-Virus

- **Virüs**, kendisini bir uygulamaya sokan ve uygulama çalıştırıldığında yürütülen bir kod parçasıdır.
- Bir ağa girdikten sonra, hassas verileri çalmak, DDoS saldırıları başlatmak veya fidye yazılımı saldırıları gerçekleştirmek için bir virüs kullanılabilir.
- Genellikle virüslü web siteleri, dosya paylaşımı veya e-posta eki indirmeleri yoluyla yayılan bir virüs, virüslü ana bilgisayar dosyası veya programı etkinleştirilene kadar uykuda kalır. Bu gerçekleştiğinde, virüs kendini çoğaltabilir ve sistemlerinize yayılabilir.
- **Virus Örneği;**
- **Stuxnet** – *Stuxnet 2010'da ortaya çıktı ve geniş çapta ABD ve İsrail hükümetleri tarafından İran'ın nükleer programını bozmak için geliştirildiğine inanılıyordu. Bir USB flash sürücü aracılığıyla yayılan, Siemens endüstriyel kontrol sistemlerini hedef alarak santrifüjlerin rekor bir hızla arızalanmasına ve kendi kendini yok etmesine neden oldu. Stuxnet'in 20.000'den fazla bilgisayara bulaştığına ve İran'ın nükleer santrifüjlerinin beşte birini mahvettiğine ve programını yıllar öncesine götürdüğüne inanılıyor.*

Zararlı Yazılım Türleri-Solucan



- Solucanlar, işletim sistemi güvenlik açıklarından yararlanarak bilgisayar ağlarına yayılır.
- Solucan, kimsenin herhangi bir işlem yapmasına gerek kalmadan diğer bilgisayarlara bulaşmak için kendini kopyalayan bağımsız bir programdır.
- Hızlı yayılabildiğinden, solucanlar genellikle bir sisteme zarar vermek için oluşturulan bir kod parçası olan bir yükü yürütmek için kullanılır. Yükler, bir ana bilgisayar sistemindeki dosyaları silebilir, bir fidye yazılımı saldırısı için verileri şifreleyebilir, bilgi çalabilir, dosyaları silebilir ve bot ağları oluşturabilir.
- **Worm Örneği;**
- **SQL Slammer**, *geleneksel dağıtım yöntemlerini kullanmayan, iyi bilinen bir bilgisayar solucanıydı. Bunun yerine, rastgele IP adresleri oluşturdu ve virüsten koruma yazılımı tarafından korunmayanları arayarak kendini onlara gönderdi. 2003'te vurduktan kısa bir süre sonra sonuç, 75.000'den fazla virüslü bilgisayarın farkında olmadan birkaç büyük web sitesinde DDoS saldırılarına karışması oldu. İlgili güvenlik düzeltme eki uzun yıllardır mevcut olmasına rağmen, SQL Slammer yine de 2016 ve 2017'de yeniden canlandı.*

Zararlı Yazılım Türleri-Casus Yazılımlar

- Casus yazılımlar, cihazınızda gizlenen, etkinliği izleyen ve finansal veriler, hesap bilgileri, oturum açma bilgileri ve daha fazlası gibi hassas bilgileri çalan bir tür kötü amaçlı yazılımlardır.
- Casus yazılımlar, yazılım güvenlik açıklarından yararlanarak yayılabilir veya meşru yazılımlarla veya Truva atlarıyla birlikte paketlenebilir.
- **Spyware Örneği;**
- **CoolWebSearch** – *Bu program, tarayıcıyı ele geçirmek, ayarları değiştirmek ve tarama verilerini yazarına göndermek için Internet Explorer'daki güvenlik açıklarından yararlanmıştır.*
- **Gator** – *Genellikle Kazaa gibi dosya paylaşım yazılımlarıyla birlikte verilen bu program, kurbanın web'de gezinme alışkanlıklarını izler ve bilgileri onlara belirli reklamlar sunmak için kullanır.*

Zararlı Yazılım Türleri-Reklam Yazılımları

- Adware, bir bilgisayar ekranında veya mobil cihazda istenmeyen ve bazen kötü amaçlı reklamlar görüntüler, arama sonuçlarını reklam veren web sitelerine yönlendirir ve kullanıcının izni olmadan reklam verenlere satılabilecek kullanıcı verilerini yakalar.
- Tüm reklam yazılımları kötü amaçlı yazılım değildir, bazıları yasaldır ve kullanımı güvenlidir. Kullanıcılar, internet tarayıcılarındaki pop-up kontrollerini ve tercihlerini yöneterek veya bir reklam engelleyici kullanarak genellikle reklam yazılımlarının sıklığını veya ne tür indirmelere izin verdiklerini etkileyebilir.
- **Adware Örneği;**
- **Fireball –** *Fireball, 2017'de İsrailli bir yazılım şirketi dünya çapında 250 milyon bilgisayara ve kurumsal ağların beşte birine virüs bulaştığını keşfettiğinde manşetlere çıktı. Fireball bilgisayarınızı etkilediğinde, tarayıcınızı devralır. Ana sayfanızı sahte bir arama motoru olan Trotus'a dönüştürür ve ziyaret ettiğiniz herhangi bir web sayfasına rahatsız edici reklamlar ekler. Ayrıca tarayıcı ayarlarınızı değiştirmenizi de engeller.*

Zararlı Yazılım Türleri-Truva Atı

- Bir Truva Atı (veya Truva Atı), bilgisayarınızda kötü amaçlı yazılım çalıştırmanız için sizi kandırmak için meşru yazılım kılığına girer.
- Güvenilir göründüğü için kullanıcılar onu indirir ve istemeden kötü amaçlı yazılımların cihazlarına girmesine izin verir. Truva atlarının kendileri bir giriş kapısıdır. Bir solucanın aksine, çalışmak için bir ana bilgisayara ihtiyaçları vardır.
- Bir cihaza bir Trojan yüklendikten sonra, bilgisayar korsanları bunu verileri silmek, değiştirmek veya yakalamak, cihazınızı bir botnet'in parçası olarak toplamak, cihazınızda casusluk yapmak veya ağınıza erişim sağlamak için kullanabilir.
- **Trojan Örneği;**
- **'Qakbot'** veya **'Pinkslipbot'** *olarak da bilinen kötü amaçlı Qbot, 2007'den beri aktif olan ve kullanıcı verilerini ve bankacılık kimlik bilgilerini çalmaya odaklanan bir bankacılık Truva Atı'dır. Kötü amaçlı yazılım, yeni dağıtım mekanizmalarını, komut ve kontrol tekniklerini ve analiz önleme özelliklerini içerecek şekilde gelişti.*

Zararlı Yazılım Türleri-Botnet

- Bot, bir bilgisayar korsanı tarafından uzaktan kontrol edilebilmesi için kötü amaçlı yazılım bulaşmış bir bilgisayardır.
- Zombi bilgisayarı olarak adlandırılan bot, daha sonra daha fazla saldırı başlatmak için kullanılabilir veya botnet adı verilen bir bot koleksiyonunun parçası olabilir.
- Bot ağları, fark edilmeden yayıldıkça milyonlarca cihazı içerebilir. Bot ağları, bilgisayar korsanlarına DDoS saldırıları, spam ve kimlik avı mesajları gönderme ve diğer kötü amaçlı yazılım türlerini yayma dahil olmak üzere çok sayıda kötü amaçlı etkinlikte yardımcı olur.
- **Botnet Örneği;**
- **Andromeda kötü amaçlı yazılımı –** *Andromeda botnet, 80 farklı kötü amaçlı yazılım ailesiyle ilişkilendirildi. O kadar büyüdü ki, bir noktada ayda bir milyon yeni makineye bulaşıyor, kendisini sosyal medya, anlık mesajlaşma, spam e-postalar, istismar kitleri ve daha fazlası aracılığıyla dağıtıyordu. Operasyon FBI, Europol'ün Avrupa Siber Suçlar merkezi ve diğerleri tarafından 2017'de durduruldu ancak birçok PC'ye virüs bulaşmaya devam etti.*

Zararlı Yazılım Türleri-Logic Bombs

- Logic(Mantık) bombaları, yalnızca belirli bir tarih ve saatte veya bir hesaba 20. kez giriş yapıldığında tetiklendiğinde etkinleşen bir kötü amaçlı yazılım türüdür.
- Virüsler ve solucanlar, yüklerini (yani kötü niyetli kodu) önceden tanımlanmış bir zamanda veya başka bir koşul karşılandığında teslim etmek için genellikle mantık bombaları içerir.
- Mantık bombalarının neden olduğu hasar, veri baytlarını değiştirmekten sabit diskleri okunamaz hale getirmeye kadar değişir.
- **Logic Bomb Örneği;**
- *2016'da bir programcı, Siemens şirketinin bir şubesinde elektronik tabloların birkaç yılda bir arızalanmasına neden oldu ve bu nedenle, sorunu çözmek için onu tekrar işe almak zorunda kaldılar. Bu durumda, bir tesadüf kötü niyetli kodu açığa çıkarana kadar kimse bir şeyden şüphelenmedi.*

Zararlı Yazılım Türleri-Keylogger

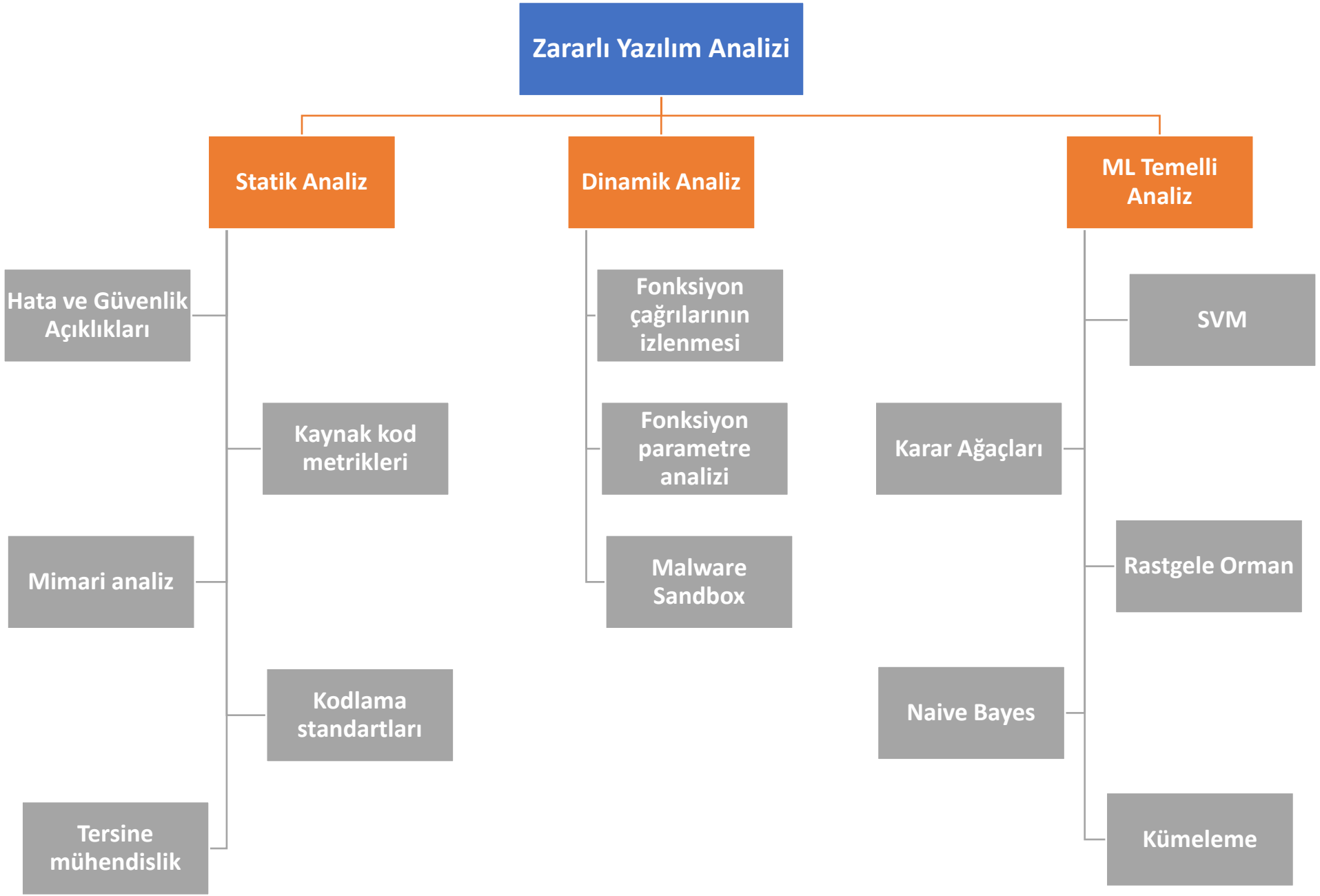
- Bir keylogger, kullanıcı etkinliğini izleyen bir tür casus yazılımdır. Keylogger'lar yasal amaçlar için kullanılabilir - örneğin, onları çocuklarının çevrimiçi aktivitelerini takip etmek için kullanan aileler veya onları çalışan aktivitelerini izlemek için kullanan kuruluşlar. Ancak, kötü amaçlarla kurulduğunda keylogger'lar parola verilerini, bankacılık bilgilerini ve diğer hassas bilgileri çalmak için kullanılabilir. Keylogger'lar, kimlik avı, sosyal mühendislik veya kötü amaçlı indirmeler yoluyla bir sisteme eklenebilir.
- **Keylogger Örneği;**
- 2017'de, bir Iowa Üniversitesi öğrencisi, notları değiştirmek ve değiştirmek için oturum açma kimlik bilgilerini çalmak üzere personel bilgisayarlarına keylogger'lar yükledikten sonra tutuklandı. Öğrenci suçlu bulundu ve dört ay hapis cezasına çarptırıldı.

Zararlı Yazılım Türleri-Ransomware ve Crypto

- Fidye yazılımı, kullanıcıları sistemlerinden kilitlemek veya bir fidye ödenene kadar verilere eri için tasarlanmış kötü amaçlı yazılımdır. Kripto-kötü amaçlı yazılım, kullanıcı dosyalarını şifreleyen ve belirli bir son tarihe kadar ve genellikle Bitcoin gibi bir dijital para birimi aracılığıyla ödeme yapılmasını gerektiren bir fidye yazılımı türüdür. Fidye yazılımı, uzun yıllardır farklı sektörlerdeki kuruluşlar için kalıcı bir tehdit olmuştur. Daha fazla işletme dijital dönüşümü benimserken, bir fidye yazılımı saldırısında hedef alınma olasılığı önemli ölçüde arttı.
- **Ransomware Örneği;**
- **CryptoLocker**, 2013 ve 2014'te yaygın olan ve siber suçluların bir sistemdeki dosyalara erişmek ve bunları şifrelemek için kullandıkları bir kötü amaçlı yazılım biçimidir. Siber suçlular, çalışanları fidye yazılımını bilgisayarlarına indirmeleri için kandırmak ve ağa bulaşmak için sosyal mühendislik taktikleri kullandı. CryptoLocker indirildikten sonra, belirtilen son tarihe kadar bir nakit veya Bitcoin ödemesi yapılırsa verilerin şifresini çözmeyi teklif eden bir fidye mesajı görüntüler. CryptoLocker fidye yazılımı o zamandan beri kaldırılmış olsa da, operatörlerinin masum kuruluşlardan zorla yaklaşık üç milyon dolar aldığına inanılıyor.

Zararlı Yazılım Türleri-Güvenlik Önlemleri

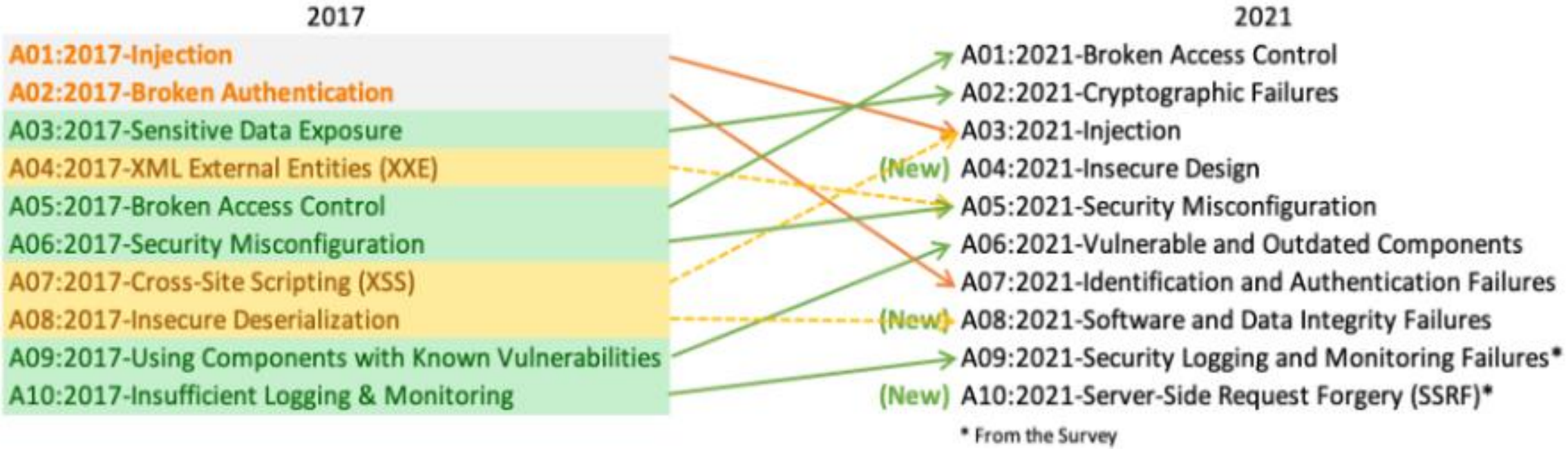
- ***Kişisel Bilgisayarlar;***
- Antivirus ve antimalware yazılımları kurulu ve güncel olmalı
- E-posta, köprü, anlık ileti veya başka bir biçimde kaynağı garanti edilemeyen hiçbir bilgiye güvenmeyin
- ***Kurumsal Yapılar;***
- Firewall, Anti-malware, WAF vb. güvenlik ürünlerinizi güncel tutup, gerekli sıkılaştırmaları yapınız.
- Statik Analiz, Dinamik Analiz ve ML temelli Analiz yöntemlerinin kullanımı


Zararlı Yazılım Analizi
Statik Analiz
Dinamik Analiz
ML Temelli Analiz
Hata ve Güvenlik Açıklıkları
Kaynak kod metrikleri
Mimari analiz
Kodlama standartları
Tersine mühendislik
Fonksiyon çağrılarının izlenmesi
Fonksiyon parametre analizi
Malware Sandbox
SVM
Karar Ağaçları
Rastgele Orman
Naive Bayes
Kümeleme

Faktörler	Statik Analiz	Dinamik Analiz
Zaman	Analiz süresi dinamik analize göre kısadır.	Analiz süresi statik analize göre daha uzundur.
İncelenmeye Konu Olan Kısım	Uygulamanın derlenmiş makine kodunun incelenmesi yeterlidir.	Bellek görüntüleri ve çalışma zamanına ait diğer verilerin de incelenmesi gerekmektedir.
Kaynak Kullanımı	Düşük bellek ve işlemci zamanı yeterli olabilmektedir.	Daha fazla bellek ve işlemci zamanına ihtiyaç duyulur.
Doğruluk	Analiz süreci, dinamik analize göre daha düşük doğruluk, fakat daha yüksek kesinlikte işletilir (düşük false-positive, yüksek false-negative).	Analiz süreci, statik analize göre daha yüksek doğruluk, fakat daha düşük kesinlikle işletilir (düşük false-negative, yüksek false-positive).
Genel Avantajlar	Kodda yer alan zayıflıklar, geliştirilmenin erken safhalarında daha hızlı ve düşük maliyetle tespit edilebilir.	Zayıflıklar, kaynak koda ihtiyaç duymadan uygulamanın çalıştırılması esnasında tespit edilebilir.
Genel Dezavantajlar	Çeşitli karıştırma, şifreleme ve sıkıştırma teknikleriyle kaynak kodun gizlenmesi durumlarında analiz süreci uzayabilir.	Eş zamanlı olarak sadece tek bir kötücül yazılımın analizi yapılabilir.

OWASP Top Ten-Genel

- OWASP İlk 10, geliştiriciler ve web uygulama güvenliği için standart bir farkındalık belgesidir.
- Web uygulamalarına yönelik en kritik güvenlik riskleri hakkında geniş bir fikir birliğini temsil eder.
- ***Geliştiriciler tarafından küresel olarak daha güvenli kodlamaya yönelik ilk adım olarak kabul edilmektedir.***



A01-Bozuk Erişim Kontrolü Saldırıları

- Erişim denetimi, kullanıcıların amaçladıkları izinlerin dışında hareket edemeyecekleri şekilde politika uygular. Başarısızlıklar tipik olarak bilgilerin yetkisiz olarak ifşa edilmesine, tüm verilerin değiştirilmesine veya imha edilmesine veya kullanıcının sınırları dışında bir iş işlevinin gerçekleştirilmesine yol açar. Yaygın erişim denetimi güvenlik açıkları şunları içerir:
  - Erişimin yalnızca belirli yetenekler, roller veya kullanıcılar için verilmesi gerektiği, ancak herkesin kullanımına açık olduğu durumlarda, varsayılan olarak en az ayrıcalık veya reddetme ilkesinin ihlali.
  - URL'yi (parametre kurcalama veya zorla tarama), dahili uygulama durumunu veya HTML sayfasını değiştirerek veya API isteklerini değiştiren bir saldırı aracı kullanarak erişim kontrolü kontrollerini atlamak.
  - Benzersiz tanımlayıcısını (güvenli olmayan doğrudan nesne referansları) sağlayarak başka birinin hesabını görüntülemeye veya düzenlemeye izin verme
  - POST, PUT ve DELETE için eksik erişim denetimleriyle API'ye erişiliyor.

A01-Bozuk Erişim Kontrolü Saldırıları-devam

- Ayrıcalığın yükselmesi. Giriş yapmadan kullanıcı olarak hareket etmek veya kullanıcı olarak giriş yaptığında yönetici olarak hareket etmek.
- Bir JSON Web Simgesi (JWT) erişim kontrol belirtecini veya ayrıcalıkları yükseltmek veya JWT geçersiz kılmayı kötüye kullanmak için manipüle edilen bir çerez veya gizli alanı yeniden oynatmak veya kurcalamak gibi meta veri manipülasyonu.
- CORS yanlış yapılandırması, yetkisiz/güvenilmeyen kaynaklardan API erişimine izin verir.
- Kimliği doğrulanmamış bir kullanıcı olarak kimliği doğrulanmış sayfalara veya standart bir kullanıcı olarak ayrıcalıklı sayfalara göz atmaya zorlayın.

A01-Bozuk Erişim Kontrolü Saldırıları-Güvenlik Çözümleri

- Erişim kontrolü yalnızca, saldırganın erişim kontrolü kontrolünü veya meta verileri değiştiremediği güvenilir sunucu tarafı kodunda veya sunucusuz API'de etkilidir.
  - Genel kaynaklar dışında, varsayılan olarak reddet.
  - Erişim denetimi mekanizmalarını bir kez uygulayın ve Kaynaklar Arası Kaynak Paylaşımı (CORS) kullanımını en aza indirmek dahil olmak üzere uygulama genelinde yeniden kullanın.
  - Model erişim denetimleri, kullanıcının herhangi bir kaydı oluşturabileceğini, okuyabileceğini, güncelleyebileceğini veya silebileceğini kabul etmek yerine kayıt sahipliğini zorunlu kılmalıdır.
  - Benzersiz uygulama iş sınırı gereksinimleri, etki alanı modelleri tarafından uygulanmalıdır.
  - Web sunucusu dizin listesini devre dışı bırakın ve dosya meta verilerinin (ör. .git) ve yedekleme dosyalarının web köklerinde bulunmadığından emin olun.
  - Erişim kontrolü hatalarını günlüğe kaydedin, uygun olduğunda yöneticileri uyarın (ör. tekrarlanan hatalar).
  - Otomatik saldırı araçlarından kaynaklanan zararı en aza indirmek için hız sınırı API'si ve denetleyici erişimi.

A02-Kriptografik Hata Saldırıları

- İlk şey, aktarılan ve bekleyen verilerin koruma ihtiyaçlarını belirlemektir. Örneğin, parolalar, kredi kartı numaraları, sağlık kayıtları, kişisel bilgiler ve ticari sırlar, özellikle bu verilerin AB'nin Genel Veri Koruma Yönetmeliği (GDPR) gibi gizlilik yasaları veya finansal veri koruması gibi düzenlemeler kapsamında olması durumunda ekstra koruma gerektirir. PCI Veri Güvenliği Standardı (PCI DSS) gibi. Tüm bu tür veriler için:
  - Açık metin olarak iletilen herhangi bir veri var mı? Bu, STARTTLS gibi TLS yükseltmelerini kullanan HTTP, SMTP, FTP gibi protokollerle ilgilidir. Harici internet trafiği tehlikelidir. Yük dengeleyiciler, web sunucuları veya arka uç sistemler arasındaki tüm dahili trafiği doğrulayın.
  - Varsayılan olarak veya eski kodda kullanılan herhangi bir eski veya zayıf kriptografik algoritma veya protokol var mı?
  - Varsayılan kripto anahtarları kullanımda mı, zayıf kripto anahtarları mı üretiliyor veya yeniden kullanılıyor veya uygun anahtar yönetimi veya rotasyonu eksik mi? Kripto anahtarları kaynak kodu havuzlarında kontrol ediliyor mu?
  - Şifreleme zorunlu değil mi, örneğin herhangi bir HTTP başlığı (tarayıcı) güvenlik direktifi veya eksik başlık var mı?
  - Alınan sunucu sertifikası ve güven zinciri doğru şekilde doğrulandı mı?
  - Başlatma vektörleri yoksayılıyor mu, yeniden kullanılıyor mu veya kriptografik çalışma modu için yeterince güvenli üretilmiyor mu? ECB gibi güvenli olmayan bir çalışma modu kullanılıyor mu? Kimliği doğrulanmış şifreleme daha uygun olduğunda şifreleme kullanılıyor mu?

A02-Kriptografik Hata Saldırıları

- Bir parola temel anahtar türetme işlevi olmadığında parolalar kriptografik anahtarlar olarak mı kullanılıyor?
- Rastgelelik, kriptografik gereklilikleri karşılamak için tasarlanmamış kriptografik amaçlar için mi kullanılıyor? Doğru işlev seçilse bile, geliştirici tarafından tohumlanması gerekiyor mu ve değilse, geliştirici, yeterli entropi/öngörülemezlikten yoksun bir tohumla yerleşik güçlü tohumlama işlevinin üzerine yazmış mı?
- Kullanımdan kaldırılan MD5 veya SHA1 gibi karma işlevler kullanılıyor mu veya kriptografik karma işlevler gerektiğinde kriptografik olmayan karma işlevler kullanılıyor mu?
- PKCS sayı 1 v1.5 gibi kullanımdan kaldırılmış kriptografik doldurma yöntemleri kullanılıyor mu?
- Kriptografik hata mesajları veya yan kanal bilgileri, örneğin doldurma oracle saldırıları şeklinde istismar edilebilir mi?

A02-Kriptografik Hata Saldırıları-Güvenlik Çözümleri

- Bir uygulama tarafından işlenen, depolanan veya iletilen verileri sınıflandırın. Gizlilik yasalarına, düzenleme gerekliliklerine veya iş gereksinimlerine göre hangi verilerin hassas olduğunu belirleyin.
- Hassas verileri gereksiz yere saklamayın. Mümkün olan en kısa sürede atın veya PCI DSS uyumlu belirteçleştirme ve hatta kesme kullanın. Saklanmayan veriler çalınamaz.
- Bekleyen tüm hassas verileri şifrelediğinizden emin olun.
- Güncel ve güçlü standart algoritmaların, protokollerin ve anahtarların yerinde olduğundan emin olun; uygun anahtar yönetimi kullanın.
- Aktarılan tüm verileri, ileri gizlilik (FS) şifreleri, sunucu tarafından şifre önceliği belirleme ve güvenli parametreler içeren TLS gibi güvenli protokollerle şifreleyin. HTTP Strict Transport Security (HSTS) gibi yönergeleri kullanarak şifrelemeyi zorunlu kılın.

A02-Kriptografik Hata Saldırıları-Güvenlik Çözümleri-devam

- Hassas veriler içeren yanıtlar için önbelleğe almayı devre dışı bırakın.
- Veri sınıflandırmasına göre gerekli güvenlik kontrollerini uygulayın.
- Hassas verileri taşımak için FTP ve SMTP gibi eski protokolleri kullanmayın.
- Argon2, scrypt, bcrypt veya PBKDF2 gibi bir çalışma faktörü (gecikme faktörü) ile güçlü uyarlanabilir ve salted hashing işlevlerini kullanarak parolaları depolayın.
- Başlatma vektörleri çalışma şekline uygun seçilmelidir. Birçok mod için bu, bir CSPRNG (kriptografik olarak güvenli sözde rasgele sayı üreteci) kullanmak anlamına gelir. Nonce gerektiren modlar için başlatma vektörünün (IV) bir CSPRNG'ye ihtiyacı yoktur. Her durumda, IV sabit bir anahtar için asla iki kez kullanılmamalıdır.
- Yalnızca şifreleme yerine her zaman kimliği doğrulanmış şifreleme kullanın.
- Anahtarlar kriptografik olarak rasgele üretilmeli ve bayt dizileri olarak bellekte saklanmalıdır. Bir parola kullanılıyorsa, uygun bir parola temel anahtar türetme işlevi aracılığıyla bir anahtara dönüştürülmesi gerekir.
- Uygun olan yerlerde kriptografik rasgeleliğin kullanıldığından ve öngörülebilir bir şekilde veya düşük entropi ile tohumlanmadığından emin olun. Modern API'lerin çoğu, geliştiricinin güvenliği sağlamak için CSPRNG'yi tohumlamasını gerektirmez.
- MD5, SHA1, PKCS sayı 1 v1.5 gibi kullanımdan kaldırılmış şifreleme işlevlerinden ve dolgu şemalarından kaçının.

A03-Enjeksiyon Saldırıları

- Genel olarak uygulamalar aşağıdaki durumlarda enjeksiyon saldırılarına açıktırlar:
  - Kullanıcı tarafından sağlanan veriler uygulama tarafından doğrulanmaz, filtrelenmez veya temizlenmez.
  - Bağlama duyarlı kaçış olmadan dinamik sorgular veya parametreleştirilmemiş çağrılar doğrudan yorumlayıcıda kullanılır.
  - Düşmanca veriler, ek, hassas kayıtları çıkarmak için nesne ilişkisel eşleme (ORM) arama parametrelerinde kullanılır.
  - Düşmanca veriler doğrudan kullanılır veya birleştirilir. SQL veya komut, dinamik sorgular, komutlar veya saklı yordamlardaki yapıyı ve kötü amaçlı verileri içerir.
- Enjeksiyon saldırılarından bazıları SQL, NoSQL, OS komutu, Nesne İlişkisel Eşleme (ORM), LDAP ve İfade Dili (EL) veya Nesne Grafiği Gezinme Kitaplığı (OGNL) enjeksiyonudur.

A03-Enjeksiyon Saldırıları-Güvenlik Çözümleri

- Kaynak kodun incelenmesi, uygulamaların enjeksiyonlara karşı savunmasız olup olmadığını tespit etmek
- Tüm parametrelerin, başlıkların, URL'lerin, tanımlama bilgilerinin, JSON, SOAP ve XML veri girişlerinin otomatik olarak test edilmesi
- Statik (SAST), dinamik (DAST) ve etkileşimli (IAST) uygulama güvenlik testi araçlarının kullanımı
- Enjeksiyonun önlenmesi, verilerin komutlardan ve sorgulardan ayrı tutulmasını gerektirir:
  - Yorumlayıcıyı tamamen kullanmaktan kaçınan, parametreleştirilmiş bir arayüz sağlayan veya Nesne İlişkisel Eşleme Araçlarına (ORM'ler) geçiş yapan güvenli bir API kullanmak,
  - Pozitif sunucu tarafı giriş doğrulaması kullanımı,
  - Artık dinamik sorgular için, söz konusu yorumlayıcıya özel kaçış sözdizimini kullanarak özel karakterlerden kaçınma,
  - SQL enjeksiyonu durumunda kayıtların toplu olarak ifşa edilmesini önlemek için sorgularda LIMIT ve diğer SQL kontrollerini kullanımı.

A04-Güvenli Olmayan Tasarım Saldırıları

- Güvensiz tasarım, "eksik veya etkisiz kontrol tasarımı" olarak ifade edilen, farklı zayıflıkları temsil eden geniş bir kategoridir. Güvenli olmayan tasarım, diğer tüm İlk 10 risk kategorisinin kaynağı değildir. Güvenli olmayan tasarım ile güvensiz uygulama arasında bir fark vardır. Tasarım kusurları ve uygulama kusurları arasında bir nedenden dolayı ayrım yapıyoruz, bunların farklı temel nedenleri ve iyileştirmeleri var. Güvenli bir tasarım, istismar edilebilecek güvenlik açıklarına yol açan uygulama kusurlarına sahip olabilir. Tanım gereği, güvenli olmayan bir tasarım mükemmel bir uygulama ile düzeltilemez, gerekli güvenlik kontrolleri hiçbir zaman belirli saldırılara karşı savunmak için oluşturulmamıştır. Güvenli olmayan tasarıma katkıda bulunan faktörlerden biri, geliştirilmekte olan yazılım veya sistemin doğasında bulunan iş risk profili oluşturma eksikliği ve dolayısıyla hangi düzeyde güvenlik tasarımının gerekli olduğunun belirlenememesidir.

A04-Güvenli Olmayan Tasarım Saldırıları-Güvenlik Çözümleri

- Güvenlik ve gizlilikle ilgili kontrollerin değerlendirilmesine ve tasarlanmasına yardımcı olmak için AppSec uzmanlarıyla güvenli bir geliştirme yaşam döngüsü oluşturun ve kullanın
- Güvenli tasarım modellerinden veya kullanıma hazır asfalt yollardan oluşan bir kitaplık oluşturun ve kullanın
- Kritik kimlik doğrulama, erişim kontrolü, iş mantığı ve anahtar akışları için tehdit modellemeyi kullanın
- Güvenlik dilini ve kontrollerini kullanıcı hikayelerine entegre edin
- Uygulamanızın her katmanına uygunluk kontrollerini entegre edin (ön uçtan arka uca kadar)
- Tüm kritik akışların tehdit modeline dirençli olduğunu doğrulamak için birim ve entegrasyon testleri yazın. Uygulamanızın her katmanı için kullanım durumlarını ve kötüye kullanım durumlarını derleyin.
- Teşhir ve koruma gereksinimlerine bağlı olarak sistem ve ağ katmanlarındaki katman katmanlarını ayırın
- Tüm katmanlarda tasarım gereği kiracıları güçlü bir şekilde ayırın
- Kullanıcı veya hizmete göre kaynak tüketimini sınırlayın

A05-Güvenlik Yanlış Yapılandırma Saldırıları

- Uygulama şu durumlarda savunmasız olabilir:
  - Uygulama yığınının herhangi bir bölümünde uygun güvenlik sıkılaştırması veya bulut hizmetlerinde yanlış yapılandırılmış izinler eksik.
  - Gereksiz özellikler etkinleştirildi veya yüklendi (ör. gereksiz bağlantı noktaları, hizmetler, sayfalar, hesaplar veya ayrıcalıklar).
  - Varsayılan hesaplar ve parolaları hala etkindir ve değiştirilmemiştir.
  - Hata işleme, kullanıcılara yığın izlerini veya diğer aşırı bilgilendirici hata mesajlarını gösterir.
  - Yükseltilmiş sistemler için en son güvenlik özellikleri devre dışı bırakılır veya güvenli bir şekilde yapılandırılmaz.
  - Uygulama sunucularındaki, uygulama çerçevelerindeki (ör. Struts, Spring, ASP.NET), kitaplıklardaki, veritabanlarındaki vb. güvenlik ayarları güvenli değerlere ayarlanmamıştır.
  - Sunucu, güvenlik üst bilgileri veya yönergeleri göndermez veya bunlar güvenli değerlere ayarlanmamıştır.

A05-Güvenlik Yanlış Yapılandırma Saldırıları-Güvenlik Çözümleri

- Aşağıdakiler de dahil olmak üzere güvenli kurulum süreçleri uygulanmalıdır:
- Tekrarlanabilir sağlamlaştırma süreci, uygun şekilde kilitlenmiş başka bir ortamın konuşlandırılmasını hızlı ve kolay hale getirir. Geliştirme, KG ve üretim ortamlarının tümü, her ortamda kullanılan farklı kimlik bilgileriyle aynı şekilde yapılandırılmalıdır. Yeni bir güvenli ortam oluşturmak için gereken çabayı en aza indirmek için bu süreç otomatikleştirilmelidir.
- Gereksiz özellikler, bileşenler, belgeler ve örnekler içermeyen minimal bir platform. Kullanılmayan özellikleri ve çerçeveleri kaldırın veya yüklemeyin.
- Yama yönetim sürecinin bir parçası olarak tüm güvenlik notlarına, güncellemelerine ve yamalarına uygun yapılandırmaları gözden geçirme ve güncelleme görevi
- Bölümlere ayrılmış bir uygulama mimarisi, bölümlere ayırma, konteynerleştirme veya bulut güvenlik grupları (ACL'ler) ile bileşenler veya kiracılar arasında etkili ve güvenli bir ayrım sağlar.
- İstemcilere güvenlik yönergeleri gönderme, örneğin Güvenlik Başlıkları.
- Tüm ortamlarda yapılandırmaların ve ayarların etkinliğini doğrulamak için otomatikleştirilmiş bir süreç.

A06-Güvenlik Açığı ve Eskimiş Bileşenler Saldırıları

- Kullandığınız tüm bileşenlerin sürümlerini bilmiyorsanız (hem istemci tarafı hem de sunucu tarafı). Bu, doğrudan kullandığınız bileşenleri ve iç içe geçmiş bağımlılıkları içerir.
- Yazılım savunmasızsa, desteklenmiyorsa veya güncel değilse. Buna işletim sistemi, web/uygulama sunucusu, veritabanı yönetim sistemi (DBMS), uygulamalar, API'ler ve tüm bileşenler, çalışma zamanı ortamları ve kitaplıklar dahildir.
- Düzenli olarak güvenlik açıkları taraması yapmıyorsanız ve kullandığınız bileşenlerle ilgili güvenlik bültenlerine abone değilseniz.
- Altta yatan platformu, çerçeveleri ve bağımlılıkları riske dayalı ve zamanında düzeltmez veya yükseltmezseniz. Bu genellikle, yama uygulamalarının değişiklik kontrolü altında aylık veya üç aylık bir görev olduğu ortamlarda olur ve kuruluşları günlerce veya aylarca gereksiz yere sabit güvenlik açıklarına maruz bırakır.
- Yazılım geliştiriciler, güncellenen, yükseltilen veya yama uygulanan kitaplıkların uyumluluğunu test etmezse.

A06-Güvenlik Açığı ve Eskimiş Bileşenler Saldırıları-Güvenlik Çöz.

- Kullanılmayan bağımlılıkları, gereksiz özellikleri, bileşenleri, dosyaları ve belgeleri kaldırın.
- Sürümler, OWASP Bağımlılık Denetimi, retire.js vb. araçları kullanarak hem istemci tarafı hem de sunucu tarafı bileşenlerin (ör. çerçeveler, kitaplıklar) sürümlerini ve bağımlılıklarını sürekli olarak envanterleyin. Ortak Güvenlik Açığı ve Etkilenmeler (CVE) gibi kaynakları sürekli izleyin ve bileşenlerdeki güvenlik açıkları için Ulusal Güvenlik Açığı Veritabanı (NVD). Süreci otomatikleştirmek için yazılım kompozisyon analizi araçlarını kullanın. Kullandığınız bileşenlerle ilgili güvenlik açıkları için e-posta uyarılarına abone olun.
- Bileşenleri yalnızca güvenli bağlantılar üzerinden resmi kaynaklardan edinin. Değiştirilmiş, kötü niyetli bir bileşen içerme olasılığını azaltmak için imzalı paketleri tercih edin (Bkz. A08:2021-Yazılım ve Veri Bütünlüğü Hataları).
- Bakımsız olan veya eski sürümler için güvenlik yamaları oluşturmayan kitaplıkları ve bileşenleri izleyin. Düzeltme eki uygulamak mümkün değilse, keşfedilen sorunu izlemek, algılamak veya bunlara karşı koruma sağlamak için sanal bir yama uygulamayı düşünün.

A07-Tanımlama ve Kimlik Doğrulama Hataları Saldırıları

- Kullanıcının kimliğinin, kimlik doğrulamasının ve oturum yönetiminin doğrulanması, kimlik doğrulamayla ilgili saldırılara karşı korunmak için kritik öneme sahiptir. Uygulama şu durumlarda kimlik doğrulama zayıflıkları olabilir:
  - Saldırganın geçerli kullanıcı adları ve parolalardan oluşan bir listeye sahip olduğu kimlik bilgileri doldurma gibi otomatik saldırılara izin verir.
  - Kaba kuvvete veya diğer otomatik saldırılara izin verir.
  - "Password1" veya "admin/admin" gibi varsayılan, zayıf veya iyi bilinen parolalara izin verir.
  - Güvenli hale getirilemeyen "bilgiye dayalı yanıtlar" gibi zayıf veya etkisiz kimlik bilgisi kurtarma ve parola unuttum işlemleri kullanır.
  - Düz metin, şifrelenmiş veya zayıf şekilde hashlenmiş şifre veri depoları kullanır
  - Eksik veya etkisiz çok faktörlü kimlik doğrulaması var.
  - URL'de oturum tanımlayıcısını gösterir.
  - Başarılı oturum açtıktan sonra oturum tanımlayıcısını yeniden kullanın.
  - Oturum Kimliklerini doğru şekilde geçersiz kılmaz. Kullanıcı oturumları veya kimlik doğrulama belirteçleri (esas olarak çoklu oturum açma (SSO) belirteçleri), oturum kapatma veya etkinlik dışı kalma süresi sırasında uygun şekilde geçersiz kılınmaz.

A07-Tanımlama ve Kimlik Doğrulama Hataları Saldırıları-Güvenlik Ç.

- Otomatik kimlik bilgisi doldurma, kaba kuvvet ve çalınan kimlik bilgilerinin yeniden kullanım saldırılarını önlemek için mümkün olduğunda çok faktörlü kimlik doğrulaması uygulayın.
- Özellikle yönetici kullanıcılar için herhangi bir varsayılan kimlik bilgisi ile göndermeyin veya dağıtmayın.
- Yeni veya değiştirilmiş parolaları en kötü 10.000 parola listesine göre test etmek gibi zayıf parola kontrolleri uygulayın.
- Ezberlenmiş Sırlar veya diğer modern, kanıta dayalı parola ilkeleri için bölüm 5.1.1'deki Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) 800-63b yönergeleriyle parola uzunluğu, karmaşıklığı ve rotasyon ilkelerini hizalayın.
- Tüm sonuçlar için aynı mesajları kullanarak kayıt, kimlik bilgisi kurtarma ve API yollarının hesap numaralandırma saldırılarına karşı güçlendirildiğinden emin olun.
- Başarısız oturum açma girişimlerini sınırlayın veya giderek geciktirin, ancak bir hizmet reddi senaryosu oluşturmamaya dikkat edin. Tüm hataları günlüğe kaydedin ve kimlik bilgileri doldurma, kaba kuvvet veya diğer saldırılar algılandığında yöneticileri uyarın.
- Oturum açtıktan sonra yüksek entropili yeni bir rasgele oturum kimliği oluşturan, sunucu taraflı, güvenli, yerleşik bir oturum yöneticisi kullanın. Oturum tanımlayıcısı URL'de olmamalı, güvenli bir şekilde saklanmalı ve oturum kapatma, boşta kalma ve mutlak zaman aşımlarından sonra geçersiz kılınmalıdır.

A08-Yazılım ve Veri Bütünlüğü Hataları Saldırıları

- Yazılım ve veri bütünlüğü hataları, bütünlük ihlallerine karşı koruma sağlamayan kod ve altyapı ile ilgilidir. Buna bir örnek, bir uygulamanın güvenilmeyen kaynaklardan, havuzlardan ve içerik dağıtım ağlarından (CDN'ler) gelen eklentilere, kitaplıklara veya modüllere dayanmasıdır. Güvenli olmayan bir CI/CD ardışık düzeni, yetkisiz erişim, kötü amaçlı kod veya sistemin tehlikeye girmesi olasılığını ortaya çıkarabilir. Son olarak, artık birçok uygulama, güncellemelerin yeterli bütünlük doğrulaması olmadan indirildiği ve daha önce güvenilir olan uygulamaya uygulandığı otomatik güncelleme işlevini içerir. Saldırganlar, dağıtılmak ve tüm kurulumlarda çalıştırılmak üzere potansiyel olarak kendi güncellemelerini yükleyebilir. Başka bir örnek, nesnelerin veya verilerin bir saldırganın görebileceği ve değiştirebileceği bir yapıya kodlandığı veya seri hale getirildiği, güvenli olmayan seri durumdan çıkarmaya karşı savunmasız olduğu durumdur.

A08-Yazılım ve Veri Bütünlüğü Hataları Saldırıları-Güvenlik Ç.

- Yazılımın veya verilerin beklenen kaynaktan olduğunu ve değiştirilmediğini doğrulamak için dijital imzalar veya benzer mekanizmalar kullanın.
- Npm veya Maven gibi kitaplıkların ve bağımlılıkların güvenilir depoları kullandığından emin olun. Daha yüksek bir risk profiliniz varsa, iyi olduğu bilinen ve incelenmiş dahili bir havuz barındırmayı düşünün.
- Bileşenlerin bilinen güvenlik açıkları içermediğini doğrulamak için OWASP Dependency Check veya OWASP CycloneDX gibi bir yazılım tedarik zinciri güvenlik aracının kullanıldığından emin olun
- Kötü amaçlı kod veya yapılandırmanın yazılım ardışık düzeninize dahil edilme olasılığını en aza indirmek için kod ve yapılandırma değişiklikleri için bir inceleme süreci olduğundan emin olun.
- Derleme ve devreye alma süreçlerinde akan kodun bütünlüğünü sağlamak için CI/CD işlem hattınızın uygun ayırma, yapılandırma ve erişim kontrolüne sahip olduğundan emin olun.
- İmzasız veya şifrelenmemiş seri hale getirilmiş verilerin, seri hale getirilmiş verilerin kurcalanmasını veya yeniden oynatılmasını algılamak için bir tür bütünlük kontrolü veya dijital imza olmadan güvenilmeyen istemcilere gönderilmediğinden emin olun

A09-Güvenlik Kaydı ve İzleme Hataları Saldırıları

- Yetersiz log kaydı, algılama, izleme ve etkin yanıt her zaman oluşur:
  - Oturum açma, başarısız oturum açma ve yüksek değerli işlemler gibi denetlenebilir olaylar günlüğe kaydedilmez.
  - Uyarılar ve hatalar, hiç, yetersiz veya net olmayan günlük mesajları oluşturur.
  - Uygulamaların ve API'lerin günlükleri şüpheli etkinlik açısından izlenmez.
  - Günlükler yalnızca yerel olarak depolanır.
  - Uygun uyarı eşikleri ve yanıt yükseltme süreçleri yerinde veya etkili olmadığında.
  - Sızma testi ve dinamik uygulama güvenlik testi (DAST) araçları (OWASP ZAP gibi) tarafından yapılan taramalar alarmları tetiklemediğinde.
  - Uygulama, gerçek zamanlı veya neredeyse gerçek zamanlı olarak etkin saldırıları algılayamaz, artıramaz veya uyaramaz.

A09-Güvenlik Kaydı ve İzleme Hataları Saldırıları-Güvenlik Ç.

- Geliştiriciler, uygulamanın riskine bağlı olarak aşağıdaki kontrollerin bir kısmını veya tamamını uygulamalıdır:
  - Tüm oturum açma, erişim kontrolü ve sunucu tarafı giriş doğrulama hatalarının, şüpheli veya kötü amaçlı hesapları belirlemek için yeterli kullanıcı bağlamıyla günlüğe kaydedilebildiğinden ve gecikmeli adli tıp analizine izin verecek kadar uzun süre tutulabildiğinden emin olun.
  - Günlüklerin, günlük yönetimi çözümlerinin kolayca tüketebileceği bir biçimde oluşturulduğundan emin olun.
  - Günlük kaydı veya izleme sistemlerine enjeksiyonları veya saldırıları önlemek için günlük verilerinin doğru şekilde kodlandığından emin olun.
  - Yüksek değerli işlemlerin, yalnızca eklenen veritabanı tabloları veya benzeri gibi kurcalamayı veya silinmeyi önlemek için bütünlük denetimleriyle bir denetim izine sahip olduğundan emin olun.
  - DevSecOps ekipleri, şüpheli etkinliklerin hızlı bir şekilde algılanması ve yanıtlanması için etkili izleme ve uyarı oluşturmalıdır.
  - Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) 800-61r2 veya üstü gibi bir olay müdahale ve kurtarma planı oluşturun veya benimseyin.

A10-Sunucu Tarafı İstek Sahtekarlığı Saldırıları

- Bir web uygulaması, kullanıcı tarafından sağlanan URL'yi doğrulamadan uzak bir kaynağı getirdiğinde SSRF kusurları oluşur. Bir saldırganın, bir güvenlik duvarı, VPN veya başka türde bir ağ erişim kontrol listesi (ACL) tarafından korunuyor olsa bile, uygulamayı beklenmedik bir hedefe hazırlanmış bir istek göndermeye zorlamasına olanak tanır.
- Modern web uygulamaları, son kullanıcılara uygun özellikler sağladığından, bir URL'nin getirilmesi yaygın bir senaryo haline gelir. Sonuç olarak, SSRF insidansı artmaktadır. Ayrıca, bulut hizmetleri ve mimarilerin karmaşıklığı nedeniyle SSRF'nin ciddiyeti de artmaktadır.

A10-Sunucu Tarafı İstek Sahtekarlığı Saldırıları-Güvenlik Ç.

- Geliştiriciler, aşağıdaki ayrıntılı savunma kontrollerinin bir kısmını veya tamamını uygulayarak SSRF'yi önleyebilir:
- ***Ağ Katmanı üzerinden;***
  - SSRF'nin etkisini azaltmak için uzaktan kaynak erişimi işlevselliğini ayrı ağlarda bölümlere ayırın
  - Temel intranet trafiği dışında tüm trafiği engellemek için "varsayılan olarak reddet" güvenlik duvarı politikalarını veya ağ erişim denetimi kurallarını uygulayın.
- ***Uygulama Katmanı üzerinden;***
  - İstemci tarafından sağlanan tüm girdi verilerini sterilize edin ve doğrulayın
  - Olumlu bir izin verilenler listesiyle URL şemasını, bağlantı noktasını ve hedefi zorunlu kılın
  - İstemcilere ham yanıtlar göndermeyin
  - HTTP yönlendirmelerini devre dışı bırak
  - DNS yeniden bağlama ve "zaman kontrolü, kullanım zamanı" (TOCTOU) yarış koşulları gibi saldırılardan kaçınmak için URL tutarlılığının farkında olun

Windows PC ve Sunucular Üzerindeki Sıkılaştırmalar

S.Nu	Alınacak Tedbir
1	Microsoft'tan en son hizmet paketlerini ve düzeltmeleri yükleyin.
2	Yama kullanılabilirliğinin otomatik olarak bildirilmesini etkinleştirin.
3	Minimum parola uzunluğunu ayarlayın.
4	Parola karmaşıklığı gereksinimlerini etkinleştirin.
5	Tersine şifreleme kullanarak parolaları saklamayın. (Varsayılan)
6	Hesap kilitleme ilkesini yapılandırın.
7	Bu bilgisayara ağdan erişme yeteneğini şu şekilde kısıtlayın: Yöneticiler ve Kimliği Doğrulanmış Kullanıcılar.
8	Hiçbir kullanıcıya 'işletim sisteminin bir parçası olarak hareket etme' hakkı vermeyin. (Varsayılan)
9	Yerel oturum açma erişimini Yöneticilerle sınırlayın.
10	Konuk hesaplarının bir hizmet, batch iş olarak yerel olarak veya RDP aracılığıyla oturum açma yeteneğini reddedin.
11	Oturum açılırken, mesaj başlığına uyarı metni yerleştirin.
12	Kullanıcıların Microsoft hesapları oluşturmasına ve bu hesaplarla oturum açmasına izin vermeyin.

Windows PC ve Sunucular Üzerindeki Sıkılaştırmalar-devam

S.Nu	Alınacak Tedbir
13	Konuk hesabını devre dışı bırakın. (Varsayılan)
14	Etkileşimli oturum açma işlemleri için Ctrl+Alt+Del gerektirin. (Varsayılan)
15	Boşta kalan interaktif oturumları korumak için makine hareketsizlik sınırını yapılandırın.
16	Microsoft Ağ İstemcisini her zaman iletişimler için dijital olarak imzalayacak şekilde yapılandırın.
17	Şifrelenmemiş parolaların üçüncü taraf SMB sunucusuna gönderilmesini devre dışı bırakın.
18	Microsoft Network Server'ı her zaman iletişimler için dijital olarak imzalayacak şekilde yapılandırın.
19	Anonim SID/Ad çevirisini devre dışı bırakın. (Varsayılan)
20	SAM hesaplarının isimsiz numaralandırılmasına izin vermeyin. (Varsayılan)
21	SAM hesaplarının ve paylaşımlarının anonim olarak numaralandırılmasına izin vermeyin.
22	Anonim izinlerinin tüm kullanıcılara uygulanmasına izin vermeyin. (Varsayılan
23	Adlandırılmış kanallara anonim olarak erişilmesine izin vermeyin.
24	Anonim erişimi, adlandırılmış kanallara ve paylaşımlara kısıtlayın.

Windows PC ve Sunucular Üzerindeki Sıkılaştırmalar-devam

S.Nu	Alınacak Tedbir
25	Hiçbir paylaşıma anonim olarak erişilmesine izin vermeyin.
26	Yerel hesaplar için "Klasik" paylaşım ve güvenlik modelini zorunlu kılın.
27	Yerel Sistemin NTLM için bilgisayar kimliğini kullanmasına izin verin.
28	Yerel Sistem NULL oturum geri dönüşünü devre dışı bırakın.
29	Kerberos için izin verilen şifreleme türlerini yapılandırın.
30	LAN Manager hash değerlerini saklamayın.
31	LAN Manager kimlik doğrulama düzeyini yalnızca NTLMv2'ye izin verecek şekilde ayarlayın ve LM ve NTLM'yi reddedin.
32	Tüm profillerde (etki alanı, özel, genel) Windows Güvenlik Duvarını etkinleştirin.
33	Gelen trafiği engellemek için tüm profillerde Windows Güvenlik Duvarı'nı yapılandırın varsayılan olarak.
34	Uzaktan erişim hizmetlerini (VNC, RDP, vb.) yalnızca yetkili kuruluş ağlarına sadece VPN ile izin verecek şekilde yapılandırın.
35	Güvenli kanal verilerini (her zaman) dijital olarak şifreleyin veya imzalayın.
36	Boşta kalan interaktif oturumları korumak için makine hareketsizlik sınırını yapılandırın.

Windows PC ve Sunucular Üzerindeki Sıkılaştırmalar-devam

S.Nu	Alınacak Tedbir
37	Önbelleğe alınacak önceki oturum açma sayısını yapılandırın.
38	Hesap Oturum Açma denetim ilkesini yapılandırın.
39	Hesap Yönetimi denetim ilkesini yapılandırın.
40	Oturum Açma/Oturum Kapatma denetim ilkesini yapılandırın.
41	İlkeyi Yapılandır Denetim ilkesini ve Ayrıcalığı Kullan denetim ilkesini değiştirin.
42	Olay Günlüğü tutma yöntemini ve boyutunu yapılandırın.
43	Log gönderimini yapılandırın (örn. Splunk'a).
44	Kullanılmayan hizmetleri devre dışı bırakın veya kaldırın.
45	Kullanıcı haklarını olabildiğince güvenli olacak şekilde yapılandırın: ‘En Az Ayrıcalık’ ilkesini uygulayın.
46	Tüm birimlerin NTFS dosya sistemini kullandığından emin olun.
47	Dosya sistemini ve kayıt defteri izinlerini yapılandırın.
48	Gerekli değilse uzaktan kayıt defteri erişimine izin vermeyin.

Windows PC ve Sunucular Üzerindeki Sıkılaştırmalar-devam

S.Nu	Alınacak Tedbir
49	Sistem tarihini/saatini ayarlayın ve senkronize olacak şekilde yapılandırın.
50	Casus yazılım önleme ve virüsten koruma yazılımı yükleyin, etkinleştirin ve günlük güncelleyin.
51	Anti-virüs yazılımını günlük olarak güncellenecek şekilde yapılandırın.
52	Gizli (kategori-I) Veriler için gerektiği şekilde güvenli depolama sağlayın. Güvenlik, aşağıdakiler gibi, ancak bunlarla sınırlı olmamak üzere, sağlanabilir: şifreleme, erişim kontrolleri, dosya sistemi denetimleri, depolama ortamı veya uygun görülen herhangi bir kombinasyonu.
53	İşletim sisteminin kritik dosya yapısının bütünlüğünü kontrol etmek için yazılım yükleyin.
54	RDP kullanılıyorsa, RDP bağlantı şifreleme düzeyini yüksek olarak ayarlayın.

Linux PC ve Sunucular Üzerindeki Sıkılaştırmalar

S.Nu	Alınacak Tedbir
1	Paket listenizi güncelleyin ve işletim sisteminizi yükseltin.
2	Gereksiz paketleri kaldırın.
3	Karındeşen (Ripper) John ile zayıf parolaları tespit edin.
4	Hiçbir hesabın boş şifresi olmadığını doğrulayın.
5	Parola kuralları belirleyin.
6	Login.defs'de parola süresinin dolmasını ayarlayın.
7	USB aygıtlarını devre dışı bırakın (başlıksız sunucular için).
8	Önyükleme sırasında hangi hizmetlerin başlatıldığını kontrol edin.
9	Tüm yazılabilir dosyaları kontrol edin.
10	Yaygın saldırıları engellemek için iptables'ı yapılandırın.
11	GRUB önyükleyici parolasını ayarlayın.
12	Açılışta etkileşimli kısayol tuşu başlatmayı devre dışı bırakın.

Linux PC ve Sunucular Üzerindeki Sıkılaştırmalar-devam

S.Nu	Alınacak Tedbir
13	Paket listenizi güncelleyin ve işletim sisteminizi yükseltin.
14	Okuma/yazma olaylarını kontrol etmek için denetlenmeyi etkinleştirin.
15	Tüm Apache sunucularını güvenli hale getirin.
16	UFW'yi yükleyin ve yapılandırın.
17	SSH'yi güvenli bir şekilde yapılandırın.
18	Telnet’i etkisizleştirin.
19	sysctl'yi güvenli bir şekilde yapılandırın.
20	Fail2Ban ile başarısız denemelerden sonra kullanıcı hesaplarını kilitleyin.
21	Root kullanıcı zaman aşımını yapılandırın.
22	netstat ile gizli açık portları kontrol edin.
23	Çekirdek sistem dosyaları için kök izinlerini ayarlayın.
24	Rootkit'leri tarayın.

Linux PC ve Sunucular Üzerindeki Sıkılaştırmalar-devam

S.Nu	Alınacak Tedbir
25	Hassas olay günlüğü uyarıları için kapatma modunun etkinleştirildiğini kontrol edin.
26	Tüm olay günlüğü verilerinin güvenli bir şekilde yedeklenip yedeklenmediğini kontrol edin.
27	Olay günlüğü izleme sürecini değerlendirin.
28	Şüpheli koşullar altında oturum açan tüm kullanıcıları izleyin.
29	Uzaktan erişim günlüklerini düzenli olarak kontrol edin.
30	Şüpheli hesap ayrıcalıklarının geçici olarak dondurulduğundan emin olun.
31	Sunucu yapılandırma kontrol sürecini değerlendirin.
32	Herhangi bir yazılım için hizmet paketlerini ve yamaları güncelleyin.
33	Olay günlüğü izlemenin doğru şekilde yapılandırıldığını kontrol edin.
34	Tüm kullanıcı hesabı girişlerinin kaydedildiğini kontrol edin.
35	Tüm sistem yapılandırma değişikliklerinin kaydedildiğini kontrol edin.
36	Sistem konfigürasyonlarını değiştirmek için yürürlükte olan bir süreç olduğundan emin olun.

Linux PC ve Sunucular Üzerindeki Sıkılaştırmalar-devam

S.Nu	Alınacak Tedbir
37	Başlatma işlemlerinin doğru yapılandırıldığından emin olun.
38	Gereksiz başlangıç işlemlerini kaldırın.
39	Normal kullanıcıların sistem başlangıç yapılandırmasını değiştirememesini sağlayın.
40	Kullanılmayan yazılım ve hizmetleri kaldırın.
41	Tam sistem anti-virüs taraması çalıştırın.
42	Sunucu güvenlik duvarı güvenlik ayarlarınızı gözden geçirin ve her şeyin uygun şekilde yapılandırıldığından emin olun.
43	Son 3 ay içinde etkin olmayan tüm kullanıcı hesaplarını kaldırın.
44	Hem yönetici grubu hem de süper yönetici grubu mümkün olduğunca az üye ile kısıtlanmıştır. Bundan emin olun.