Necmettin Erbakan Üniversitesi

Bilgi Güvenliği
2022-2023 Güz Dönemi

Dr. Alperen Eroğlu
aeroglu@erbakan.edu.tr

Hafta-13

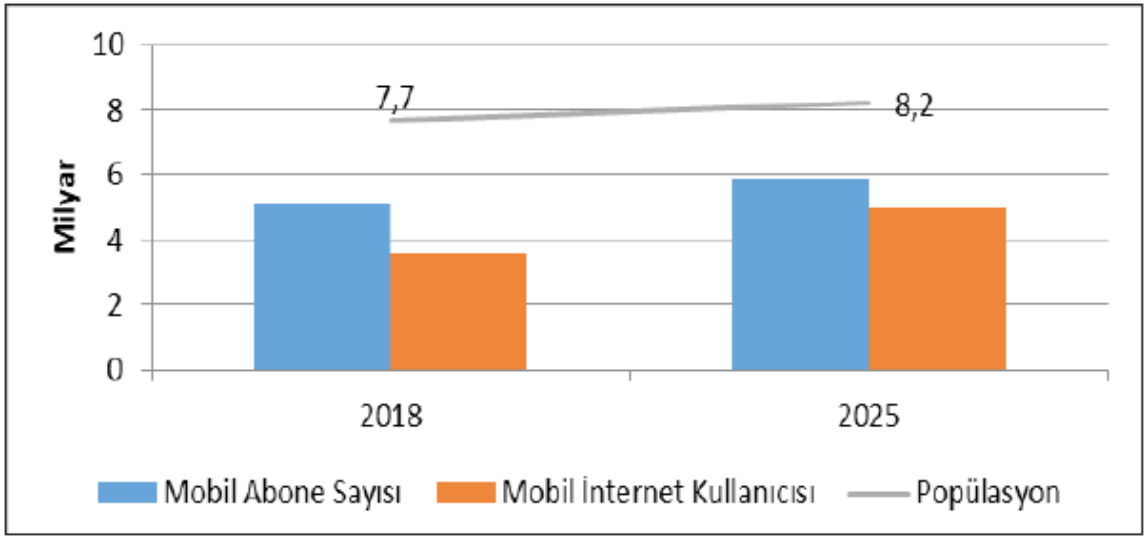
Mobil Cihazlar ve Web Uygulama Zafiyetleri Ve Önlemler, Yazılım Tanımlı Ağlar (SDN) ve Siber Güvenlik

https://fordefence.com/

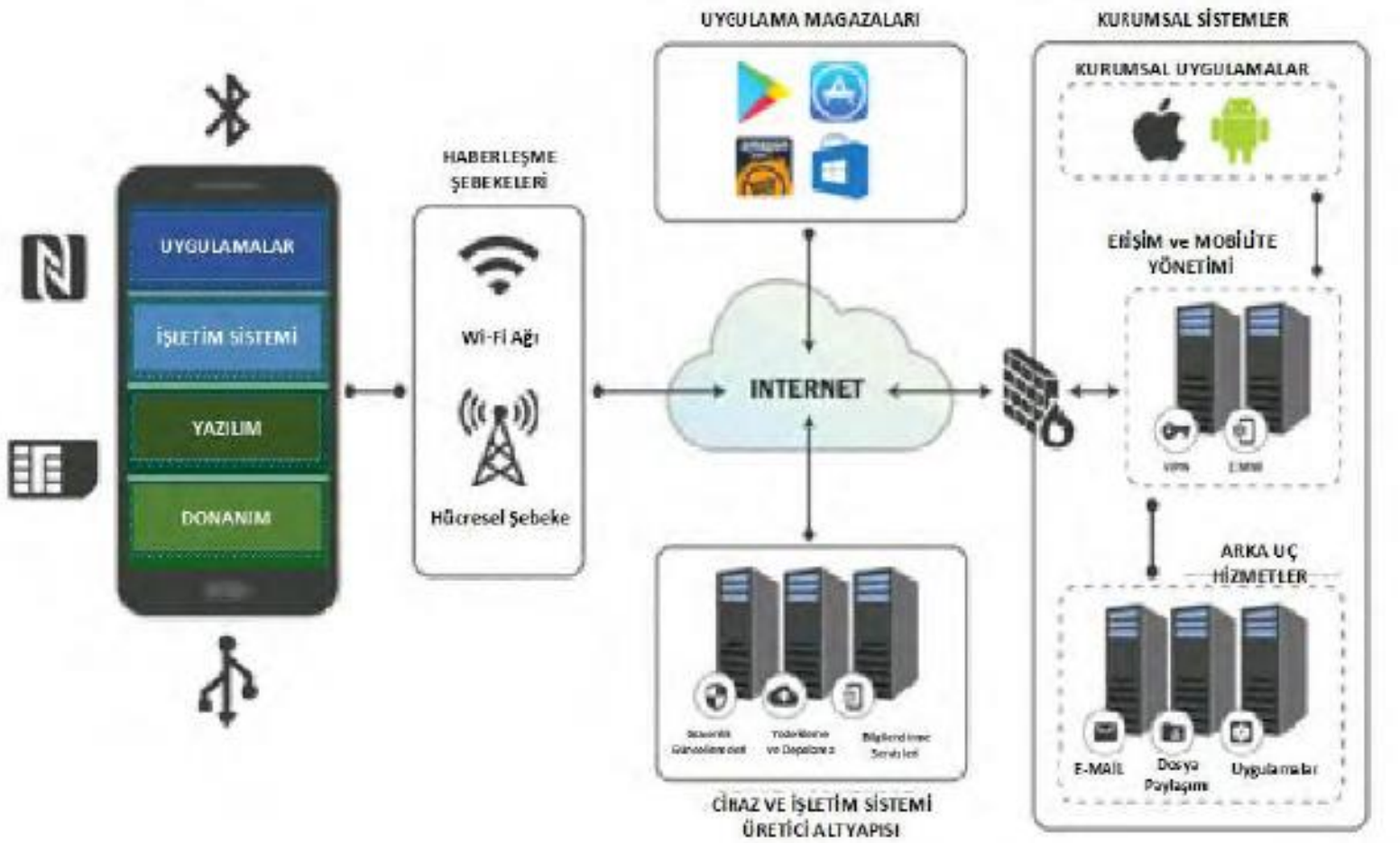
Hafta-13

Mobil Cihazlarda Siber Güvenlik

- Dünyada kullanılan mobil cihazların %76,88'i android, %20,38'i ise iOS işletim sistemi kullanmaktadır. Geriye kalan %1,23'lük kısımda ise kullanılan işletim sistemi bilinmemektedir.
- Cihaz üreticileri açısından küresel piyasadaki son duruma bakıldığında, 2018 ikinci çeyrek akıllı cihaz satış rakamlarının %20,9'unu Samsung, %15,8'ini Huawei, %12,1'ini Apple, %9,3'ünü Xiaomi, %8,6'sını OPPO ve geri kalan %33,2'lik kısmını ise diğerleri oluşturmaktadır.
- Dünya genelinde uygulama marketlerinde bulunan uygulamaları indirme sayısı 2018 yılı itibariyle 200 milyarı geçmiştir. Uygulama indirme sayısının 2022 yılında 250 milyarı geçmesi beklenmektedir.
- Akıllı telefon kullanımında artış ile birlikte, mobil uygulama kullanımı da önemli artışlar göstermiştir.



Mobil Cihazlarda Siber Güvenlik



Mobil ekosistem

Mobil Cihazlarda Siber Güvenlik

Mobil cihazlarda bulunan arayüzler

Mobil Cihazlarda Siber Güvenlik

Tür	Tanımlama	Örnekler
Trojan	Yasal uygulamalar gibi davranan programlardır.	Android.Pjapps Trojan, Rogue apps, Hydraq
Virüs	Yerleştiği bilgisayardaki veya mobil cihazdaki dosyalara zarar veren, kendini kopyalama yeteneğine sahip yazılımlardır.	Stuxnet
Botnet	Siber saldırganlar tarafından bilgisayarları kontrol etmek ve gerektiğinde farklı sistemlere saldırı düzenlemek amacıyla kullanılan yazılımlardır. Mobil cihazlardaki sosyal medya uygulamaları botnetler için yeni bir ortam sağlamaktadır.	Opt-in botnet, Aurora botnet, Rustock
Toolkit	Network tabanlı yaygın saldırılar yapmak için kullanılan yazılımlardır.	Phoenix toolkit
Kötücül Reklam (Malvertising)	Sahte internet siteleri ile bağlantılı özgün görünen reklamlardır.	TweetMeme gibi sosyal medya uygulamalarında kullanılan kötücül reklamlar.
Solucan	Mobil şebekelerde havadan yayılabilen ve kendi kendini çoğaltabilen kötücül programlar.	iPhoneOS.Ikee.B, iPhoneOS. Ikee

Akıllı telefonları hacklemekte kullanılan kötücül yazılımlar

Mobil Cihazlarda Siber Güvenlik

Mobil tehditler: fiziksel, ağ tabanlı, sistem tabanlı ve uygulama tabanlı olmak üzere farklı kategorilere ayrılabilir!

Fiziksel Tehditler: mobil cihazın kaybolması veya çalınması durumunda ortaya çıkmaktadır.

Özellikle mobil cihazların çalınması veya kaybolması durumunda kötü niyetli kişiler tarafında kullanımının engellenmesi amacıyla IMEI bloklama yöntemi kullanılmaktadır. IMEI bloklama yönteminde kaybolan veya çalınan cihaza ait IMEI numarası, hizmet alınan mobil işletmeci tarafından iletişime kapatılmaktadır.

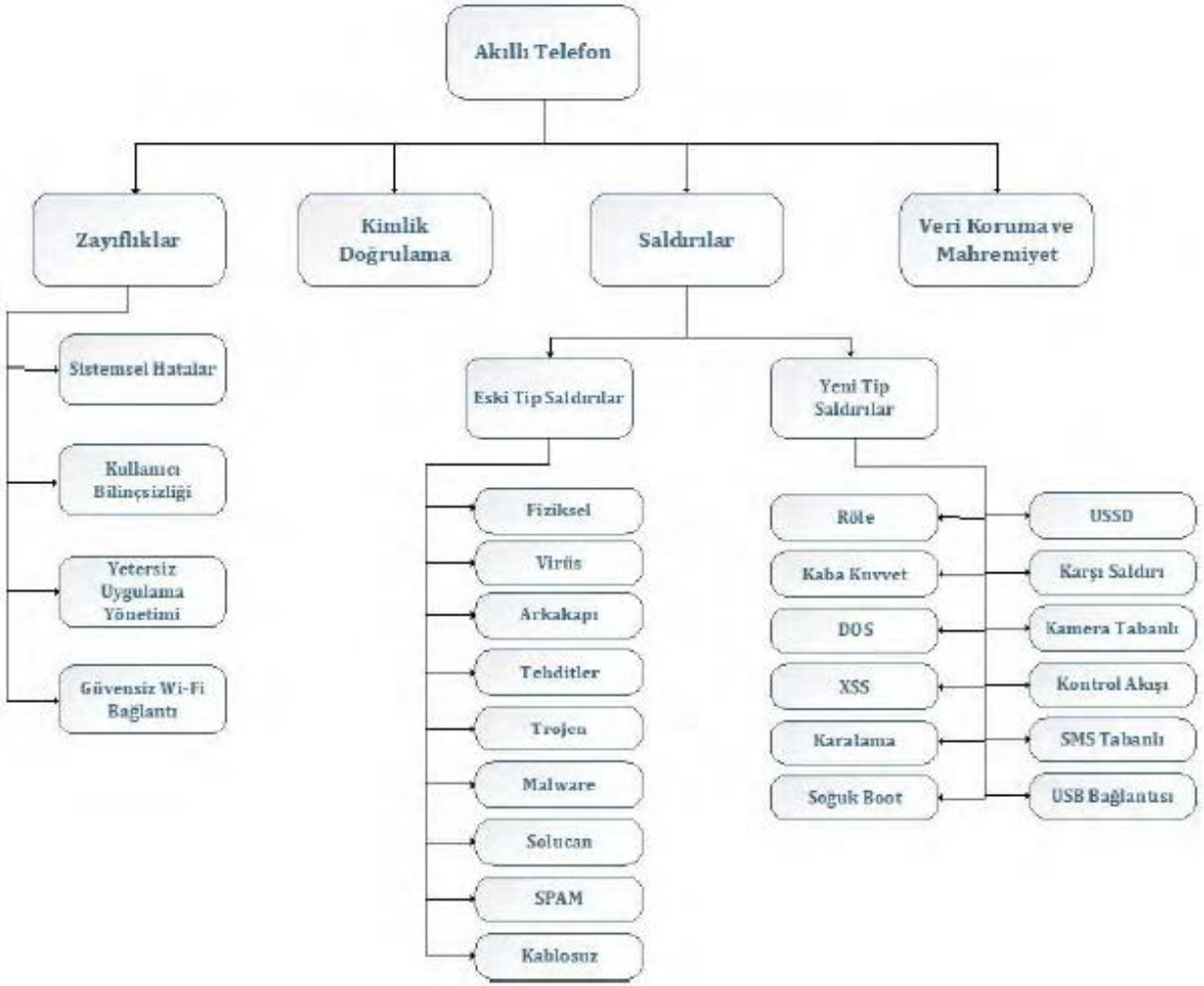
https://www.trhaber.com/bilim-teknoloji/ikinci-el-cihaz-alanlar-dikkat-evraklarinizi-unutmayin-h20990.html

Ağ tabanlı tehditler: Mobil cihazlarda genellikle bağlantı için Wi-Fi veya bluetooth kullanılmaktadır. Bu arayüzlerin her biri kendi kalıtımsal açıklıklarına sahiptir ve Wifite veya Aircrack-ng Suite gibi araçlar kullanılarak gizli dinleme yapılmaya karşı hassastırlar. Kullanıcılar, WPA2 veya daha iyi ağ güvenlik protokolleri kullanarak sadece güvenilen ağlara bağlanmalıdır.

Sistem tabanlı tehditler: Cihaz üreticileri bazen istemeden de olsa cihazları zayıf noktaları ile birlikte üretmektedir. Örneğin, Samsung Android cihazlarda kullanılan SwiftKey gizli dinleme girişimlerine karşı korumasız bulunmuştur. Benzer şekilde, Apple cihazlarda kullanılan iOS'da da kritik açıklıklar vardır. No iOS Zone zayıf noktası, kapsama alanında bulunan iOS cihazlara otomatik olarak bağlanmakta ve cihazı kullanım dışı bırakmaktadır

Uygulama tabanlı tehditler: Sistem açıklıklarına benzer şekilde, cihaz üzerinde yüklü olan üçüncü parti uygulamalar güncelliğini yitirmiş olabilmektedir. Bazı uygulama geliştiricileri zamanında uygulamaların güncel sürümlerini yayınlamazlar. Bazen de kullanıcılar uygulamaları güncellemeyi ihmal etmektedirler. Güncel olmayan uygulamaların kullanımı bu uygulamalardaki zayıf noktaların siber saldırganlar tarafından istismar edilmesi riskini artırmaktadır.

Mobil Cihazlarda Siber Güvenlik



Akıllı cihaz güvenlik riskleri

Mobil Cihazlarda Siber Güvenlik

- Kaspersky Lab araştırmacıları tarafından litetatürde Cabir adı verilen ilk mobil kötücül yazılım 2004 yılında tespit edilmiştir.
- Cabir, dönemin en popüler Symbian işletim sistemine sahip cep telefonlarını hedef almıştır.
- Cabir bir kez telefona bulaştığında, “Caribe” kelimesi telefon her açıldığında telefon ekranında görüntülenmekteydi. Bu solucan bluetooth iletişimi açıklık olan diğer telefonlara kendini kopyalayabilme özelliğine sahipti.
- Aslında, Cabir kötücül bir yazılım değildi, ancak sonradan Cabir’in kullanmış olduğu yöntem siber saldırganlar tarafından siber saldırı amacıyla kullanıldığından mobil telefonlara yönelik ilk solucan olarak kabul edilmektedir

- 2005 yılında, Cabir'in kullandığı yöntemi kullanan Commwarrior adında yeni bir kötücül yazılım ortaya,
- 2006 yılında, RedBrowser Commwarrior'un yapısını geliştirerek java üzerinde çalışabilen çoklu mobil platformlara bulaşabilen ilk trojan,
- 2007 yılında ortaya çıkan FlexiSpy, mobil cihazlarda casusluk amacıyla kullanılan ilk kötücül yazılımlardandır,
- 2007 yılında ilk jenerasyon iPhone telefonlar piyasaya çıktıktan sonra, iOS'a yönelik kötücül yazılımlar da ortaya çıkmaya başlamıştır. 2009'da IKee solucanı jailbreak yapılmış iPhone telefonlara bulaşarak telefonların duvar kağıdını solucanı yazan yazılımcının fotoğrafı ile değiştirmiştir

Yeni tip saldırılar ve önlemler

Saldırı Adı	Zayıf noktalar	Çözüm	Etki
Röle saldırısı	Güvensiz ağ ortamı, yetkisiz Proxy servislerinin kullanımı	Güvenli ağların ve Proxy uygulamalarının kullanımı.	İletişim sırasında bilgilerin ele geçirilmesi (hacklenmesi)
Cold Boot saldırısı	RAM ve şifreleme/şifre çözme anahtarlarına yetkisiz erişim.	Anahtar verilerini RAM yerine chip üzerinde tutan sistemlerin kullanımı. Güçlü şifreleme ve şifre çözme yöntemlerinin kullanılması.	Şifreleme anahtarı ele geçirilebilir (hacklenebilir). Bilgi güvenliğini zayıflatır.
Kaba kuvvet saldırısı	Telefon parolasının kırılması için parola kombinasyonlarının ardı ardına denenmesi.	Parola denemesine limit konulması.	Parolanın kırılması, CPU hızının düşmesi
Smudge saldırısı	Dokunmatik ekranın kirli veya yağlı elle tutulması.	Cihazın ekranının temiz tutulması ve temiz elle cihaz dokunulması.	Parola paterninin kolaylıkla tahmin edilmesi.
DoS saldırısı	Diğer cihazların kullanımı ile mobil geniş band bağlantının düşürülmesi. Sahte Wifi bağlantısı ile bağlanma.	İnternet erişim yetkilendirme protokolü kullanımı.	Ağın meşgul olması. Akıllı telefonun meşgul edilmesi ve hizmetlerin bloklanması.

Mobil Cihazlarda Siber Güvenlik

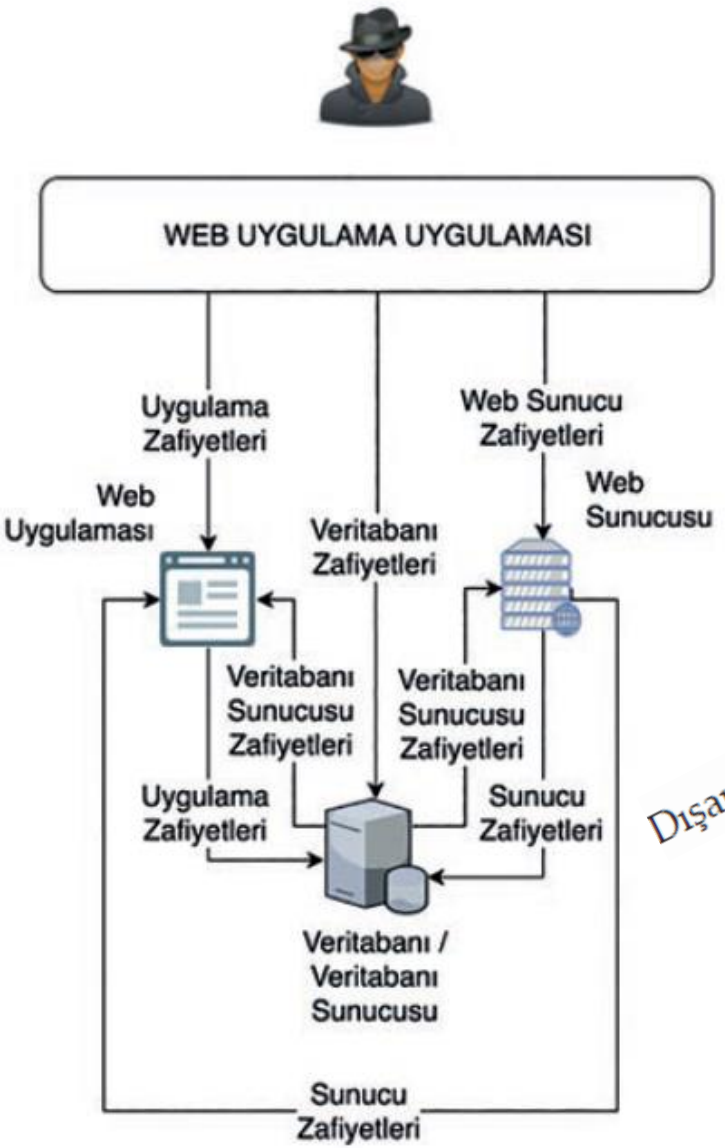
Saldırı Adı	Zayıf noktalar	Çözüm	Etki
XSS saldırısı	Bir uygulamaya veya yazılıma yerleştirilen HTML 5 tabanlı kötücül kodlar.	Popüler ve özgün uygulamaların kullanımı. Uygulamaların zayıflıklarının tespit edilmesi için tarama araçları kullanımı.	Akıllı telefona kötücül kodların bulaşması Bilgilerin elegeçirilmesine (hacklenmesine) ve arka kapılar açılmasına neden olur.
SMS tabanlı saldırlar	Saldırgan oltalama linklerinin reklamını yapabilir.	Mesaj ayalarında düzenleme yapılarak cihaz korunabilir.	Hassas bilgilerin ele geçirilmesi.
USSD Saldırıları	Bilinmeyen aramalar, mavi ekran korsanlığı	Anomali tabanlı saldırı tespit sistemi kullanımı	Kişisel bilgiler çalınabilir. Akıllı telefon zarar görebilir.
USB bağlantı saldırıları	Root erişimi	Saldırgan olmayan şarj istasyonlarının kullanımı.	Hassas bilgilerin çalınması. Her hangi bir kötücül yazılımın kolaylıkla bulaşabilmesi.
ABD saldırısı	Açıklık komut işlemci aracı	Geriye doğru dilimleme, statik analizör ve dizin analizör kullanımı.	Hassas bilgilerin çalınması.
Kamera tabanlı saldırılar	Kötücül program, yetkisiz kaynaklar.	Casus kamera desteği, etkin erişim kullanımı.	Akıllı telefon güvenliğinin zayıflatılması. Bilgilerin çalınması.
Kontrol akış saldırıları	Kod yerleştirme, hafızada veri taşması	Mobil kontrol akış bütünlük çerçevesi kullanımı.	Kullanıcının SMS veya kontak veri tabanının ele geçirilmesi, hafıza bozulmasının istismar edilmesi.

Yeni tip saldırılar ve önlemler

Web Uygulamaları Zafiyetleri ve Önlemler

- HTML statik bir dildir. Dinamik işlemler için web sunucularında başka programlama dilleri kullanılmaktadır.
- PHP, ASP.NET, Java, Cold-Fusion, Ruby, JavaScript, Perl, Python, Erlang gibi geliştirme dilleri en çok kullanılan web yazılımı geliştirme araçlarıdır.
- Tarayıcılar üzerinden erişilen web uygulamaları Hyper Text Transfer Protocol (HTTP) adı verilen bir protokol üzerinden çalışmaktadır. TCP/IP protokolü üzerinde uygulama seviyesinde çalışan HTTP protokolü Web'in çalışma altyapısını oluşturmaktadır.
- Metin tabanlı olan bu protokol üzerinden yapılan istekler web sunucuya iletilmekte ve web sunucu tarafından dönen cevap tarayıcı tarafından yorumlanarak kullanıcıya gösterilmektedir. İstemci (web tarayıcıları) web sunucularına web sayfaları ve resimler gibi web elementlerine erişim istekleri göndermektedirler.
- HTTP ile alakalı tüm kurallar Internet Engineering Task Force (IETF) ve World Wide Web Consortium (W3C) tarafından oluşturulup yönetilmektedir

Web Uygulamaları Zafiyetleri ve Önlemler



Dışarıdan erişim ile web uygulamasına gelebilecek atak vektörleri

Güvenlik Testi ve Zafiyet Analizi

Zafiyetlerin tetiklenmesi sonucu oluşabilecek bilgi güvenliği ihlallerini önceden tespit etmek ve önlemek amaçlı iyi niyetli siber güvenlik uzmanları tarafından ilgili varlık üzerinde siber güvenlik testleri (sızma testi) gerçekleştirilmektedir. Gerçekleştirilen güvenlik testleri belirlenen kapsam içerisindeki tüm varlıkları siber saldırgan gözüyle zarar vermeden incelenip raporlanmasını kapsamaktadır.

Güvenlik testlerinin ilk aşaması bilgi toplamadır.

Aktif ve Pasif Bilgi Toplama!!!

Pasif Bilgi Toplama

Bir web uygulamasında bilgi toplama aşaması pasif olarak aşağıdaki adımlar ile sağlanabilir:

- Alan adı / IP kayıt bilgileri (whois)
- Sitelerin geçmişini kayıt eden servisler ile yapılan incelemeler
- Arama motorlarının kullanımı ve özel aramalar
- E-posta adreslerinin tespit edilmesi (hedefin dışında)
- DNS sorguları

Hedef sistemdeki alan adlarına ait e-posta adreslerini bulmak için açık kaynak yazılımlar kullanılabilmektedir. TheHarvester adlı yazılım alan adına göre internetteki belirli web uygulamalarını tarayarak e-posta adreslerini tespit etmektedir. Tespit edilen e-posta adresleri sonraki aşamalarda sosyal mühendislik saldırılarından, kaba kuvvet saldırılarına kadar birçok alanda kullanılabilirler.

Aktif Bilgi Toplama

- Servis bilgileri edinme
- Port tarama
- DNS kaba kuvvet saldırıları ve
- Bağlantı tespitidir.

Aktif bilgi toplamada servis bilgileri ve port tarama hedef sisteme gönderilen ağ paketleri ile hedef sistemde çalışan servislerin sürümleri ile açık portları hakkında bilgi edinmeyi kapsamaktadır. DNS kaba kuvvet saldırıları DNS sunucusundan dönen cevapları kullanarak hedef sistemdeki alt alan adlarını veya farklı alan adlarını tespit etme işlemidir. Web uygulamalarında bağlantı tespiti ise bu çalışmanın konusunu oluşturmaktadır.

Bağlantı tespiti için arama motorları, web sitesindeki bağlantılar veya zafiyet tarama araçları gibi farklı yöntemler kullanılmaktadır.

Eğer herhangi bir sayfa arama motorlarında, otomatik zafiyet tarama araçlarında veya web sitesi içerisinde gezinerek bulunamıyorsa tespit edilmesi için tahmin saldırıları yapılmaktadır. Dizinlere yapılan kaba kuvvet olarak da bilinen dosya/dizin tahmin saldırıları bir kelime listesinin web uygulamalarındaki dizinlere erişim için kullanılarak sunucudan dönen cevabı incelemek için kullanılmaktadırlar.

Web Uygulama Zafiyetleri ve Çözüm Önerileri

Siteler Arası Betik Çalıştırma Zafiyeti

JavaScript web uygulamalarına kullanılan tarayıcı tarafında yorumlanan ve genellikle yalnızca tarayıcı tarafında çalışan bir programlama dilidir ve çerez bilgilerine erişimden, web sitelerindeki verilere erişime kadar birçok işlem gerçekleştirebildiğinden dolayı siber saldırganlar tarafından zararlı amaçlar için kullanılabilmektedir.

Saldırganlar tarafından hedef sistem üzerinde JavaScript kodu çalıştırmasına olanak tanıyan zafiyetler Siteler arası betik çalıştırma zafiyeti (Cross Site Scripting, XSS) olarak bilinirler. Siteler arası betik çalıştırma zafiyeti günümüzdeki web uygulamalarında en çok tespit edilen zafiyetlerden biridir.

Web Uygulama Zafiyetleri ve Çözüm Önerileri

Siteler Arası Betik Çalıştırma Zafiyeti

XSS zafiyetleri kullanıcıdan alınan verilerin web uygulamalarında doğru şekilde filtrelenmemesinden dolayı ortaya çıkan zafiyetlerdir.

Zafiyetlerin tetiklenme türüne gürüne göre, yansıtılmış, depolanmış ve DOM tabanlı olarak üç ana başlık altında toplanabilmektedir.

SQL Enjeksiyonu Zafiyeti

Web uygulamalarındaki dinamik sayfalarda çoğunlukla kullanıcıya sunulan bilgiler veri tabanlarından okunarak servis edilir. Veri tabanından okuma işlemi veri tabanına özel kurallar çerçevesinde gerçekleştirilir. Web uygulamalarında kullanıcıdan alınan değerler SQL sorgularına dahil edilebilir. Yazılımcıların, kullanıcıdan aldığı parametreleri SQL sorgularına kullanması ile oluşan sorgulara dinamik SQL sorgularıdır. Saldırganların dinamik sorgulara müdahale ederek hedef sistemde çalışan SQL kodlarını değiştirerek yaptığı saldırılar SQL enjeksiyonu saldırıları olarak adlandırılmaktadır.

SQL enjeksiyonu zafiyetlerini tessit eden ve sömürmekte kullanılan SQL Map adlı açık kaynak zafiyet tarama aracı bu zafiyetleri, körlemesine mantıksal tabanlı (boolean-based blind), körlemesine zaman tabanlı (time-based blind), hata tabanlı (error-based), birleştirilmiş sorgu tabanlı (union query-based) ve yığın sorgular (stacked queries) türleri olarak beşe ayırmıştır.

Siteler Arası İstek Sahteciliği

Siteler arası istek sahteciliği (Cross-Site request forgery, CSFR) web kullanıcılarına yönelik, saldırganın kurbanın tarayıcısı ile güvenilir bir web uygulamasına istenmeyen bir istek yapması ile oluşan saldırılardır

Güvenilir web sitesinde oturum bilgisi ile işlem yapan kullanıcı, içerisinde zararlı kodların olduğu başka bir sayfayı ziyaret edebilir. Bu durumda zararlı web sitesi içerisinden güvenilir web sitesine, kullanıcının oturum bilgisinin de içerisinde olduğu bir istek iletilebilir. Bu istek kullanıcının tarayıcısı tarafından gönderilmektedir. Yapılan istek içerisinde oturum bilgisi yer aldığından dolayı saldırgan sanki kullanıcıymış gibi güvenilir web sitesinde özel işlemler gerçekleştirebilmektedir.

Basit Parola Denemeleri ve Kaba Kuvvet Saldırıları

Kötü niyetli kullanıcılar web uygulamaların kimlik doğrulama sayfalarına (genellikle üye giriş ara yüzleri) kullanıcı adı ve parola denemeleri gerçekleştirebilirler.

Yetkisiz Erişim Zafiyeti

Yetkisiz erişim doğru bilgilere (kullanıcı adı, parola, tek girişlik parola, vb.) sahip olmadan yetkili bir kullanıcı haklarının bir kısmına veya tamamına sahip olmaktır.

Kimlik doğrulama mekanizmaları sonrasında atanan yetkiler genellikle kullanıcının tarayıcısından web uygulamasına gönderilen oturum bilgileri ile tutulmaktadır. Bu oturum bilgileri yetkilerin kontrol edilmesi gereken her sayfada kontrol edilmelidir. Kontrol edilmediği durumlarda saldırganların erişim yapması bazı bilgilerin dışarıya çıkmasına sebebiyet verebilir.

Yetkisiz erişimler erişim kontrolleri olmayan ayrı sayfaları test edilerek tespit edilebileceği gibi web sayfalarına giden ağ trafiği üzerinde değişiklik yapılarak da test edilebilir.

Dosya Çağırma

Uygulamalarda yer alan kodlar içerisinde bazı durumlarda uzaktaki veya uygulama ile aynı alandaki (yerel) sistemlerden dosya çağıran kod parçaları bulunur. Bu kod parçaları web uygulaması içerisinde yapılması gereken işlerin bir kısmını veya tamamını yerine getirmek için kullanılabilir. Çağırılan dosyaların türüne göre komut çalıştırmaktan, dosya içerisindeki komutları kullanmaya kadar birçok farklı alanlarda web uygulamalarına dışarıdan dosya çağırılabilmektedir. Bazı çalışmalar internet sitesi, dizinler veya aynı disk üzerindeki gibi farklı bir yerde bir kısım kodları çağırılmasına uzaktan dosya çağırma (remote file inclusion, RFI) zafiyeti olarak tanımlanır.

Diğer Zaafiyetler

- XML enjeksiyonu zafiyetleri
- LDAP (Lightweight Directory Access Protocol) enjeksiyonu
- İşletim sistemi komutu enjeksiyonu

Yazılım Tanımlı Ağlar (SDN) ve Siber Güvenlik

Yazılım tanımlı ağ (SDN) teknolojisi ile gelen programlanabilirlik ve merkezi kontrol, İnternet'teki sorunlara karşı pratik ve etkili çözümler üretmeyi kolaylaştırmaktadır.

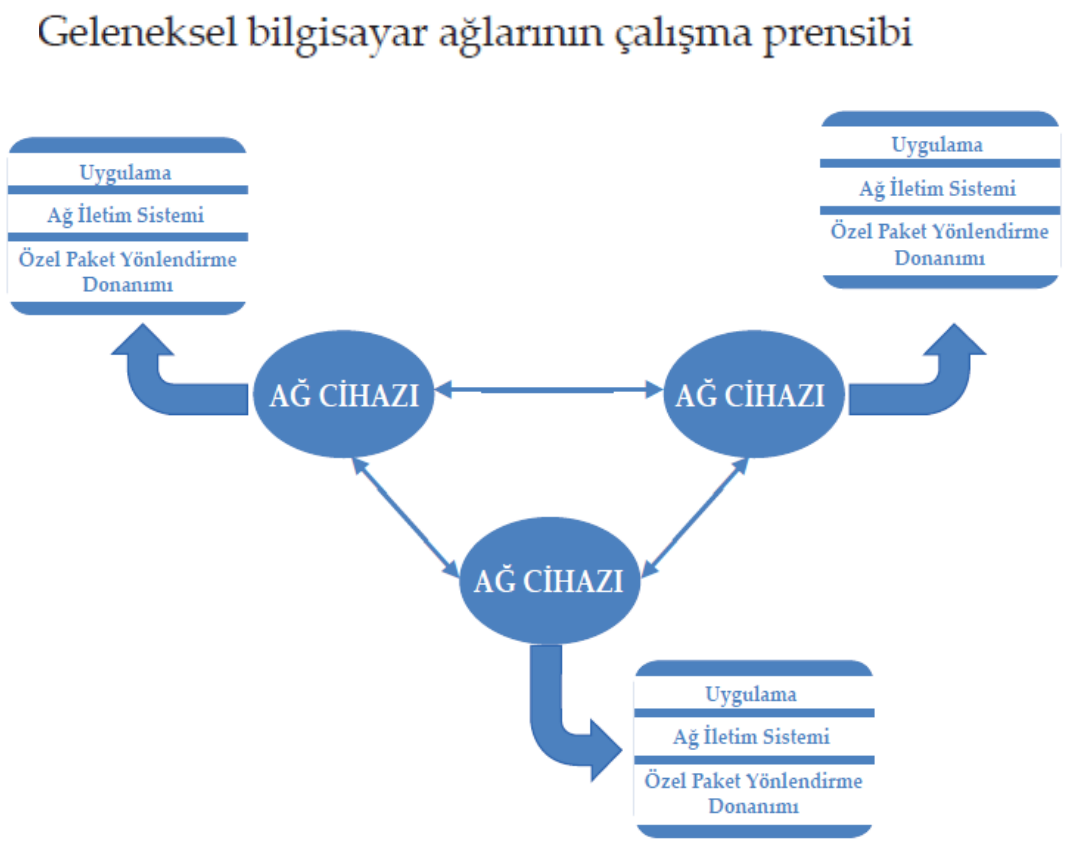
SDN, veri merkezlerinden servis sağlayıcı ağlarına kadar birçok alanda kullanılmakta ve hızla yaygınlaşmaktadır.

SDN siber güvenlik açısında değerlendirildiğinde, hem güvenliği sağlamaya katkı yapan prensiplere hem de güvenlik risklerini arttıran özelliklere sahip olduğu görülmektedir.

https://www.longlinenetwork.com/sdn-software-defined-network-nedir/

Yazılım Tanımlı Ağlar (SDN) ve Siber Güvenlik

Bu mimarideki ağ cihazları dikey bütünleşmeye (vertical integration) sahip özelleşmiş kutulardır. Dikey bütünleşme, ağ cihazı içerisindeki donanım ve yazılımın yalnızca üreticisi tarafından sağlanabilmesi, üretici firma dışında kimse tarafından kapsamlı biçimde değiştirilememesi anlamına gelmektedir.



Daha açık bir ifadeyle, bir cihaza kendi üreticisinden bağımsız bir şekilde farklı bir yazılım yüklenememekte ve müdahale edilememektedir. Dolayısıyla ağ cihazları firmalara bağlı kaldıkça yeni fikirler rahatlıkla uygulanamamakta, yazılımda ve donanımda gelişmeler yavaşlamakta, esneklik yitirilmektedir.

Yazılım Tanımlı Ağlar (SDN) ve Siber Güvenlik

İnternet mimarisine yitirilen esnekliği kazandırmak ve yeni servisler eklemeyi kolaylaştırmak amacıyla öne çıkan teknolojilerinden biri **ağ sanallaştırma**dır . Fiziksel bir ağın üzerinde birden fazla mantıksal (sanal) ağın çalışmasını sağlayan soyutlama olarak tanımlanan ağ sanallaştırma ile düğümler, diskler, bağlar gibi ağ bileşenleri sanallaştırılmaktadır. Fakat ihtiyaç duyulan durumlarda dinamik bir şekilde sanal makine göçünün yapılması ve ağ yapılandırması oldukça pahalı ve zaman alıcı işlemlerdir. Dolayısıyla büyük çaplı sanal ağların yönetiminin kolaylaştırılması da alt yapıda yer alan fiziksel ağın karmaşıklığının giderilmesine bağlıdır.

Yazılım Tanımlı Ağlar (SDN) ve Siber Güvenlik

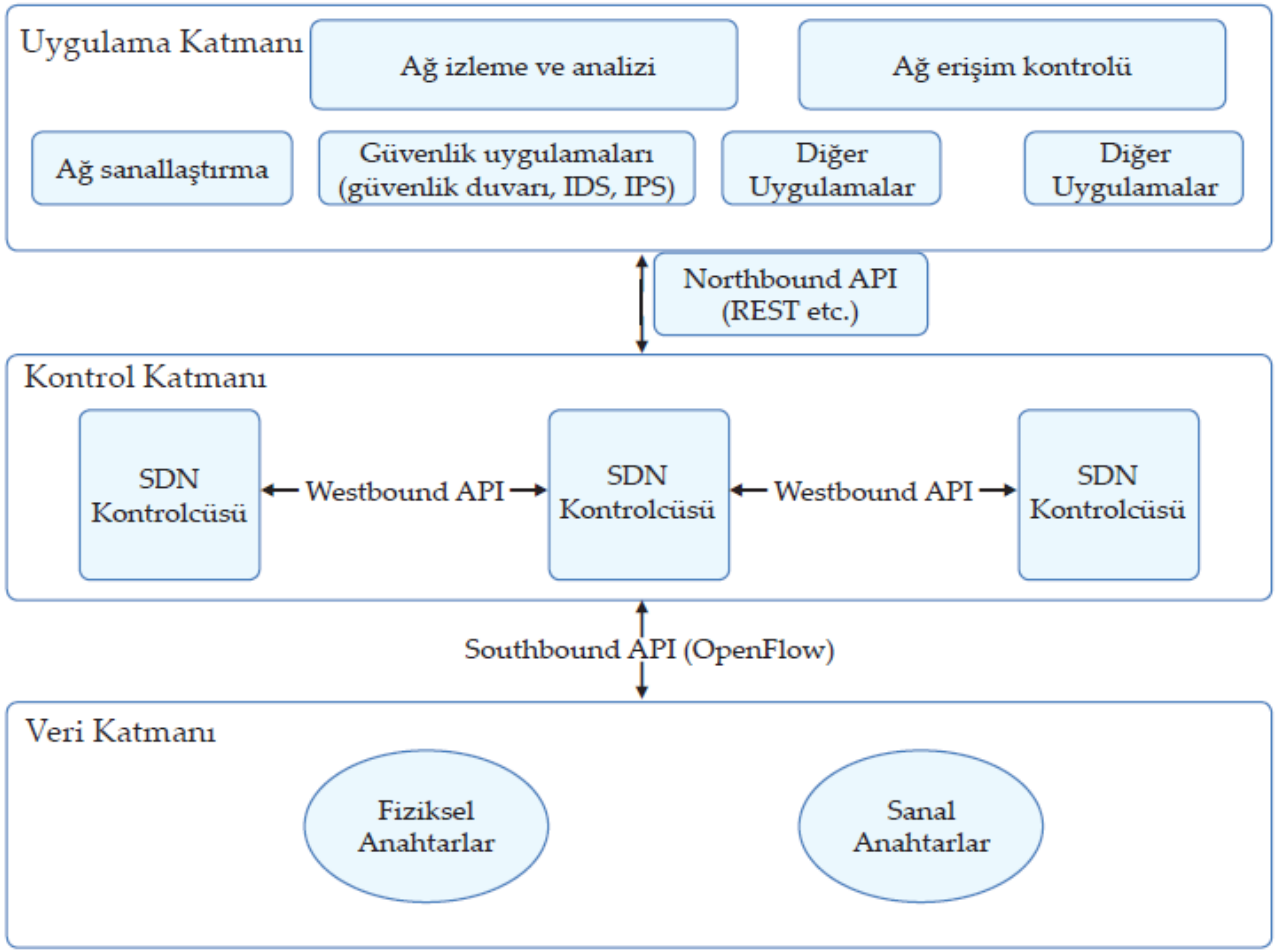
Yazılım Tanımlı Ağlar (Software Defined Networks), ağdaki kontrol birimini altyapıdaki yönlendirici ve anahtarlardan ayırarak, kontrolü mantıksal bir şekilde merkezileştiren, ağın merkezi bir yazılım birimi tarafından programlanmasına imkân sağlayan ve böylelikle yukarıda bahsedilen problemlere çözümler sunan yeni bir paradigmadır.

Kontrol ve Veri Düzlemlerinin Ayrılması

Yazılım Tanımlı Ağların (SDN) temel felsefesi kontrol katmanını veri katmanından ayırmaktır. Ağın beyni olarak da nitelendirilebilecek kontrol katmanı, yönlendirme kurallarını belirleyerek trafiğin nereye gönderileceğine dair kararları alan bir kontrol yazılımından oluşmaktadır. Söz konusu kararları icra eden veri katmanında ise kontrol yazılımının belirlediği kurallar dâhilinde yönlendirme yapan programlanabilir ağ cihazları bulunmaktadır. Uygulama katmanında, kontrolcünün üzerinde çalışan çeşitli ağ fonksiyonları (yük dengeleyici, güvenlik duvarı, saldırı tespit sistemi vb.) ile kullanıcı uygulamaları bulunmaktadır.

Kontrol ve Veri Düzlemlerinin Ayrılması

Şekil'de SDN mimarisinin çalışma mantığı gösterilmektedir.



Veri Katmanı

Altyapı katmanı olarak da bilinen bu düzlemde, geleneksel ağ mimarisine benzer şekilde paket anahtarlama ve iletiminden sorumlu yönlendirme elemanları bulunmaktadır. Geleneksel ağ cihazlarından farklı olarak bu katmandaki elemanlar kendi kontrol yazılımlarını içermediklerinden özerk kararlar alamazlar. Onun yerine bu katmandaki programlanabilir yönlendirici ve anahtarlar, kontrol katmanında çalışan kontrolcü yazılımının belirlediği kurallar doğrultusunda paket iletimi işlemini gerçekleştirmektedirler.

Switch Light, Open vSwitch, OpenFlow Reference, Pica8 SDN mimarisi için geliştirilmiş bazı programlanabilir anahtar örnekleridir

Kontrol Katmanı

Bu katmanda ağın beyni olarak adlandırılabilecek bir veya daha fazla kontrolcü yazılımı bulunmaktadır. Kontrolcünün görevi, ağın hedefleri doğrultusunda önceden veya veri katmanındaki anahtarlar bir paketi nereye yönlendirileceğini sorduğunda, yönlendirme kuralları oluşturmak ve bunu güney arayüzü aracılığıyla anahtarların akış tablolarına yazmaktır. Günümüzde farklı amaçlar için geliştirilmiş birçok kontrolcü yazılımı bulunmaktadır. NOX, POX, Floodlight, Beacon, DIFANE vb. bunlara örnek olarak gösterilebilir. Kontrolcü seçimi yapılırken kullanım amacı, programlama dili kolaylığı ve performansı, öğrenme kolaylığı ve kullanıcı tabanı ve destek hizmetleri göz önünde bulundurulmalıdır.

Güney Arayüzü (Southbound API)

Bu arayüz, kontrolcünün veri katmanındaki yönlendirme elemanları ile iletişim kurmasını sağlamaktadır. Bu amaçla kullanılan en önemli protokol ONF (Open Networking Foundation) tarafından geliştirilen OpenFlow protokolüdür. OpenFlow, kontrolcü ile anahtarlar arasında akan mesajların şeklini belirleyerek güvenli bir biçimde iletişim kurulmasını sağlar. Kontrolcü, OpenFlow mesajları vasıtasıyla anahtara akış tablosunda değişiklikler yapmasını söyler.

OpenFlow protokolüne göre sırasıyla;

- Anahtar kendisine gelen paket için paketin başlıkları ile akış tablosundaki girdiler arasında eşleşme olup olmadığına bakar.
- Eşleşme varsa, daha önceden bu paketi nasıl yönlendireceğine dair kural kontrolcü tarafından akış tablosuna yazılmış demektir, dolayısıyla yapılması söylenen işlem gerçekleştirilir (paketi ilet, düşür, kuyruğa sok, başlık alanını değiştir vb.).
- Eşleşme yoksa anahtar ne yapacağını bilemediği için paketi OpenFlow protokolü aracılığıyla kontrolcüye gönderir.
- Kontrolcü paket ile ilgili kuralı hesaplar ve yine OpenFlow güvenli kanalı üzerinden anahtarın akış tablosuna yazar.

Uygulama Katmanı

Bu katmanda, ağ yönetimi, kontrolü ve operasyonunu sağlamak için gerekli olan yük dengeleme, güvenlik duvarı, trafik izleme, saldırı tespit sistemi, derin paket inceleme gibi farklı işlevleri olan uygulamalar bulunmaktadır. Bu uygulamalardan her biri, kendi görevini gerçekleştirmesi için gereken politikaları tanımlar. Kuzey arayüzü tarafından kontrolcüye iletilen bu politikalar, sonrasında derlenip OpenFlow kurallarına dönüştürülerek veri katmanındaki anahtarların programlanmasında kullanılır.

Kuzey Arayüzü (Northbound API)

Kuzey arayüzü, uygulama katmanındaki uygulamaların kontrolcü ile haberleşmesinde kullanılan arayüzdür. Bir başka deyişle kuzey arayüzü, uygulamaların ağı programlamasına imkân veren yapıdır. Bu arayüz, geliştiricilere Python, Java, C++ vb. yüksek seviyeli diller kullanılarak uygulama geliştirme imkânı sunar. Ağ yöneticileri, servis sağlayıcıları ve araştırmacılar tarafından ağda karmaşık kurallar uygulamak için üst seviye bir dilde geliştirilen uygulamalar kuzey arayüzü tarafından derlenerek OpenFlow kuralları haline getirilmekte ve kontrolcüye iletilmektedir.

Yazılım Tanımlı Ağlar (SDN) ve Siber Güvenlik

Yazılım Tanımlı Ağların Siber Güvenliğe Katkısı

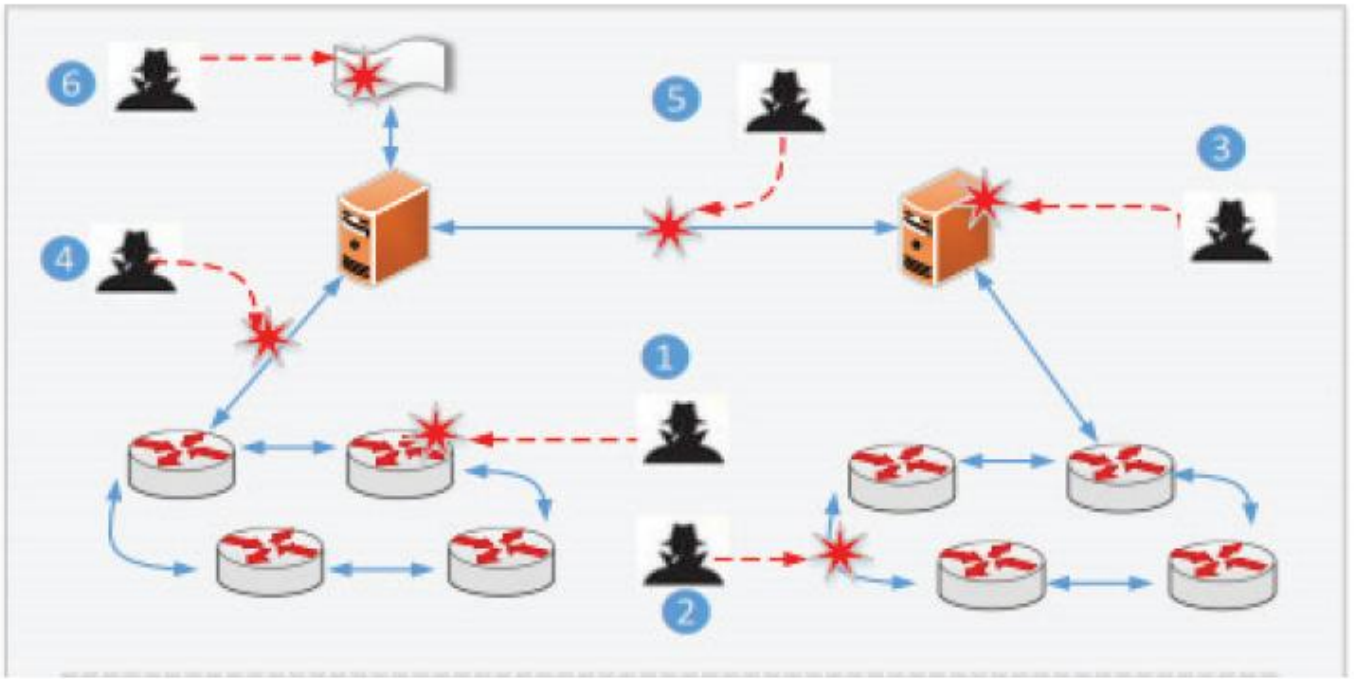
SDN'in sunduğu özellik	Açıklama	Siber Güvenliğe Katkısı	Savunmadaki Rolü
Dinamik trafik kontrolü	Trafiğin dinamik bir şekilde yönlendirilmesi, durdurulması vb.	Zararlı veya şüpheli ağ trafiğinin dinamik bir şekilde kontrol edilebilmesi ve normal trafikten ayırılabilmesi	Önleme, saldırıya cevap verme
Merkezi kontrol mekanizması	Ağ cihazlarının durumu ve ağa gelen trafiğin merkezi bir kontrolcü yazılımı tarafından izlenmesi ve yönetilmesi	Ağ çapındaki tüm güvenlik servislerinin izlenebilmesi, saldırıların veya anormal trafiğin daha etkin ve etkili bir şekilde tespit edilebilmesi	Tespit, saldırıya cevap verme
Ağın programlanabilir olması	Ağ fonksiyonlarının programlanabilmesi	Güvenlik fonksiyonlarının kolay bir şekilde geliştirilebilmesi ve güncellenebilmesi	Tespit, saldırıya cevap verme
Basitleştirilmiş veri katmanı	Kontrol mantığının veri katmanından ayrılarak merkezi bir kontrolcü yazılımına verilmesi	Yeni güvenlik servislerinin eklenmesi ve bunların diğer servislerle olan etkileşiminin kolaylaşması	Önleme, tespit, saldırıya cevap verme

Yazılım Tanımlı Ağların Siber Güvenliğe Katkısı

SDN'de siber güvenliğin sağlanması için saldırı tespiti yapan (saldırı tespit sistemi, zararlı yazılım tarayıcılar, DDoS detektörü ve derin paket inceleme), engelleyen (güvenlik duvarı, saldırı engelleme sistemi) ve saldırı yakalayan (balküpü) güvenlik fonksiyonlarının sanallaştırılarak ilgili sunucular üzerinde çalıştırılması yöntemi giderek yaygınlaşmaktadır.

SDN mimarisi üzerindeki muhtemel saldırı noktaları

Bir saldırgan SDN mimarisi üzerindeki (i) anahtarları, (ii) anahtarlar arasındaki yolları, (iii) kontrolcü yazılımını, (iv) kontrolcü ile anahtarlar arasındaki bağlantı noktalarını, (v) birden fazla kontrolcü olduğu durumda kontrolcüler arasındaki iletişim noktalarını ve (vi) uygulama katmanında yer alan fonksiyonları amacına yönelik saldırılar gerçekleştirmek üzere hedef alabilmektedir.



Sorular

Bir sonraki ders Kripto Para, Blokzincir Sistemi ve Siber Güvenlik İlişkisi konusuna giriş yapılacak.