NİSAN-HAZİRAN 2023

SİBER TEHDİT DURUM RAPORU

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi

SORUMSUZLUK VE FİKRİ MÜLKİYET HAKKI BEYANI
İşbu eserde/internet sitesinde yer alan veriler/bilgiler ticari amaçlı olmayıp tamamen kamuyu bilgilendirmek amacıyla yayımlanan içeriklerdir. Bu eser/internet sitesinde bulunan veriler/bilgiler tavsiye, reklam ya da iş geliştirme amacına yönelik değildir. STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. işbu eserde/internet sitesinde sunulan verilerin/bilgilerin içeriği, güncelliği ya da doğruluğu konusunda herhangi bir taahhüde girmemekte, kullanıcı veya üçüncü kişilerin bu eserde/internet sitesinde yer alan verilere/bilgilere dayanarak gerçekleştirecekleri eylemlerden ötürü sorumluluk kabul etmemektedir.
Bu eserde/internet sitesinde yer alan bilgilerin her türlü hakkı STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.'ye ve/veya eserde atıf yapılan kişi ve kurumlara aittir. Yazılı izin olmaksızın eserde/internet sitesinde yer alan bilgi, yazı, ifadenin bir kısmı veya tamamı, herhangi bir ortamda hiçbir şekilde yayımlanamaz, çoğaltılamaz, işlenemez.

İÇİNDEKİLER

ŞEKİLLER

GİRİŞ

2023 yılının ikinci çeyreğinde Siber Güvenlik Müdürlüğü tarafından hazırlanan raporumuzda yine birbirinden ilginç konularla karşınızdayız.

ChatGPT, çıkışından itibaren büyük ilgi gördü ve oldukça geniş bir kitle tarafından kullanılmaya başladı. Bundan ötürü ilk konumuzda, geçtiğimiz mart ayında ChatGPT'de yaşanan kesinti hakkında detaylı bilgiler vermekteyiz.

Geçtiğimiz çeyrekte ALPHV/BlackCat tehdit aktörü kendi fidye yazılımını kullanarak "Automatic Systems" isimli güvenli giriş kontrol üretim firmasına saldırdı. Raporumuzun ikinci bölümünde bu olayı inceliyoruz.

Bulut sistemlerinin verilerin güvenli ve erişilebilir şekilde depolanmasını sağlaması ve daha birçok başka katkısı, bu konuyu ilgi çekici hâle getirmektedir. Bu raporumuzda bulut sistemlerini ayrıntılı bir şekilde ele alıyoruz.

Raporumuza web uygulamaları geliştirmede kullanılan "Django Web Framework" tanıtımıyla devam ediyoruz. Django, güçlü web uygulamaları geliştirmede büyük kolaylıklar sağlayan bir çerçevedir. Python dili tabanlı ve açık kaynak olması sayesinde günümüzde oldukça popülerdir.

Bu raporumuzda Haziran ayında yayınlanan "Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği" konusunda ayrıntılı bir inceleme yer alıyor.

Sonraki yazımızda çeşitli sektörlerde yazılım geliştirme ve dağıtım süreçlerini kapsayan "Software Bill of Materials" (SBOM) ve yazılım tedarik zinciri güvenliği konusunda aydınlatıcı bilgilere yer veriyoruz.

Hemen ardından, CPS (Cyber-Physical System) olarak bilinen ve fiziksel ile dijital bileşenlerin birlikte çalıştığı gerçek zamanlı yeni nesil gömülü sistemlerin siber güvenliği konusu ele alınıyor.

Bu raporumuzun dönem konusu olarak NATO tarafından ülkelerin savunma yeteneklerini artırmak ve işbirliğini en üst seviyeye çıkarmak amacıyla düzenlenen "Locked Shields" tatbikatını seçtik.

Raporumuzun en sonunda ise her zaman olduğu gibi güncellenmiş honeypot verilerine yer ayırdık.

Keyifli okumalar dileriz.

TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

1. ChatGPT Kesintisi

ChatGPT, insan benzeri konuşma ve sohbetler yapabileceğiniz doğal dil işlemeye dayalı bir yapay zekâ aracıdır. ChatGPT sohbet etmenin yanı sıra kod yazma, e-posta yazma gibi benzeri işlevleri de yerine getirmektedir.

ChatGPT'nin kendisini beslemesi ve eğitmesi için veriye ve geniş bir kitleden geribildirim almaya ihtiyacı vardır. Bunu da ücretsiz versiyonu ile sağlamaktadır. Ayrıca isteklere daha geniş bir şekilde yanıt verebilen Şubat ayından itibaren kullanıma sunulan ChatGPT Plus adlı ücretli bir abonelik sürümü de vardır.

Neden Kesinti Oldu

ChatGPT'de Mart ayının son haftasında birkaç saatlik kesinti olmuştur. Bu kesintinin sebebi ChatGPT'nin kullandığı açık kaynak bir kütüphanedir. Bu kütüphanede kullanıcıların birbirlerinin sohbet geçmişlerini görebilmesine olanak veren bir zafiyet bulunmuştur.

Bu veri teşhirine sebep olan açık kaynaklı kütüphane redis-py'dir. İptal edilen istekler kimi zaman yanlış veya beklenmedik veri dönüşlerine sebep olmuştur. Bu durumda bu veriler başka kullanıcılar tarafından görüntülenmiştir. OpenAI'ın açıklamasına göre[1], bundan kaynaklı olarak ChatGPT Plus üyeliği olan kullanıcıların yüzde 1,2'sinin -belli bir dokuz saat diliminde aktif bir şekilde platformu kullandılarsa- ödeme bilgilerinde veri ifşası gerçekleşmiş olabilir. O zaman dilimindeki aktif kullanıcıların; isim, soy isim, e-posta adresi, fatura adresi, kredi kartı tipi, kredi kartının son dört hanesi ve kredi kartının son kullanma tarihi gibi verileri görüntülenebilmiştir.

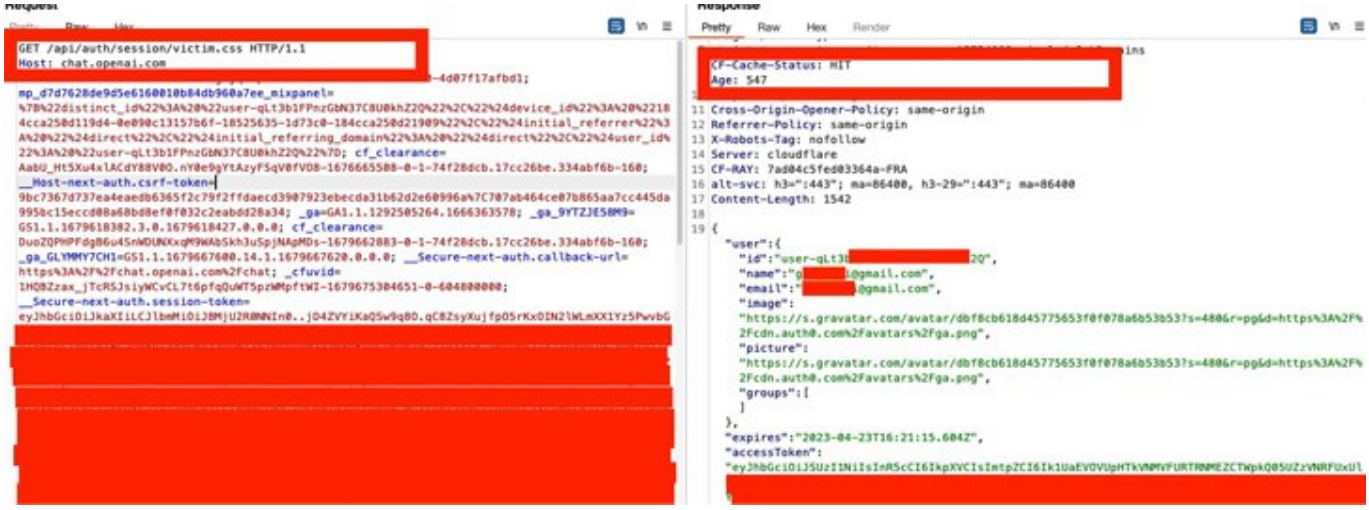
CVE-2023-28858 Zafiyeti

Bu zafiyet, redis-py kütüphanesinde bulunan ve Redis'in 4.5.3'ten önceki tüm sürümlerini etkileyen bir yarış -birden fazla thread'in aynı hafızayı değiştirmesi- durumudur. Redis caching, session yönetimi ve message broker olarak günümüz teknolojilerinde sıklıkla kullanılan bir veritabanıdır. Redis asenkron bağlantılara izin vermektedir. Bu da birden fazla bağlantının aynı anda yapılmasına izin verir.

Gönderilen istek asenkron ise ve bu istek iptal edildiyse bağlantı açık kalır. Bu durum birden fazla istek aynı anda atıldığında gerçekleşebilmektedir. Açık kalan bağlantı da sunucunun bir yanıt beklediğini göstermektedir. Sunucu bu açık kalmış bağlantıya yanıt gönderirse, client tarafından alakasız bir istek olarak alınabilir. Bu da gönderilen verilerinin yanlış client'a gönderildiği anlamına gelir ve veri sızıntısına neden olabilir[2].

Alınan Önlemler

Zafiyete çözüm bulmak için OpenAI, Redis ile iletişime geçmiştir. Redis yapılan asenkron isteklerin bağlantısı



Şekil 1: Araştırmacı tarafından yapılan çalışmanın sonucu.

kopunca, o bağlantıdaki bütün verileri boşalttığına emin olup session'ın bağlantısını kopartmıştır. Redis 4.3.6, 4.4.3 ve 4.5.3 versiyonlara yama yaparak bu zafiyeti kapatmıştır.

Hesap Ele Geçirme Hatası

Son zamanlarda ortaya çıkan, araştırmacı Gal Nagli tarafından fark edilen bir hatadır. Araştırmacı yaptığı çalışmada başka kullanıcıların hesaplarını onların bilgileri olmadan ele geçirebildiğini, sohbet geçmişlerini görüntüleyebildiğini ve fatura bilgilerine erişebildiğini fark etmiştir. Şekil 1'de görüntüde yaptığı çalışma sonucu ele geçirdiği bilgiler görüntülenmektedir.

Araştırmacı, "chat.openai[.]com/api/auth/session/" uç noktasına bir tane .css dosyası yerleştirerek, kullanıcıyı bu bağlantıya tıklaması için kandırarak, yanıtın içinde bulunan ve CloadFlare'in CDN önbelleğinde tutulan JSON objesindeki accessToken'ı ele geçirmiştir. Saldırgan, bu durumda araştırmacı cached yanıt ile kullanıcının JSON Web Token (JWT) bilgilerini çıkarmıştır. Bu bilgilerle kullanıcının hesabını ele geçirmiştir[3].

OpenAI bu zafiyeti de kısa bir sürede kapatmıştır.

Sonuç

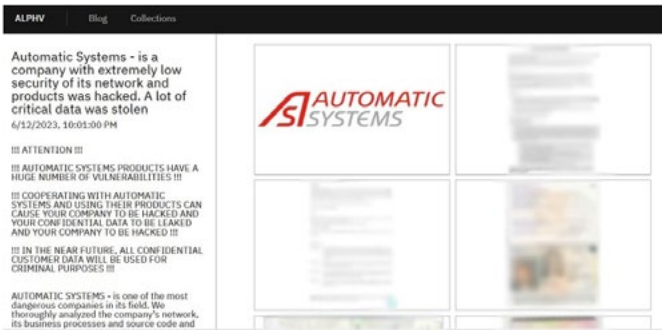
Yapay zekâ (YZ) insanların hayatına her gün daha fazla girmektedir. ChatGPT gibi kullanımı kolay ve insanların günlük hayatını kolaylaştıran platformların kullanıcı sayısı hızla artmaktadır. Tüm yeni teknolojilerde olduğu gibi, gelecekte YZ ile ilgili yeni güvenlik sorunlarının keşfedilmesi muhtemeldir.

2. BlackCat ALPHV Fidye Yazılımı ile Siber Saldırı

Yakın zamanda ALPHV/BLACK grubu Automatic System'e yaptığı saldırıyla gündeme geldi. Araç ve yolcu geçiş kontrol sistemleri üreten Automatic System'in yaklaşık 400 çalışanı vardır. Saldırganların, güvenli giriş kontrol üreticisi "Automatic Systems"in AliBaba, NATO, Thales gibi bazı müşterilerinin gizli verilerini ve pasaport bilgileri gibi bilgilerini yayınlandığı ortaya atıldı. 3 Haziran tarihinde Automatic Systems, web sitesinin saldırıya uğradığını ve izinsiz girişin kullanıcıların belirli bir kısmını hedef aldığını kabul etti. Paylaşılan gönderi şirketin ortaklarının ve müşterilerinin kişisel bilgilerini içermektedir. Bu açıklamanın ardından "Automatic Systems" ilerlemeyi durdurmak için hemen önlem aldı.

Automatic Systems'a yapılan bu saldırıyı Rusya tabanlı ALPHV/BlackCat fidye yazılım grubu üstlendi. ALPHV/BlackCat grubunun DarkWeb sitesindeki gönderisinden anlaşıldığı üzere çalınan veriler arasında Çinli dev

Şekil 2: Automatic Systems[4].



Şekil 3: Automatic Systems ile ilgili haber[5].

perakendeci AliBaba ile ilgili gizlilik unsuru içeren veriler ile Automatic Systems şirketinin Fransız savunma müteahhidi Thales ile imzaladığı belgeler ve diğer veriler de bulunmaktadır.

ALPHV fidye yazılımı; uzantıların, fidye notlarının verilerin nasıl şifreleneceğinin, hariç tutulan klasörlerin\dosyalarının\uzantıların ve hizmet ve işlemlerin otomatik olarak sonlandırılmasını içerir[6]. ALPHV/BlackCat, 2021 yılından beri mevcut olan ve çok çeşitli kurumsal ortamlara saldırılara imkân veren son derece özelleştirilmiş bir fidye yazılımıdır. BlackCat, saldırganların altyapılara ve kötü amaçlı kodlara erişimini sağlamakta [7], bunun karşılığında fidyeden belirli bir pay almaktadır. BlackCat'in şifreleyici özelliği sayesinde saldırganlar hem Windows hem de Linux ortamlarında çalışan kötü amaçlı yazılım sürümleriyle saldırılar düzenleyebilmektedir. Diğer bir hizmeti ise zafiyetli bir sistemden veri sızdırmak için kullanılan Fendr yardımcı programıdır.

Şekil 4: BlackCat Ransomware Grubu[8].

BlackCat'e Karşı Alınabilecek Güvenlik Önlemleri

- BlackCat, ilk erişimi elde etmek için daha önce elde edilen oturum açma bilgilerini kullanır. Erişim için çok faktörlü kimlik doğrulamanın (MFA) gerekli kılınması potansiyel olarak giriş noktalarının ele geçirilmesini engelleyebilir [9].
- BlackCat, veri hırsızlığına DDoS yöntemini de dahil etmiştir. Kuruluşların bu durumu önlemek için DDoS koruma hizmetlerinden faydalanması gerekmektedir.

3. Bulut Sistemlerine Giriş

Bulut Bilişim Nedir?

Bulut sistemleri, kişilerin ya da organizasyonların sözleşme karşılığında, ihtiyaçları olan bilişim sistemlerine kolay bir şekilde ulaşabileceği yapılardır. Bu sistemler her geçen gün hayatımızda daha çok yer kaplamaktadır. Aslına bakacak olursak günümüzde birçoğumuzun hayatının bir noktasında bulut bilişim vardır. Örneğin e-posta kullanıyorsanız (Gmail, Hotmail, Yandexmail vb.), Online Ofis programı kullanıyorsanız, oyun konsollarında çevrimiçi oyuncuysanız aslında siz de bir bulut kullanıcısısınız.

Bulut bilişim denildiği zaman karşımıza birçok kavram çıkmaktadır. Bu kavramlar gerek üreticiler gerekse düzenlemeciler tarafından tanımlanmıştır. Tanımlar benzerlik göstermekle birlikte bazı konularda tam bir terim birliği sağlanamamaktadır. Kavramlar tam olarak özümsenmeden konuyla ilgili girişimde bulunmak beklenmedik kaynak kayıplarına (işgücü, maliyet vb.) neden olabilmektedir. Bu yüzden bu yazımızda temel tanımlar ve gereksinimler üzerinde duracağız.

Bulut bilişim nedir sorusunu, Gartner 2022 bulut sağlayıcılar listesinin liderler sekmesinde bulunan tanımlarla ele alalım.

Amazon Web Services (AWS): Bulut bilişim, IT kaynaklarının internet üzerinden, istek üzerine ve kullandıkça ödeme fiyatlandırmasıyla sunulmasıdır[10].

Microsoft Azure: Basitçe açıklamak gerekirse, bulut bilişim, bilgi işlem hizmetlerinin (sunucu, depolama, veritabanı, ağ, yazılım, analiz ve makine zekâsı dahil), daha hızlı yenilik, esnek kaynaklar ve ekonomik ölçeklendirme sunmak üzere, İnternet ("bulut") üzerinden sağlanması anlamına gelir [11].

Google Cloud: Bulut bilişim, bilgi işlem kaynaklarının internet üzerinden hizmetler olarak tedarik etme, yapılandırma veya yönetme ihtiyacının karşılanmasını sağlar ve kullanıcılar yalnızca kullandıkları kadarını öderler[12].

Bu tanımları bir de NIST (National Institute of Standards and Technology) tanımı ile pekiştirelim.

NIST: Bulut bilişim, minimum yönetim çabası veya hizmet sağlayıcı etkileşimi ile hızlı bir şekilde sağlanabilen ve kullandırılabilen, yapılandırılabilir bilgi işlem kaynaklarının paylaşılan bir havuzuna her yerde hazır, uygun, isteğe bağlı ağ erişimi sağlayan bir modeldir[13].

ChatGPT: Bulut sistemleri, bilgisayar ve veri depolama hizmetlerinin internet üzerinden sunulduğu bir teknoloji modelini ifade eder. Bu sistemler, kullanıcıların ihtiyaç duydukları bilgi işlem kaynaklarını (örneğin sunucular, depolama, veritabanları, ağlar) hizmet olarak kiralayabilecekleri veya paylaşabilecekleri sanal bir ortam sağlar. Bulut sistemleri, birçok avantaj sunar. Kullanıcılar, bilgisayarlarına veya cihazlarına bağımlı olmadan herhangi

bir yerden ve herhangi bir zamanda veri ve uygulamalara erişebilirler. Ayrıca, büyük miktarda veriyi depolamak veya karmaşık işlemleri gerçekleştirmek için yüksek performanslı bilgi işlem kaynaklarına kolayca erişebilirler.

Tanımlardaki ortak noktalar bulut karakteristiğini anlatmaktadır. Bu karakteristiklerin tanımlarını ele alacak olursak;

Broad network access: Servisin internet üzerinden sürekli olarak erişilebilir olması.

On-demand self-service: Servisle ilgili bir ihtiyaç olduğunda bulut sağlayıcıyla minimum etkileşimle ilgili hizmet değişikliğin gerçekleştirilebilmesidir.

Resource pooling: Bu, bulut sağlayıcısının finansal olarak kârlı kalabilmesini sağlayan özelliktir. Bulut sağlayıcı ilk aşamada ciddi bir kaynak yatırımı yapar ve müşteriler bu kaynakları bir havuzdan çekebilirler.

Rapid elasticity and scalability: Bulut müşterisinin istediği anda daha fazla ya da daha az hizmet alabilmesini sağlayan özelliklerdir. İkisi genellikle aynı anlamda kullanılsa da aralarında bir nüans vardır. Scalability sadece talebe bağlı olarak artma azalmayı ifade eder. Otomatik olması zorunlu değildir. Elasticity ise müşterinin anlık kullanım durumuna göre eğer isterse hizmette otomatik olarak büyüme ya da küçülme sağlayabilmesi demektir.

Measured service: Bazı kaynaklarda "metered service" olarak da geçmektedir. Müşterinin yalnızca kullandığı kadar ödeme yapması avantajını sağlar. Kullandığın kadar kavramı almış olduğun hizmetin ne olduğuyla ilgilidir.

Bulut Sistemlerine Geçiş

IT ile ilgili birçok kararda olduğu gibi bulut sistemlerine geçiş de bir IT kararı değildir. Bu yönetimsel bir karardır ve bu karar alınmadan önce organizasyonun mevcut durumunun analiz edilmesi gerekir. Mevcut durum analiz edildikten sonra bulut hizmetleriyle ilgili fayda/maliyet analizi yapılmalıdır.

Kullanıcıların bulut sistemlerine geçerken belli beklentileri vardır.

İlk Yatırım Maliyetlerinin Azalması: Temel beklentilerden biri ilk yatırım maliyetlerinin düşürülmesidir. Bu beklentinin gerçekleşmesi seçilecek bulut dağıtım modeliyle yakından ilgilidir. Bazı durumlarda ilk yatırım maliyeti azalacak olsa bile geçerli yasalar ve regülasyonlar çerçevesinde sizin söz konusu modeli seçmemeniz gerekebilir.

Personel Maliyetlerinin Azalması: Doğru bir yapılanma ile bulut sistemlerinin personel maliyetlerini azaltması olasıdır. Aldığınız hizmet modeline bağlı olarak (IaaS/PaaS/SaaS) artık bazı işler doğrudan bulut sağlayıcı tarafında yapılacaktır. Ancak unutmamak gerekir ki bulut sistemlerine geçme kararı ile birlikte yeni işgücüne ihtiyacınız olacak. Bunun için ya mevcut personeli eğitmeniz ya da yeni personel istihdam etmeniz gerekecektir.

Operasyonel Maliyetlerin Azaltılması: Bulut müşterisi her durumda bu beklentiye sahiptir. Neticede artık organizasyon adına bazı operasyonlar bulut sağlayıcı tarafından yapılacaktır. Ancak planlama doğru yapılmazsa bu beklenti gerçekleşmeyebilir. Bulut hizmetleri, doğası gereği minimum etkileşimle alınabilmekte ve artırıp azaltılabilmektedir. Servis alım sürecinin merkezileştirilmemesi, gereğinden fazla alım yapılması gibi durumlar operasyonel maliyetleri çok ciddi bir şekilde artırabilir.

Veri Yedekleme/İş Sürekliliği Maliyetinin Azalması: Hâlihazırda konuyla ilgili yatırım yoksa ya da iyileştirme planlanıyorsa (cold side'dan warm/hot side'a geçiş, yedekleme bileşenlerinin artık yetmemesi vb.) organizasyonlar iş sürekliliği ve veri kurtarma operasyonlarında bulut ortamına geçiş yaparak büyük faydalar sağlayabilirler.

Servis Kategorileri

Bulut sağlayıcılarının çok farklı beklentileri olan müşterileri vardır. Bazı kullanıcılar sadece düzgün çalışan bir uygulama isterken bazı müşteriler tüm IT sistemlerini bulutta yönetmek isteyebilirler. Bu sebepten ötürü servis sağlayıcılar tek bir strateji ile tüm ihtiyaçlara cevap veremezler. Temel olarak bulut servisleri üç kategoride ele alınmaktadır. Bu kategoriler aşağıda tanımlanmıştır.

Software as a Service (SaaS)

Bu kategoride açık bulut servis sağlayıcı müşterisine bütün bir yazılım hizmeti sunar. Organizasyonlar sadece hizmete abone olur ve depolama alanı, ürünün çalışma mantığı, ağ yapılandırma vb. gibi ürünün yönetimiyle ilgili herhangi bir işlem yapmadan doğrudan hizmeti kullanmaya başlar.

E-posta hizmeti, takvim hizmeti çok yaygın olarak birçoğumuzun gündelik hayatta kullandığı SaaS örneklerindendir.

Platform as a Service (PaaS)

Bu kategoride bulut sağlayıcı müşterilerine belirli bir altyapı ve müşterilerinin kendi ürettikleri kodları deneyebileceği işletim sistemi sunar. Yazılım ekiplerinin, özellikle test ortamları için sunucu ayağa kaldırması ve gerekli ayar ve kurulumları yapması yükünü ortadan kaldırır.

Yönetilen veritabanları, Fonksiyon servisi (FaaS: Bulut müşterisinin özelleştirilmiş fonksiyonları zamanlamasını ve/veya bir event sonrasında otomatik olarak tetiklemesini sağlayan servis) IaaS örneklerindendir.

Infrastructure as a Service (IaaS)

Bulut sağlayıcı müşterilerin kullanabilmesi için altyapıyı (sunucu, elektrik, ağ vb.) sağlar. Müşteri altyapı hizmetini

kiralar. Kurulum, güncelleme (yazılım, işletim sistemi vb.) gibi sorumlulukları müşteri üstlenir.

X as a Service (XaaS)

X bir pazarlama stratejisidir. Bulut üreticileri müşterilerine verdikleri hizmetleri x ile anlatırlar. Kulağa çok cazip gelse de bu hizmetler temel olarak yukarıda bahsedilen üç kategoriden biridir (SaaS, PaaS, IaaS).

Bazı X örneklerini ele alacak olursak;

- NaaS: networking as a service
- CaaS: compliance as a service
- DSaaS: data science as a service vb.

Her ne kadar sorumluluklar sonraki yazılarda daha detaylı olarak ele alınacak olsa da burada çok önemli iki konunun altını çizmekte fayda vardır.

- Genel hatları ile modellere göre sorumluluklar yukarıda belirtildiği şekilde ele alınsa da ana bağlayıcı unsur bulut sağlayıcısı ile bulut müşterisi arasında olan sözleşmedir. Sözleşmede hangi tarafın, hangi durumlarda neden sorumlu olacağı konusunda bulanıklık olmamalıdır.
- Eğer hizmet alan taraf müşteri bilgileri tutan bir organizasyon ise bulut sağlayıcıdan kaynaklı bir olay yaşandığında nihai durumda hizmeti alan taraf yasalar önünde müşterilerine karşı sorumlu taraf olmaktadır. Devamında bulut sağlayıcı ile hizmet alan taraf arasında yasal süreç ilerlemektedir. Bunu sadece müşteri verisi tutan organizasyon olarak ele almayabilirsiniz. Eğer bulut tarafında yaşanan bir sorundan ötürü bulut müşterisinin verileri konusunda bir olay (incident) yaşanırsa yasalara karşı asıl sorumlu taraf bulut müşterisi olmaktadır.

Bulut Dağıtım Modelleri

Bulut dağıtım modelleri müşteriye sunulan bulut hizmetinin kullanımının nasıl olacağını anlatan konsepttir. Bu modeller kategoriler ile aynı ana sebepten ötürü çıkmıştır, bir model tüm ihtiyaçları karşılayamamaktadır. Her modelin artıları ve eksileri vardır. Modellerin hiçbiri diğerinden üstün olarak düşünülmemelidir.

Ana dağıtım modelleri;

Private Cloud (Özel Bulut Çözümü): Bu modelde kaynaklar yalnızca bir müşteriye adanmıştır. Ortam çok kullanıcılı (multi-tenant) değildir. Bulut kullanıcısı özel organizasyon bulut sistemlerinin; esneklik, ölçeklenebilirlik ve hızlı hareket edebilme özelliklerinden faydalanır.

Public Cloud (Açık Bulut Çözümü): Multitenancy (çok kullanıcılı/çoklu kiralamalı) modeli kullanılan bir çözümdür. Bulut sağlayıcının sahip olduğu çok büyük bir havuzdan tüm müşteriler eşit koşullarda (kullandığın kadar öde) faydalanır.

Hibrid Bulut Çözümü: Özel ve açık bulutların tanımlarından anlaşılacağı üzere, bazı konularda açık bulutun avantajları çok yüksekken bazı durumlarda özellikle yasal gereksinimlerin devreye girdiği ya da çok kritik verilerin tutulduğu noktalarda organizasyonlar özel bulut çözümlerine yönelmektedir. Hibrid bulut çözümü dediğimiz konsept bunu ifade eder. Bulut müşterisi hem özel bulut çözümünü hem de açık bulut çözümünü farklı işler için bir arada kullanır.

Multi-Cloud Çözümü: Organizasyonlar birçok farklı sebepten ötürü birden çok farklı bulut sağlayıcıdan hizmet alabilirler. Bu durum multi-cloud (çok bulutlu) çözümü olarak tanımlanmaktadır.

Topluluk Bulut Çözümü: Topluluk bulut çözümü birçok yönden özel bulut çözümüne benzer. En temel fark sadece bir organizasyon için özel durumda olmamasıdır. Benzer amaçlar için bir araya gelen bir topluluğa özel çözümdür. Oyun toplulukları çok belirgin bir örnektir. Oyun konsol sağlayıcısı Identity Access Managemet (IAM) çözümü sunar. Oyun sağlayıcılar ise genellikle Information Right Management (IRM) sistemlerini yürütür. Bu şekilde oyunu satın alan kişiler tek bir platform üzerinden kolaylıkla istediği oyunu satın alabilir ve oynayabilir.

Multitenancy (Çoklu Kiralama)

Türkçeleştirmesi en zor kavramlardan biridir. Bu kavramı "Gartner" tanımlaması ile ele alacak olursak; "bir ya da birden çok uygulamanın birden çok bağımsız eş görünümünün paylaşılan bir ortamda çalıştığı yazılımların işletim kipine yönelik bir başvurudur. Eş görünümler (kiracılar) mantıksal olarak yalıtılmış, ancak fiziksel olarak tümleştirilmiştir. Mantıksal yalıtım derecesi tamamlanmalıdır, ancak fiziksel bütünleşmenin derecesi değişecektir[14]."

Çoklu Kiralama bulut sağlayıcının kârlılığını artırabilmesi için kıymetli bir unsurdur. Her ne kadar yalıtılmış olarak ele alınsa da belirli servisler için yasal yükümlülüklerden ötürü kullanımına dikkat etmek çok kritiktir.

Bulut Sistemlerinde Rol ve Sorumluluklar

Bulut sistemlerinde sağlayıcı ve kullanıcı olarak başlıca iki rol vardır. Ancak sistemlerin düzgün ve düzenlemecilerin izin verdiği şekilde çalışabilmesi için diğer roller ortaya çıkmıştır. Rolleri aşağıda belirtildiği gibi özetleyebiliriz.

Cloud Service Provider (Servis Sağlayıcı): Bulut sistemini sağlayan ana işletmedir. Bu işletme doğrudan müşterilere ya da hizmet sağlamada yardımcı olacak üçüncü taraflara hizmet sağlar.

Customers (Servis Kullanıcı): Hizmet alan taraftır.

Cloud service partners: Bulut ekosisteminin verimli ve sağlıklı kullanılabilmesi için önemli bir roldür. Bulut hizmetleri doğrudan alınıp kullanılabilir olmakla birlikte gene de bir entegrasyon gerekmektedir. Kalifiye personelin

istihdam edilmesi her zaman mümkün ya da maliyet verimli olmayabilir. Bu tür gereksinimleri karşılamak için kurulmuş üçüncü taraflardır.

Regulators: Regülasyonları hazırlayan ve yayınlayan taraflardır. Bulut sistemlerine geçmeyi düşünen organizasyonlar; bağlı oldukları ülke, üst kurum, sahip oldukları veri türleri vb. konular çerçevesinde regülasyonlara uygun bir şekilde adımlar atmalıdır. İlgili kanunlara ya da regülasyonlara uymamak bulut sistemi kullanan organizasyonlar için ciddi problemlere yol açabilir.

Cloud Access Security Broker (CASB): Bulut bilişim ortamlarında sistemlerin ve verilerin güvenliğinin sağlanması için kullanılan teknolojidir. CASB, bulut hizmet sağlayıcıları ve kuruluşlar arasında bir köprü görevi görerek, bulut ortamındaki uygulamaları ve verileri yönetir, izler ve korur.

CASB'nin temel amacı, bulut hizmetlerine erişim sırasında güvenlik politikalarının uygulanmasını sağlamaktır. Bulut ortamında verilerin depolanması, kullanıcıların kimlik doğrulama ve erişim kontrolleri, veri şifrelemesi, tehdit tespiti ve engelleme gibi güvenlik gereksinimlerini yönetir.

ISO 17789 Bulut Sistemleri Referans Mimarisi

The International Organization for Standardization (ISO) 17789 dokümanı bulut referans mimarisini ele almaktadır. Bu dokümanda temel terminoloji ve rol sorumlulukları bulunmaktadır. İsmi tersini çağrıştırsa da içinde referans mimarisi yoktur; sadece bulut ortamına geçecek organizasyonlar için yardımcı, bilgilendirici bir dokümandır. Konuları sade bir dille ve net anlatışıyla önemli bir başlangıç noktasıdır. Bulut bilişimle ilgilenecek organizasyon ve kişilerin okuması kıymetli bir artı olacaktır[15].

ISO 17789 dokümanına göre bulut kullanıcısının sorumluluğunda olan bazı işlemler:

- Hizmet denemeleri gerçekleştirmek
- Hizmetleri izlemek
- Hizmet güvenliğini yönetmek
- Sorun raporlarını işlemek
- Hizmet seçimi yapmak
- Denetim raporları istemek

ISO 17789 dokümanına göre bulut servis sağlayıcısının sorumluluğunda olan bazı işlemler:

- Sistemleri hazırlamak
- Hizmetleri izlemek ve yönetmek
- Denetim verileri sağlamak
- Müşteri ilişkilerini ve müşterilerin taleplerini yönetmek

ISO 17789 dokümanına göre bulut servis partnerlerinin sorumluluğunda olan bazı işlemler:

- Hizmet bileşenlerini tasarlamak ve oluşturmak
- Test hizmetleri
- Denetimler gerçekleştirmek
- Yasal anlaşmalar oluşturmak
- Pazarı değerlendirmek

Bu maddeler gerçek hayatta tam olarak uygulanmayabilir. Ancak genel bakış açısını anlamak için kıymetlidir.

Bulut Bilişim Hususları

Hangi bulut dağıtım modeli seçilirse seçilsin bulut sistemlerine geçilirken aşağıda belirtilen hususları ele almak gerekmektedir.

Güvenlik Hususları

Bulut sistemleri, IT sistemleri ile temelde aynı güvenlik endişelerini taşır. Ancak bazı sorunlar bulut teknolojisinde IT sistemlerine göre daha yoğundur. Örneğin IT sistemlerinde verinin nerede olduğu bilinir, ancak bulut sistemlerinde bu durum değişmektedir. Bu sebepten ötürü bulut sistemlerinde denetlenebilirlik ve yasal yükümlülükler hususlarına farklı perspektiflerde dikkat edilmelidir.

En temel hususlar IT sistemlerinde de olduğu gibi CIA (Confidentiality, Integrity, Availability) üçlüsüdür.

Gizlilik, Bütünlük ve Erişilebilirlik gereksinimlerinin yanı sıra bulut sistemlerinde "Kişisel verilerin gizliliği (Privacy)", "denetlenebilirlik (Auditability)" ve "yasal yükümlülükler" de ele alınması gereken hususlardır.

Yanlış anlamaların önüne geçmek amacıyla denetlenebilirlik gereksinimini biraz açmakta fayda vardır.

Auditability (Denetlenebilirlik): Bulut bilgi işlem sözleşmeleri, müşterinin bulut sağlayıcılarını doğrudan veya bir üçüncü taraf aracılığıyla denetleme hakkına sahip olduğunu belirtmelidir. Bu denetimler planlı veya plansız olarak gerçekleştirilebilir ve müşterinin bulut satıcısının güvenlik yükümlülüklerini yerine getirdiğine dair güvence almasına olanak tanır. Denetimler yasal sorumlulukların yanı sıra operasyonel ve finansal hususları da içerebilir.

Operasyonel Hususlar

Erişilebilirlik

Erişilebilirlik hem güvenlikle ilgili hem de operasyonel bir unsurdur. Bulut performansının en önemli performans göstergelerinden biridir. Unutmamak gerekir ki öncesinde organizasyonun iş etki analizi ile sistemleri için RTO (Recovery Time Object), RPO (Recovery Point Object) ve MTD (Maximum Tolerable Downtime) gibi özellikleri belirmiş olmaları gerekmektedir.

Örnek olarak ihtiyaç yüzde 90 erişilebilirlik ise (downtime per year = 35,53 gün) ama sektörde çok sık olarak karşımıza çıktığı gibi yüzde 99,999 (five-nines, downtime per year = 5,26 dakika)) seçilir ise çok ciddi maliyet artışı olacaktır. Tam tersi bir durumda ise organizasyonlar ciddi

mali kayıplar ve itibar kayıplarıyla ve erişilebilirlik yasal yükümlülük ise daha ciddi yasal problemlerle yüzleşmek durumunda kalabilirler.

İdame ve Versiyon Kontrolü

Versiyon kontrolü ve bakım işlemleri IT sistemleri için çok önemlidir. Ancak bu süreç bir o kadar da zahmetli ve karmaşıktır, özellikle de söz konusu olan bulut sistemlerse. Sistemlerin versiyon kontrolünü hangi tarafın yürüteceği net olarak belirlenmiş olmalıdır. Eğer versiyon güncelleştirme işlemleri bulut sağlayıcısı tarafından yapılacak ise ilgili güncellemelerin ne gibi etkilerinin olacağı önceden değerlendirilip gereken hazırlıklar yapılmalıdır.

Temin Hususları

Bulut sistemlerine geçiş kararı ile birlikte artık bazı operasyonların kontrolü kaybedilmektedir. Bu fonksiyonlar her ne kadar bulut kategorilerine göre ve sözleşmelere göre değişiklik gösterse de artık yeni bir yüklenicinin olduğu aşikâr. Bulut geçiş sürecinde sağlayıcı seçimi ve sözleşme maddeleri çok kritiktir.

Organizasyonlar, "bir şekilde buluta geçiş planlandığı gibi gitmez ise tekrar kendi sistemlerimize dönüş yapabilir miyiz?" "Ne kadar sürede yapabiliriz?" "Bu durumun bize maliyeti (işgücü, maliyet vb.) ne olur?" gibi konuları derinlemesine analiz etmelidir. B, C planları her zaman için bulundurulmalıdır.

Organizasyonlar, yeni bir bulut çözümünü etkinleştireceği zaman bulut sağlayıcıların birlikte çalışabilirliğini göz önünde bulundurmalıdır. Bu, özellikle SaaS ve PaaS ürünleri için önemlidir. IT ekiplerinden çözümleri düzenli olarak entegre etmeleri istenir ve sağlayıcının bu entegrasyonları destekleme becerisi çok önemlidir.

Ele alınması gereken bir diğer husus **vendor lock-in** diye tabir edilen belli bir bulut sağlayıcısına bağımlı kalma durumudur. Bunun tam tersi taşınabilirlik (portability) olarak geçmektedir. Tasarım aşamasında amaçlarımızdan birisi taşınabilirliği yüksek bir yapı olmasıdır. Ancak bu her zaman mümkün olmayabilir. Bulut sağlayıcı ile yaşanabilecek bir diğer büyük sorun ise **vendor lock-out** diye tabir edilen, bulut sağlayıcının şu ya da bu nedenden çalışmayı durdurması olayıdır. Bulut müşterileri böyle bir durumla karşı karşıya kalmamak adına sağlayıcının geçmişte yaşadığı olaylara, finansal istikrarına dikkat ederek seçim yapmalıdır.

Daha önce de değindiğimiz gibi gerek bir servisin gerekse tüm IT altyapısının buluta geçiş kararının IT ya da IT ekibi ile ilgisi yoktur. Bu kararlar tamamen yönetimsel kararlardır. Bilgi eksiği varsa ve gerekli altyapı oluşturulamaz ise bulut sistemlerine geçiş çabası büyük hayal kırıkları ve kaynak kayıpları ile sonuçlanabilir. Bu gibi durumların önüne geçilmesi için öncelikle aynı dili konuşmak, doğru analizleri yapmak ve gerekli işgücünü geliştirmek gerekmektedir.

4. Django Web Uygulama Çerçevesi

Django, Python programlama dili ile geliştirilen açık kaynaklı bir web uygulama çerçevesidir. Web uygulamalarının hızlı ve etkili bir şekilde geliştirilmesini sağlayan bir araç seti ve yapısı sunar. Django, basit ve karmaşık web projeleri için birçok bileşene ve özelliğe sahiptir.

Django'nun temel hedefi, geliştiricilerin web uygulamalarını hızlı oluşturmalarına yardımcı olmaktır. Django, önceden tanımlanmış kalıpları ve yapıları kullanarak geliştirme sürecini hızlandırır ve tekrarlayan görevleri otomatikleştirir. Bu sayede, geliştiriciler daha az kod yazarak daha fazla iş başarabilirler.

Django'nun bazı temel özellikleri şunlardır:

1. **ORM (Object-Relational Mapping):** Django, veritabanı ile etkileşimde bulunmak için bir ORM sağlar. Bu, veritabanı tablolarını Python sınıflarıyla temsil etmeyi ve veritabanı işlemlerini nesne yönelimli bir şekilde gerçekleştirmeyi sağlar.
2. **MVC (Model-View-Controller) veya MVT (Model-View-Template) Mimari:** Django, uygulama mantığını, veritabanı işlemlerini ve kullanıcı arayüzünü ayrı bileşenlere ayırarak bir MVC veya MVT yapısını takip eder. Bu, kodun daha düzenli, modüler ve sürdürülebilir olmasını sağlar.
3. **Otomatik Yönlendirme**: Django, URL yapılandırmasını kolayca yönetmek için bir yönlendirme mekanizması sağlar. Bu mekanizma, gelen URL taleplerini doğru view'e yönlendirir ve işleme koymak için gerekli parametreleri sağlar.
4. **Otomatik Admin Arayüzü**: Django, veritabanı modellerine dayalı olarak otomatik bir yönetici arayüzü sağlar. Bu arayüz sayesinde, veritabanı verilerini düzenlemek, eklemek veya silmek için bir yönetici paneli oluşturmak kolaylaşır.
5. **Form İşleme**: Django, form oluşturma ve form verilerini doğrulama gibi işlemleri kolaylaştıran bir form işleme mekanizması sağlar. Bu, kullanıcı girişlerini kontrol etmek ve verileri güvenli bir şekilde işlemek için geliştiricilere olanak tanır.

Django, güçlü bir topluluğa sahiptir ve sürekli olarak geliştirilmekte ve güncellenmektedir. Açık kaynaklı olması, geliştiricilere esneklik ve özelleştirme imkânı sağlar. Django, birçok büyük web uygulamasında kullanılmaktadır ve yaygın olarak kabul edilen bir web çerçevesi hâline gelmiştir.

Django'nun dışında birçok başka açık kaynaklı web uygulama çerçevesi bulunmaktadır. İşte Django'yu diğer bazı popüler açık kaynaklı web uygulama çerçeveleriyle karşılaştıran bazı faktörler:

Flask: Flask, Python tabanlı bir web uygulama çerçevesidir. Django'ya kıyasla daha hafif bir yapıya sahiptir ve daha az bileşen içerir. Flask, daha esnek bir yapı sunar

ve minimalist bir yaklaşım benimser. Django, daha kapsamlı bir çerçeve olarak iş mantığınızı ve veritabanı işlemlerinizi yönetmek için daha fazla bileşene sahiptir.

Ruby on Rails: Ruby on Rails (RoR), Ruby programlama diliyle geliştirilen bir web uygulama çerçevesidir. RoR, Django'ya benzer şekilde veritabanı işlemlerini ve model-view-controller (MVC) mimarisini destekler. Django, Python dilini kullanan geliştiriciler için daha doğal bir tercih olabilirken, RoR daha çok Ruby diline hâkim olan geliştiriciler için iyi bir tercih olabilir.

Laravel: Laravel, PHP tabanlı bir web uygulama çerçevesidir. Laravel, Django'ya benzer şekilde MVC yapısını destekler ve veritabanı işlemleri için ORM sağlar. Laravel, PHP topluluğunda oldukça popülerdir ve geniş bir eklenti ve paket ekosistemine sahiptir.

Express.js: Express.js, Node.js tabanlı bir web uygulama çerçevesidir. Django'dan farklı olarak, JavaScript kullanarak hem sunucu tarafı hem de istemci tarafı kodlamayı mümkün kılar. Express.js, hızlı ve hafif bir yapıya sahiptir ve minimalist bir yaklaşım benimser. Django ise daha kapsamlı bir çerçeve olarak gelişmiş veritabanı işlemleri ve otomatik yönlendirme gibi özellikleri içerir.

Django'yu seçmeniz için bazı nedenler şunlar olabilir:

Hızlı Geliştirme: Django, geliştirme sürecini hızlandırmak için bir dizi araç ve yapı sunar. Hazır olarak gelen bileşenler ve otomatik oluşturulan yönetici arayüzü gibi özellikler, web uygulamalarının hızlı bir şekilde oluşturulmasını sağlar.

Güvenlik: Django, güvenlik konusuna büyük önem verir. Kimlik doğrulama ve yetkilendirme mekanizmaları, kullanıcı bilgilerinin güvenli bir şekilde işlenmesini sağlar. Ayrıca, Django'nun güncellemeleri ve topluluk tarafından sağlanan güvenlik düzeltmeleri sayesinde güvende kalmanızı sağlar.

Veritabanı İşlemleri: Django, güçlü bir ORM (Object-Relational Mapping) sistemine sahiptir. Bu sayede, veritabanı işlemleri nesne yönelimli bir şekilde gerçekleştirilir ve veritabanı bağımsızlığı sağlanır. Django, birçok yaygın veritabanı sistemiyle uyumlu çalışabilir.

Modüler ve Ölçeklenebilir: Django, modüler bir yapıya sahiptir. Uygulamalarınızı küçük ve bağımsız bileşenlere bölebilir ve gerektiğinde genişletebilirsiniz. Django, büyük ve karmaşık projeler için ölçeklenebilirlik sağlar.

Zengin Topluluk Desteği: Django, büyük ve aktif bir topluluğa sahiptir. Birçok geliştirici ve uzman, Django ile ilgili sorulara cevap vermek, kaynak paylaşmak ve çözümler sunmak için topluluk forumlarında bulunur. Bu da sizin sorunlarınızı çözmek ve geliştirmenizi desteklemek için bir kaynak havuzuna erişiminiz olduğu anlamına gelir.

Özelleştirme ve Esneklik: Django, açık kaynaklı bir çerçeve olduğu için tamamen özgürce özelleştirilebilir. İhtiyaçlarınıza ve projenizin gereksinimlerine göre çerçevenin çeşitli bileşenlerini değiştirebilir veya özelleştirebilirsiniz.

Django, güvenlik konusuna büyük önem veren bir web uygulama çerçevesidir. Aşağıda bununla ilgili bazı örnekleri görebilirsiniz:

1. *Cross-Site Scripting (XSS) Koruması:*

Django, varsayılan olarak XSS saldırılarına karşı koruma sağlar. Template'lerde otomatik olarak HTML özel karakterlerini kaçırır ve kullanıcı girişlerini güvenli bir şekilde temsil eder.

Python:

```python
from django.utils.html import escape

def my_view(request):
    user_input = request.GET.get('input')
    safe_input = escape(user_input)
    return HttpResponse(safe_input)
```

Şekil 5: Django XSS koruması.

2. *Cross-Site Request Forgery (CSRF) Koruması:*

Django, CSRF saldırılarına karşı varsayılan olarak koruma sağlar. Her bir form talebi için otomatik olarak bir CSRF tokeni üretilir; formda bu token'ın kullanılması gerekmektedir.

Html:

```html
<form method="post" action="/my_view/">
    {% csrf_token %}
    <!-- form fields -->
    <input type="submit" value="Submit">
</form>
```

Şekil 6: Django CSRF koruması.

3. *Kimlik Doğrulama ve Yetkilendirme:*

Django, kullanıcı kimlik doğrulama ve yetkilendirme işlemleri için güvenli bir yapı sağlar. Kullanıcıların oturum açma, oturumu sonlandırma, parola sıfırlama gibi işlemlerini kolaylaştırır.

Python:

```python
from django.contrib.auth.decorators import login_required
from django.contrib.auth.models import User

@login_required
def my_view(request):
    # Sadece oturumu açık kullanıcılar bu view'e erişebilir
    user = request.user
    # Kullanıcının yetkilendirme işlemleri
    # ...
```

Şekil 7: Django kimlik doğrulama.

4. *Veritabanı İşlemleri ve ORM:*

Django'nun ORM (Object-Relational Mapping) sistemi, güvenli veritabanı işlemlerini destekler. Sorguların doğru şekilde parametrelendirilmesini sağlar ve SQL enjeksiyonu saldırılarını önler.

Python:

```python
from django.db import models

class Product(models.Model):
    name = models.CharField(max_length=100)
    price = models.DecimalField(max_digits=10, decimal_places=2)
```

Şekil 8: Django veritabanı işlemleri ve ORM.

5. *Güncelleme ve Güvenlik Düzeltmeleri:*

Django, güvenlik açıklarını düzeltmek için düzenli güncellemeler yayınlar. Güvenlik düzeltmeleri, Django'nun topluluk tarafından tespit edilen ve çözülen güvenlik açıklarını giderir.

Django kimlik doğrulama ve yetkilendirme işlemleri kolay bir şekilde yapılandırılabilir:

Django'da kimlik doğrulama ve yetkilendirme işlemleri, projenizin ana dizin yapısı içinde bulunan settings.py, urls.py, views.py ve models.py gibi dosyalarda yapılandırılır.

1. Proje Dizin Yapısı:

Django projesi genellikle aşağıdaki gibi bir dizin yapısına sahiptir:

```
myproject/
    manage.py
    myproject/
        __init__.py
        settings.py
        urls.py
        wsgi.py
    myapp/
        __init__.py
        models.py
        views.py
```

Şekil 9: Django proje yapısı.

2. **settings.py** dosyası:

Kimlik doğrulama ve yetkilendirme ayarları, settings.py dosyasında yapılandırılır. Bu dosyada AUTHENTICATION_BACKENDS ve AUTH_USER_MODEL gibi ilgili ayarlar bulunur.

```python
# settings.py

# Kimlik doğrulama arka planını belirleme
AUTHENTICATION_BACKENDS = [
    'django.contrib.auth.backends.ModelBackend',
]

# Kullanıcı modelini özelleştirme
AUTH_USER_MODEL = 'myapp.CustomUser'
```

Şekil 10: Django kimlik doğrulama ayarları.

3. **models.py** dosyası:

Kullanıcı modeli, models.py dosyasında özelleştirilir. **AbstractUser** veya **AbstractBaseUser** sınıflarından türetilen bir özel kullanıcı modeli oluşturulabilir.

```python
# models.py

from django.contrib.auth.models import AbstractUser
from django.db import models

class CustomUser(AbstractUser):
    # Özel kullanıcı alanları
    age = models.IntegerField()
```

Şekil 11: Django veritabanı modelleri.

4. **views.py** dosyası:

Kimlik doğrulama ve yetkilendirme ile ilgili işlemler, views.py dosyasında tanımlanır. Örneğin, kullanıcı kaydı, oturum açma ve oturumu kapatma gibi işlemler burada yer alır.

```python
# views.py

from django.contrib.auth import authenticate, login, logout
from django.shortcuts import render, redirect

def register(request):
    if request.method == 'POST':
        # Kayıt formundan verileri al
        # Yeni kullanıcı oluştur ve kaydet
        # Oturumu aç ve ana sayfaya yönlendir
        pass
    else:
        # Kayıt formunu göster
        return render(request, 'register.html')

def user_login(request):
    if request.method == 'POST':
        # Oturum açma formundan verileri al
        # Kullanıcıyı kimlik doğrula
        # Oturumu aç ve ana sayfaya yönlendir
        pass
    else:
        # Oturum açma formunu göster
        return render(request, 'login.html')

def user_logout(request):
    # Oturumu kapat ve çıkış yap
    # Ana sayfaya yönlendir
    pass
```

Şekil 12: Django views.py dosyası.

5. **urls.py** dosyası:

Kimlik doğrulama ve yetkilendirme işlemlerinin URL rotaları, urls.py dosyasında tanımlanır. Bu rotalar, ilgili görünümlere yönlendirme yapar.

```
# urls.py

from django.urls import path
from myapp import views

urlpatterns = [
    path('register/', views.register, name='register'),
    path('login/', views.user_login, name='login'),
    path('logout/', views.user_logout, name='logout'),
]
```

Şekil 13: Django urls.py dosyası.

Bu örnekler, Django'da kimlik doğrulama ve yetkilendirme işlemlerinin temel yapısını göstermektedir. Projelerin gereksinimlerine ve özel senaryolarına göre bu yapı özelleştirilebilir.

Django, güçlü ve esnek yapısıyla web uygulama geliştirme sürecini büyük ölçüde kolaylaştıran bir çerçevedir. Django, geliştiricilere hızlı ve güvenli bir şekilde web projeleri oluşturma imkânı sunar. Ayrıca, Django REST Framework gibi ek paketlerle API geliştirme deneyimini daha da güçlendirir. Django'nun kapsamlı belgelendirmeleri, geniş topluluğu ve büyük bir ekosistemi bulunmaktadır. Bu nedenlerle, Django, web geliştirme alanında popüler bir seçenek hâline gelmiştir.

5. Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği

6 Haziran 2023 tarihli ve 32213 sayılı *Resmi Gazete*'de Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği yayınlanmıştır. Bu yönetmeliğin amacı; enerji sektöründe kullanılan endüstriyel kontrol sistemlerinin siber güvenliğini sürekli olarak gelişen ihtiyaç ve tehditlere göre iyileştirmeye, asgari kabul edilebilir güvenlik seviyesini tanımlamaya ve bu kontrol sistemlerinin siber dayanıklılığına, yeterliliğine ve olgunluğuna ilişkin usul ve esasları düzenlemektir.

Yönetmelik Bilgi ve İletişim Güvenliği Rehberi, Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları, TS ISO/IEC 27001 Standardı, TS EN ISO/IEC 27019 Standardı ve Enerji sektöründe EKS güvenlik kontrollerini referans almaktadır.

Yetkinlik modeli ana kontrol başlıkları ise Endüstriyel Ağ Güvenliği, Endüstriyel İstemci ve Sunucu Güvenliği, Endüstriyel Tehdit ve Zafiyet Yönetimi, Endüstriyel Siber Güvenlik Risk Yönetimi, Endüstriyel Varlık, Değişim ve Konfigürasyon Yönetimi, Endüstriyel Kimlik ve Erişim Yönetimi, Endüstriyel Olay Yönetimi ve Süreklilik, Akıllı Cihaz Güvenliği, Endüstriyel Operasyon Güvenliği, İnsan Kaynakları Güvenliği, Fiziksel Güvenlik, Tedarikçi Yönetimi ve PLC güvenliği şeklindedir.

Yetkinlik modeli kapsamında yükümlü kuruluşların kritiklik seviyeleri yüksek olandan düşük olana göre; A Sınıfı, B Sınıfı, C Sınıfı olarak üçe ayrılmıştır. Belirlenen A, B ve C Sınıfı kritiklik derecelerinin asgari uygulamaları gereken yetkinlik seviyeleri ise sırasıyla Seviye 3, Seviye 2 ve Seviye 1 kontroller olarak tanımlanmıştır.

Kritiklik Derecesi	Açıklama	Asgari Seviye	Açıklama
A Sınıfı	İlgili sektörde kritiklik derecesi en yüksek olan yükümlü kuruluşların sınıfını ifade eder.	Seviye 3	Bu seviyede yer alan kontroller yeni bir projelendirme ya da uzun soluklu değişim gerektirir.
B Sınıfı	İlgili sektörde kritiklik derecesi orta olan yükümlü kuruluşların sınıfını ifade eder.	Seviye 2	İlgili kontrollerin uygulanabilmesi için yükümlü kuruluş sistemlerinde veya süreçlerinde değişiklik yapılmasını gerektiren maddeler bu seviyede toplanır.
C Sınıfı	İlgili sektörde kritiklik derecesi beklenen seviyede olan yükümlü kuruluşların sınıfını ifade eder.	Seviye 1	İlgili kontrollerin hâlihazırda uygulandığı ya da kolayca uygulanabileceği değerlendirilen maddeler bu seviyede toplanır.

Tablo 1: Kritiklik derecesi asgari seviyeleri.

Asgari uygulanacak kontroller, elektrik dağıtım şirketleri için asgari Seviye 2 ve doğalgaz dağıtım şirketleri için asgari Seviye 1 olarak belirlenmiştir. Özdenetim/Fark Analizlerinden sonra ilgili kontrol maddelerinin hedeflenen tamamlanma süreleri ise Seviye 1, 2 ve 3 için sırasıyla 12 ay, 18 ay ve 24 ay olarak ifade edilmiştir.

Yükümlü kuruluşların sektörel kritiklik dereceleri EPDK tarafından belirlenecektir. Yetkinlik modeli uygulama yükümlülüğü EPDK tarafından yapılan bilgilendirme sonrasında başlayacaktır. Yükümlü kuruluşların yetkinlik modeline uyumluluğu üç aşamada gerçekleşecektir;

1. Aşama Öz Denetim/Fark Analizi: İlgili kontrol maddelerini kuruluşların kendi iç kaynakları ile denetlemesi sürecidir. Bu sürecin, yükümlülüklerin başlamasından itibaren üç ay içerisinde tamamlanması gerekmektedir. Tamamladıktan sonra en geç bir ay içerisinde raporlar Enerji Piyasası Bildirim Sistemi aracılığı ile EPDK'ya iletilecektir.
2. Aşama Sektörel Denetim: Yönetmelik kapsamında belirlenen şartlara uyan denetim firması tarafından gerçekleştirilen çalışmalardır. Bağımsız denetim olarak da değerlendirilir.

3. Aşama Kurum Denetimleri: Denetçi firmaların ve yükümlü kuruluşların denetlendiği çalışmalardır. Çapraz denetim ya da kontrol denetimi olarak da değerlendirilen çalışmalardır. Bu denetimler süreç içinde her zaman yapılabilecektir.

Yükümlü kuruluşlar, hedeflenen tamamlama süresinde uygulamakla yükümlü oldukları Elektrik/Doğalgaz Dağıtım Sektörü Siber Güvenlik Yetkinlik Modeli Teknik Kontrol Maddeleri kontrollerini değerlendirirken "Tam Uyum", "Kısmen Uyum", "Uyumsuz", "Kapsam Dışı" sınıflandırmalarını kullanacaktır.

Denetçi firma ve personelinin Bilgi ve İletişim Güvenliği Denetim Rehberinde hizmet alımı ile oluşturulan denetim ekibi için belirlenen kriterlere ek olarak, yetkinlik modeli denetimlerini yapacak firma personelinde Kritik Altyapılar Ulusal Test Yatağı Merkezi tarafından verilen EKS eğitimleri sonrası başarı sertifikası aranmaktadır. Firmaların Yetkinlik Modeli denetimi yapabilmeleri için başvuru dilekçelerini EPDK'ya iletmeleri gerekmektedir.

6. Software Bill Of Materials (Sbom) Ve Yazılım Tedarik Zinciri Güvenliği

Yazılım tedarik zinciri, günümüzde birçok sektörde kritik öneme sahip olan yazılımların geliştirilmesi ve dağıtılması sürecini kapsar. Ancak, karmaşık bir tedarik zinciri boyunca güvenlik açıklarının ve zayıflıklarının ortaya çıkması yaygın bir durumdur. Bir yazılımın tüm bileşenlerinin ve bunların güvenlik durumlarının izlenmesi, güvenli yazılım geliştirme sürecinde kritik bir gerekliliktir. Bu noktada, Software Bill of Materials (SBOM) devreye girer[16].

SBOM, bir yazılım projesinde kullanılan bileşenlerin envanterini tutan bir meta veri dosyası olarak tariflenebilir.

Bu dosya içinde geliştirilen yazılımda kullanılan açık kaynak kütüphaneler, üçüncü taraf bileşenler, ticari yazılımlar ve hizmet sağlayıcılar tarafından sağlanan bileşenler tutulmaktadır. Her bileşen için ad, sürüm, lisans bilgileri ve kaynak bağlantıları gibi bilgileri içeren bir yapı sağlanmaktadır[17].

Örnek bir SBOM yapısı aşağıda verilmiştir[18].

```
<SoftwareBillOfMaterials xmlns="http://example.com/sbom"xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://example.com/sbom sbom.xsd">
  <ProjectName>Örnek Uygulama</ProjectName>
  <Version>1.0</Version>
  <CreationDate>2023-06-15</CreationDate>
  <UpdatedDate>2023-07-01</UpdatedDate>
  <Components>
    <Component>
      <Name>Örnek Kütüphane</Name>
      <Version>2.1.0</Version>
      <License>MIT License</License>
      <Source>https://github.com/example-library</Source>
    </Component>
    <Component>
      <Name>Yardımcı Kütüphane</Name>
      <Version>1.3.5</Version>
      <License>Apache License 2.0</License>
      <Source>https://github.com/helper-library</Source>
    </Component>
    <Component>
      <Name>Arayüz Kütüphanesi</Name>
      <Version>3.2.1</Version>
      <License>BSD License</License>
      <Source>https://github.com/interface-library</Source>
    </Component>
</SoftwareBillOfMaterials>
```

SBOM, yazılım ekosistemlerinde şeffaflığı artırır, riskleri azaltır ve güvenli yazılım geliştirmeyi destekler. Hem yazılım geliştiricileri hem de tedarik zinciri paydaşları için önemli bir araçtır ve güvenlik, lisans uyumluluğu ve yönetim süreçlerini iyileştirmeye yardımcı olur[19].

SBOM'un tedarik zinciri güvenliğinde sağladığı faydalar aşağıdaki başlıklarda ele alınabilir[20].

1. **Bileşen İzleme ve Güvenlik Değerlendirmeleri:** SBOM, tedarik zinciri boyunca kullanılan bileşenlerin izlenmesine olanak tanır. Her bileşenin sürümü ve kaynak bilgileri sağlandığı için, güvenlik açıkları ve zayıflıklarının tespit edilmesi ve değerlendirilmesi kolaylaşır. SBOM üzerinden bileşenlerin güvenlik değerlendirmeleri yapılabilir ve riskli bileşenler belirlenerek düzeltici önlemler alınabilir.
2. **Lisans Uyumluluğu ve Lisans Yönetimi:** SBOM, kullanılan bileşenlerin lisans bilgilerini içerir. Bu, yazılım projelerinin lisans uyumluluğunu sağlamak için kritik öneme sahiptir. SBOM, açık kaynak bileşenlerin lisans gerekliliklerini takip etmek, lisans ihlallerini önlemek ve yasal gerekliliklere uygunluk sağlamak için kullanılabilir.
3. **Güncel Kalma ve Güvenlik Yamaları:** SBOM, kullanılan bileşenlerin sürüm bilgilerini içerir. Bu sayede, güncellemelerin takip edilmesi ve güvenlik yamalarının uygulanması kolaylaşır. Bileşenlerin güncel sürümlerinin izlenmesi, güvenlik açıklarının hızlı bir şekilde giderilmesini ve yazılımın güvenliğinin artırılmasını sağlar.
4. **Soruşturma ve Geriye Dönük İzleme:** SBOM, her bileşenin tanımlanması ve izlenebilir olmasını sağlar. Bu, yazılım projelerinde meydana gelen güvenlik

olayları veya hatalar durumunda geriye dönük soruşturma yapmayı kolaylaştırır. SBOM üzerindeki bilgileri kullanarak, olayın kaynağına hızlı bir şekilde ulaşılabilir ve gerekli önlemler alınabilir.

SBOM, yazılım tedarik zinciri güvenliğinin sağlanması için önemli bir araçtır. SBOM kullanımı, yazılımı oluşturan hazır bileşenlerin izlenmesi, güvenlik değerlendirmeleri yapılması, lisans uyumluluğunun sağlanması, güncellemelerin takip edilmesi ve geriye dönük izlemeye imkân verir. SBOM, yazılım projelerinin güvenlik risklerini azalttığı ve yazılım tedarik zinciri güvenliğinin artmasına katkı sağladığı değerlendirilmektedir.

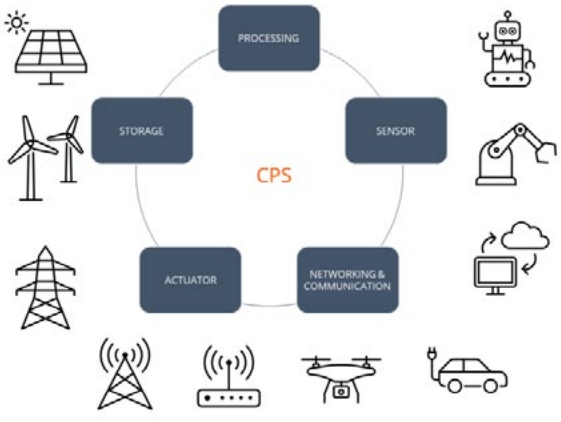
7. Siber-Fiziksel Sistemlerin Güvenliği ve Önemi

CPS (Cyber-Physical System), yani Siber-Fiziksel Sistemler, fiziksel ve dijital bileşenlerin birlikte çalıştığı gerçek zamanlı yeni nesil bir gömülü sistemdir.

Yakın zamana kadar bazı akademik makaleler de dahil olmak üzere IoT (Internet of Things - Nesnelerin interneti) ile CPS terimlerinin aralarında büyük bir gri örtüşme alanı olmasından dolayı birbirlerinin yerine kullanıldığı gözlemlenmektedir.

Genel olarak, IoT adlandırma, algılama ve işleme yeteneklerine sahip olan nesneleri birbirine bağlayan bir iletişim ağı olarak tanımlanır. Buna karşılık CPS terimi, fiziksel dünyadaki varlıkların izlenmesi ve kontrolü için bilgi işlem ve iletişim yetenekleri ile bütünleşmiş gerçek zamanlı dağıtık kontrol sistemlerini de içeren sistemlerle ilgilidir. Dahası, CPS, birbirine bağlı ve işbirlikçi akıllı bilgi ve iletişim teknolojisi olarak yeni nesil gömülü sistem olarak anılmaktadır[21].

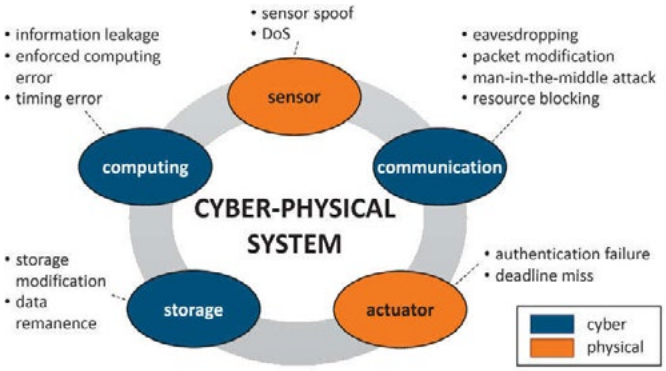
Gün geçtikçe daha popüler hâle gelen bu sistemler artık günlük hayatımızda bile birçok alanda karşımıza çıkmaktadır. Örnek olarak, bir fabrikada otomatik makinelerin, robotların birlikte çalışması veya sağlık sektöründe tıbbi cihazların veri paylaşımı, sivil ve askeri birçok alandaki



Şekil 14: CPS Siber-Fiziksel Sistem[22].

sistemlerde gerçek zamanlı veri paylaşımı ve/veya işlenmesi ile fiziksel bileşenlerin hareketleri CPS örnekleri olarak karşımıza çıkar.

CPS'ler kötü niyetli kişilerin siber saldırılarına maruz kalabilir. Bu saldırılar sistemin siber güvenliğin temel bileşenlerinden olan erişilebilirliğine, gizliliğine ve bütünlüğüne zarar verebilir. Diğer bir ifade ile sistemin kapalı kalma süresine, veri kaybına, hatalı çalışmasına ve hatta kullanıcıların fiziksel olarak zarar görmesine neden olabilir. Bu nedenle CPS'i bu tehditlerden korumak ve sistemlerin doğru ve güvenli bir şekilde çalışmasını sağlamak için güvenlik önlemleri alınması önemlidir.



Şekil 15: CPS siber saldırı örnekleri[23].

Bu önlemler siber güvenliğin temel bileşenleri ekseninde sistemin ve varlıklarının kritikliği referans alınarak belirlenmelidir.

Önlemlerin direktif, caydırıcı, önleyici, telafi edici, tespit edici, düzeltici ve iyileştirici kontroller olarak tiplerine göre sınıflandırılması da tespit edilen risklere karşı önlemlerin etkilerini gözlemlemek ve yeterliliğine karar verebilmek için faydalı olacaktır.

Önlemleri ayrıca veri güvenliği, ağ güvenliği, yazılım güvenliği gibi alanlara göre gruplandırılabiliriz.

CPS'lerin işleyişinde veri paylaşımı temel bir gerekliliktir. Bu nedenle, verilerin doğru, güvenli ve değiştirilmeden saklanması, iletilmesi ve kullanılması önemlidir. Veri güvenliği için verilerin maruz kalabileceği durumlarına göre belirlenmiş tehditler ve bu tehditlere karşı önlemlerin belirlenmesi modüler ve analitik yaklaşım içinde faydalı olacaktır. Belirlenecek bu önlemlerden verilerin gizliliği için başlıca verilerin şifrelenmesi, yani gizli bir şekilde saklanması ve/veya iletilmesi büyük önem taşır. Şifreleme, verilerin sadece yetkili kişiler/sistemler tarafından anlaşılabilir hâle gelmesini sağlar. Ayrıca, veri bütünlüğünün sağlanması için dijital imzalar kullanılabilir. Dijital imzalar, verilerin değiştirilip değiştirilmediğini ve güvenilirliğini kontrol etmek için kullanılır. Böylece, verilerin güvenliği ve doğruluğu sağlanır. Verilerin erişilebilirliğini sağlamak adına da verilerin işlenmesi iletimi ve depolanması süreçlerinde kullanılan varlıkların

yedeklenmesi düşünülebilir. Bunlar olası istenmeyen durumlarda veriye erişimin kesintiye uğramamasına katkı sağlayacaktır.

Ağ güvenliği, CPS'lerin bir ağ üzerinden iletişim kurduğu düşünüldüğünde kritik bir öneme sahiptir. CPS'lerin bağlı olduğu ağlar özellikle internete bağlı ise siber saldırılara karşı çok daha savunmasız olabilir. Ağın yapısına bağlı olarak çok farklı önlemler alınabilir. Örneğin güvenlik duvarları gibi önlemler kullanılarak ağın korunması sağlanabilir. Güvenlik duvarları, yetkisiz erişimi engeller ve sadece güvenilir kaynaklardan gelen trafiği geçirir. Ayrıca, ağın izlenmesi ve saldırı tespiti için ağ izleme araçları da kullanılabilir. Bu sayede, herhangi bir saldırı veya anormal durum hızlı bir şekilde tespit edilebilir ve önlem alınabilir.

Yazılım güvenliği için öncelikle CPS'lerde kullanılan yazılımların güncel ve güvenli olması sağlanmalıdır. Yazılım güncellemeleri düzenli olarak yapılmalı ve güvenlik açıkları giderilmelidir. Yazılım bileşenleri, gömülü yazılımlar da dahil olmak üzere güvenilir kaynaklardan temin edilmeli ve kötü niyetli yazılımların sisteme girmesi engellenmelidir. Ayrıca, yazılım bileşenlerinin doğrulanması ve test edilmesi de önemlidir. Bu sayede, yazılım kaynaklı güvenlik açıkları en aza indirilir ve sistemin güvenliği sağlanır.

CPS güvenliği, sürekli bir çaba gerektirir. Güvenlik uzmanları, CPS sistemlerini düzenli olarak kontrol etmeli, güncellemeler yapmalı ve güvenlik açıklarını tespit etmelidir. Ayrıca, güvenlik politikaları ve prosedürleri düzenli olarak gözden geçirilmeli ve geliştirilmelidir. Çünkü siber saldırılar ve tehditler sürekli olarak evrim geçirir. Güvenlik önlemleri sürekli olarak güncel tutulmalı ve iyileştirilmelidir.

CPS güvenliği, bireylerin ve toplumun güvenliğini sağlamada büyük bir rol oynar. Örneğin, sivil havacılık alanında yolcuların güvenle seyahat edebilmesi sağlanır. Tıbbi CPS sistemlerinin güvenliği, hastaların güvenliğini ve sağlık hizmetlerinin kalitesini etkiler. Enerji sektöründe CPS güvenliği, enerji kaynaklarının etkin kullanılmasını ve enerji tedarikinin güvenliğini sağlar. Askeri alanda yürütülecek bir operasyonda kullanılacak sistemlerde veya platformlarda CPS güvenliği toplumun ve ülkenin güvenliğinin temin edilmesine yadsınamaz bir katkı oluşturmaktadır.

Sonuç olarak, CPS'lerin hayatımızın her alanında günbegün varlığı ile beraber CPS güvenliği daha önemli hâle gelmektedir. Güvenlik uzmanları, CPS sistemlerini sürekli olarak değerlendirmeli, güncellemeler yapmalı ve güvenlik açıklarını tespit etmelidir. CPS güvenliğine odaklanarak askeri/sivil teknoloji ve inovasyon alanlarında daha güvenli bir geleceğe adım atabiliriz.

DÖNEM KONUSU

8. Locked Shields

Günümüzde siber güvenlik, kurumlar ve devletler için giderek artan bir tehdit hâline gelmiştir. Karmaşık ve sofistike siber saldırılar, hassas verilere erişim sağlayarak büyük zararlara neden olabilir. Bu nedenle, savunma yeteneklerini geliştirmek ve uluslararası düzeyde işbirliği yapmak hayati önem taşımaktadır. Bu bağlamda, NATO CCDCOE (Siber Savunma Mükemmeliyet Merkezi) tarafından 2010 yılından beri düzenlenmekte olan Kilitli Kalkan (Locked Shields) adlı uluslararası siber güvenlik tatbikatı, siber dünyada yetkinliklerini değerlendirmek ve geliştirmek isteyen katılımcılar için büyük bir imkân sunmaktadır.

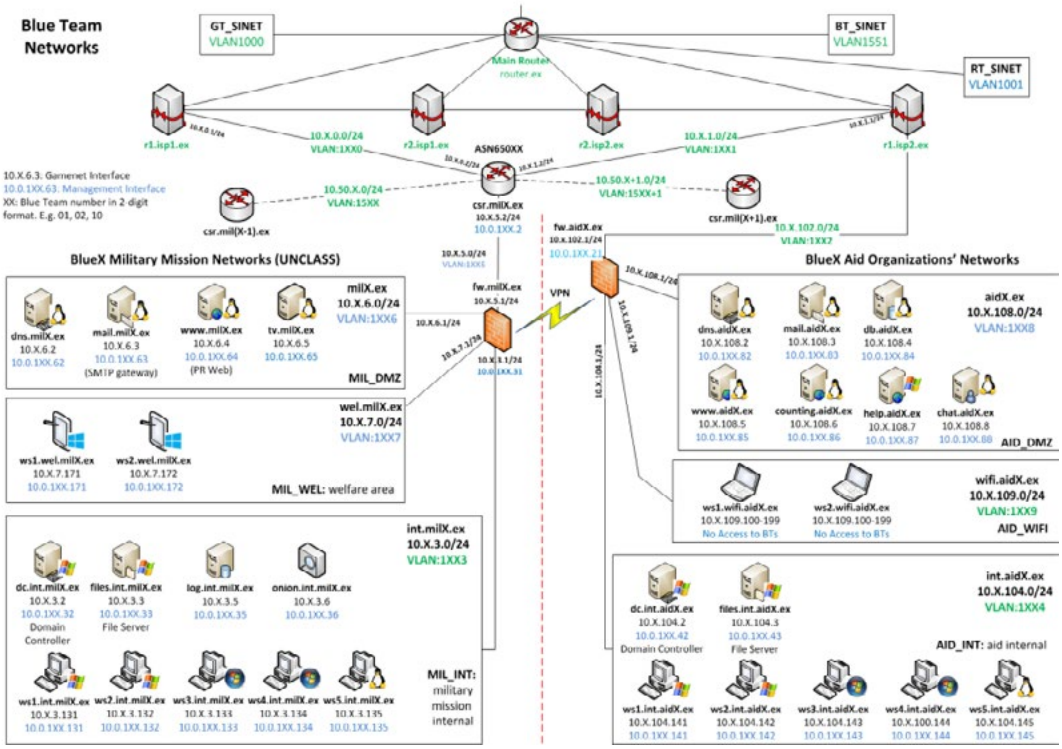
Kilitli Kalkan Tatbikatının Amacı

Kilitli Kalkan tatbikatı her yıl Estonya'da gerçekleştirilmektedir. Tatbikatın başlıca amacı, katılımcı ülkelerin siber savunma yeteneklerini test etmek, geliştirmek ve uluslararası işbirliğini güçlendirmektir. Ayrıca bir siber olayda hukuksal süreçlerin nasıl yönetileceğini, teknik ve kamuoyu için nasıl raporlanacağını, medya ve sosyal medya iletişimlerinin nasıl ilerletileceğini de kapsayan çok disiplinli bir tatbikattır.

Kilitli kalkan tatbikatı, genel olarak şöyle bir senaryoyla ilerler. NATO üyesi bir ülke siber saldırıya uğramıştır. Ülke takımları bu ortama erişim sağlayarak olay müdahale, tehdit avcılığı, sistemlerin sıkılaştırılması gibi teknik konularla ilgilenirler. Böylelikle tatbikat katılımcıların gerçekçi senaryolar üzerinde siber savunma yeteneklerini test etmelerine olanak sağlar. Tatbikat, gerçek zamanlı karmaşık saldırı senaryolarını simüle ederek katılımcıların saldırıları hızlı bir şekilde tespit etme, analiz etme ve etkin bir şekilde savunma stratejileri geliştirme becerilerini sınar. Ayrıca, saldırıların ardından sistemleri yeniden kurma ve zararları en aza indirme yeteneklerini de test eder[24].

Locked Shields, farklı ülkelerden ve kuruluşlardan katılımcıların bir araya gelerek işbirliği yapmalarını da teşvik eder. Tatbikat, katılımcı ekiplerin saldırılara karşı koordine bir şekilde hareket etmelerini, bilgi paylaşımı yapmalarını ve etkili bir iletişim ağı kurmalarını sağlar. Bu, uluslararası düzeydeki siber güvenlik işbirliğinin artmasına ve daha etkili savunma stratejilerinin geliştirilmesine katkı sağlar[25].

Aynı zamanda tatbikat ortamından ayrı bir CTF (Capture the Flag) yarışması da düzenlenmektedir. Burada amaç tamamen verilen sorulara cevap vererek puan



Şekil 16: 2013 yılına ait örnek bir tatbikat topolojisi[26].

kazanmaktır. Tatbikat ortamı gibi gerçek zamanlı saldırılar olmamaktadır. Adli bilişim uzmanları soruları çözerek ilerlerler.

2013 yılından bir topoloji aşağıda paylaşılmıştır. Yıllar ilerledikçe topoloji daha da büyümüş finans sistemleri, eks sistemleri, uydu sistemleri başta olmak üzere birçok farklı sistem de eklenmiştir.

Takımlar ve Katılımcılar

Locked Shields tatbikatında, farklı takımlar ve katılımcılar yer alır. Her takımın belirli bir rolü ve sorumlulukları vardır[26]. Bunlar:

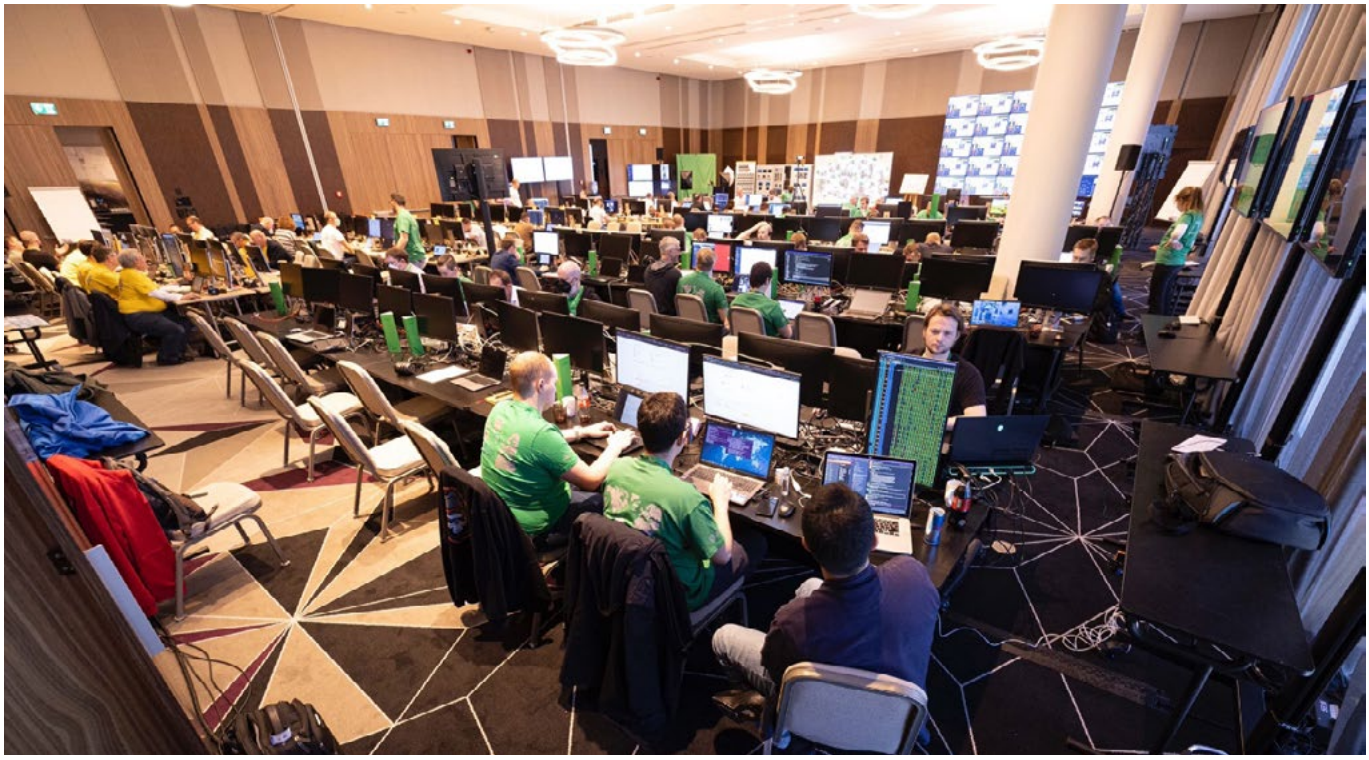
Şekil 17: Tatbikat takımlarına genel bakış[26].

Mavi Takım (Blue Team): Mavi takım, tatbikatın savunan tarafını temsil eder. Bu takım, sistemleri ve ağları güvende tutma sorumluluğunu üstlenir. Tehdit avcılığı, saldırıları tespit etme, savunma stratejileri geliştirme, zafiyetleri ele alma ve saldırıların ardından sistemleri yeniden kurma gibi görevleri yerine getirir. Mavi takım, savunma yeteneklerini en üst düzeye çıkarmak için düzenli eğitim almış uzmanlardan oluşur.

Kırmızı Takım (Red Team): Kırmızı takım, tatbikatın saldıran tarafını temsil eder. Bu takım, gerçekçi saldırı senaryoları geliştirir ve bu senaryolar üzerinden saldırı gerçekleştirir. Amacı, mavi takımın savunma önlemlerini aşarak sisteme sızmak, zafiyetleri ortaya çıkarmak ve hedefleri etkisiz hâle getirmektir. Kırmızı takım, siber saldırı tekniklerinde uzmanlaşmış yetenekli bireylerden oluşur.

Beyaz Takım (White Team): Beyaz takım, tatbikatın organizasyon ve yönetiminden sorumludur. Bu takım, tatbikatın düzgün bir şekilde ilerlemesini sağlar, skorlama yapar, senaryoları yönetir ve takımlar arasındaki iletişimi koordine eder. Beyaz takım, tatbikatın başarıyla gerçekleştirilmesi ve katılımcıların deneyimlerinden en iyi şekilde yararlanması için çalışır.

Yeşil Takım (Green Team): Yeşil takım, çekirdek altyapının kurulması, yapılandırılması, sanallaştırılması, kullanıcı hesaplarının oluşturulması gibi teknik altyapı işlerinden sorumlu takımdır. Tatbikat sırasında da altyapıyı izler, doğru çalıştığından emin olur ve bir problemle karşılaştığında çözüm üretir.



Şekil 18: Tatbikat ortamına genel bakış[24].

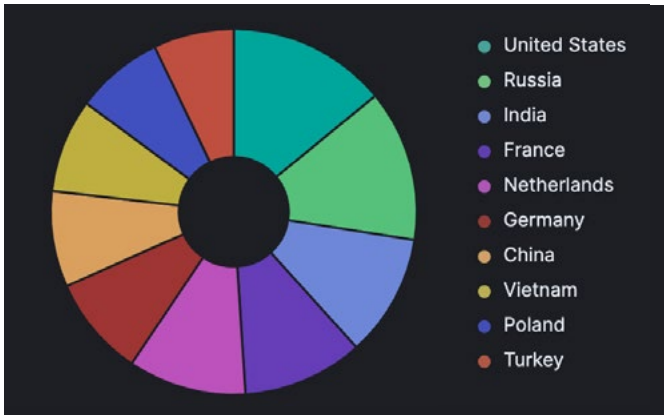
Sarı Takım (Yellow Team): Sarı takım, genel olarak kırmızı takımı destekleyen bilgi güvenliği bilgisi zayıf olan çalışanlar rolüne bürünür. Örnek olarak kırmızı takım bir atak senaryosunu zararlı yazılım indiren bir e-posta göndermek olarak tanımlamıştır. Burada sarı takım ilgili e-postayı açıp zararlı yazılımı indirip çalıştıran ekiptir.

Sonuç

Kilitli Kalkan tatbikatı, siber güvenlik alanında uluslararası düzeyde bir işbirliği ve eğitim platformu olarak önemli bir rol oynamaktadır. Katılımcılar, gerçekçi ve güncel senaryolar üzerinde siber savunma yeteneklerini test ederken, işbirliği ve koordinasyon becerilerini geliştirirler. Tatbikat, katılımcılara gerçek dünya senaryolarında pratik deneyimi kazandırarak siber saldırılara karşı daha güçlü ve hazırlıklı olmalarını sağlar. Kilitli Kalkan tatbikatı, siber güvenlik topluluğunda saygın bir etkinlik hâline gelmiş olup uluslararası düzeyde güvenlik standartlarının yükseltilmesine katkı sağlamaktadır.

Honeypot Verileri

Bu rapor son üç ay içinde Honeypot sensörlerimizden topladığımız verilerle oluşturulmuştur. En çok saldırı toplanan ülkeler, portlar, en çok denenen kullanıcı adları ve parolalarla ilgili veriler azalan sırada listelenerek inceleme için sunulmuştur. Ocak, Şubat ve Mart ayları boyunca Honeypot sensörlerimize toplam 3.304.664 saldırı gelmiştir.



Şekil 19: Gelen saldırıların ülkelere göre dağılımı.

Saldırıların Geldiği Ülke	Saldırı Sayısı
ABD	194.946
Rusya	185.375
Hindistan	150.136
Fransa	147.938
Hollanda	144.770
Almanya	123.355
Çin	117.778
Vietnam	114.443
Polonya	107.889
Türkiye	98.439

Tablo 2: En çok saldırı gelen 10 ülke ve saldırı sayıları.

Toplanan veriler incelendiğinde, en çok saldırı gelen ülkenin ABD (%14,07) olduğu, onu Rusya (%13,38), Hindistan (%10,84), Fransa (%10,68) ve Hollanda'nın (%10,45) takip ettiği görülmektedir. Türkiye %7,11'lik oran ile listenin 10'uncu sırasında yer almaktadır.

Saldırılan Port	Saldırı Sayısı
445 - SMB	1.249.741
3389 - RDP	261.825
25 - SMTP	154.821
5900 - VNC	44.851
22 - SSH	15.719
23 - TELNET	12.071
8080 - TCP/HTTP	9.453
7070 - TCP	8.733
1433 - MSSQL	8.634
7547 – TR-069	7.216

Tablo 3: En çok saldırı gelen portlar, bu portları kullanan servisler ve saldırı sayıları.

Tablo 3'de de görüldüğü üzere en çok saldırı 445 portuna gelmiştir. 445 portunda sunucuların yazıcı ve paylaşılan dosyalar için kullandığı SMB servisi çalışmaktadır. Bu yüzden SMB servisinin diğer servislerden daha çok saldırı alması beklenen bir durum olarak kabul edilebilir. SMB servisini sırasıyla RDP, SMTP, VNC, SSH ve TELNET takip etmekte. Bir önceki çeyrekten bu yana MSSQL ve tr069 servislere yapılan saldırılarda görülen artış dikkat çekmektedir. MSSQL servisi veritabanı iletişimini sağlayan servistir. Saldırganlar, bu portu hedef alarak SQL enjeksiyonu veya yetkisiz veritabanı erişimi gibi saldırı yöntemlerini kullanabilirler.

TR-069 servisi (CPE WAN Management Protocol) olarak bilinen bir protokole aittir ve genellikle internet servis sağlayıcıları tarafından kullanılmaktadır. Modem, router gibi internete bağlı cihazlar bu port üzerinden, uzaktan yönetilebilirler. İnternette bilinen exploit'leri bulunmaktadır.

Denenen Parola	Deneme Sayısı
3245gs5662d34	1.008
345gs5662d34	1.006
123456	659
(boş)	475
admin	368
password	270
123	237
12345	193
Accept-Encoding: gzip	184
Host: azenv.net	183

Tablo 4: SSH ve RDP honeypotlarımız üzerinde en çok denenen parolalar ve deneme sayıları.

Denenen parolalar incelendiğinde, birçok yönetim arayüzünün standart olarak kullandığı parolalar olan 345gs5662d34, 123456, admin gibi terimler gözlemlenmektedir. Bu parolaların test veya deneme süreçleri tamamlanır tamamlanmaz değiştirilmesi ve karmaşık, 12-16 karakterli, özel karakter içeren parolalarla değiştirilmesi analistlerimiz tarafından tavsiye edilmektedir. Ayrıca kolay hatırlanması ve girilmesi için herhangi bir harf, özel karakter içermeden sadece sıralı sayılar ile oluşturulmuş parolalar kullanmaktan kaçınılmalıdır.

Denenen Kullanıcı Adı	Deneme Sayısı
root	7.565
345gs5662d34	1.006
sh	877
admin	857
$	428
.	402
(boş)	327
user	318
guest	198
default	194

Tablo 5: SSH ve RDP honeypotlarımız üzerinde en çok denenen kullanıcı adları ve deneme sayıları.

Şekil 20: Parola etiket bulutu.

Şekil 21: Kullanıcı adı etiket bulutu.

Denenen kullanıcı adları incelendiğinde, yeni kurulmuş olan sistemlerin sıklıkla kullandığı root, admin, user gibi kullanıcı adlarının saldırganlar tarafından tercih edildiği görülmektedir. Kurulumu tamamlanan servislerin ve yönetim panellerinin kullanıcı adlarının en kısa zamanda değiştirilmesi ve kurulan sistemlerin kendi isimlerinin kullanılmaması (örn. ubuntu, postgres, oracle, testuser) tavsiye edilmektedir.

KAYNAKÇA

[1] OpenAI, «openai.com,» OpenAI, 24 March 2023. [Çevrimiçi]. Available: https://openai.com/blog/march-20-chatgpt-outage#OpenAI .

[2] O. Ouzan, «securityboulevard.com,» 31 March 2023. [Çevrimiçi]. Available: https://securityboulevard.com/2023/03/chatgpt-vulnerability-redis-vulnerability-exposes-user-payment-data/.

[3] R. Lakshmanan, «thehackernews.com,» The Hacker News, 25 March 2023. [Çevrimiçi]. Available: https://thehackernews.com/2023/03/openai-reveals-redis-bug-behind-chatgpt.html.

[4] *Bolloré subsidiary attack exposes Thales, Alibaba data.* [Art].

[5] *Bolloré subsidiary attack exposes Thales, Alibaba data.* [Art].

[6] I. S. X-Force.

[7] H. Aver, 18 Nisan 2022. [Çevrimiçi]. Available: https://www.kaspersky.com.tr/blog/black-cat-ransomware/10634/.

[8] *The Rise of BlackCat Ransomware.* [Art].

[9] August 26, 2022. [Çevrimiçi]. Available: https://socradar.io/dark-web-profile-blackcat-alphv/.

[10] A. AWS. [Çevrimiçi]. Available: https://aws.amazon.com/tr/what-is-cloud-computing.

[11] Azure. [Çevrimiçi]. Available: https://azure.microsoft.com/en-us/.

[12] G. Cloud. [Çevrimiçi]. Available: https://cloud.google.com/.

[13] Nist. [Çevrimiçi]. Available: https://csrc.nist.gov/publications/detail/sp/800-145/final.

[14] Gartner. [Çevrimiçi]. Available: https://www.gartner.com/en/information-technology/glossary/multitenancy.

[15] ISO. [Çevrimiçi]. Available: https://www.iso.org/standard/60545.html.

[16] Ntia. [Çevrimiçi]. Available: ntia.gov.

[17] S. U. C. Ntia. [Çevrimiçi]. Available: https://ntia.gov/sites/default/files/publications/ntia_sbom_use_cases_roles_benefits-nov2019_0.pdf.

[18] N. S. f. e. brief. [Çevrimiçi]. Available: https://www.ntia.doc.gov/files/ntia/publications/ntia_sbom_formats_energy_brief_2021.pdf.

[19] a. s. c. s. sbom. [Çevrimiçi]. Available: https://www.aquasec.com/cloud-native-academy/supply-chain-security/sbom/.

[20] N. s. s. c. software. [Çevrimiçi]. Available: https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1.

[21] I. o. T. a. C.-P. Systems. [Çevrimiçi]. Available: https://www.sciencedirect.com/science/article/pii/S2667345221000055 .

[22] c. d. s. a. c. t. f. o. c. p. systems. [Çevrimiçi]. Available: https://www.cleantech.com/data-security-and-cleantech-the-future-of-cyber-physical-systems/ .

[23] A. s. o. C. P. S. CPS. [Çevrimiçi]. Available: https://www.researchgate.net/figure/Attack-surface-of-Cyber-Physical-System-CPS-24_fig1_332826219 .

[24] n. a. t. p. i. w. l. c. s. e. l. shields. [Çevrimiçi]. Available: https://www.ncia.nato.int/about-us/newsroom/nato-agency-to-participate-in-worlds-largest-cyber-security-exercise-locked-shields.html.

[25] L. Shields. [Çevrimiçi]. Available: https://ccdcoe.org/exercises/locked-shields/.

[26] k. k. n. c. l. learned. [Çevrimiçi]. Available: https://www.enisa.europa.eu/events/2nd-enisa-conference/presentations/kaur-kasak-nato-ccdcoe-lessons-learned-from-the.pdf.

STM

www.stm.com.tr

/STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/STMThinkTech