Cloud Security

Ali Altan
Püren Tap
Ata Türkoğlu
Doğan Can Hasanoğlu

Abstract

1.Giriş:

Bulut Bilişim Teknolojileri, Bilgisayar programlarının bir Dağıtılmış sistem içerisinde ,internet ortamında yaratılması ve "Kullandığın kadar öde" sisteminde yalnızca kullanıcının kullandığı kadarını ödemesi ile yapılan sanallaştırılmış bir sistemdir Bu sistem sayesinde kullanıcılar, istedikleri zaman, istedikleri yerde, istedikleri makineden normalde makinelerinin kaldıramayacağı, veya makinenin kendi içinde bulunmayan sistemleri kullanabilirler. Bulut Bilişim teknolojilerinin en basit ve yaygın terimsel açıklaması NIST tarafından "*Minimum yönetim çabası veya servis sağlayıcı etkileşimi ile hızla tedarik edilebilen ve serbest bırakılabilen, paylaşılabilir ve yapılandırılabilir hesaplama kaynakları havuzuna uygun (örneğin ağlar, sunucular, depolama, uygulamalar ve servisler), isteğe bağlı ağ erişimini sağlamak için bir model*" olarak yapılmıştır. AWS, Microsoft Azure gibi birçok büyük şirketlerin sunduğu bulut bilişim teknolojileri hayatı kolaylaştırmak ve bir şirketin elindeki bilgi ve kontrolü merkezileştirmek gibi amaçları olsa da, aynı sürede bu teknoloji yanında teknik ve güvenlik açısından birçok boşluk getiriyor. Bu raporda biz Yapı Kredi'nin Gelecekte yapabileceği potansiyel bir hareket olan genel bilgi merkezini buluta taşıma hamlesinin Güvenlik olarak hangi, sıkıntıları barındırabilecek olduğunu inceledik. Rapor 8 bölümden oluşmakta ve sırasıyla, **Bulut Bilişim Teknolojilerine Güvenlik Tarafından Bakış, Bulut Sistemlerindeki Önemli Tehditler ve Kaygılar,Bulut'da Görünürlüğünü Arttırmak için İzlenecek Yollar,Yetkisiz Erişimi ve Güvenlik Zaafiyetlerini Azaltmak için Azure AD Monitoring Stratejiler,Bulut Alt Yapısındaki Bileşenlerin Güvenliği, Bulut Güvenliği için Teknolojiler ve Çözümler ve Bulut Tercihleri Sırasında Dikkat Edilecek Hususlar** dir.

2. Bulut Bilişim Teknolojilerine Güvenlik Tarafından Bakış:

2.1 Bulut Bilişim Teknolojilerinin Genel hatlarına bakış:

Bulut Bilişim Teknolojileri, 2000 li yılların başından beri gündemde olan , ama 2015 ve sonrasında toplu olarak kullanımı yaygınlaşan bir teknolojidir. Dağıtık Sistemler (Distributed Systems) içerisinde olan bu teknoloji, Özel, halka açık veya karma olarak üç farklı şekili olmakla beraber, bilgi tutmaktan Uzaktan sanal bilgisayar kullanmaya her işe yarayabilir. Bulut bilişim teknolojilerinin en iyi tarafları kullanıcılarının kullanmak istedikleri kadarını kullanabilmeleri ve bu yüzden ortalama giderlerini azaltmaları, daha güvenilir bir sistem üzerinde çalışarak kendileri usta olmadığı konularda (sistem inşası veya Bina soğutması gibi) usta seviyelerde hizmet almalarına ve en önemlisi de, kullanan parti işini büyüttüğünde anında istediği kadar bilgisayar veya depolama alanına sahip olabiliyor. Fakat bu sistemin bazı dezavantajları da mevcuttur. Bunlardan birkaçına örnek, sistemlerin servis alınan şirket tarafından çökmesi veya genel siber savunmada oluşabilecek bir yanlış anlaşılma, uyuşmayan poliçeler veya iletişimde olacak sızıntı lardır.Ülkemizde 2021 senesi süresince mümkün olmasa da, izin verilen ülkelerin bankalarının tamamen buluta geçmeleri

söz konusudur. Teknolojinin gidişatına göre , bulut bilişim teknolojileri, yeni normal olacak ve bu teknolojiye avantajlı bir şekilde geçmek, hizmet veren bir şirket için yapıcı veya yıkıcı bir sonuç doğurabilir.

Bu yazının önemi , Yapı Kredi'nin zamanın önemli teknolojik gelişmelerine hazır olup kendini siber savunma yönünden bilgili ve farkındalığı yüksek girmesidir.

2.2 Bulut Güvenliğinin Avantajları ve dezavantajları

Bulut Bilişim Sistemlerinin Avantajları ve dezavantajları, aşağıda gösterildiği gibidir.

Avantajları

- Kolay Bilgi Kurtarma
- Açıklık
- Materyalle ulaşım Zorluğu
- Profesyonel Server Güvenliği

Dezavantajları

- Bandwidth Sıkıntıları
- Direkt Giriş Olmaması
- Ortaklık ilişkisinin komplikasyonları
- Çalışanlardan dolayı oluşabilecek sızıntılar

2.3 Global Bulut Security Use Cases

Use Case, bir sistemin veya servisin nerede, nasıl kullanılabileceğini açıklar.Konumuzda, Use case ler çoğunlukla saldırı tipleri metodları ve bunların analizini açıklar.Bilişim teknolojilerinde, saldırılar sayılı ve yapılması gereken hareketler ise bellidir. Bunlar için hazırlanmış Küresel olarak kabul gören ve çoğunlukla savunmasının en önemli olan durumları biz, Global Bulut Security Use Cases diye açıklayabiliriz.Bu caselerden en önemlileri:

1) Privileged Account Access

En Önemli sayılabilecek olan bir konu, çalışanlarınızın sisteminize giriş izinleri ve tipleridir. Yanlış verilmiş bir izin, yanlış konuşlanmış güven veya izin hieralşisinin tanınmaması, bulut bileşen sistemlerinde en büyük açıklara yol açabilirler.Mantık olarak herkese sadece gerekli izinin verilmesi doğru olsa da, gerçekte bu sistem olası yavaşlamalara sebep olduğu için bazen göz ardı edilebilir. Bu durumdan dolayı oluşabilecek en büyük sıkıntı, olası açıklar sırasında izinin büyüklüğüne göre oluşan hasarın artmasıdır. Mesela, Turkiye bazlı bir firma, Brezilyadan giriş aldığında, bu girişi göz altında tutup emin olmalıdır ve bu yüzdende VPN gibi sistemlerin kullanılmasına izin vermemelidir.

2) Data Exfiltration

Bulut Bilişim Sistemleri çoğunlukla farklı tipte ve hassas bilgiler barındırırlar.Bu bilgilerin her zaman filtrelenmesi ve isteklerin doğru, mantıklı ve kabul edilebilir olması önemlidir.Dikkat edilmediğinde, istenmeyen istekler, istenmeyen kişilere gidebilir ve bu da ciddi sıkıntılara yol açabilir.

3) Suspicious Network Connections

Bulut Bilişim Teknolojilerinde olabilecek başka bir saldırı tipi de SQL injection veya diğer türlü Remote file injection saldırıları dır. Bunları engellemek için sadece belirli kişilerden istek almak veya, istekleri direkt kabul etmek yerine moderasyon ile almak doğru olacaktır.Sıkıntılı bilinen isteklerin kara listeye alınması, belli beklenebilir hareket zincirini yapıldığında istekleri durdurmak veya yavaşlatmak, dışarıdan yapılan saldırıları durdurmaya veya başka yol arttırmaya zorlayabilir.

4) Man-in-the-Bulut Attack

Man-in-the-Bulut Saldırısı, MITM saldırısına oldukça benzer, kullanıcı ve bağlandığı server arasına girilerek yapılan bir saldırıdır. Bu saldıranın karşısına Token sistemi veya session sistemi ile geçilebilir. Bu verilen tokenlerin iyi monitörlenmesi, SSL decryption yapılması, Bulut Bilişim Teknolojilerinde başlangıcı bu gibi olan saldırıların önüne geçecektir.

Sonuç olarak, Bulut Bilişim Teknolojilerinin, her sistemde olduğu gibi boşlukları vardır. Bu boşlukları dosyanın ilerleyen taraflarında incelemeye devam edeceğiz, fakat başlangıçta altı çizilmesi gereken yer, büyük hataların, sistemsel değil, eğitimsel yollar ile çözülebileceğidir.

3. Bulut Sistemlerindeki Önemli Tehditler ve Kaygılar

3.1 Görünürlüğün Yetersizliği

Bulut ortamındaki görünürlüğün yetersiz olması, bulut güvenliğindeki problemlerin başında gelmektedir. SANS'ın 2021 yılında yaptığı ankette, "İşlenen verinin ne olduğunun ve bulutta nerede bulunduğunun bilinmemesi" şirketlerin %49'unun başlıca problemi olarak 1. sırada yer almaktadır.
Bir sistemde görünürlüğün olması, o sistemde bulunan herhangi bir veriye erişebilme olanağıdır. Şirketin hangi verilere sahip olduğunu bilmesi, hangi veriyi korumak istediğini bilmesi, bu verilerin ne amaçla kullanıldığı ve nerede bulunduğunu bilmesi görünürlüğün temelindedir. Böylece şirket, herhangi bir performans sorununu anında anlayabilir,

gerçekleşebilecek saldırıları öngörüp gerçekleşmeden engelleyebilir ve bulut yapısında bulunan fakat efektif kullanılmayan kaynakları verimi arttırmak adına iptal edebilir. Yetersiz bulut görünürlüğüne sebep olan etkenler olarak şirketlerin çoğu kaynağını, altyapısını bilmediği bulut ortamına koyması, şirketlerin on-prem güvenlik çözümlerini bulutta uygulayamaması ve buluta entegre olan üçüncü şahıs güvenlik araçlarının yetersizliğini gösterebiliriz.

3.2 Yetkisiz Erişim

Cybersecurity Insiders tarafından hazırlanan 2020 Bulut Güvenliği raporunda, şirketlerin %58'i public bulut sistemlerinde yetkisiz erişimi büyük bir tehdit olarak görmektedir. Yetkisiz erişim birkaç farklı şekilde olabilir. Şirket dışından biri şirketin bulut sistemine sızmışsa ve aslında ulaşmaması gereken sistemlere, ağlara,serverlara, uygulamalara ve verilere ulaşabiliyorsa bu yetkisiz erişimdir. Aynı zamanda saldırgan, bir şirket çalışanının hesabını ele geçirip o hesabın yetkisi dahilindeki bulut kaynaklarına ulaşması veya bir şirket çalışanının aslında ulaşmaya yetkisi olmadığı bir kaynağa ulaşabilmesi de yetkisiz erişime birer örnektir. Bulut, dağıtılmış bir sistem olduğu ve internetten erişime açık olduğu için, saldırılara da açık haldedir. Saldırganlar tarafından gerçekleştirilecek yetkisiz erişimi önlemek için gerekli güvenlik önlemleri alınmalı ve şirket çalışanlarının yetkileri de Kimlik Ve Erişim Yönetimi (IAM) ile düzenlenmelidir.

3.3 Incident Response Yetersizliği

Şirketlerin güvenlik olayları karşısında aldıkları önceden belirlenmiş stratejiler vardır. Belirledikleri stratejiler, NIST'in tanımladığı Incident Response Lifecycle bağlamında belirlenir. Bu döngü Hazırlık - Tespit Etme ve Analiz - Önleme, Yok etme, Kurtarma - Otopsi Raporu aşamalarından oluşur. Incident Response Döngüsü'nün her aşaması bulut sistemlerinde farklı etkilenebilir. Bu farklılıkları göz önünde bulundurarak şirketin stratejilerini güncellemesi önemlidir.

Hazırlık :
Şirket ile bulut sağlayıcısı kendi üzerine düşen sorumlulukları anlamalıdır..
Bir güvenlik zafiyeti meydana geldiğinde, bulutta bulunan her hizmet için ne tür verilerin ve logların şirkete sağlanacağı belirlenmelidir.
Bulut logların toplanabileceği gerekli araçlar olmalı ve bu logların analizinin yapılabilmesi gereklidir.
Bulut platformu herhangi bir tehdide daha hızlı karşılık verilebilecek şekilde planlanmalıdır.

Tespit Etme ve Analiz

Bulutta gerçekleşen olayları izleme (monitoring) buluttaki mevcut kaynakların yanı sıra management plane'e de uygulanmalıdır.
Veri kaynakları on-premdeki veri kaynaklarından farklılık gösterebilir. Çoğu veri kaynağı (örn: sistem logları) aynı olmasına rağmen yeni kaynaklar (örn: management plane) da mevcuttur.
Gerekli olduğu durumlarda instancelardan, konteynırlardan ve uygulamalardan loglar alınabilir.
IOC tespiti ve saldırganlarla ilgili bilgi almak için şirket dışından tehdit istihbaratı (threat intelligence) yardımı alınabilir.

Önleme, Yok etme, Kurtarma
Yönetim düzleminin (Azure için denetim düzlemi) saldırganlardan temizlendiğine emin olunmalıdır.
Bulutun bu aşamada sağladığı kolaylıklar vardır. Sanal makine kolaylıkla karantinaya alınabilir ve sanal firewallarla izole edilebilir.
Güvenlik açığının yolu tespit edilmeli ve buluttaki diğer kaynaklar için de kullanılamayacağından emin olunmalıdır.

3.4 Güvenilmeyen Arayüzler/API'lar

Bulut üzerinde bulunan kaynakların ve hizmet alıcılarının yönetilmesi uygulama ara yüzleri ve API'ler ile yapılmaktadır. Bu ara yüzlerin ve API'lerin güvenliğini sağlamak için yazılımlarının mümkün olan en ileri teknolojilere sahip olması, gerekli sertifikaları ve uyumlulukları bulundurmaları önemlidir. Bulut ortamları arasında bilgiler API'ler üzerinden sıkça gönderilebilmektedir. Yeterli güvenlik önlemlerinin alınmaması datalara yetkisiz erişimlere ve konfigürasyonların değiştirilmesine sebep olabilir.

3.5 Hesapların Ele Geçirilmesi

Üyelik gerektiren bulut hizmetleri kullanılırken sistemde birden fazla kullanıcı bulunması ve bunların tek bir panel üzerinden yönetilmesi sisteme giriş bilgilerinin çalınması durumunda büyük güvenlik açıklarına sebep olabilir. Bunun önüne geçilebilmesi için kurumlar tarafından sıkı güvenlik politikaları uygulanmalı ve kimlik doğrulamada birden fazla faktörün kullanılması yetkisiz işlemlerin önüne geçecektir. Bulut ortamlarında kullanıcıların uç noktaları ve bulut, açık internet üzerinden bağlantı kurmaktadır. Kullanıcı hatası veya man-in-the-middle-attack gibi yöntemlerle erişim sağlayan saldırganları engellemek için Data Loss Prevention ve benzeri çözümler kullanılmalıdır. Kimlik, yetkilendirme ve erişim yönetimini geliştirmeye yönelik uygulamalardan bazıları şöyledir:

- Harici bulut sağlayıcılarına bağlanırken mevcut ağlar genişletildiğinde Federated Identity Management (FIM) yöntemleri kullanılabilir.

- Uygun olduğunda kimlik brokerlerinin kullanımı düşünülebilir.

- Şirket içi seçenekler gereksinimleri karşılamadığında bulutta barındırılan dizin sunucuları kullanılmalıdır.

- Bulut kullanıcıları tüm harici bulut hesapları için çok faktörlü doğrulamayı kullanmalıdır.

- Bulut bilişimi için Role-Based Access Control yerine Attribute-Based Access Control tercih edilmelidir.

3.6 Verilerin Organizasyon Dışındakilere Sızdırılması/Paylaşılması

Bulut bilişiminin kullanılmasıyla ilgili endişelerden biri hizmet sağlayıcısı ve alıcısı arasındaki görev ve sorumlulukların kesin olarak belli olmadığı durumların olabilmesidir. Bir başka endişe de verilerin nerede ve nasıl saklandıklarının, nasıl yönetildiklerinin, fiziksel olarak veri depolama alanının kontrolünün ve bunun için gerekli olan altyapının nasıl yönetildiğinin uygunluğudur. Hizmet sağlayıcısı veri depolama sunucularını nasıl ve hangi güvenlik önlemleriyle konumlandırdığını şeffaf bir biçimde hizmet alıcısı ile paylaşmalıdır. Herhangi bir bakım çalışmasında hizmet alıcısının altyapıdan kaynaklı aksaklıklar yaşamaması ve hizmet sağlayıcısına kolayca ulaşabiliyor olması oldukça önemlidir.

Verilerin güvenliğine dair bir endişe de bulut hizmeti sağlayıcılarının farklı ülkelerde veri merkezleri bulundurması ve bulunduğu ülkelerdeki yasalara tabi olurken uyum sağlamalarında doğacak olan sorunlardır. Bulut hizmeti kullanan müşterilerin veri gizlilikleri başka ülkelerde işleyen yargı süreçleri sonucunda tehlikeye girebilir.

Bulut hizmeti sağlayıcılarının bir veri sızıntısına karşı her türlü önlemi alması, kaynakların farklı alıcılar tarafından kullanıldığı göz önüne alınırsa, büyük önem arz etmektedir. Önemli bilgilerin güvenliğini sağlamak için veri sızdırma engelleme yazılımları kullanılmalıdır. Ayrıca hizmet sağlayıcısı, alıcının hangi kaynaklara eriştiğini ve hangi işlemleri yaptığını alıcıların log bilgilerini takip ederek inceleyebilmektedir. Bu şekilde farklı hizmet alıcılarının erişim yetkileri kontrol edilebilmektedir. Veri sızıntılarına karşı şifreleme ile alınabilecek bazı önlemler ise şöyledir:

- AES ve RSA gibi algoritmalar ve sayısal imzalar kullanılarak veri transferi sırasında bilgilerin güvenliği sağlanabilir.

- Homomorfik şifreleme ile hesaplamaların şifrelenmiş veriler üzerinde yapılması sağlanmaktadır. Ham veri üzerinde direkt olarak yapılan hesaplama sonuçları ile aynı sonuçlar elde edilecek şekilde deşifreleme işlemi olmadan ve herhangi bir özel anahtar

bilinmeden şifreli veriler üzerinde çeşitli işlemler yapılabilmektedir. Bu, şifreli verileri buluta dış kaynak olarak sunan bulutlar için büyük bir avantaj olabilir.

- Proxy re-encryption ile, bir kullanıcının genel anahtarı kullanılarak şifrelenen verilerin, başka bir kullanıcının özel anahtarı kullanılarak çözülebilecek biçime dönüştürülmesini sağlanmaktadır.

- Özellik tabanlı şifreleme ile şifreleme anahtarları ya da şifreli metinler sistem kullanıcıları için tanımlayıcı nitelik kümeleri ile etiketlenir ve belirli bir kullanıcı, yalnızca bu özel anahtar ile eşleşen özel bir şifreli metni deşifreleyebilir.

3.7 DDoS Saldırıları

Saldırganların büyük çaplı bir uygulama katmanı saldırısı başlatmalarının maliyeti bulut ortamlarına verdiği zarar ile kıyaslandığında oldukça düşüktür. DDoS saldırıları ağ trafiği tıkanıklıklarına yol açarak bulut servisi sağlayıcılarının kalitesini düşürmektedir. DoS saldırılarına kıyasla trafiğin birden fazla kaynaktan gelmesi kötücül trafiğin tespit edilmesi ve yok edilmesini zorlaştırmaktadır. Çoğunlukla virüs kullanılarak zombi haline getirilen birçok sayıdaki bilgisayarın eş zamanlı ve çok sayıda isteği farklı ağ bağlantıları üzerinden göndermesi ağ trafiğinde tıkanıklığa ve sunucuların çalışamaz hale gelmesine yol açmaktadır. Trinoo gibi saldırı araçları kullanılarak yapılan saldırılar sonucunda hizmet sağlayıcılarının hizmet verememesi büyük maliyetli zararlara sebebiyet vermektedir. Bir DDoS saldırısının en belirgin özelliği internet sitesinin veya servisinin bir anda yavaşlaması veya çalışmaması olacaktır. Yine de daha detaylı sorgulama yapılmadan sorunun kaynağının ne olduğu kesin olarak belirlenemez. Olası bir aksaklıkta ilk olarak incelenmesi gereken göstergeler şunlar olacaktır:

- Tek bir IP adresi veya skalasından şüphe uyandıracak kadar fazla trafik gelmesi.

- Cihaz tipi, coğrafi konum, veya web tarayıcısı gibi özellikleri birbirine oldukça benzer olan çok sayıda trafik akışı.

- Tek bir sayfaya ya da uç noktaya açıklanamaz bir biçimde artış gösteren talepler gelmesi.

- Günün beklenmedik zamanlarında tuhaf trafik desenleri görülmesi.

DDoS saldırıları çeşitlerine göre uygulama katmanı, protokol, ve volümetrik olarak üç kategoriye ayrılabilir.

Protokol saldırıları:

Bu saldırı çeşidi sunucu kaynaklarını veya güvenlik duvarları ve yük dengeleyicileri gibi ağ ekipmanlarını tüketerek hizmet kesintileri oluşturmayı amaçlar. Layer 3 ve 4 üzerindeki zayıflıklara odaklanır. Bu kategoride SYN flood ve Ping of Death gibi saldırı yöntemleri bulunmaktadır .

SYN flood: TCP bağlantısındaki three-way-handshake protokolünü birden fazla SYN talebi yollayarak suistimal eder. Saldırgan gönderdiği SYN taleplerine karşılık gelen SYN-ACK cevaplarını görmezden gelir ya da yanıltıcı bir IP adresinden SYN taleplerini yollamaya devam eder. Belirli bir süre sonra talep gönderilen alıcı ağdaki bekleme ve sıra yüzünden denial of service durumuna geçer.

Ping of Death: IP başlığı dahil olmak üzere doğru oluşturulmuş bir IPv4 paketinin boyutu, toplam 84 baytlık yük boyutu dahil 65.535 bayttır. Bu sayıdan büyük bir ping paketi göndermek internet protokolünü ihlal ettiği için saldırganlar hatalı oluşturulmuş paketleri parçalar halinde gönderir. Hedef sistem parçaları birleştirmeye çalıştığında büyük boyutlu bir paketle karşılaşır ve bellek taşması meydana gelir. Bu saldırı türünde saldırganın kimliği kolayca değiştirilebilirken saldırılan makine hakkında IP adresi dışında herhangi başka bir bilgiye de ihtiyaç duyulmamaktadır. Yeni ve gelişmiş sistemlerde bu güvenlik açığı kapatılmış olmasına rağmen Ping of Death yöntemine karşı bazı sistemler hala açıklar vermektedir.

Volümetrik saldırılar:

Bu saldırı çeşidi ile hedefin internet ile arasındaki tüm bant genişliğinin tüketilmesi ve tıkanıklık yaratılması amaçlanmaktadır. Çok sayıda veri bir botnet veya başka bir yükseltici kullanılarak hedefe gönderilir. UDP ve ICMP floodları bu saldırı çeşidine örnek olarak verilebilir.

UDP flood: Hedefi UDP paketleri ile tıkar. Bu, hedefin o bağlantı noktasını dinleyen uygulamayı tekrar tekrar kontrol etmesine ve bir ICMP hedefe ulaşamadı paketiyle yanıt vermesine yol açar. Bunun sonunda da hedefteki kaynaklar tükenir.

ICMP flood: UDP flooda benzer olacak şekilde hedefi ICMP Echo Request yani ping ile tıkar. Cevap beklemeden ardı ardına gönderilen paketler giden ve gelen bant genişliğini tüketir ve sistemin yavaşlamasına sebep olur.

Uygulama katmanı saldırıları:

Saldırganlar web sitelerinin HTTP taleplerine karşılık sunucular üzerinde oluşturulduğu katmanı hedef alır (Layer 7). HTTP flood örnek olarak verilebilir.

HTTP flood: Bu saldırı bir web sitesini birden fazla bilgisayar üzerinden sürekli yenilemeye benzetilebilir. Çok sayıda HTTP talebi gelmesi üzerine denial of service meydana gelir. Saldırgan sorunsuz görünen HTTP GET ve POST taleplerini sunucuya veya uygulamaya gönderir. Hedefin maksimum kapasitesi kullanılarak çalışamaz hale gelmesi sağlanır.

3.8 Siber Saldırılar

Saldırganlar bulut bilişim hizmeti sağlayıcılarına erişim sağlamak içi yeni yollar aramaktadırlar. En çok kullanılan yöntemlere hakim olmak bulut geliştiricilerine ve kullanıcılarına yeni güvenlik çözümleri bulmalarında yardımcı olacaktır. Bazı en çok kullanılan siber saldırı yöntemleri şöyle sıralanabilir:

- Kötü amaçlı yazılım enjeksiyonu saldırıları ile bir SaaS ya da PaaS çözümüne virüslü bir uygulama modülü gönderilir. Bir IaaS çözümüne sanal makine ekleme yöntemleri de kullanılmaktadır. Bulut sistemi başarılı bir şekilde aldatıldığında kullanıcı isteklerini saldırganların bilgisayarlarına yollamış olur.

- Yan kanal saldırılarında bulut sistemi kullanıcılarına sunulan sanal makineler kullanılmaktadır. Yan kanal saldırısında saldırganın amacı hedef sanal makineyle aynı hosta kötü amaçlı bir sanal makine yerleştirmek ve hedef sanal makinedeki bilgileri dışarıya sızdırmaktır.

- Bir web servisi kullanıcısı alıcı web servisine mesaj gönderdiği sırada imzalı olan verilerde yapılan kötü niyetli bir değişiklik, imza algoritmasının kendisi kırılmamışsa, web servisi sağlayıcısı tarafından algılanmaktadır. Bir XML imza sarma saldırısında saldırgan imzayı geçersiz kılmadan imzalı bölümün içeriğini değiştirebilir.

- Advanced Persistent Threat (APT) yöntemleri ile ağa ulaşan saldırganlar orada uzun bir süre kalmayı amaçlarlar. Sisteme veya ağa zarar vermeyerek verileri çalmayı hedeflerler. Bulut ortamları gibi dinamik ve karışık altyapılarda başarıya ulaşan APT yöntemlerini geleneksel metotlar kullanarak tespit etmek oldukça zordur.

3.9 Malicious Insiderlar

Hem genel hem de özel bulut ortamlarında bütün kullanıcıların güvenilir olması beklenilemez. Ancak genel bulut ortamlarındaki kötü niyetli kullanıcıların hizmet ettiği kuruluşa verebileceği zarar, özel bulut hizmetleri kullanan kuruluşlara kıyasla daha fazla olabilir. Malicious insider şüphesi uyandırabilecek bazı durumlar aşağıdaki gibidir:

- Arka kapı hesapların veya saklı sunucuların kullanılması.
- Uzaktan ağ yönetim araçları kullanılması.

- Anti virüs uygulamalarının, güvenlik duvarlarının ve sistem loglarının hizmet dışı bırakılması, kullanıcı geçmişinin silinmesi.
- Yüksek büyüklükte kurum verisinin indirilmesi.
- Kurum dışına gönderilen hassas veriler, mesai saatleri dışında sunuculara erişilmesi, iş ile ilgili olmayan bilgilere erişilmesi.

4. Bulut Sistemlerinde Görünürlüğünü Arttırmak için İzlenecek Yollar

Bulut sistemlerinde görünürlüğü arttırmak için atılacak ilk adım, NIST CSF'nin de ilk adımı Identify bağlamında bulut ortamında bulunan sistemleri, verileri, kullanıcıları belirlemektir. Böylece şirket, bulut ortamında bulunan kaynakların bir envanterini çıkarmış olur ve neleri koruması gerektiğine dair bir fikir sahibi olur. Bu adım iyi bir başlangıç noktası olmasına rağmen tek başına yeterli değildir ve şirket gerekli alanlarda görünürlüğünü arttırmaya da odaklanmalıdır.

4.1 Görünürlük Sağlanacak Alanlar

Network Görünürlüğü

Network görünürlüğünü arttıran elementler olarak firewall, IPS/IDS, proxyler, network flow loglarının toplanması ve analizlenmesini söyleyebiliriz. Bu kategoriler için bulutta bulunan araçların yanında network güvenliğine hakim üçüncü şahıs satıcıların buluta entegre olan ürünleri de kullanılabilir.
Azure'da Network Security Group (NSG) kullanılarak inbound ve outbound güvenlik kuralları oluşturulabilir, kurallar için source ve destination portları belirlenebilir ve flow logları da etkinleştirilerek alınabilir. Böylece hem network trafiği filtrelenmiş olur hem de loglara ulaşım sağlanır.
2021 RSA Konferansı'nda önerilen yol; NSG flow loglarının etkinleştirilmesi, bu flow logları için bir depolama hesabı yaratılması ve logların bu hesapta 365 gün depolanmasıdır. Daha sonrasında bu logların Azure Traffic Analytics kullanılarak analizinin yapılmasıdır. Logların depolama hesabından Traffic Analytics'te toplanma süresi minimum 10 dakika veya maksimum 60 dakika olarak seçilebilir.

Uygulama Görünürlüğü

Microsoft verilerine göre Bilişim Teknoljoileri departmanındaki çalışanlar ortalama 1000 farklı bulut uygulaması kullanmakta. Kullanıcıların sistemlerinde kullandıkları uygulamaların tespiti ve bu uygulamaların ne kadar riskli olduğu Azure Shadow IT ile yapılabilir . Buna ek olarak, kullanıcıların kullandığı uygulamaların ve konteynırlarda bulunan uygulamaların logları bulut ortamında API'larla SIEM araçlarına gönderilebilir.

Sanal Makine Görünürlüğü

Sanal Makine görünürlüğünü arttırmak için Bulut üzerindeki sistemlerden loglar sürekli olarak toplanıp merkezileştirilmiş SIEM araçlarına gönderilmelidir. Sanal makinede bir güvenlik ihlali olma durumunda alertler oluşturulmalı ve ona göre gerekli önlemler alınmalıdır.

Database/Depolama Alanı Görünürlüğü

Depolama alanı görünürlüğünü arttırmak için loglar, verilerin şifrelenerek konulması ve hangi dataya hangi kullanıcının erişebileceğini belirleyen erişim yetkileri ve izinler kullanılabilir.

4.2 Otomasyon

Güvenlik alanında otomasyon önemli bir yere sahiptir. Hem çalışan üzerindeki iş yükünü hafifletip çalışanın başka önemli işlerle ilgilenmesine yardımcı olurken hem de tehdit tespit sürelerini önemli bir şekilde azaltır. Şirketler bir ay boyunca binlerce, belki de milyonlarca saldırıyla karşılaşır ve birçok alert alır. Eğer otomasyona başvurulmazsa, bu alertlere çalışanların teker teker bakması gerekeceğinden birçok tehdite karşı bir cevap verilemeyebilir.
SIEM tarafında otomasyonla, veri kaynakları izlenirken toplanan loglardan gerekli olmayanlar temizlenir, gerekli olan loglar belirlenir, karşılaşılan problemler risk seviyelerine göre çalışanlara alert olarak gönderilir, böylece çalışanlar kullandıkları SIEM araçlarını sürekli açıp kontrol etmek zorunda kalmaz ve zamandan kazanırlar. Eğer mümkünse, gelen alerte alınacak önlemler de otomasyona bağlanabilir.

4.3 AI ve ML Kullanılarak Gelişmiş Çözümlemeler Yapılması

Bulut ortamındaki logların incelenmesi için AI ve ML kullanan gelişmiş analiz yeteneğine sahip araçların kullanılması daha faydalı olur. Şirkette geçmişte toplanan her veri bu modellerin eğitilmesinde kullanılabilir. Böylece modeller, toplanan büyük veriden bir anlam çıkarabilir, bulut kaynaklarının normal davranışlarını anlayabilir ve gerçekleşebilecek herhangi bir sistemsel sorun veya tehdit durumunda anomalilerin tespiti kolaylaşır.

4.4 Şirkette Kullanılan Otomasyon Araçlarının Standartlaştırılması

Şirket içinde bulutta otomasyona başvuran güvenlik, operasyon, development gibi farklı takımlar olabilir. Her takımın kendi otomasyon araçlarının olması, ayrı ayrı scriptler çalıştırmaları görünürlüğün önünde bir engel yaratır. Bu yüzden şirkette otomasyon tek bir merkezde toplanmalı, playbooklar oluşturularak buluttaki kaynakların önceden belirlenmiş bir amaç için birbirleriyle nasıl çalıştığı belirtilmelidir.

5. Yetkisiz Erişimi ve Güvenlik Zaafiyetlerini Azaltmak için Azure AD Monitoring Stratejileri

5.1 Kullanıcı Hesapları

Alınması gereken loglar:

Azure AD Audit Logları
Sign-in Logları
Microsoft 365 Audit Logları
Azure Key Vault Logları
Riskli Kullanıcı Logları
User RiskEvent Logları

Hesap Yaratma

Hesap yaratılmasında oluşan anomaliler bir güvenlik zafiyeti olabilir. Kısa ömürlü hesaplara, isim kurallarına uymayan hesaplara ve önceden normal kabul edilen hesap yaratma adımlarına uymadan yaratılan hesaplara dikkat edilmelidir.

Kısa Ömürlü Hesaplar

Kısa ömürlü hesaplar, yaratıldıktan kısa süre sonra silinen hesaplardır. Saldırgan, yarattığı hesapları kullanıp silerek tespit edilmesini zorlaştırmaya çalışıyor olabilir.
Aynı zamanda, kısa ömürlü hesaplar onaylanmamış kişilerin veya işlemlerin hesap yaratıp silme yetkisi olabileceği anlamına da gelir.

İzlenmesi Gereken Olaylar	Risk Seviyesi	Notlar
Yaratıldıktan sonra kısa bir süre içerisinde silinen hesaplar	Yüksek	User principal name (UPN) eventlerinde aranacak. Yaratıldıktan sonra 24 saat içinde silinen hesaplara bakılmalı
Yetkili bir role atanan hesaplar	Yüksek	Eğer hesap Azure AD rolüne, Azure rolüne veya yetkili gruplara atandıysa alert oluşturulmalı ve araştırılmasına önem verilmeli.

Belirlenmiş İsim Kurallarına Uymayan Hesaplar

Şirketin kullanıcıları isimlendirmek için bazı kurallar koymalıdır. Bu şekilde hem kullanıcıların yönetimi hem de şirket dışından birisi tarafından yaratılan hesapların tespiti kolaylaşır. Şirket dışından birisi belirlenen bu kuralları bilmiyor olabilir, bu yüzden belirlenmiş isim kurallarına uymayan hesapların şirket dışından birileri tarafından yaratılma ihtimali yüksektir.
Örnek bir admin hesabı: ADM_isim.soyisim@ykteknoloji.com.tr
Örnek bir kullanıcı hesabı: isim.soyisim@ykteknoloji.com.tr

Bunlara ek olarak şirket kullanıcılar için bazı fieldlar belirlemeli ve bu fieldları tanımsız olan hesaplara da dikkat edilmelidir.

İzlenmesi Gereken Olaylar	Risk Seviyesi	Notlar
Fieldları tanımsız olan hesaplar	Düşük	Standart fieldları null veya yanlış formatta olan hesaplar

		tespit edilmeli
Belirlenmiş isim kurallarına uymayan kullanıcı hesapları	Düşük	-
Belirlenmiş isim kurallarına uymayan yetkili hesaplar	Yüksek	Yetkili hesaplarda belirlenmiş kurallara uymayan hesaplar için alert oluşturulmalı. Örneğin önünde ADM_ olmayan mail hesapları.

Normal Hesap Yaratma Adımlarına Uymadan Yaratılan Hesaplar

Hesap yaratmak için önceden belirlenmiş adımların olması hem bu adımlara uymayan hesapların daha sonrasında güvenlik tehdidine açık halde olmasının önüne geçer hem de saldırganlar tarafından yaratılan hesapların tespitini kolaylaştırır.

İzlenmesi Gereken Olaylar	**Risk Seviyesi**	**Notlar**
Onaylanmamış kullanıcılar veya işlemler tarafından yaratılan veya silinen hesaplar	Orta	Eğer hesap onaylanmamış bir kullanıcı tarafından yaratıldıysa alert gönderilmeli
Onaylanmamış kaynaklar tarafından yaratılan ve silinen hesaplar	Orta	Alert gönderilmeli

Alışılmadık Hesap Girişleri

Kullanıcıların kimlik doğrulamasında bazen yanlış kullanıcı adı veya şifre girmek gibi hatalar olabilir. Fakat bu hataların bloklar şeklinde çok fazla olması veya belirli bir motifi takip etmesi password spray, brute force saldırıları veya bir kullanıcının bilgilerinin açığa çıkması gibi sorunlara işaret edebilir. Bu yüzden belirli motifleri izleyip onlara göre alertler oluşturmak önem teşkil eder.
Alışılmadık hesap girişlerinin tespiti için Azure Identity Protection kullanılabilir. Identity Protection, kimlik bazlı tehditleri tespit etme, koruma ve çözüm bulma aşamalarını otomatize eder. Ayrıca makine öğrenmesi kullanarak kullanıcı hesap girişlerindeki riskleri tespit eder ve bir risk skoru atar. Şirket risk skorlarına göre hangi hesap girişlerine izin verip vermeyeceği konusunda kendi önlemlerini alabilir.

İzlenmesi Gereken Olaylar	Notlar
Başarısız kimlik doğrulama	Bir eşik değer belirlenip ona göre alert oluşturulmalı.
Kesintiye uğrayan kimlik doğrulamalar	Bir eşik değer belirlenip ona göre alert oluşturulmalı.
Smart lock out	Azure smart lock out ile yabancı hesaplar engellenebilir. Bloklanan hesapların incelenmesi gerekir.
IP adresi değişiklikleri	Farklı ip adreslerinden gelen fazla sayıda başarısız kimlik doğrulamalar sorun teşkil edebilir. VPN'ler false positive olabilir. IP değişiklikleri incelenmelidir, Identity Protection kullanılabilir.
Lokasyonlar	Bir kullanıcı lokasyon değiştirmesinin imkansız olduğu süreler içerisinde farklı lokasyonlardan giriş yapmaya çalışıyorsa bir sorun teşkil edebilir. VPN'ler false positive olabilir. Farklı lokasyonlardan giriş yapmaya çalışan kullanıcılar incelenmelidir. Identity Protection kullanılabilir.

5.2 Yetkili Hesaplar

Alınması Gereken loglar:
Azure AD Audit Logları
Microsoft 365 Audit Logları
Azure Key Vault Insights

Acil Durumlar için Erişim Hesapları

Azure AD'de bir acil durum esnasında yetkili hesapların kullanılamaması durumunda yaratılan acil durum hesapları kullanılabilir. Acil durum hesapları çok fazla ayrıcalığa sahiptir ve herhangi bir bireye ait değildir. Normal zamanlarda kullanılmamalıdır. Normal zamanlarda acil durum hesaplarından loglar gelmemelidir.
Acil durum hesaplarından alınması gereken loglar aşağıdaki gibidir

- Hesaba giriş yapılması
- Hesabın şifresinin değiştirilmesi
- Hesabın yetkilerinin veya rolünün değiştirilmesi
- Kimlik bilgileri veya kimlik doğrulama eklenmesi, çıkarılması

Yetkili Hesaplara Girişler

Yetkili hesaplara girişler, Azure AD Sign-in loglarından izlenebilir.

İzlenmesi Gereken Olaylar	**Risk Seviyesi**	**Notlar**
Hesaba girişin başarısız olması	Yüksek	Bir eşik değer belirlenip ona göre alert oluşturulmalı.
Conditional Access koşullarının başarısız olması	Yüksek	Hesaba erişmeye çalışan bir saldırganın olabilir.
Belirlenmiş isim kurallarına uymayan yetkili hesaplar	Yüksek	
Kesintiler	Yüksek/Orta	Saldırgan hesabın şifresine erişimi vardır fakat MFA'yı geçemiyor olabilir.
MFA kullanmayan yetkili hesaplar	Yüksek	Bu hesaplar denetlenmeli. Bilerek mi MFA kullanılmıyor yoksa gözden mi kaçmış anlaşılmalıdır.
Lockout	Yüksek	Bir eşik değer belirlenip ona göre alert oluşturulmalı.
Hesaba girişlerin bloklanması	Düşük	Şirketten ayrılan birisinin hesaba erişmeye çalıştığını belirtir. Hesabın bloklu olmasına rağmen bu olau loglanıp alert oluşturulmalıdır.
MFA fraud alertleri	Yüksek	
Beklenen kontrollerin dışından yapılan yetkili hesap girişleri		Belirli kurallara göre onaylanmamış sayılan hesap girişleri izlenmeli ve alert oluşturulmalı.
Normal giriş saatleri dışında	Yüksek	Yetkili hesapların çalışma

yapılan hesap girişleri		saatleri belirlenmeli ve eğer o saatler dışında bir giriş yapılıyorsa alert oluşturulmalı
Identity Protection riskleri	Yüksek	
Şifre değişimleri	Yüksek	Herhangi bir yöneticinin şifre değişiminde alert oluşturulmalı. Özellikle global adminlere, kullanıcı adminlerine, subscription adminlerine ve acil durum hesaplarına dikkat edilmeli.
Yeni cihaz veya lokasyon	Yüksek	Çoğu yönetici hareketi yönetici cihazlarından ve kısıtlı sayıda lokasyondan yapılmalı.
Audit alert ayarlarının değişitilmesi	Yüksek	Alert oluşturulmalı.

Yetkili Hesaplar Tarafından Yapılan Değişiklikler

Yetkili hesapların yaptığı ve yapmaya çalıştığı her değişiklik izlenmelidir. Böylece her yetkili hesap için normal davranış belirlenebilir ve anormal bir davranışta alert oluşturulabilir. Bu değişikliklerin izlenmesi için Azure AD Audit logları kullanılır.

Yetkili Hesaplara Yapılan Değişiklikler

İzlenmesi Gereken Olaylar	**Risk Seviyesi**	**Notlar**
Yetkili hesap yaratılması	Orta	Yaratılan yetkili hesaplar izlenmeli. Özellikle yaratılması ve silinmesi arasında kısa bir süre olan hesaplara bakılmalı.
Kimlik doğrulama yöntemlerine yapılan değişiklikler	Yüksek	Saldırgan, hesaba sürekli erişimi olması için kimlik doğrulama yöntemi ekliyor olabilir.

Yetkili hesapların izinlerinde yapılan değişikliklerde alertler oluşturulmalı	Yüksek	Özellikle bilinmeyen rollere atanan veya normal sorumlulukları dışında kalan rollere atanan hesaplara dikkat edilmeli
Kullanılmayan yetkili hesaplar	Orta	İnaktif yetkili hesaplar her ay gözden geçirilmeli
Conditional Access'ten muaf hesaplar	Yüksek	CA'yı yapmayan hesaplar tehditlere daha açık haldedir

5.3 Yetkili Kimliklerin Yönetimi (PIM)

Privileged Identity Management (PIM) şirketteki önemli kaynaklara erişimi yönetmeye, denetlemeye ve izlemeye olanak sağlayan bir Azure AD hizmetidir.
PIM aşağıdaki riskleri azaltmada kullanılabilir:

- Güvenli bilgilere ve kaynaklara erişimi olan kişileri belirleme ve sayısını en aza indirme
- Hassas kaynaklarda aşırı, gereksiz veya kötüye kullanılan erişim izinlerini algılama
- Kötü amaçlı bir aktörün güvenli bilgilere veya kaynaklara erişme şansını azaltma
- Yetkisiz bir kullanıcının hassas kaynakları yanlışlıkla etkileme olasılığını azaltma

Alınması gereken loglar:

- Azure AD Audit logları
- Sign-in logları
- Microsoft 365 Audit logları
- Azure Key Vault logları

İzlenmesi Gereken Olaylar	**Risk Seviyesi**	**Notlar**
Azure AD Rol Ataması	Yüksek	
Azure kaynakları için rol yapılandırması	Yüksek	Planlı bir değişiklik yoksa hemen araştırılmalıdır. Bu ayar, bir saldırganın ortam içerisindeki Azure aboneliklerine erişmesine olanak sağlar.

İzlenmesi Gereken Olaylar	Risk Seviyesi	Notlar
Yetkili hesap izinlerine değişiklik ekleme uyarısı	Yüksek	Yetkili rol yöneticisi ve genel yönetici değişiklikleri izlenmeli ve her zaman alert oluşturulmalıdır Bu, bir saldırganın rol atama ayarlarını değiştirmek için ayrıcalık elde etmeye çalıştığına dair bir gösterge olabilir. Eğer önceden tanımlanmış bir eşik değeri yoksa, normal kullanıcılar için 60 dakikada 4, yetkili hesaplar için 60 dakikada 2 alert alınır.
Yetkili hesap izinlerine yapılan toplu silme değişiklikleriyle ilgili uyarı	Yüksek	Planlı bir değişiklik yoksa hemen araştırılmalı. Bu ayar, bir saldırganın ortam içerisindeki Azure aboneliklerine erişmesine olanak sağlar.
PIM ayarlarına yapılan değişiklikler	Yüksek	Yetkili Rol Yöneticisi ve Genel Yönetici değişiklikleri her zaman izlenmeli ve uyarı oluşturulmalı. Bir saldırganın rol atama ayarlarını değiştirmek için değiştirme erişimine sahip olduğu anlamına gelebilir. Bu eylemlerden biri PIM yükseltme güvenliğini azaltarak saldırganların yetkili bir hesap edinmesini kolaştıracaktır.
Onaylar ve yükseltmeyi reddetme	Yüksek	Bütün yetki yükseltmeler izlenmeli. Bir saldırının zaman çizelgesinin net bir göstergesi olduğu için tüm yükseltmelerin logları tutulmalı.

Alert ayarının devre dışı olarak değişmesi	Yüksek	Her zaman alert oluşturulmalı. Kötü bir aktörün, Azure MFA gereksinimleriyle ilgili oluşan alertleri devre dışı bırakarak yetkili erişim yapmasının tespitinde yardımcı olur.

Azure Kaynakları için Rol Yapılandırması

Azure kaynaklarına yapılan rol atamalarını izlemek kaynak rolleri için etkinlik ve etkinleştirmelere görünürlük sağlar. Bunlar, bir kaynağa saldırı yüzeyi oluşturmak için kullanılabilir. Bu tarz bir etkinliği izlerken aşağıdakileri tespit etmeye çalışıyor oluruz:

- Belirli kaynaklarda rol atamalarını sorgulama
- Tüm alt kaynaklar için rol atamaları
- Tüm etkin ve uygun rol ataması değişiklikleri

İzlenmesi Gereken Olaylar	**Risk Seviyesi**	**Notlar**
Yetkili hesap etkinlikleri için Audit Alert Kaynağı loglarının denetlemesi	Yüksek	Her zaman alert oluşturulmalı. Kötü bir aktörün Azure'daki tüm kaynakları yönetebilmesi için geçerli bir rol atamasını önler.
Uyarıyı devre dışı bırakmak için Audit Alert Kaynağının denetlenmesi	Orta	Kötü bir aktörün Uyarılar bölmesinden alertleri devre dışı bırakması sonucu herhangi bir tehditin gözden kaçmasını önler.

Azure Kaynakları ve Abonelikleri için Erişim Yönetimi

Owner veya User Access Administrator rollerine atanan kullanıcıların ve abonelik yönetimi ayarını açan Azure AD global yöneticilerinin kaynak yöneticisi izinleri vardır. Bu yöneticiler rol atayabilir, rol ayarlarını değiştirebilir, Azure kaynaklarına PIM ile yapılan erişimleri görebilir ve kaynaklar için PIM'i yönetebilir. Bundan dolayı bu hesaplar ile kötü bir aktöre

yetkili erişim verilmemesi, onların Azure kaynaklarına rol atama yetkisinin olmaması için bu hesaplarla yapılan yükseltmeler de izlenmelidir.

5.4 Uygulamalar

Uygulamalar, kullanıcı hesapları kadar sık olmasa da güvenlik açıkları için bir yüzey oluşturabilir ve her ihtimale karşı izlenmelidir.
Uygulamalar izlenirken aşağıdaki olayların gözden geçirilmesi zararlı bir aktivitenin normal bir aktiviteden ayırt edilmesinde yardımcı olur:

- Normal iş süreçleri ve zamanları dışında olan tüm değişiklikler
- Uygulama kimlik bilgileri değişiklikleri
- Uygulama izinleri
    - Bir Azure AD veya Azure RBAC rolune atanan hizmet sorumlusu (service principal)
    - Yüksek ayrıcalıklı izinler verilen uygulamalar
    - Azure Key Vault değişiklikleri
    - Uygulamalara onay veren son kullanıcı
    - Risk seviyesine göre durdurulan son kullanıcı onayı

- Uygulama yapılandırma değişiklikleri
    - Evrensel kaynak tanımlayıcı (URI) değişiklikleri
    - Uygulama sahiplerine yapılan değişiklikler
    - Değiştirilen oturum açma URL'leri

Alınması gereken loglar:

- Azure AD Audit Logları
- Sign-in Logları
- Microsoft 365 Audit Logları
- Azure Key Vault Logları

İzlenmesi Gereken Olaylar	**Risk Seviyesi**	**Notlar**
Mevcut uygulamalara eklenen kimlik bilgileri	Yüksek	Kimlik bilgileri; ● Normal çalışma saatleri dışında eklendiğinde ● Ortamınızda kullanılan türde olmadığında ● Hizmet sorumlularını destekleyen SAML dışı bir akışa eklendiğinde

		Alert oluştur.
Şirket ilkesinin izin verdiğinden daha uzun süreye sahip olan kimlik bilgileri	Orta	
Azure AD veya Azure RBAC rolüne atanan uygulamalar	Yüksek ve Orta	Genel yönetici gibi roller için risk yüksektir. Daha düşük ayrıcalıklı roller için risk orta düzeydedir. Bir uygulama normal değişiklik yönetimi veya yapılandırma dışında bir Azure veya Azure AD rolüne atanırsa alert oluşturulmalı.
Uygulamaya yüksek ayrıcalıklı izinler verilmesi ".All" gibi	Yüksek	
Yöneticinin uygulamaya izinler vermesi veya yüksek ayrıcalıklı izinler verilmesi	Yüksek	Genel yönetici, uygulama yöneticisi veya bulut uygulaması yöneticisi bir uygulamayı onaylarsa alert oluştur.
Uygulamaya Microsoft Graph, Exchange, SharePoint veya Azure AD için izinler verilmesi	Yüksek	Genel yönetici, uygulama yöneticisi veya bulut uygulaması yöneticisi bir uygulamayı onaylarsa alert oluştur.
Diğer API'lar için uygulama izinleri verilmesi	Orta	Genel yönetici, uygulama yöneticisi veya bulut uygulaması yöneticisi bir uygulamayı onaylarsa alert oluştur.
Tüm kullanıcılar adına yüksek ayrıcalıklı temsilci izinleri verilmesi	Yüksek	Genel yönetici, uygulama yöneticisi veya bulut uygulaması yöneticisi bir uygulamayı onaylarsa alert oluştur.
Key Vault'a kimin eriştiği ve ne zaman eriştiğinin izlenmesi	Orta	Key Vault'a normal saatler dışında erişim izlenmeli Key Vault ACL'ye yapılan

		değişiklikler izlenmeli
Uygulamaya son kullanıcı onayı	Düşük	Yüksek ayrıcalıklı hesaplar izlenmeli. Yüksek riskli izinler talep eden uygulamalar izlenmeli. Şüpheli isimlere sahip olan uygulamalar izlenmeli.
Bir karşılığı bulunmayan URI'lar	Yüksek	
AppID URI'a yapılan değişiklikler	Yüksek	URI ekleme, değiştirme veya kaldırma gibi AppID URI değişikliklerine bakılmalı
Uygulama sahipliğinde yapılan değişiklikler	Orta	Normal değişiklik yönetimi dışında bir uygulama sahibi olarak eklenen kullanıcılara bakılmalı
Oturum kapama URL'ine yapılan değişiklikler	Düşük	Oturum kapama URL'ine yapılan değişiklikler izlenmeli. Boş girişler veya mevcut olmayan konumlara yapılan girişler kullanıcının oturumunu sonlandırmayı durdurur.

5.5 Cihazlar

Cihazlar genellikle kimlik tabanlı saldırılarda hedef değildir. Fakat güvenlik kontrollerini karşılamak, kandırmak veya kullanıcıların kimliğine bürünmek için saldırganlar tarafından kullanılabilir.
Cihazların Azure AD ile dört ilişkisi olabilir:

- Kayıtsız
- Azure AD kayıtlı (registered)
- Azure AD'ye katılanlar (joined)
- Hybrid Azure AD'ye katılanlar (joined)

Kayıtlı ve katılmış cihazlara, birincil kimlik doğrulama yapıtı olarak ve bazı durumlarda da MFA yapıtı olarak kullanılan Primary Refresh Token (PRT) çıkar. Saldırganlar kendi cihazlarını kaydetmeyi, geçerli cihazlardaki PRT'leri kullanarak iş verilerine erişmeyi, geçerli

kullanıcı cihazlarındaki PRT'leri çalmayı veya Azure AD'deki cihaz tabanlı denetimlerdeki yanlış yapılandırmaları bulmayı hedefler.
Kötü aktörlerin cihazlar aracılığıyla altyapınıza saldırmasını engellemek için aşağıdakiler izlenmelidir:

- Cihaz kayıtları ve Azure AD'ye katılmalar
- Uygulamalara erişen uyumlu olmayan cihazlar
- BitLocker anahtarı alma
- Cihaz yöneticisi rolleri
- Sanal makinelerde oturum açma

Alınması gereken loglar:

- Azure AD Audit Logları
- Sign-in Logları
- Microsoft 365 Audit Logları
- Azure Key Vault Logları

İlkeler Dışında Cihaz Kayıtları ve Katılımları

Zararlı aktörlerin cihazları kayıt etmesini ve katılmalarını engellemek için her bir cihazın kaydı ve katılımında MFA zorunlu olmalıdır.

İzlenmesi Gereken Olaylar	**Risk Seviyesi**	**Notlar**
Cihaz kaydı veya birleştirme işleminin MFA olmadan tamamlanması	Orta	MFA olmadan kaydedilen veya katılan herhangi bir cihaz olursa alert oluşturulmalı
Azure AD'deki Cihaz Kaydı MFA'ya yapılan değişiklikler	Yüksek	Devre dışı olup olmadığı gözlenmeli. Bir log akışı yok o yüzden periyodik olarak kontrol edilmeli
Etki alanında olan veya uyumlu cihaz gerektiren Conditional Access ilkelerindeki değişiklikler	Yüksek	Etki alanında olan veya uyumlu cihazlarla ilgili ilkelerdeki herhangi bir değişiklikte alert oluşturulmalı. Güvenilen lokasyonların değişikliklerinde alert oluşturulmalı. MFA ilkesinden muaf tutulan hesaplar veya cihazlara yapılan eklemelerde alert oluşturulmalı.

Uyumlu Olmayan Cihazlarda Oturum Açma

Uyumlu cihazlar gerektiren Conditional Access ilkeleri ile buluta ve hizmet olarak yazılım uygulamalarına erişimi engellemek mümkün olabilir. Bu yüzden dikkat edilmelidir.

İzlenmesi Gereken Olaylar	Risk Seviyesi	Notlar
Uyumlu olmayan cihazlar tarafından yapılan oturum açmalar	Yüksek	Uyumlu olmayan bir cihaz tarafından yapılan oturum açmada alert oluşturulmalı. MFA olmadan veya güvenilmeyen bir lokasyondan yapılan erişimlerde alert oluşturulmalı.
Bilinmeyen cihazlar tarafından yapılan oturum açmalar	Düşük	

Eski Cihazlar

Eski cihazlar, belirli bir süre boyunca oturum açmamış hesapları içerir. Bir kullanıcı yeni bir cihaz aldığında veya eskisini kaybettiğinde, Azure AD'ye katılmış cihaz silindiğinde veya yeniden bağlandığında cihazlar eski hale gelebilir. Ayrıca, kullanıcılar artık kiracı ile ilişkili olmadığında da cihazları katılmış veya kayıtlı durumda kalabilir. PRT'lerin kullanılabilmesi için eski cihazların kaldırılması gereklidir.

İzlenmesi Gereken Olaylar	Risk Seviyesi	Notlar
Son oturum açma tarihi	Düşük	Eski cihazları tanımlamak ve kaldırmak için Graph API ve PowerShell kullanılabilir.

BitLocker Anahtar Alımı

Bir kullanıcının cihazına sızan saldırganlar, Azure AD'de BitLocker anahtarlarını alabilir. Normal kullanıcıların anahtar almaları yaygın değildir ve izlenmesi gerekir.

İzlenmesi Gereken Olaylar	Risk Seviyesi	Notlar

Anahtar alımı	Orta	

Cihaz Yöneticisi Rolleri

Genel yöneticiler ve bulut cihaz yöneticileri, tüm Azure AD 'ye katılmış cihazlarda yerel yönetici haklarını otomatik olarak alır. Ortamınızı güvenli tutmak için kimin bu haklara sahip olduğunun izlenmesi önemlidir.

İzlenmesi Gereken Olaylar	**Risk Seviyesi**	**Notlar**
Genel veya cihaz yöneticisi rollerine eklenen kullanıcılar	Yüksek	

5.6 Altyapı

Altyapı, düzgün yapılandırılmadığı takdirde güvenlik açıklarının oluşabileceği birçok bileşene sahiptir. Altyapı için izleme ve uyarı stratejisinin bir parçası olarak, aşağıdaki alanlarda belirtilmiş olayları izlenmelidir ve gerektiği durumlarda uyarılar oluşturulmalıdır:

- Kimlik doğrulama ve yetkilendirme
- Federasyon sunucularını da içeren Hibrit Kimlik Doğrulama bileşenleri
- Politikalar
- Abonelikler

Kimlik doğrulama altyapısının bileşenlerini izlemek ve uyarı oluşturmak önem arz eder. Herhangi bir güvenlik ihlali, tüm ortamın tamamen ele geçirilmesine yol açabilir. Azure AD kullanan birçok kuruluş, karma kimlik doğrulama ortamında çalışır. Bu hem bulut hem de şirket içi bileşenlerin izleme ve uyarı oluşturma stratejisine dahil edilmesi gerektiği anlamına gelir. Hibrit bir kimlik doğrulama ortamına sahip olmak, ortama başka saldırı vektörleri de sunar.
Tüm bileşenlerin, bunları yönetmek için kullanılan hesapların yanı sıra Kontrol Düzlemi / Katman 0 varlıkları olarak değerlendirilmesi önerilir. Beklenmeyen olayları ve olası saldırıları tespit edebilmenin ilk adımı bir temel oluşturmaktır.

Alınması gereken loglar:

- Azure AD Audit Logları
- Sign-in Logları
- Microsoft 365 Audit Logları
- Azure Key Vault Logları

Azure portalından Azure AD Denetim logalarını görüntülenebilir ve CSV veya JSON dosyaları olarak indirilebilir. Azure portalı, Azure AD loglarını daha fazla izleme ve uyarı oluşturma otomasyonuna olanak tanıyan diğer araçlarla tümleştirmenin çeşitli yollarına sahiptir. Bu yollar aşağıdaki gibi sıralanabilir:

- Azure Sentinel – güvenlik bilgileri ve olay yönetimi (SIEM) yetenekleri sağlayarak kurumsal düzeyde akıllı güvenlik analitiği sağlar.
- Azure Monitörü – çeşitli koşulların otomatik olarak izlenmesini ve uyarılmasını sağlar. Farklı kaynaklardan gelen verileri birleştirmek için çalışma kitapları oluşturabilir veya kullanabilir.
- Azure Event Hubs ile entegre SIEM- Azure AD logları diğer SIEM araçlarıyla tümleşik ile getirilebilir; Splunk, ArcSight, QRadar.
- Microsoft Bulut Uygulama Güvenliği (MCAS) – uygulamaları keşfetmeye ve idare etmeye, uygulamaları ve kaynakları yönetmeye ve bulut uygulamalarının uyumluluğunu kontrol etmeye olanak tanır.

Kimlik Doğrulama Altyapısı

Hem şirket içi hem de bulut tabanlı kaynakları ve hesapları içeren hibrit ortamlarda, Active Directory altyapısı, kimlik doğrulama yığınının önemli bir parçasıdır. Bu yığın ayrıca saldırılar için bir hedeftir, bu nedenle güvenli bir ortam sağlamak için yapılandırılmalı ve uygun şekilde izlenmelidir. Kimlik doğrulama altyapısına karşı kullanılan mevcut saldırı türlerinin örnekleri, Password Spray ve Solorigate tekniklerini kullanır.
Aşağıda listelenen olaylar aranacak belirli olaylardır:

İzlenmesi Gereken Olaylar	**Risk Seviyesi**	**Notlar**
Extranet kilitleme eğilimleri	Yüksek	Azure AD Connect Health
Başarısız oturum açma işlemleri	Yüksek	Health Portalı Bağlayın

Gizlilik uyumlu	Düşük	Azure AD Connect Sağlık
LDAP'ye olası kaba kuvvet saldırısı	Orta	Kimlik için Microsoft Defender
Hesap numaralandırma keşif	Orta	Kimlik için Microsoft Defender
Azure AD ve Azure AD FS arasındaki genel bağıntı	Orta	Kimlik için Microsoft Defender

Parola Koruma Politikaları

Azure AD Parola Koruması uygulanırsa, izleme ve raporlama önemli görevlerdir.
Etki alanı denetleyicisi (DC) aracısı ve proxy hizmetleri, olay logları iletilerini loglara kaydeder. Aşağıda açıklanmış tüm PowerShell cmdletler yalnızca proxy sunucusunda kullanılabilir.
Her etki alanı denetleyicisinde, DC aracısı hizmeti yazılımı, her bir parola doğrulama işleminin sonuçlarını aşağıdaki yerel olay günlüğüne yazar:

- \Applications and Services Logs\Microsoft\AzureADPasswordProtection\DCAgent\Admin
- \Applications and Services Logs\Microsoft\AzureADPasswordProtection\DCAgent\Operational
- \Applications and Services Logs\Microsoft\AzureADPasswordProtection\DCAgent\Trace

DC aracısı Yönetici günlüğü, yazılımın nasıl davrandığına ilişkin birincil bilgi kaynağıdır. Varsayılan olarak, İzleme logları kapalıdır ve veriler loglara kaydedilmeden önce etkinleştirilmelidir.
Bu olaylar için bilgiler aşağıda belirtilen yerlerdedir:

- Applications and Services Logs\Microsoft\AadApplicationProxy\Connector\Admin
- Azure AD Audit Logları, Kategori Uygulama Ara Sunucusu

6. Bulut Alt Yapısındaki Bileşenlerin Güvenliği

6.1 Hesaplar

Çoğu kuruluş, kimlik doğrulama ve yetkilendirme için kullanılan iki tür hesaba sahiptir. Birincisi, genellikle çalışanlar veya yükleniciler tarafından, işlerine yardımcı olan görevleri ve işlevleri yerine getirmek üzere sistemlerde ve uygulamalarda oturum açmak için kullanılan insan kullanıcı hesaplarıdır. İkincisi ise sistemler ve uygulamalar tarafından, sistemde yerel veya ağ üzerinden kaynaklara erişmek için kullanılan insan dışı hesaplardır. Çoğu zaman, bir uygulama içinde, bazen bir insan hesabı tarafından başlatılan, otomatikleştirilmiş görevleri veya API çağrılarının bir kısmını gerçekleştirmek için kullanılırlar. Hizmet hesapları, sistem ayrıcalıkları bağlamında uygulamaları yürüten işletim sistemlerinde tipik olarak kullanılan bir tür insan olmayan, belli işleri yerine getirmek veya diğer ağ kaynaklarıyla bağlantı kurmak için belirli yerel sistem ayrıcalıklarını gerektiren bir uygulamanın yüklenmesi sırasında oluşturulan tanımlı hesaplardır.

Buluttaki hizmet hesapları genellikle ayrıcalıklı hesaplardır ve kritik altyapı hizmetlerine erişim sağlayabilirler. Herhangi bir güvenlik ihlali durumunda saldırganlar bulut ağlarına erişebilir, hassas kaynaklara ve verilere erişim hakkı elde edebilir. Yeni bulut kaynakları oluşturduğunuzda, bulut kaynaklarını ölçeklendirdiğinizde veya kod olarak altyapıyı (IaC) kullanan hazır ortamlar oluşturduğunuzda hizmet hesapları otomatik olarak oluşturulabilir. Yeni hesapların varsayılan ayarları olabilir, bu da bazı durumlarda kimlik doğrulamanın zayıf olduğu veya hiç olmadığı anlamına gelir.

Hizmet hesaplarına erişimi ve kimlik doğrulamasını denetleyen politikalar belirlemek için kimlik ve erişim yönetimini (IAM) bağlamında önlemler alınması doğru bir yaklaşım olacaktır. Güvenli olmayan hesapları otomatik olarak algılamak ve düzeltmek için bir bulut yapılandırma izleme aracı kullanılması önerilir. Son olarak, şüpheli etkinliği tespit etmek ve yanıt vermek için hassas hesapların kullanımı izlenmelidir.

6.2 Sunucular

Bulut sunucusu, bir bulut bilişim ortamında çalışan (fiziksel bir sunucu yerine) sanal bir sunucudur . İnternet üzerinden bir bulut bilgi işlem platformu aracılığıyla oluşturulur , barındırılır ve teslim edilir ve uzaktan erişilebilir. Sanal sunucular olarak da bilinirler. Bulut sunucuları, çalıştırmak için ihtiyaç duydukları tüm yazılımlara sahiptir ve bağımsız birimler olarak işlev görebilir.
Bir bulut ortamı sanallaştırılırken, perde arkasında birden fazla coğrafi konumda dağıtılan fiziksel donanımlardan oluşur. Buna fiziksel sunucular, depolama aygıtları, yük dengeleyiciler ve anahtarlar ve yönlendiriciler gibi ağ ekipmanları dahildir.

Bir bulut sunucusunun güvenliğini sağlamanın birkaç yolu aşağıdaki gibi sıralanabilir:

- Gelen ve giden iletişimi denetleme: Sunucunun yalnızca ağlara ve işlemleri için gereken belirli IP aralıklarına bağlanmasına izin verilmelidir. Örneğin, bir veri tabanı sunucusunun, hizmet verdiği uygulama eş görünümleri dışında, genel internete veya başka bir IP'ye erişimi olmamalıdır.
- İletişimleri şifreleme: İletişimler ister genel ağlar üzerinden ister güvenli bir özel ağ içinde olsun, man-in-the-middle (MITM) saldırılarını önlemek için şifrelenmelidir. Telnet veya FTP gibi güvenli olmayan protokollerin kullanımından kaçınılmalıdır. Tüm verileri HTTPS veya SCP (Güvenli Kopyalama) veya SFTP (Güvenli FTP) gibi diğer güvenli protokoller üzerinden iletilmesi gerekir.
- SSH anahtarlarını kullanma: Bulut sunucularına parola kullanarak erişmekten kaçınılması gerekmektedir. Çünkü bunlar kaba kuvvet (Brute Force) saldırılarına karşı savunmasızdır ve kolayca ele geçirilebilir. Daha güvenli erişim için genel/özel anahtar şifrelemesinden yararlanan SSH anahtarlarının kullanılması önerilir.
- Ayrıcalıkları belirleme ve kısıtlama: Bir sunucuya sadece kesinlikle erişmesi gereken kullanıcılara veya hizmet rollerine erişim izni verilmelidir. Yalnızca belirli dosya ve klasörlere erişildiğinden ve roller doğrultusunda gereken belirli işlemlerin gerçekleştirildiğinden emin olmak için her hesabın erişim düzeyi dikkatlice kontrol edilmelidir. Tüm yetkili kullanıcıyı kullanmaktan kaçınılmalıdır ve herhangi bir işlem tanımlanmış kullanıcı hesapları kullanılarak gerçekleştirilmelidir.

6.3 Hipervizörler

Hipervizör, sanal makineleri oluşturan ve her biri ayrı bir işletim sistemine sahip birkaç sanal makineyi (VM) çalıştırmayı mümkün kılan yazılım veya donanımdır. Bulut sistemleri hipervizörlere dayanmaktadır. Bu nedenle, hipervizörler önemli bir güvenlik sorunudur, çünkü hipervizörün ele geçirilmesi (hyperjacking olarak bilinen saldırı), saldırganın üzerinde çalışan tüm ana bilgisayarlara ve sanal makinelere erişmesini sağlar.
Ortak bulut sistemlerinde hipervizör güvenliği, bulut sağlayıcısının sorumluluğundadır, bu nedenle bununla ilgilenmenize gerek yoktur. Yalnızca bazı ürünlerde genel bir bulutta sanallaştırılmış iş yükleri çalıştırırken, hipervizörün güvenliğini sağlamaktan sorumlu taraf müşteridir.
Özel bulut sistemlerinde hipervizör her zaman müşteri sorumluluğundadır.

Hipervizör güvenliği sağlamanın birkaç yolu aşağıdaki gibi sıralanabilir:

- Hipervizör çalıştıran makinelerin sağlamlaştırıldığından, yama uygulandığından, genel ağlardan izole edildiğinden ve veri merkezinizde fiziksel olarak güvenli olduğundan emin olmak esastır.
- Hipervizöre erişimi dikkatlice kontrol ederek yerel kullanıcı hesaplarına en az ayrıcalık atanmalıdır.

- Sanal makine monitörü ve sanallaştırma yönetim yazılımı çalıştıran makineler sağlamlaştırılmalı, güvenli hale getirilmeli ve yakından izlenmelidir.
- Hipervizör tarafından kullanılan ortak donanım önbelleklerini ve ağları güvenli hale getirin ve izleyin
- Geliştirme ve test ortamlarında hipervizörlere dikkat gösterilmeli; üretime yeni bir hipervizör dağıtıldığında uygun güvenlik önlemlerinin uygulandığından emin olunmalıdır.

6.4 Depolama

Bulut depolama, bir hizmet olarak veri depolamayı yöneten ve işleten, bir bulut bilgi işlem sağlayıcısı aracılığıyla verileri internette depolayan bulut bilgi işlem modelidir. Bu, "her zaman, her yerde" ideolojisi kapsamında veri erişimiyle size çeviklik, küresel ölçek ve dayanıklılık sağlar. Bulut sistemlerinde, donanım sistemlerinden depolamayı soyutlamak için sanallaştırma kullanılır. Depolama sistemleri, otomatik olarak sağlanabilen ve ölçeklendirilebilen esnek depolama havuzları veya sanallaştırılmış kaynaklar haline gelir.

Bulut depolama hizmetlerinin güvenliği sağlamanın birkaç yolu aşağıdaki gibi sıralanabilir:

- Hangi cihazların ve uygulamaların bulut depolamaya bağlandığını, kuruluş genelinde hangi bulut depolama hizmetlerinin kullanıldığı belirlenmeli ve veri akışları haritalandırılmalıdır.
- Bulut depolamaya ihtiyacı olmayan dahili kullanıcılar için erişim engellenmeli ve son kullanıcılar tarafından bulut hizmetlerinin gölge kullanımını ortadan kaldırılmalıdır.
- Veriler hassasiyet seviyelerine göre sınıflandırılmalıdır. Bu güvenlik veya uyumluluk etkileri olan bulut depolamada depolanan verilere odaklanılmasına yardımcı olur.
- Kullanılmayan verileri kaldırılmalıdır. Bulut depolama kolayca ölçeklenebilir ve gereksiz verilerin veya artık kullanılmayan tüm veri birimlerinin veya anlık görüntülerin tutulması yaygın bir durumdur. Saldırı yüzeyini ve uyumluluk yükümlülüklerinizi azaltmak için kullanılmayan veriler belirlenmeli ve ortadan kaldırılmalıdır.
- Kimlik ve erişim yönetimi (IAM) sistemlerini kullanarak, bulut ve şirket içi sistemler için tutarlı güvenlik ilkeleri uygulayarak verilere erişim dikkatlice kontrol edilmelidir.
- Şüpheli veri aktarımlarını, veri değiştirmeyi, silmeyi veya kötü amaçlı ya da kazara veri erişimini tespit etmek ve engellemek için bulut veri kaybı önleme (DLP) araçları kullanılmalıdır.

6.5 Veri Tabanları

Buluttaki veri tabanları ortak ağlara kolayca maruz kalabilir ve genellikle hassas veriler içerir. Bu durum onları yakından bir güvenlik riski haline getirir. Veri tabanları, hizmet ettikleri uygulamalarla ve diğer bulut sistemleriyle entegre olduklarından, veri tabanının güvenliğinin ihlal edilmesini önlemek için bu bitişik sistemlerin de güvence altına alınması gerekir.

Veri tabanı güvenliği sağlamanın birkaç yolu aşağıdaki gibi sıralanabilir:

- Yapılandırmayı ve örnekleri sağlamlaştırma: Herhangi bir bilgi işlem örneğinde bir veri tabanının kullanıcı tarafından dağıtılırsa, örneği sağlamlaştırmak ve veri tabanını güvenli bir şekilde yapılandırmak yine kullanıcı sorumluluğundadır. Yönetilen bir veri tabanı hizmeti kullanılıyorsa, bu sorunlar genellikle bulut sağlayıcısı tarafından ele alınır.
- Veri tabanı güvenlik ilkeleri: Veri tabanı ayarlarının kullanan kuruluşun güvenlik ve uyumluluk ilkeleriyle uyumlu olduğundan emin olunmalıdır. Güvenlik gereksinimleri ve uyumluluk yükümlülükleri bulut veri tabanı sistemlerindeki belirlenmiş ayarlarla eşleştirilmelidir. Tüm veri tabanı örneklerine güvenli ayarların uygulanmasını sağlamak için CSPM (Bulut Güvenliği Durum Yönetimi)gibi otomatik araçlar kullanılmalıdır.
- Ağ erişimi: Genel geçer bir kural olarak, veri tabanları hiçbir zaman genel ağlara açık bırakılmamalı ve alakası olmayan altyapılardan izole edilmelidir. Mümkünse, bir veri tabanı yalnızca hizmet etmesi amaçlanan belirli uygulama örneklerinden gelen bağlantıları kabul etmelidir.
- İzinler: Kullanıcılara, uygulamalara ve hizmet rollerine yalnızca minimum düzeyde izin verilmelidir. Kapsamlı izinlere sahip "süper kullanıcılar" ve yönetici kullanıcılardan kaçınılmalıdır. Her yöneticinin üzerinde çalıştığı belirli veri tabanlarına erişimi olmalıdır.
- Son kullanıcı cihaz güvenliğ: Güvenlik, bulut ortamıyla sınırlı değildir. Yöneticilerin veri tabanına bağlanmak için hangi uç nokta cihazlarını kullandığını dikkate alınmalıdır. Bu cihazların güvenliği sağlanmalı, bilinmeyen veya güvenilmeyen cihazlardan gelen bağlantılara izin vermemeli ve şüpheli etkinliği tespit etmek için oturumlar izlenmelidir.

6.6 Ağ

Bulut ağı, bir bulut bilişim altyapısı içinde bulunan veya bir bulut bilişim altyapısının parçası olan bir bilgisayar ağı anlamına gelir. Bulut tabanlı veya bulut özellikli uygulama, hizmetler ve çözümler arasında ağ bağlantısı sağlayan bir bilgisayar ağıdır. Bulut ağı, bulut tabanlı ağ veya bulut etkin ağ olabilir.

Bulut ağlarının güvenliğini sağlamanın birkaç yolu aşağıdaki gibi sıralanabilir:

- Bulut kaynakları arasında hangi trafiğin akabileceğini tanımlayan kuralları tanımlamak için güvenlik grupları kullanılmalıdır. Güvenlik gruplarının bilgi işlem örneklerine sıkı bir şekilde bağlı olduğunu ve bir örneğin güvenliğinin ihlal edilmesinin güvenlik grubu yapılandırmasına erişim sağladığını ve bu nedenle ek güvenlik katmanlarının gerekli olduğu göz önüne alınmalıdır.
- Sanal özel ağlara erişimi kontrol etmek için Ağ Erişim Kontrol Listelerini (ACL) kullanılmalıdır. ACL'ler hem izin verme hem de reddetme kuralları sağlar ve güvenlik gruplarından daha güçlü güvenlik kontrolleri sağlar.
- Kötü amaçlı trafiği aktif olarak algılamak ve engellemek için hizmet olarak güvenlik duvarları (FWaaS) ve web uygulaması güvenlik duvarları (WAF) gibi ek güvenlik çözümleri kullanılmalıdır.
- Bulut ağlarını otomatik olarak gözden geçirmek, güvenli olmayan veya savunmasız yapılandırmaları tespit etmek ve bunları düzeltmek için Bulut Güvenliği Durum Yönetimi (CSPM) araçları devreye alınmalıdır.

6.7 Kubernetes

Kubernetes kümesinin dağıtılmış, dinamik yapısı nedeniyle Kubernetes güvenliği, kapsayıcı yaşam döngüsü boyunca önemlidir. Bir uygulama yaşam döngüsünün üç aşamasının her biri için farklı güvenlik yaklaşımları gereklidir: oluşturma, dağıtma ve çalıştırma zamanı. Bulut üzerinde Kubernetes çalıştırırken, Kubernetes kümesini diğer bulut bilişim katmanlarından ayırmak neredeyse imkansızdır. Bunlar, uygulamanın veya kodun kendisini, kapsayıcı görüntülerini, bilgi işlem örneklerini ve ağ katmanlarını içerir. Her katman bir önceki katmanın üzerine inşa edilmiştir ve derinlemesine savunma için tüm katmanlar korunmalıdır.

Kubernetes güvenliği "4 Cs"(Code, Containers, Clusters, Bulut) olarak bilinen dört açılı yaklaşımı önerir:

- Kod: Containerlardaki kodun kötü amaçlı olmamasını ve güvenli kodlama uygulamalarını kullanmasını sağlar.
- Containerlar: Güvenlik açıkları için kapsayıcı görüntülerini tarar ve en iyi uygulamalara göre güvenli bir şekilde yapılandırıldıklarından emin olmak için containerları işleyiş süresinde korur.
- Kümeler: Kubernetes ana düğümlerini korur ve küme yapılandırmasının en iyi güvenlik uygulamalarıyla uyumlu olmasını sağlar.
- Bulut: Bilgi işlem örnekleri ve sanal özel bulutlar (VPC) dahil olmak üzere temel altyapının güvenliğini sağlamak için bulut sağlayıcı araçlarını kullanır.

Bulutta yerel bir ortamda en iyi güvenlik uygulamaları, endüstri standartları, karşılaştırma ölçütleri ve dahili organizasyon stratejileri ile uyumluluk zorluklarla karşı karşıyadır. Uyumluluğu sürdürmenin yanı sıra, kuruluşlar uyumluluğun kanıtını da sağlamalıdır. Kubernetes ortamının, mevcut uygulama mimarisi için orijinal olarak oluşturulan kontrollere uyması için stratejinin ayarlanması gerekir.

7. Bulut Güvenliği İçin Teknolojiler ve Çözümler

7.1 Bulut Erişimi Güvenlik Aracısı

Bir Bulut Erişimi Güvenlik Aracısı veya CASB, bulut tabanlı yazılım veya kurum içi yazılım veya donanım olarak kullanıcılar ve bulut servis sağlayıcıları arasında bir arabulucu olarak görev yapar. CASB, kimlik doğrulama, yetkilendirme, tek oturum açma, kimlik bilgisi eşleme, cihaz profili oluşturma, şifreleme belirteci ve günlüğe kaydetme gibi birden çok türde güvenlik ilkesi uygulamasını birleştirir. Bir Bulut Erişimi Güvenlik Aracısı'nın

güvenlikteki boşlukları ele alma yeteneği, hizmet olarak yazılım (SaaS), hizmet olarak platform (PaaS) ve hizmet olarak altyapı (IaaS) ortamlarını kapsar. Bir CASB, görünürlük sağlamanın yanı sıra, kuruluşların güvenlik politikalarının erişimini mevcut şirket içi altyapılarından buluta genişletmesine ve buluta özel bağlam için yeni politikalar oluşturmasına da olanak tanır.

CASB'ler, yakın zamanda kurumsal güvenliğin hayati bir parçası haline geldi ve işletmelerin hassas kurumsal verileri korurken bulutu ortamını güvenli bir şekilde kullanmasına olanak sağladı. CASB, yönetilmeyen akıllı telefonlar, IoT cihazları veya kişisel dizüstü bilgisayarlar dahil olmak üzere, ne tür bir cihazın erişmeye çalıştığından bağımsız olarak, birden fazla türde güvenlik politikası uygulamasını birleştirerek ve bunları firmanın bulutta kullandığı her şeye uygulayarak bir politika uygulama merkezi olarak hizmet verir.

7.2 Bulut Şifrelemesi

Data korumanın en iyi yollarından olan biri bulut şifreleme aslında mantık olarak basit, pratikte ise biraz karmaşıktır. Mantık olarak yaptığınız, bilginizi, bulut bilgisayara yüklemeden önce şifrelemek ve böylece şifreli bir şekilde bilgilerinizi yüklemektir. Bunu yaparken amacınız ise, eğer bilgi paylaşımı dinleniyor veya bilgi sızıntısı olsa bile, bilgilerinizi gizli tutmaktır. Bu tekniğin beklendiği gibi çalışması için, servis aldığınız parti size bir şifreleme anahtarı verir ve bu anahtar sayesinde siz servis aldığınız partil ile

konuşabilirsiniz. Şifre çözme işlemi ise her partinin tarafında, bilgiyi okumak gerektiğinde verilen anahtar kullanılarak yapılır.

Şifrelenmiş bilgiler 3 şekilde olabilirler. Data-in-use Data-in-transit veya Data-at-rest. Bunlar sırası ile anlık kullanılmakta olan ve şifrelenmemiş data, Anlık olarak geçişte olan ve şifrelenmiş olan data ve anlık olarak bekleyen ve şifrelenmiş olan datalardır.
Şifreleme 2 method ile olabilir. Symmetric veya Asymmetric. Symmetric'de kullanılan encryption anahtarları aynı iken Asymmetric kullanılan şifreleme anahtarları kişiye özeldir ve 2 anahtar barındırılır. Bu sistemin en büyük avantajları güvenilirliği ve devamlılığıdır. Sızıntı olsa bile doğru bulut şifreleme ile çalınan bilgilerin bir işe yaramayacaktır Dezavantajı ise, bu teknik, biraz zaman alır .

7.3 Bulut Güvenlik Duvarı

Bulut güvenlik duvarları,bir bulut bilgisayara olan, istenmeyen veya güvenilmeyen kaynaktan gelen bilgileri filtrelemek için kullanılan bir tekniktir. Normal bir bilgisayarda olan güvenlik duvarı ile neredeyse aynı işi görür ve kullanan parti tarafından ayarlanabilen bir sistemdir. Bu sistemin İki türü vardır. SaaS ve Next Gen Firewalls (NGF). Saas, geleneksel güvenlik duvarları ile aynı mantıkta çalışır ve tek arkı bir bulut bilgisayardan gelmesidir. Next Gen Firewalls (NGF) ise Bulut bilgisayarlarına özel olarak yapılmış duvarlardır. Bu sistemler çoğunlukla P.a.a.S.(platform servisi) sistemini kullanarak çalışırlar. Bulut güvenlik duvarının kritik olmasının nedeni, bulut bilişim teknolojilerinde, şirketlerin virtüel makine kullanmaktansa , sistemleri direkt bulutta çalıştırma istekleridir. Bu yenilik de bağlantı uçlarının (endpoints) güvenliğinin önemini arttırdı. Hızlı değişkenlik gösteren ve her halükarda korunması gereken bağlantı uçlarını koruma ve regüle etmenin en kolay yolu ise güvenlik duvarıdır. Güvenlik duvarları sayesinde istenmeyen yerlerden gelen bağlantılar filtrelenebilir ve krizler daha oluşmadan engellenebilir.

7.4 Bulut Güvenliği Durum Yönetimi

Bir şirket çoğunlukla bulut bilişim teknolojilerini güvende tutmaya çalışırken birden fazla sistemi aynı anda kullanılır. Bu sistemlerin çoğu, S.a.a.S (servis üzerinden satış) ile çalışır ama bunun dışında farklı poliçeler de olabilir. Bu sistemlerin hangilerinin ne kadar bilgiye giriş sahibi oldukları, hangi zamanda çalışmaları gerektikleri ve nasıl birbirleri ile iş birliğinde bulunacaklarını belirleyen poliçe sistemine, bulut güvenlik durum yönetimi denir. Hangi tarafın hangi bilgiyi koruma sorumluluğu olduğunu da belirleyen poliçeler bütünlüğünde birkaç önemli noktaya dikkat edilmelidir. Bunlardan birkaçı, sorumlulukların partiler arasında açıkça belirtilmiş olması, partiler arası komünikasyon ve parçaların açıklığıdır. Sorumlulukları belirleyerek, iki parti de ne yapması gerektiğini bilir.Bu sadece bulut bilişiminde çalışan insanların içinden çıkamayacağı, kullanan insanlardan dolayı oluşan problemlerin büyük bir bölümünü çözer. Partiler birbiri ile iyi bir komünikasyon içinde olursa, arkada, çalışanların gözünün önünde olan ama farkında olmadıkları sıkıntılar göz önüne çıkarılabilir. Parça açıklığının olduğundan emin olarak, normalde komünikasyon ile

bulunmayacak olan hatalar, bulut personeli tarafından bulunabilir ve böylece krizler daha oluşmadan çözülebilir.

7.5 Container Güvenliği

Konteyner güvenliği, kod ve yazılım bağımlılıklarını tutan standart yazılım birimi olan ‘konteyner' bütünlüğünü korumak ve sağlamak için güvenlik araçlarının ve ilkelerinin kullanılmasını içerir. Konteyner güvenliği, altyapının korunması, yazılım tedarik zinciri, çalışma zamanı ve bunların arasındaki her şey dahil olmak üzere, konteynerdeki her şeyin amaçlandığı gibi çalıştığından emin olmak için güvenlik araçlarını ve ilkelerini uygulama sürecidir. Konteyner güvenliği, konteyneri, uygulamasını ve performansını, ayrıca konteynerin altyapısını, yazılım tedarik zincirini ve sistem araçlarını ve kitaplıklarını korur. Konteyner güvenliği, güvenlik uygulamalarının özelliklerinin yapılandırılması ve tasarımı yoluyla ölçeklenebilir. Konteynerlerin emniyete alınması süreci süreklidir. Geliştirme sürecine entegre edilmeli, manuel temas noktalarının sayısını ortadan kaldıracak şekilde otomatikleştirilmeli ve temel altyapının bakım ve işletimine kadar genişletilmelidir. Bu, derleme işlem hattı kapsayıcı görüntülerinizi ve çalışma zamanı ana bilgisayarı, platformu ve uygulama katmanlarını korumak anlamına gelir. Sürekli teslimat yaşam döngüsünün bir parçası olarak güvenliği uygulamak, iş sürecinin riskini hafifleteceği ve sürekli büyüyen bir saldırı yüzeyinde güvenlik açıklarını azaltacağı anlamına gelir.
Konteyner güvenliği hakkında önemli hususlar şu şekilde sıralanabilir:

- Konteyner ana bilgisayarının güvenliği
- Konteyner ağı trafiği
- Uygulamanın konteyner içindeki güvenliği
- Uygulama içindeki kötü niyetli davranışlar
- Konteyner yönetimi yığınının güvenliğini sağlama
- Uygulamanızın temel katmanları
- Yapı hattının bütünlüğü

7.6 CI/CD (Sürekli Entegrasyon Sürekli Teslimat)

CI/CD araçları ve yazılım iskeletleri, güvenlik açıklarını, hataları ve kusurları belirlemek ve bunlardan korunmak için uygulama yaşam döngüsü boyunca otomasyon ve izleme sağlar. Sürekli Entegrasyon/Sürekli Teslimat (CI/CD) işlem hattı, yazılım teslim süreçlerini otomatikleştirir. Kod oluşturur, testler yapar ve uygulamanın yepyeni bir sürümünü güvenli bir şekilde dağıtır. Uygulamada, CI/CD ardışık düzenleri, uygulama tesliminin birçok yönünü otomatikleştirmeyi mümkün kılan bir kod, süreç (örneğin, iş akışlarını oluşturma ve test etme) ve araçların bir karışımıdır. Geleneksel olarak, CI/CD ardışık düzen araçları ve süreçleri

Kaynak → İnşa → Test → Teslim

akışlarını dağıtmaya odaklanır.
CI/CD güvenliği, yazılım işlem hattından akan her şeyi güvenlik öğeleriyle güçlendirmek anlamına gelir. Fakat bazı durumlarda işlem hattının kendisi bir hedef olabilir.

CI/CD güvenliği için aşağıdaki koruyucu adımlar dikkate alınmalıdır:

- Tehditleri ve güvenli bağlantıları saptama
- Erişim kontrolünü sıkılaştırma
- Görevleri ayırma ve izinleri uygulama
- Gizli bilgileri güvende tutma
- Kod kaynağını kilit altında tutma
- Titiz gözetim ve temizleme
- Bilinçli olma ve plan doğrultusunda hareket etme

7.7 Kimlik ve Erişim Yönetimi

Kimlik ve erişim yönetimi, her sistemde kritik bir yer tuttuğu doğrudur, fakat bulut bilişim teknolojilerinde, doğru veya yanlış yapılan bir kimlik ve erişim yönetimi, bir sistemin doğru çalışması veya kaotik çalışması arasındaki basit ama önemli bir farktır.Kimlik ve diğer adı ile Authentikasyon sistemi, bir parçanın, başka bir parça tarafından doğrulanmasına verilir.Bu mantığı kullanarak, programlar, insanların kendilerini tanıttıkları kişi olup olmadığından emin olabilirler.Bu işlem çoğunlukla programlar veya program ve fiziksel insanlar tarafından yapılır. Çoklu bağlantılı sistemlerde popüler olarak kullanılan sistemlerden birkaçı, Çoklu Authentikasyon, 3D şifre uygulamaları,biyometrik doğrulama ve basit yazılabilir şifrelemedir. Şu an çoğu bulut bilişim teknolojisi, identifikasyon doğrulama sistemini kullanarak çalışır.

Fiziksel doğrulama mekanikleri, yüz doğrulamaları, göz doğrulamalar, parmak izi doğrulamaları gibi hızlı ama fiziksel bedene bağlı olan veya identifikasyon kartı gibi kişiye özel parçalar ile yapılabilir. Bulut bilişiminin istek üzerine ani hizmet sisteminden dolayı kullanan insan için kolaylık sağlayamasa da, fiziksel doğrulama çoğu sistem tarafından güvenilirliği ve kesinliğinden ötürü diğer sistemlerle beraber kullanılmaktadır.

Kimlik bilgileri ve SSH, bir başka popüler identifikasyon tekniğidir. Tek seferli şifreler ve captcha gibi sistemler ile kullanıcıların doğruluğu tamamlanması, uzun süreden beri kullanılan bir sistemdir.Bu sistemlerin popülerliğinin nedeni ekleme kolaylığı ve gerektiğinde çıkarabilmenin basitliğidir. SSH ise bağlanan kişinin kullandığı SSH bağlantı nın doğruluğunu sorgulayarak kişinin doğruluğunun test edildiği bir metoddur. Bu metodun güçlü tarafı, kişinin bir giriş yapmasına gereksinimi olmamasıdır. Böylece, bağlantı izlense de identifikasyon naamına geçecek bilgi bulunamaz.

Multifaktör kimlik tanımı, tek seferlik şifre ve benzeri bol değişkenlik gösteren bir şifre ve yanında başka bir kimlik gösterme sisteminin harmanlanmış versiyonundan oluşur. Basitliğinden ve yüksek güvenlik standardından dolayı çoğu sistem tarafından bu kimlik yenileme mantığı kullanılır. Buna örnek olarak , para çekerken kullandığınız tek seferlik şifre ve normal şifreniz örnek verilebilir.

SSO ve federasyon sistemi de kullanılabilecek bir sistemdir. S.a.a.S kullanan sistemlere ulaşım için daha kullanılabilirliği fazla olan bu sistem, merkezleşmeci ve bilgi alışverişini izleyici bir mantık güder. Çoğunlukla şirketler, sistemlerini emin ellerde tutmak için birkaç farklı sistemi aynı anda kullanılır ve bu da uzun şifre ve tanınma prosedürleri oluşturup kullanıcıya zorluk çıkartır.Bunun karşısına çıkmak için, Single Sign On (SSO) tekniği vardır. SSO, her kullanıcı için bir şifre verir, ve diğer şifreleri kendi elinde tutar ve çoğu identifikasyonu kendisi yapar. Bunun doğruluğunu sağlamak için de iki tane alt başlık olarak Enterprise SSO ve OpenID gibi bilinen iki sistemden bahsedeceğim.

Enterprise SSO, bir bağlantı kurulduğunda, bu bağlantının özel şifrelenmiş çerezini oluşturur. Bu çerez kullanıcı bir Bulut aplikasyonundan diğerine geçerken, her istek yaptığında yeniden ve yeniden doğrulanır.Eğer çerez doğru ise, kullanıcıya izin verilir, eğer değilse, kullanıcı yeniden kimlik doğrulama ekranına gönderilir.Doğrulandığında, yeni bir çerez oluşturulur ve kullanıcı devam eder.

OpenID ise kimlik doğrulama için 3. parti aplikasyonlarını kullanır. Bu relying Party (RP) denilen taraflar çoğunlukla identifikasyon isteyen taraftır. SSO ile çok benzer çalışan bu sistem, identifikasyon elimizde olmadığı için sistemlere daha az zorunluluk çıkarması dışında daha az merkeziyetçi bir sistem olarak gereken yükü azaltır.

7.8 Kod Olarak Altyapı (IaC)

Kod olarak altyapı, ağlar, veri merkezleri, sanal makineler, yük dengeleyiciler ve bağlantı topolojisi dahil olmak üzere BT altyapısının yönetimini ve sağlanmasını otomatikleştiren açıklayıcı bir kodlama dilidir. IaC, DevOps'ta kritiktir çünkü tutarlı kaynak kodu kullanarak altyapının hızlı bir şekilde oluşturulmasını ve versiyonlanmasını sağlar. Kod Olarak Altyapı (IaC), mühendislerin DevOps süreçlerinden yararlanırken bulut altyapısını sürüm kontrolüne, devreye almasına ve geliştirmesine olanak tanır. Bu aynı zamanda, bulut altyapısının duruşunu proaktif olarak iyileştirme ve güvenlik ve operasyon ekipleri üzerindeki yükü azaltma fırsatı sunar.

7.9 Kod Olarak Politika (PaC)

Kod Olarak Politika (Policy as Code), politikaları yönetmek ve otomatikleştirmek için üst düzey bir dil olarak kod yazma planıdır. Kod Olarak Altyapı (IaC) kavramına benzer şekilde, Kod Olarak Politika (PaC), politikaların kodlanması kavramına dayanır. Tıpkı Kod Olarak Altyapı gibi, Kod Olarak Politika da IaC konseptini politikalara göre doğrulayarak altyapı otomasyonunu bir adım daha ileri götürür. Politikayı geçen ortamlar inşa edilmeye devam ederken, bu aşamada başarısız olanlar durdurulur. Bu, uyumlu olmayan ortamların bir ekosisteme dönüşmesini önlemenin iyi bir yoludur.

Üst düzey dil tarafından oluşturulan politikaları uygulamak için öncelikle politikayı, sorguyu ve istenen verileri girdi olarak alacak ve eklenen/yayımlanan politikaya göre sorgu sonucunu verecek bir politika motoruna sahip olmanız gerekir. Kod Olarak Politika, kuruluş genelinde veya belirli kümeler içinde belirli kuralları uygulayarak kuruluşun içinde bir standardın korunmasına yardımcı olur. Kodlanmış ilkelere sahip olmak, yönetilen kümede veya ortamda yanlış kurulum ve yapılandırmayı önleyen kuralları uygulayarak görevlerdeki otomasyonu ve verimliliği artırır. Uygulanmak istenen politikalar, uyulması gereken yönergeleri veya üzerinde anlaşmaya varılan sözleşmeleri ve en iyi uygulamaları içerebilir.

7.10 Güvenli Web Geçidi

Güvenli Web Geçidi, şirket içi veya bulut tarafından sağlanan bir ağ güvenlik hizmetidir. Güvenli Web Geçidi çözümleri, internet erişim politikalarını uygulamak için web filtrelemesi uygular. Ayrıca, istenmeyen ve kötü amaçlı yazılımların kullanıcı tarafından indirilmesine karşı da koruma sağlarlar. Güvenli Web Geçidi, şirket politikasını uygulayarak ve İnternet'e bağlı trafiği filtreleyerek bir kuruluşu çevrimiçi güvenlik tehditlerinden ve istilalardan korur. Kullanıcılar ve İnternet arasında yer alan güvenli web ağ geçitleri, kötü amaçlı uygulamaların ve web sitelerinin engellendiğinden ve erişilemez olduğundan emin olmak için web isteklerini şirket politikasına göre inceleyerek gelişmiş ağ koruması sağlar. Güvenli Web Geçidi çözümleri, URL filtreleme, HTTPS/SSL denetimi, veri kaybı önleme, antivirüs, uzak tarayıcı izolasyon kabiliyetleri ve uygulama kontrolünü içerir.

8. Bulut Ağ Güvenliği

8.1 Bulut Ağ Güvenliği Bileşenleri

Bulut ağ güvenliği çözümleri, uygulamaları ve ağları güçlendirmeye yarayan hizmetler sunmaktadır. Güvenlik duvarları ve grupları, birden çok bulut ağındaki trafiği yönetmeye olanak tanıyarak DDoS saldırılarını ve veri hırsızlığını önlemeye yardımcı olur. Şifreleme anahtarı yöneticileri ise veri şifreleme anahtarlarını tek bir güvenli bulut tabanlı yönetim

çözümünde oluşturmaya ve saklamaya olanak sağlar. Yazılım Tanımlı Ağlar (SDN'ler), bulut ağ güvenliği mimarilerinin merkezi bileşenini temsil eder. Trafik yönlendirme kararlarını veren mantıksal ağ katmanı olarak da bilinen kontrol düzlemini, ağ trafiğini yönlendiriciler aracılığıyla ileten mekanizma olan temel veri düzleminden ayırmaktadırlar.

SDN'ler, ağ trafiği programlanabilirliği ve politika yönetimi ile kontrol sağlarken, genel bulut sağlayıcılarının ağ donanımı kaynaklarından yararlanır. Şifrelenmiş tünellerle bağlanan SDN'ler, sanallaştırılmış ağlar arasında gelişmiş işlevsellik sağlayan ağ hizmetleri kümelerini oluşturur. Bir SDN üzerinden hareket eden trafik, uygulama veya hizmet türüne göre sınıflandırılabilir ve ardından ağ trafiğini optimize eden merkezi olarak yönetilen politikalara göre önceliklendirilebilir. SDN çözümleri, BT yöneticilerinin ağ altyapılarını ve güvenlik kontrollerini entegre etmelerine olanak sağlar. İnternet trafiği önceliklendirmesi, DNS filtrelemesi, güvenlik duvarı oluşturulması ve tehlike yönetimi bir web portalı üzerinden sağlanabilir.

8.2 Yazılım Tanımlı Ağ (SDN) Teknolojisinin SD-WAN Uygulaması

SD-WAN, bir tür yazılım tanımlı geniş alan ağı olarak da bilinir. Yerel ve küresel siteler arasında dağıtılan, kolayca yapılandırılabilir ve ölçeklenebilir bir geniş alan ağı oluşturmak için ağ veri merkezinden veya şube ofis donanımından soyutlanacak şekilde sanallaştırılmıştır. SDN teknolojisinin SD-WAN uygulaması, kurumsal ağları çekirdek SDN'nin ötesinde oluşturmak ve genişletmek için yazılım tabanlı bir yaklaşım kullandığından, VPN tabanlı WAN çözümlerinden daha güvenilir, ölçeklenebilir ve uygun maliyetli hale getirir. Şube ofislerini kurumsal ağlara bağlamak için geleneksel ve pahalı çok protokollü etiket değiştirme (MPLS) bağlantıları, güvenlik duvarları veya özel donanım kullanmak yerine SD-WAN çözümleri kullanılabilir. Şifreli tünellerle bağlanan SD-WAN sanal cihazları, sanallaştırılmış ağ genelinde gelişmiş işlevsellik sağlayan ağ hizmetlerine bağlanır. Bir SD-WAN cihazına ulaşan trafik, ağ trafiğini optimize etmek için merkezi olarak yönetilen politikalar kullanılarak uygulama veya hizmet türüne göre sınıflandırılabilir.

SD-WAN'lar , internet trafiği önceliklendirmesi ile ağda hareket ederken kritik verileri tanımlayabilir ve ağ performansını ve verimliliğini artırabilir. İçerik filtreleme ile erişimi kısıtlayabilir veya seçilen sitelere bant genişliği tahsis edebilir. Fiziksel ekipmanı ortadan kaldırdıkları için, normalde ağ donanımı dağıtımlarıyla ilişkili yönetim süresinden ve işçilik maliyetlerinden tasarruf edilebilir. Daha pahalı olan MPLS'yi bulut tabanlı geniş bant bağlantı seçenekleriyle değiştirmek maliyetleri daha da düşürür.

8.3 Ağ Sanallaştırmada Güvenlik Avantajları

Sanal ağda güvenlik, kaynakların tam izolasyonunu, segmentasyonu, dağıtım güvenlik duvarını, ACL'leri ve güvenlik gruplarını sağlamalıdır.

Sanal Ağ İzolasyonu

ACL'lerin veya fiziksel cihazlarda güvenlik duvarı kurallarının manuel olarak yapılandırılması yoluyla geleneksel ortamlarda izolasyon sağlanmıştır. Sanal dünyada ağ fiziksel ve diğer sanal ağlardan izole edilmiştir. Sanal ağ yalıtımı, genellikle aynı veya farklı hipervizörlerde bulunan veri merkezi içinde dağılmış farklı iş yüklerinden elde edilir. Farklı hipervizörler arasındaki iletişim kapsüllenir, böylece veri merkezindeki fiziksel cihazlar sanal ağdaki iş yüklerinden farklı bir adres alanında çalışır. Sanal ağ içindeki uygulama iş yükü tarafından bir saldırı başlatılırsa, bulutun fiziksel altyapısı bu izolasyon ile tamamen korunur.

Sanal Ağ Segmentasyonu

Geleneksel veri merkezlerinde ağ segmentasyonu, bir ağ sınırında oturan ve segmentler arasındaki trafiğe izin veren veya trafiği reddeden fiziksel bir yönlendirici veya güvenlik duvarı tarafından gerçekleştirilir. Segmentasyon, daha küçük VM gruplarına güvenlik kontrolleri ekler. Bir sanal ağda, ACL ve güvenlik duvarı hizmetleri genellikle bir uygulama iş yüküyle sağlanır. Fiziksel bir güvenlik duvarında yapılandırılması ve sürdürülmesi için ağ segmentasyonuna gerek yoktur çünkü sanal ortamdaki iletişim ağ içinde kalır.

Dağıtılmış Güvenlik Duvarı

Dağıtılmış bir güvenlik duvarı, tüm VM'lere doğrudan bağlı olması ve güvenliğinin ilk ve son atlamada her yerde mevcut olması bakımından tipik fiziksel ve sanal güvenlik duvarı modelinden farklıdır. Dağıtılmış güvenlik duvarının büyük bir yararı, güvenlik kurallarının IP adreslemeden ayrılmasıdır.

Güvenlik Duvarları ve Ağ ACL’leri

Güvenlik grupları, sanal özel buluttan hem gelen hem de giden trafiği kontrol etmek için bir güvenlik duvarı gibi davranabilir. Güvenlik grupları, anlık olarak çalışır, bu nedenle ilk savunma katmanıdır. Öte yandan, ağ ACL'leri, gelen ve giden trafiği kontrol ederken ilişkili subnetler için bir güvenlik duvarı görevi görür. ACL'ler subnet düzeyinde çalışırak ikinci bir savunma katmanı oluştururlar.

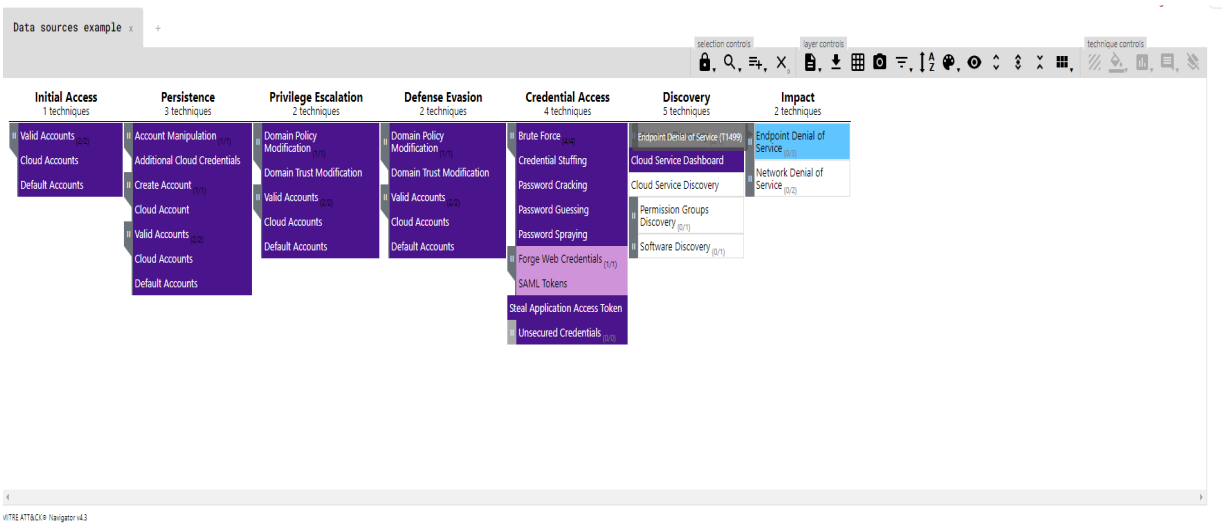
8.4 Verilerin Korunması

Şirket içi ağlarda BT ve güvenlik ekiplerinin ağı genişletmesi yavaş ve zahmetlidir. Tüm yeni altyapının denetlenmesi ve yapılandırılması zorlu olsa da bulut ağları ile kıyaslandığında daha güvenlidir. Bulut ağları ile şirket elemanlarının doğrudan katılımı olmadan, doğru yetkilendirmeye sahip herhangi bir sistem tarafından yeni altyapı eklenebilir. Bu şekilde ağı genişletmek daha kolay olacaktır ama beklenmedik güvenlik zayiatlarına sebep olabilir. Bulut ortamlarındaki teknolojinin sürekli olarak değişmesi güvenliği sağlamayı zorlaştırmaktadır. Otomatik ölçeklendirme ve sunucusuz bilgi işlem gibi teknolojiler ile bulut ağındaki varlıklar sürekli olarak görünüp kaybolur. Sadece birkaç dakikalığına var olan bir güvenlik tehdidine karşı ağı savunmak için güvenlik açığı taraması gibi yöntemler yeterli olmayacaktır. Haftalık veya günlük güvenlik taramalarında tespit edilemeyen bir güvenlik açığı, sadece birkaç dakika içerisinde sisteme büyük zararlar verebilir. Hibrit veya çoklu bulut ortamında görünürlüğü güvenceye almaya ve sürdürmeye çalışan kuruluşlar, BT ayak izinin tüm parçalarını güvence altına almaktan tek bir ekibin sorumlu olduğundan emin olmalıdır. Bir ekibin şirket içi güvenlikten, diğerinin bulut güvenliğinden sorumlu olması genellikle kör noktalara ve ağlar arasında hareket eden kötü niyetli bir aktörün izlenmesinde zorluklara yol açar. Birçok eski güvenlik çözümünün, bulut ağlarını desteklemek için optimize edilmemiş olması, ekiplerin şirket içi ve bulut ortamlarını güvence altına almak için farklı araçlar kullanmasına neden olabilir. Bundan dolayı tüm BT ayak izi için güvenliği tek bir yerde yöneten araçlar aranması daha sağlıklı olabilir. Dikkate alınması gereken bazı bulut ağ güvenliği ilkeleri şöyledir:

- Güvenlik duvarı katmanları kullanılarak birden fazla bölge arasındaki izolasyon garanti edilmelidir.
- Uçtan uca aktarım için şifreleme kullanılmalıdır.
- Sanal özel bulut dağıtılırken IPSEC, SSH, SSL gibi standart güvenli kapsülleme protokolleri kullanılmalıdır.

9.Yapı Kredi Cloud Coverage

Yapı Kredi'nin bulut sistemleri üzerinde yapılan saldırıları ne kadar kapsadığını bulmak amaçlanmıştır. Bunun için öncelikle QRADAR üzerinden Azure AD'deki veri kaynaklarından gelen loglar incelenmiş; bu veri kaynakları, kendilerine karşılık gelen MITRE ATTACK veri kaynakları ile DeTTECT yardımıyla eşleştirilmiş ve daha sonrasında MITRE ATTACK Navigator ile Yapı Kredi'nin Azure AD'ye yapılan saldırıları ne kadar kapsadığını gösteren aşağıdaki harita çıkarılmıştır.



Kaynakça:

https://dergipark.org.tr/tr/download/article-file/751027
https://www.theamegroup.com/cloud-computing-advantages-disadvantages/
https://resources.infosecinstitute.com/topic/5-key-cloud-security-use-cases/
https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/1202/17032015093613-3.pdf
https://ab.org.tr/ab16/bildiri/131.pdf
https://openaccess.maltepe.edu.tr/xmlui/bitstream/handle/20.500.12415/3403/171110125-B%C3%9CNYAM%C4%B0NARSLAN-BULUT_B%C4%B0L%C4%B0%C5%9E%C4%B0M%E2%80%99%C4%B0N_AVANTAJLARI_VE_DEZAVANTAJLARI.pdf?sequence=1&isAllowed=y
https://www.copado.com/devops-hub/blog/cloud-security-advantages-and-disadvantages-to-accessibility
https://www.geeksforgeeks.org/advantages-and-disadvantages-of-cloud-security/
https://pentestmag.com/advantages-and-disadvantages-of-cloud-security-main-benefits-current-risks-and-the-way-to-avoid-them/
https://www.youtube.com/watch?v=kd33UVZhnAA
https://blog.rsisecurity.com/what-is-cloud-encryption/
https://identitymanagementinstitute.org/cloud-security-and-access-management-concepts/
https://www.sciencedirect.com/science/article/pii/S2215098617316750#:~:text=Presently%2C%20Identity%20and%20Access%20Management,provisioning%20of%20storage%20and%20verification.
https://www.aquasec.com/cloud-native-academy/cspm/cloud-infrastructure-security/
https://www.guidepointsecurity.com/education-center/cloud-security-architecture/
https://www.guidepointsecurity.com/education-center/cloud-security/
https://www.rapid7.com/fundamentals/cloud-network-security/
https://www.stratoscale.com/blog/networking/security-cloud-networking-fw-acls/
https://www.perimeter81.com/glossary/cloud-network-security
https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks

https://www.imperva.com/learn/ddos/ddos-attacks/
Azure Active Directory security operations guide | Microsoft Docs
https://www.kaspersky.com/resource-center/definitions/what-is-cloud-security
SANS 2021 Cloud Security Survey | SANS Institute
How to Build a Security Visibility Strategy in the Cloud | SANS Institute
Cloud Visibility: 3 Critical Challenges and Solutions (netapp.com)
4 Steps to Adopting Security Automation for Efficient Security Teams (reliaquest.com)
What is Cloud Security? How to Secure the Cloud | McAfee