BULUT BİLİŞİM (CEH 312.50 v12)

Bulut bilişim; çevrimiçi iş uygulamaları, çevrimiçi veri depolama ve web postası gibi bilişim hizmetlerini internet üzerinden sunan yeni bir teknolojidir. Bulut uygulaması; dağıtılmış iş gücü sağlayarak kuruluş giderlerini azaltıp veri güvenliği sağlamaktadır. Avantajlar nedeniyle, günümüzde birçok işletme kuruluşu verilerini ve altyapısını buluta taşımaktadır. Fakat bulut ortamı kuruluşlar için birçok tehdit ve risk de oluşturmaktadır. Saldırganlar, bulut yazılımındaki güvenlik açıklarını hedef alarak, içinde depolanan değerli verilere yetkisiz erişim elde etmektedir. Bulut güvenliği hem bireyler hem de işletmeler için önemli bir rol oynamaktadır.

Bulut bilişim, internet üzerinden çeşitli hizmet ve uygulama türleri bizlere sunmaktadır. Bu hizmetler; kullanıcıların uzak konumlarda üçüncü taraflarca yönetilen yazılım ve donanımları kullanmasını sağlar. Başlıca bulut hizmeti sağlayıcıları arasında Google, Amazon ve Microsoft bulunur.

Bulut bilişim, BT altyapısı ve uygulamalarının abonelere ağlar üzerinden ölçülü hizmetler olarak sağlandığı, BT yeteneklerinin talep üzerine sunulması da diyebiliriz. Bulut çözümlerine örnek olarak Gmail, Facebook verilebilir.

Bulut Bilişimin Özellikleri; Birçok işletmenin bulut teknolojisini benimsemesini sağlayan bulut bilişimin özellikleri şunlardır

İsteğe bağlı self servis: Bulut hizmeti sağlayıcıları tarafından sunulan ve bulut kaynakları için bilgi işlem gücü, depolama ve ağ gibi, her zaman talep üzerine, hizmet sağlayıcılarla insan etkileşimine gerek kalmadan hükümler sağlayan hizmet türüdür.

Dağıtılmış depolama: Buluttaki dağıtılmış depolama, verilerin daha iyi ölçeklenebilirliğini, kullanılabilirliğini ve güvenilirliğini sunmaktadır. Bunun yanında bulut dağıtılmış depolama potansiyel olarak güvenlik ve uyumluluk endişelerini artırabilir.

Hızlı esneklik: Bulut, talebe göre hızla yukarı veya aşağı ölçeklendirmek için anında yetenekler sağlama olanağı sunar. Tüketicilere göre, sağlama için mevcut kaynaklar sınırsız gibi görünür ve herhangi bir zamanda satın alınabilir.

Otomatik yönetim: Kullanıcı katılımını en aza indirerek, bulut otomasyonu süreci hızlandırarak işçilik maliyetlerini ve insan hatası olasılığını azaltmaktadır.

Geniş ağ erişimi: Bulut kaynakları ağ üzerinden kullanılabilir ve dizüstü bilgisayarlar, cep telefonları ve kişisel dijital asistanlar dahil olmak üzere çok çeşitli platformlar aracılığıyla standart prosedürler aracılığıyla erişilir.

Kaynak havuzu: Bulut hizmeti sağlayıcısı, çok kiracılı ortamda birden fazla müşteriye hizmet vermek için tüm kaynakları bir araya getirir; fiziksel ve sanal kaynaklar, bulut tüketicisi tarafından talep üzerine dinamik olarak atanır ve yeniden atanır.

Ölçülen hizmet: Bulut sistemleri "kullanıma göre ödeme" ölçüm yöntemini kullanmaktadır. Aboneler bulut hizmetleri için aylık abonelikle veya depolama seviyeleri, işlem gücü, bant genişliği gibi kaynakların kullanımına göre ödeme yapar. Bulut hizmet sağlayıcıları, müşterilerin kaynak tüketimini tam şeffaflıkla izleyerek kontrol eder, raporlar ve ücretlendirir.

Sanallaştırma teknolojisi: Buluttaki sanallaştırma teknolojisi, sanallaştırılmamış ortamların başaramayacağı bir şekilde kaynakların hızlı şekilde ölçeklenmesini sağlar.

Bulut Bilişimin Sınırlamaları ; Kuruluşların sınırlı kontrolü ve esnekliği. Kesintilere ve diğer teknik sorunlara yatkınlık. Güvenlik, gizlilik ve uyumluluk sorunları. Sözleşmeler ve kilitlenmeler. Ağ bağlantılarına bağımlılık. Her bileşen çevrimiçi olduğundan saldırılara karşı potansiyel güvenlik açığı. Bir hizmet sağlayıcıdan diğerine geçişte zorluk.

Bulut Bilişim Hizmetleri Türleri ;

Altyapı Hizmeti Olarak (IaaS) ; Abonelerin bilgi işlem gücü, sanallaştırma, veri depolama ve ağ gibi temel BT kaynaklarını talep üzerine kullanmasını sağlar. Bu hizmet, bir hizmet uygulama programlama arayüzü (API) aracılığıyla kontrol edilebilen sanal makineler ve diğer soyut donanım ve işletim sistemleri sağlar. Bulut hizmeti sağlayıcıları; temel bulut bilişim altyapısını yönetmekten sorumlu olduğundan, aboneler insan sermayesi, donanım ve diğer maliyetlerden kaçınabilir.

Avantajlar; Dinamik altyapı ölçekleme. Garantili çalışma süresi. Yönetimsel görevlerin otomasyonu. Elastik yük dengeleme (ELB). Politika tabanlı hizmetler. Küresel erişilebilirlik.

Dezavantajlar; Yazılım güvenliği yüksek risk altındadır. Performans sorunları ve yavaş bağlantı hızları.

Platform-as-a-Service (PaaS) ; Uygulamaların ve hizmetlerin geliştirilmesine olanak tanır. Abonelerin altındaki yazılımı ve altyapıyı satın alması ve yönetmesi gerekmez fakat dağıtılan uygulamalar ve uygulama barındırma ortamı yapılandırmaları üzerinde yetkiye sahiptir. Abonelerin özel uygulamalar geliştirmek için kullanabileceği isteğe bağlı geliştirme araçları, yapılandırma yönetimi ve dağıtım platformları sunmaktadır. PaaS ortamında uygulama yazmanın avantajları arasında dinamik ölçeklenebilirlik, otomatik yedeklemeler ve bunlar için açıkça kodlamaya gerek kalmadan diğer platform hizmetleri bulunur.

Avantajlar: Basitleştirilmiş dağıtım. Önceden oluşturulmuş iş işlevselliği. laaS'a kıyasla daha düşük güvenlik riski. Anında topluluk. Kullanım başına ödeme modeli. Ölçeklenebilirlik.

Dezavantajlar: Tedarikçi bağımlılığı. Veri gizliliği. Sistem uygulamalarının geri kalanıyla entegrasyon.

Yazılım Hizmeti Olarak (SaaS) ; Abonelere internet üzerinden talep üzerine uygulama yazılımı sunar. Sağlayıcı, hizmet için kullanım başına ödeme, abonelik, reklam veya birden fazla kullanıcı arasında paylaşım temelinde ücret alır.

Avantajlar: Düşük maliyet. Kolay yönetim. Küresel erişilebilirlik. Yüksek uyumluluk.

Dezavantajlar: Güvenlik ve gecikme sorunları. İnternete tam bağımlılık. SaaS satıcıları arasında geçiş yapmak zordur.

Kimlik Hizmeti Olarak (IDaaS) ; Abone olunan işletmelere kimlik doğrulama hizmetleri sunarak kimlik ve erişim yönetimi hizmetleri sağlamak için üçüncü taraf bir satıcı tarafından yönetilir. Tek Oturum Açma (SSO), Çok Faktörlü Kimlik Doğrulama (MFA), Kimlik Yönetimi ve Yönetimi (IGA), erişim yönetimi ve istihbarat toplama gibi hizmetler sağlar. Bu hizmetler, abonelerin hassas verilere hem şirket içinde hem de şirket dışında daha güvenli şekilde erişmesini sağlar. OneLogin, Centrify Kimlik Hizmeti, Microsoft Azure Active Directory, Okta örnek verilebilir.

Avantajlar: Düşük maliyet. Gelişmiş güvenlik. Uyumluluğu basitleştirme. Azaltılmış zaman. Kullanıcı hesaplarının merkezi yönetimi.

Dezavantajlar: Tek sunucu arızası hizmeti kesintiye uğratabilir veya diğer kimlik doğrulama sunucularında yedeklilik oluşturabilir. Hesap ele geçirme saldırılarına karşı savunmasızdır.

Güvenlik Hizmeti Olarak (SECaaS) ; Güvenlik hizmetlerini kurumsal altyapıya uygun maliyetli şekilde entegre etmektedir. SaaS temel alınarak geliştirilmiştir ve fiziksel donanım veyahut ekipman gerektirmez. Bu nedenle de kuruluşların kendi güvenlik yeteneklerini oluşturduklarında harcanan maliyete kıyasla maliyeti önemli ölçüde azaltır. Penetrasyon testi, kimlik doğrulama, izinsiz giriş tespiti, kötü amaçlı yazılımlara karşı koruma, güvenlik olayı ve olay yönetimini içerir. eSentire MDR, Switchfast Technologies, OneNeck IT Solutions, Foundstone Managed Security Services gibi hizmetler sağlar.

Avantajlar: Düşük maliyet. Azaltılmış karmaşıklık. Sürekli koruma. En iyi güvenlik uzmanlığıyla iyileştirilmiş güvenlik. En son ve güncellenmiş güvenlik araçları. Hızlı kullanıcı sağlama. Daha fazla çeviklik. Temel yeterliliklere daha fazla zaman ayrılması.

Dezavantajlar: Artan saldırı yüzeyleri ve güvenlik açıkları. Bilinmeyen risk profili. Güvensiz API'ler. İş ihtiyaçlarına göre özelleştirme yok. Hesap ele geçirme saldırılarına karşı savunmasız.

Konteyner-hizmet-olarak (CaaS) ; Abonelerine hizmet olarak konteynerler ve kümeler sağlamaktadır. Konteyner motorlarının sanallaştırılması, konteynerlerin, uygulamaların ve kümelerin web portalı veya API aracılığıyla yönetimi gibi hizmetler sağlar. Aboneler, bu hizmetleri kullanarak bulut veya yerinde veri merkezleri aracılığıyla zengin ölçeklenebilir konteynerleştirilmiş uygulamalar geliştirebilir. CaaS, hem laaS hem de PaaS'ın özelliklerini devralmaktadır. Amazon EC2, Google Kubernetes Engine (GKE) örnek verilebilir.

Avantajlar: Konteynerleştirilmiş uygulamaların akıcı şekilde geliştirilmesi. Kaynak başına ödeme. Artan kalite. Taşınabilir ve güvenilir uygulama geliştirme. Düşük maliyet. Az kaynak. Uygulama konteynerinin çökmesi diğer konteynerleri etkilemez. Gelişmiş güvenlik. Gelişmiş yama yönetimi. Hatalara gelişmiş yanıt. Yüksek ölçeklenebilirlik. Akıcı geliştirme.

Dezavantajlar: Yüksek operasyonel yük. Platform dağıtımı geliştiricinin sorumluluğundadır.

Hizmet Olarak İşlev (FaaS) ; Gerekli altyapıyı oluşturma ve sürdürme karmaşıklığı olmadan uygulama işlevlerini geliştirmek, çalıştırmak ve yönetmek için platform sağlar (sunucusuz mimari). Bu model çoğunlukla mikro hizmetler için uygulamalar geliştirirken kullanılır. Destekleyici altyapıyı kapatan ve kullanılmadığında hiçbir ücret ödemeyen abonelere talep üzerine işlevsellik sağlar. Bağlı cihazlar, mobil ve web uygulamaları için Nesnelerin İnterneti (IoT) hizmetleri gibi veri işleme hizmetleri sağlar. AWS Lambda, Google Cloud Functions, Microsoft Azure Functions, Oracle Functions örnek verilebilir.

Avantajlar: Kullanım başına ödeme. Düşük maliyet. Verimli güvenlik güncellemeleri. Kolay dağıtım. Yüksek ölçeklenebilirlik.

Dezavantajlar: Yüksek gecikme. Bellek sınırlamaları. İzleme ve hata ayıklama sınırlamaları. Kararsız araçlar ve çerçeveler.Tedarikçi bağımlılığı.

Hizmet Olarak Her Şey (XaaS) ; Kullanıcının talebine göre internet üzerinden her şeyi hizmet olarak sunan bulut bilişim ve uzaktan erişim hizmetidir. Hizmet, araçlar, uygulamalar ve teknolojiler gibi dijital ürünleri , yiyecek, ulaşım ve tıbbi danışmanlık gibi diğer hizmet türlerini içerebilir. Hizmet, kullanıma göre ödenir ve normal ürünler olarak satın alınamaz veya lisanslanamaz. Hizmet olarak yazılım (SaaS), hizmet olarak platform (PaaS) ve hizmet olarak altyapı (laaS) gibi yaygın bulut hizmetlerinin yanı sıra, XaaS, hizmet olarak ağ gibi hizmetleri de içerir ; ağ-hizmeti-olarak (NaaS), hizmet olarak depolama (STaaS), hizmet olarak test (TaaS), hizmet olarak kötü amaçlı yazılım (MaaS), hizmet olarak felaket kurtarma (DRaaS). XaaS, müşteri ilişkileri yönetimi (CRM), bulut bilişim ve dizin hizmetleri gibi güvenli hizmetler sunar. NetApp, AWS Elastic Beanstalk, Heroku ve Apache Stratos'u örnek verebiliriz.

Avantajları: Son derece ölçeklenebilir. Konumdan ve cihazlardan bağımsız. Hata toleransı ve azaltılmış yedeklilik. Azaltılmış sermaye harcaması. Hızlı esnekliği ve kaynak paylaşımını destekleyerek iş sürecini iyileştirir.

Dezavantajları: XaaS internete bağlı olduğundan hizmet kesintisi olasılığı. Aynı kaynakların yüksek kullanımı nedeniyle performans sorunları. Bazen son derece karmaşık ve sorun gidermesi zor.

Hizmet Olarak Güvenlik Duvarları (FWaaS) ; Ağ trafiğini filtreleyerek kullanıcıları ve kuruluşları hem iç hem de dış tehditlerden korur. FWaaS; paket filtreleme, ağ analizi ve IPsec gibi güvenlik işlevlerine ek olarak kötü amaçlı yazılım saldırılarını tespit etme yeteneği de dahil olmak üzere gelişmiş veri analizi yeteneklerini içerir.

Avantajlar: Kötü amaçlı web trafiğini engeller. Birden fazla bulut dağıtımını korur. Standartlaştırılmış politika uygulaması. İyileştirilmiş ağ görünürlüğü. Gelişmiş güvenilirlik. Daha basit mimari. Daha kolay bakım.

Dezavantajlar: Kabul edilmeye karşı direnç. Ağ gecikme sorunları.

Masaüstü-hizmet-olarak (DaaS) ; Abonelere talep üzerine sanal masaüstleri ve uygulamalar sunar. Bulut hizmet sağlayıcıları altyapı, bilgi işlem gücü, veri depolama, yedekleme, yama ve bakım sağlamaktan sorumludur. Bulut sağlayıcıları DaaS'yi çoklu kiracı aboneliği olarak sunar. Sağlayıcı, hizmet için öngörülebilir ödeme-ihtiyacınız-oldukça modeliyle ücret alır. Amazon WorkSpaces, Citrix Yönetilen Masaüstleri ve Azure Windows Sanal Masaüstü'nü örnek verebiliriz.

Avantajlar: Küresel erişilebilirlik. Basitleştirilmiş yönetim. Azaltılmış kesinti süresi. Düşük maliyet. Yüksek esneklik. Yüksek ölçeklenebilirlik.

Dezavantajları: Güvenlik sorunları. Ağ bağlantı sorunları. Yüksek lisans maliyetleri.

Mobil Arka Uç Hizmet Olarak (MBaaS) ; Uygulama geliştiricilerinin ön uç uygulamalarını uygulama programlama arayüzü (API) ve yazılım geliştirme kiti (SDK) aracılığıyla arka uç altyapısıyla entegre etmelerine olanak tanır. Bu hizmet; geliştiricilerin arka uç işlevselliğini geliştirmeye harcadıkları zamanı azaltır. Uygulamaları geliştirmek için kullanıcı yönetimi, anında bildirimler, bulut depolama, veritabanı yönetimi ve coğrafi konum sağlar. Google'ın Firebase, AWS Amplify, Kinvey, Apple'ın CloudKit, Backendless Cloud'u örnek verebiliriz.

Avantajları: İyileştirilmiş geliştirme verimliliği. Son derece esnek. Ölçeklenebilirlik. Ödedikçe kullan modeli.

Dezavantajları: Güvenlik sorunları. Yüksek başlangıç maliyetleri.

Makineler Hizmet Olarak (MaaS) İş Modeli ; Ekipman-hizmet-olarak (EaaS) olarak da bilinir ve üreticilerin müşterilere makine satmalarına veya kiralamalarına, bu makinelerin ürettiği kârın bir yüzdesini almalarına olanak tanır. Bu model, hem üreticilerin hem de müşterilerin yararına yaygın olarak kullanılır ve uygulanır. Müşterinin ve üreticinin makineden gerçek zamanlı ürünler üretmesine ve izlemesine olanak tanıyan gelişmiş bulut modelidir.

Avantajları: Düşük yatırım maliyeti. Gelişmiş uyarlanabilirlik. Güvenilir ve uygun maliyetli gelir kaynağı. Gelişmiş ürün kalitesi ve miktarı.

Dezavantajları: Bakım ve onarımlar pahalıdır. Makineler insan işçilerin yerini alır ve işsizliğe neden olur.

Bulutta Sorumlulukların Ayrılması; Bulut bilişimde, abonelerin ve hizmet sağlayıcıların sorumluluklarının ayrılması esastır. Görevlerin ayrılması, çıkar çatışmasını, yasadışı eylemleri, dolandırıcılığı, kötüye kullanımı ve hatayı önleyerek bilgi hırsızlığı, güvenlik ihlalleri, güvenlik kontrollerinden kaçınma gibi güvenlik kontrol hatalarının belirlenmesine yardımcı olur. Bir bireyin sahip olduğu etki miktarını kısıtlamaya yardımcı olarak çakışan sorumlulukların olmamasını sağlar.

Esas olarak üç tür bulut hizmeti vardır; laaS, PaaS ve SaaS. Belirli bulutlara ve modellerine erişirken her bulut hizmeti dağıtım modelinin sınırlamalarını bilmek önemlidir.

Bulut Dağıtım Modelleri ; Bulut dağıtım modeli seçimi kurumsal gereksinimlere dayanmaktadır. Bulut hizmetleri, şu faktörlere göre farklı şekillerde dağıtılabilir: Bulut bilişim hizmetlerinin ana bilgisayar konumu. Güvenlik gereksinimleri. Bulut hizmetlerinin paylaşımı. Bulut hizmetlerinin bir kısmını veya tamamını yönetme yeteneği. Özelleştirme yetenekleri.

Dört standart bulut dağıtım modelleri şöyledir ;

Genel Bulut ; Sağlayıcı, uygulamalar, sunucular, veri depolama gibi hizmetleri internet üzerinden herkese açık hale getirir. Bu sebeple genel bulutun ve BT kaynaklarının oluşturulmasından, sürekli bakımından sorumludur. Genel bulut hizmetleri ücretsiz olabilir veya kullanım başına ödeme modeline dayalı olabilir Amazon Elastic Compute Cloud (EC2), Google App Engine, Windows Azure Services Platform, IBM Bluemix örnek verebiliriz.

Avantajlar: Basitlik ve verimlilik. Düşük maliyet. Azaltılmış zaman (çökerse geri dönme zamanı). Bakım olmaması (genel bulut hizmeti tesis dışında barındırılır). Sözleşmesizdir (uzun vadeli taahhüt yok)

Dezavantajları: Güvenlik garanti edilmez. Kontrol eksikliği (üçüncü taraf sağlayıcılar sorumludur). Yavaş hız (İnternet bağlantılarına dayanır ve veri aktarım hızı sınırlıdır)

Özel Bulut ; Dahili veya kurumsal bulut olarak da bilinen özel bulut, tek bir kuruluş tarafından işletilen ve kurumsal güvenlik duvarı içinde uygulanan bulut altyapısıdır. Kuruluşlar, kurumsal veriler üzerinde tam kontrolü korumak için özel bulut altyapıları dağıtır. BMC Software, VMware vRealize Suite, SAP Cloud Platform'u örnek verebiliriz.

Avantajlar: Güvenlik iyileştirmesi (hizmetler tek bir kuruluşa ayrılmıştır). Kaynaklar üzerinde artan kontrol (kuruluş sorumludur). Yüksek performans (güvenlik duvarı içinde bulut dağıtımı yüksek veri aktarım hızları anlamına gelir). Özelleştirilebilir donanım, ağ ve depolama performansları (kuruluş özel buluta sahip olduğundan). Sarbanes Oxley, PCI DSS ve HIPAA uyumluluk verilerine ulaşmak çok daha kolaydır.

Dezavantajlar: Yüksek maliyet. Yerinde bakım.

Topluluk Bulutu; Güvenlik, düzenleyici uyumluluk, performans gereksinimleri ve yargı yetkisi gibi ortak bilgi işlem endişelerine sahip belirli bir topluluktan kuruluşlar arasında paylaşılan çok kiracılı bir altyapıdır. Topluluk bulutu, şirket içinde veya şirket dışında olabilir, katılan kuruluşlar veya üçüncü taraf yönetilen hizmet sağlayıcısı (Cisco Cloud Solutions ve Salesforce Health Cloud örnek verebiliriz) tarafından yönetilebilir.

Avantajlar: Özel buluta kıyasla daha az maliyetli. Topluluğun ihtiyaçlarını karşılama esnekliği. Yasal düzenlemelere uyum. Yüksek ölçeklenebilirlik. Kuruluşlar, internet üzerinden her yerden bir kaynak havuzunu paylaşabilir.

Dezavantajlar: Kaynak kullanımında tüketiciler arasında rekabet. Gerekli kaynakların yanlış tahmin edilmesi. Sorumluluk durumunda tüzel kişiliğin olmaması. Orta düzeyde güvenlik (diğer kiracılar verilere erişebilir). Kiracılar arasında güven ve güvenlik endişeleri.

Hibrit Bulut; Benzersiz varlıklar olarak kalan fakat birden fazla dağıtım modelinin avantajlarını sunmak için birbirine bağlı iki veya daha fazla buluttan (özel, genel veya topluluk) oluşan bulut ortamıdır. Kuruluş bazı kaynakları şirket içinde kullanıma sunarak yönetir ve diğer kaynakları harici olarak sağlar. Microsoft Azure, Zymr, Parangat Cloud Computing, Logicalis'i örnek verebiliriz.

Avantajlar: Yüksek ölçeklenebilirlik (hem genel hem de özel bulutları içerir). Hem güvenli hem de ölçeklenebilir genel kaynaklar sunar. Yüksek güvenlik seviyesi (özel bulutu içerir). Gereksinimlere göre maliyeti düşürmeye ve yönetmeye olanak tanır.

Dezavantajlar: Hem genel hem de özel bulutları kullandığı için ağ düzeyindeki iletişim çakışabilir. Veri uyumluluğunu sağlamak zordur. Kesintiler durumunda kuruluş dahili BT altyapısına güvenir (üstesinden gelmek için veri merkezleri arasında yedekliliği korumalıyız). Karmaşık hizmet seviyesi anlaşmaları (SLA).

Çoklu Bulut; Uzun vadeli iş hedeflerine ulaşmak için tek tescilli arayüz üzerinden yönetilen birden fazla bulut satıcısı arasında iş yüklerini birleştiren dinamik, heterojen ortamdır. Farklı bulut satıcılarından birden fazla bilgi işlem ve depolama hizmeti kullanır. Bulut varlıklarını, yazılımları, uygulamaları vb. çeşitli bulut barındırma ortamlarına dağıtır. Çoklu bulut ortamları çoğunlukla tamamen özel, tamamen genel veya her ikisinin bir kombinasyonudur. Kuruluşlar, bilgi işlem kaynaklarını dağıtmak için çoklu bulut ortamlarını kullanır. Bilgi işlem gücünü ve depolama kapasitelerini artırarak veri kaybı ve kesinti riskini büyük ölçüde sınırlar. Microsoft Azure Arc, Google Cloud Anthos'u örnek verebiliriz.

Avantajlar: Yüksek güvenilirlik ve düşük gecikme. İş ihtiyaçlarını karşılama esnekliği. Maliyet-performans optimizasyonu ve risk azaltma. Dağıtılmış hizmet reddi (DDoS) saldırıları riskinin düşük olması. Artan depolama kullanılabilirliği ve bilgi işlem gücü. Tedarikçiye bağımlı kalma olasılığının düşük olması.

Dezavantajlar: Çoklu bulut sistemi arızası iş çevikliğini etkiler. Birden fazla sağlayıcı kullanmak yedekliliğe neden olur. Karmaşık ve büyük saldırı yüzeyi nedeniyle güvenlik riskleri. Operasyonel ek yük.

Diğer bulut dağıtım modelleri şunları içerir;

Dağıtılmış Bulut ; Tek bir kontrol düzleminde kontrol edilen coğrafi olarak dağıtılmış genel veya özel bulutlardan oluşan, site içinde veya dışında bulunan son kullanıcılara hizmet sağlamak için merkezi bulut ortamıdır. Son kullanıcı yerel veri merkezi olarak her yerden verilere erişebilir, veri gizliliğini iyileştirmek, yerel yönetim politikalarını karşılamak için uç bilgi işlem yeteneği sağlar. Son kullanıcılara yerel sunucularındaki uzak verilere erişiyormuş gibi hizmet sağlar. Gereksinimlere bağlı olarak, dağıtılmış bulut hizmetleri ağ, operatör ve müşteri kenarları gibi farklı konum türlerinde ve yerel veri merkezleri olarak kullanılabilir. Dağıtılmış bulut, yapay zeka (AI), makine öğrenimi (ML) ve nesnelerin interneti (IoT) (Google Dağıtılmış Bulut ve Cloudflare CDN'i örnek verebiliriz) gibi uygulamaların otomasyonuna hizmet sağlar.

Avantajlar: Yüksek performans. Azaltılmış gecikme. Hibrit ve çoklu buluta kıyasla yüksek yönetim ve operasyonel tutarlılık. Yerinde modernizasyon. Uç bilişim yetenekleri. Yerinde veri işleme yeteneği. Sıkı veri güvenliği. Otomasyon uygulamaları.

Dezavantajlar: Güvenlikle ilgili güvenlik açıkları ortaya çıkabilir. Yüksek maliyet (ağ altyapısı dağıtım maliyeti). Sınırlı yazılım desteği. Karmaşık sorun giderme.

Poly Cloud ; Farklı diğer bulutlara sağlanabilen çeşitli bulut hizmeti türlerini barındırır. Çoklu buluttan farklı olarak da kullanıcılara gereksinimlerine göre farklı bulut hizmetlerinden özellikler sağlamak için tek bir platformda çeşitli bulutların özelliklerini sağlar. Kullanıcıların iş ortamlarında farklı görevleri gerçekleştirmek için her buluttan gereken belirli bir özelliği seçmelerine yardımcı olur. Yapay Zeka ve Makine Öğrenimi hizmetleri (Google Cloud Platform (GCP) ve Amazon Web Hizmetleri (AWS) örnek verebiliriz) gibi özel otomasyon uygulamaları sağlar.

Avantajlar: Yüksek esneklik. Çevresel seçim. Altyapı ve yatırım getirisi (ROI) optimizasyonu. Özel Yapay Zeka ve Makine Öğrenimi hizmetleri sağlar. Maliyet açısından etkili. Yüksek performans.

Dezavantajlar: İlk kurulum için zaman alıcı. Sabit bir aracın olmaması. Aracın uygulanmasından önce yüksek Ar-Ge maliyeti. Küçük ve orta ölçekli şirketler tarafından karşılanamaz. Sabit bir modelin olmaması.

NIST Bulut Dağıtım Referans Mimarisi ; Bu diyagram da bulut bilişimin kullanımlarını, gereksinimlerini, özelliklerini ve standartlarını daha iyi anlamak için tasarlanmış genel bir üst düzey mimariyi gösterir.

Beş önemli aktör şunlardır:

Bulut Tüketicisi; Bulut hizmet sağlayıcıları (CSP) ile iş ilişkisi sürdüren, bulut bilişim hizmetlerinden yararlanan bir kişi veya kuruluştur. Bulut tüketicisi, CSP'nin hizmet kataloğu isteklerine göz atarak istenen hizmetler için CSP ile hizmet sözleşmeleri kurar (doğrudan veya bulut aracısı aracılığıyla) ve hizmetleri kullanır.

CSP, tüketiciye sağlanan hizmetlere göre fatura keser. CSP, bulut tüketicisinin hizmet kalitesi, güvenlik ve performans başarısızlığı için çözümler gibi teknik performans gereksinimlerini belirttiği hizmet düzeyi anlaşmasını (SLA) yerine getirmelidir. CSP, bulut tüketicilerinin kabul etmesi gereken sınırlamaları ve yükümlülükleri de tanımlayabilir.

PaaS, laaS ve SaaS modellerinde bulut tüketicisine sunulan hizmetler şunlardır;

PaaS ; veritabanı (DB), iş zekası, uygulama dağıtımı, geliştirme ve test etme ve entegrasyon.

laaS ; depolama, hizmet yönetimi, içerik dağıtım ağı (CDN), platform barındırma, yedekleme ve kurtarma ve bilgi işlem.

SaaS ; insan kaynakları, kurumsal kaynak planlama (ERP), satış, müşteri ilişkileri yönetimi (CRM), işbirliği, belge yönetimi, e-posta ve ofis üretkenliği, içerik yönetimi, finansal hizmetler ve sosyal ağlar.

Bulut Sağlayıcısı ; İlgili taraflara ağ erişimi yoluyla hizmet sağlamak için tasarlanmış bilgi işlem altyapısını edinen ve yöneten kişi veya kuruluştur.

Bulut Taşıyıcısı ; CSP'ler ile bulut tüketicileri arasında bağlantı ve taşıma hizmetleri sağlayan aracı görevi görür. Bulut taşıyıcısı, tüketicilere ağ, telekomünikasyon veya diğer erişim cihazları aracılığıyla erişim sağlar.

Bulut Denetçisi ; Bulut hizmeti kontrollerinin bağımsız incelemesini gerçekleştirerek bu konuda görüş bildiren taraftır. Denetimler, nesnel kanıtların incelenmesi yoluyla standartlara uyumu doğrular. Bir bulut denetçisi, CSP tarafından sağlanan hizmetleri güvenlik kontrolleri , gizlilik etkisi, performans vb. açısından değerlendirebilir.

Bulut Aracısı ; Bulut hizmetlerinin entegrasyonu bulut tüketicilerinin yönetemeyeceği kadar karmaşık hale gelmektedir. Bu sebepledir ki bulut tüketicisi doğrudan CSP ile iletişime geçmek yerine bulut aracısından bulut hizmetleri talep edebilir. Bulut aracısı, kullanım, performans ve teslimatla ilgili bulut hizmetlerini yöneten ve CSP'ler ile bulut tüketicileri arasındaki ilişkiyi sürdüren bir kuruluştur.

Bulut aracıları tarafından sağlanan hizmetler üç kategoriye ayrılır;

Hizmet Aracılığı ; Belirli bir yeteneği kullanarak belirli bir işlevi iyileştirir ve bulut tüketicilerine katma değerli hizmetler sağlar.

Hizmet Toplama ; Birden fazla hizmeti bir veya daha fazla yeni hizmete birleştirir ve entegre eder.

Hizmet Arbitrajı ; Hizmet toplamaya benzer fakat toplanan hizmetlerin düzeltilmesi olmadan bulut aracısı birden fazla kurumdan hizmet seçebilir.

Bulut Depolama Mimarisi ; Bulut depolama, ağ kullanarak mantıksal havuzlarda dijital verileri depolamak için kullanılan bir ortamdır. Fiziksel depolama, barındırma şirketine ait olan birden fazla sunucuya dağıtılır. Kuruluşlar; kullanıcı, kuruluş veya uygulama verilerini depolamak için bulut depolama sağlayıcılarından depolama kapasitesi satın alabilir. Bulut depolama sağlayıcıları sadece verileri yönetmekten ve verileri kullanılabilir, erişilebilir tutmaktan sorumludur. Bulut depolama hizmetlerine bulut bilişim hizmeti, web hizmeti API'si veya bulut masaüstü depolama, bulut depolama ağ geçidi, web tabanlı içerik yönetim sistemleri gibi API'yi kullanan herhangi bir uygulama kullanılarak erişilebilir.

Bulut depolama hizmeti, Amazon S3 gibi şirket dışı bir hizmetten çalıştırılır. Bulut depolama mimarisi; ölçeklenebilirlik, erişilebilir arayüzler ve ölçülü kaynaklar açısından bulut bilişimle aynı özelliklere sahiptir. Son derece sanallaştırılmış bir altyapı üzerine kurulmuş olup kullanıcılara sürekli depolama hizmetleri sağlamak için birden fazla katmana güvenir. Üç ana katman; ön uç, ara yazılım ve arka uca karşılık gelir. Ön uç katmanına son kullanıcı erişir ve veri depolama yönetimi için API'ler sağlar. Ara yazılım katmanı, veri çoğaltma ve veri çoğaltma gibi işlevleri gerçekleştirir. Arka uç katmanı, donanımın uygulandığı yerdir.

Bulut depolama, dağıtılmış kaynaklardan oluşur. Yedeklilik sayesinde son derece hata toleranslıdır, veri çoğaltmayla tutarlıdır ve son derece dayanıklıdır. Yaygın olarak kullanılan nesne depolama hizmetleri arasında Amazon S3, Oracle Cloud Storage ve Microsoft Azure Storage, Open Stack Swift vb. bulunur.

Bulut Bilişimde Yapay Zekanın Rolü; Günümüzde, bulut hizmeti sağlayıcıları kuruluşlara daha verimli, stratejik ve öngörü odaklı bulut hizmetleri sunmak için yapay zeka (AI) ve makine öğrenimi (ML) yeteneklerini bulut altyapılarına entegre etmektedir. Bu entegrasyon ayrıca kuruluşların verileri kendi başlarına verimli şekilde yönetmelerine, verilerde desenler aramak ve öngörüler elde etmek için sistemler oluşturmalarına ve eğitmelerine, müşteri deneyimini artırmalarına ve iş akışlarını optimize etmelerine yardımcı olur.

Yapay Zekayı bulut bilişimle entegre etmenin faydaları; Kendi kendine yönetilen bulut Yapay Zekayı BT altyapısıyla entegre etmek, kuruluşların iş akışlarını ve tekrarlayan görevlerini otomatikleştirmelerine yardımcı olur. Özel ve genel bulutlar, uzaktan yönetim, izleme ve sorun giderme gibi süreçleri otomatikleştirmek için Yapay Zeka araçlarından yararlanmaktadır. Temel iş akışlarını ve süreçlerini otomatikleştirmek, bulut ortamının verimliliğini artırır ve BT ekiplerinin üst düzey stratejik faaliyetlere odaklanmasını sağlar.

Azaltılmış maliye; Bulut ortamında AI araçlarından yararlanmak, kuruluşların yerinde veri merkezleri bulundurma ihtiyacını ve veri merkezlerini, sunucuları yönetmek için BT uzmanları işe alma masraflarını ortadan kaldırmasını sağlar. Dahası, buluta erişen kuruluşlar ek maliyet ödemeden eyleme dönüştürülebilir, öngörüler elde etmek ve pratik iş kullanım durumlarını çıkarmak için AI'ı kullanabilir.

Sorunsuz veri erişimi; Bulutta AI kullanımı, kullanıcılarına sorunsuz veri erişimi sağlayarak erişilemezlik sorunlarını çözme engellerini ortadan kaldırır. AI, bulut platformunun toplanan verilerden öğrenmesini, tahminlerde bulunmasını ve olası sorunları önceden çözmesini sağlar.

Geliştirilmiş veri yönetimi; AI, günümüz iş süreçleri tarafından üretilen geniş veri depolarını toplama, kataloglama ve yönetme gibi sıkıcı görevi basitleştirebilir. AI araçları; kuruluşların verileri analiz etmesine ve müşterilere doğru ve gerçek zamanlı veri ve hizmetler sağlamak için ilgili kalıpları çıkarmasına yardımcı olur.

Artan üretkenlik; İş akışlarını düzene sokmak ve tekrarlayan görevleri otomatikleştirmek, BT ekiplerinin stratejik iş faaliyetlerine ve hedeflerine odaklanmasını sağlar.

Artan güvenilirlik; Yapay Zeka'dan yararlanan bulut hizmetleri iş sürekliliğini, hızlı felaket kurtarmayı ve veri yedeklemeyi garanti altına alır.

Al-SaaS entegrasyonuyla gelişmiş deneyim; Al'ı SaaS platformuyla entegre etmek, müşterilere gelişmiş hizmet verimliliği ve işlevselliği sağlar.

Gelişmiş bulut altyapısının kullanılabilirliği; Maksimum performans ve çıktı için, Al çözümleri çok pahalı olan birden fazla ve hızlı grafik işleme biriminden (GPU) yararlanır. Bulut ortamında hizmet olarak Al, kuruluşların uygun fiyata uygulama geliştirmelerine Al yeteneklerini dahil etmelerini sağlar.

Gelişmiş bulut güvenliği; Al bulut verilerini işler, anormallikleri tespit eder, alarmlar verir ve yetkisiz bulut erişimini daha da önler. Herhangi bir kötü amaçlı veya anormal olayı tespit edebilir, bunları engelleyebilir, kötü amaçlı kodun buluta girmesini kısıtlayabilir. Al, birden fazla konuma yayılmış bilgileri toplar, analiz eder ve inceler. Böylelikle kuruluşların proaktif olay işleme faaliyetlerinde bulunmasını sağlar.

Daha iyi karar alma; Al, kuruluşların daha iyi iş kararları almasına yardımcı olur. Bulutu kullanan kuruluşlar, büyük veri kümelerinden benzer kalıpları ve eğilimleri çıkarabilir. Al, geçmiş verilerden sık görülen kalıpları öğrenir, bunları eyleme dönüştürülebilir iş öngörüsü sağlamak için gelişen veri kümelerindeki mevcut kalıplarla karşılaştırır. Bu nedenle, Al hızlı veri analizi sağlar ve müşteri gereksinimlerini çözmek için değerli öneriler üretir.

Bulutta Sanal Gerçeklik ve Artırılmış Gerçeklik; Sanal gerçeklik/artırılmış gerçeklik (VR/AR) ve bulut bilişim, ortaya çıkan en önemli teknolojilerden ikisidir. Birlikte kullanıldıklarında, yeni türde uygulamalar ve kullanım modelleri yaratabilirler. Bulut ortamı, günümüzde mevcut olan çok çekirdekli CPU gücüne erişim sağlayabilirse, VR/AR uygulamalarının ham bilgi işlem gereksinimlerini kolayca karşılayabilir. Günümüzde bulut tabanlı veri merkezlerinin çoğu, VR/AR uygulamaları tarafından talep edilen GPU uygulamalarını hesaplamak için grafik gücüne erişim sağlar. Dahası da VR/AR uygulamaları piyasada bulunandan daha fazla dijital motor hızı talep eder. VR/AR uygulamaları için kullanılan bilgi işlem cihazlarının maliyetli yükseltmelerini yapmak yerine çekirdek altyapının hızını artırmak için bulut hizmetinden yararlanmak yeterli olacaktır. VR/AR uygulamalarının gelişen doğası, yazılım işlevselliğinde ve kullanıcı arayüzünde (UI) hızlı değişikliklere neden olacaktır. Bu tür uygulamaların bulut tabanlı dağıtımından yararlanmak, son kullanıcılar veya tüketiciler için sorunsuz bir deneyim sağlayacaktır. VR/AR tabanlı uygulamalar sıklıkla kullanılmadığından, bu uygulamalar kullanım başına ödeme, hizmet tabanlı bulut modelleri olarak kullanılabilir.

Fog Bilişim; Dünya çapında IoT cihazlarındaki muazzam büyüme, bu cihazlar tarafından muazzam miktarda veri üretilmesiyle sonuçlanmıştır. Bu verileri analiz etme ve işleme konusundaki artan talebi karşılamak için, bulut bilişimle birlikte fog bilişiminin uygulanması ideal bir çözümdür.

Sis bilişim, uygulamaların ve veri depolamasının veri kaynakları (veri üreten cihazlar) ve bulut hizmeti arasında konumlandırıldığı dağıtılmış ve bağımsız dijital ortamdır. Fog bilişim, son kullanıcılara hizmet erişimini sağlamak için doğrudan fiziksel cihazlara bağlı birden fazla uç düğümden oluşan bulut bilişimin genişletilmiş bir sürümüdür.

Genel olarak Fog bilişim; IoT ve bulut bilişim ile yakın bağlantıları olan dağıtılmış ağ altyapısında bireysel katman oluşturma fikrini ifade eder. Donanım ve uzak sunucular arasında bir aracı görevi görerek akıllı ağ geçidi olarak da adlandırılır. Hızlı ve verimli şekilde gelişmiş veri işleme, depolama ve analiz için kullanılabilir. Birçok kuruluş, hızlı ve verimli veri işleme, depolama ve analiz için ek işlevler sağlayabildiği için bu teknolojiyi benimsemiştir.

Fog Bilişiminin Çalışması; İnternet bağlantısı, hesaplama yetenekleri ve veri depolaması olan cihazlara Fog düğümleri denir. Fog düğümleri ağdaki herhangi bir yere yerleştirilebilir. Fog düğümleri için IoT uygulamaları ağ kenarında taşınır. Ağ kenarına yakın Fog düğümleri, IoT cihazlarından veri alarak kenarda kısa vadeli analizler yapılmasını sağlar. Fog bilişim, kararsız internet bağlantısı durumunda çok faydalı olabilir. Acil istekler doğrudan Fog'a iletilir ve yerel ağda gerçek zamanlı olarak işlenir. Fog bilişim; akıllı şehirler, akıllı şebekeler, bağlı arabalar ve gerçek zamanlı analizler gibi uygulamalarda kullanılabilir.

Avantajlar; Fog bilişim; IoT, büyük veri ve gerçek zamanlı analiz alanında faydalı olmuştur. Ayrıca;

Düşük gecikme: Coğrafi olarak son kullanıcılara daha yakın olduğundan ve hızlı yanıtlar sunabildiğinden büyük miktarda veriyi gecikme olmadan işleyebilir.

Yüksek iş çevikliği: Geliştiriciler, Fog örneklerini kolayca ve hızlı şekilde tasarlayabilir ve gereksinime göre dağıtabilir.

Bant genişliğinde aksaklık olmaması: Tüm veriler tek kanal aracılığıyla tek bir merkeze birlikte iletilmek yerine farklı noktalarda toplanır, böylelikle bant genişliğiyle ilgili sorunlardan kaçınılır.

Bağlantı kaybı olmaması: Birkaç birbirine bağlı kanalın varlığı bağlantı kaybına neden olmaz.

Yüksek güvenlik: Fog bilişim, veri işleme karmaşık dağıtılmış sistemde çok sayıda düğüm tarafından gerçekleştirildiğinden güvenliği artırır.

Düşük işletme maliyeti: Fog bilişim, veriler analiz için buluta gönderilmek yerine yerel olarak işlendiğinden ağ bant genişliğinin korunması yoluyla maliyeti önemli ölçüde azaltabilir.

Yüksek güç verimliliği: Uç cihazlar Zigbee, Z Wave veya Bluetooth gibi güç tasarrufu sağlayan protokolleri çalıştırır.

Dezavantajları:

Ek harcamalar: Kuruluşlar yönlendiriciler, hub'lar ve ağ geçitleri gibi ek uç cihazlar satın almalıdır.

Karmaşık sistem: Veri işleme ve depolama sisteminde ekstra bir katman olduğundan, tüm sistemi karmaşık hale getirir.

Sınırlı ölçeklenebilirlik: Bulut kadar ölçeklenebilir değildir.

Edge Bilişim; Geleneksel bulut bilişiminin veri güvenliği, düşük performans ve yüksek işletme maliyetlerine yol açan artan veri depolama ile ilgili bazı sorunları vardır. Bu sorunlar, geleneksel bulut bilişimin Edge bilişim ile değiştirilmesiyle çözülebilir. Edge bilişim, Fog bilişiminin bir alt kümesidir ve veri işleme yaklaşımı Fog bilişimine benzerdir. Fog bilişiminde, akıllı ağ geçidi LAN'da işleme gerçekleştirirken, edge bilişiminde, edge ağ geçidi zekası programlanabilir otomasyon denetleyicileri gibi cihazlarda gerçekleştirilir. Edge bilişim, küçük ve acil işlemlerin milisaniyeler içinde işlenmesini gerektiren çözümlerde kullanılır.

Edge bilişim, hesaplama ve veri işlemenin edge cihazlara yakın bir yerde gerçekleştirildiği dağıtılmış, merkezi olmayan bilişim modelidir. Verileri, verilerin toplandığı cihazlara yakın yerlerde depolar. İnternet bant genişliği kullanımını ve veri yükünü azaltır. Birçok kuruluş, hızlı işleme, hızlı yanıtlar ve verimli gerçek zamanlı uygulamalar için otomasyon sistemleri oluşturmak amacıyla bu teknolojiden yararlanabilir.

Bulut / Fog Bilişim / Edge Bilişim; Edge bilişim ve fog bilişim, bulut bilişimin uzantılarıdır. Bulut bilişim, gerçek zamanlı olarak veri işleyen binlerce sunucu içeren merkezi bir modeldir.

Edge computing; veri işlemenin edge aygıtlarının (IoT aygıtları) yakınında gerçekleştirildiği dağıtılmış, merkezi olmayan model olarak çalışan sonsuz sayıda (milyarlarca) sanal/donanım uç noktası içerir. Fog bilişim altyapısı, veri depolama, veri işleme ve analizinin hızlı ve verimli şekilde gerçekleştirildiği sayısız düğüm içerir. Bir veri kaynağı ile bulut altyapısı arasında herhangi bir yere konumlandırılmış merkezi olmayan akıllı ağ geçididir.

Bulut Bilişim ve Grid Bilişim; En popüler iki bilişim modeli olan bulut bilişim ve grid bilişim, sırasıyla istemci-sunucu ve dağıtılmış bilişim mimarisine dayanmaktadır.

Bulut Hizmet Sağlayıcıları;

Amazon Web Service (AWS); Bireylere, kuruluşlara, hükümete vb. kullanım başına ödeme temelinde talep üzerine bulut bilişim hizmetleri sağlar. Bu hizmet; dağıtılmış bilgi işlem ve araçlar aracılığıyla gerekli teknik altyapıyı sağlar. AWS tarafından sağlanan sanal ortam, CPU, GPU, RAM, HDD depolama, işletim sistemleri, uygulamalar, web sunucuları, veritabanları ve CRM gibi ağ yazılımlarını içerir.

Microsoft Azure; Azure veri merkezleri aracılığıyla uygulama ve hizmetleri oluşturmak, test etmek, dağıtmak, yönetmek için bulut bilişim hizmetleri sağlar. SaaS, PaaS ve laas gibi her türlü bulut bilişim hizmetini sağlar. Bilgi işlem, mobil depolama, veri yönetimi, mesajlaşma, medya, makine öğrenimi ve IoT gibi çeşitli bulut hizmetleri sunar.

Google Cloud Platform (GCP); laaS, PaaS ve sunucusuz bilgi işlem hizmetleri sağlar. Bunlara bilgi işlem, veri depolama ve analitiği, makine öğrenimi, ağ oluşturma, büyük veri, bulut AI, yönetim araçları, kimlik ve güvenlik, IoT ve API platformları dahildir.

IBM Cloud; Gelişmiş veri ve AI araçları, derin sektör uzmanlığından oluşan sağlam bir pakettir. Genel, özel ve hibrit bulut dağıtım modelleri aracılığıyla laaS, SaaS ve PaaS gibi çeşitli bulut hizmetleri sağlar. Bu hizmetlere bilgi işlem, ağ oluşturma, depolama, yönetim, güvenlik, veritabanları, analitik, AI, IoT, mobil, geliştirme araçları, blok zinciri dahildir.

Konteyner Teknolojisi; Gelişmekte olan konteyner tabanlı sanallaştırma hizmetidir. Geliştiricilerin ve BT ekiplerinin, hizmet sağlayıcının API'sini veya web portalı arayüzünü kullanarak konteynerleştirilmiş uygulamaları geliştirmelerine, çalıştırmalarına ve yönetmelerine yardımcı olur. Konteynerler ve kümeler şirket içi veri merkezlerine veya buluta dağıtılabilir.

Konteyner, bulut ortamındaki diğer işlemlerden bağımsız olarak çalışan kitaplık ve yapılandırma dosyaları, ikili dosyalar ve diğer kaynaklar gibi tüm bağımlılıklarını içeren uygulama/yazılım paketidir. Tüm bu kaynak dosyaları, uygulamalar bulut ortamları arasında taşındığında uyumluluk sorunlarını çözmek için bir birim olarak teslim edilir. Bu konteynerler abonelere CaaS biçiminde sağlanır. CaaS hizmeti, orkestratörler aracılığıyla konteynerlerin sanallaştırılmasını ve yönetilmesini içerir. Aboneler bu hizmetleri kullanarak bulut veya şirket içi veri merkezleri aracılığıyla zengin, ölçeklenebilir konteynerleştirilmiş uygulamalar geliştirebilir. Hem laaS hem de PaaS'ın özelliklerini devralır. Popüler konteyner hizmetleri arasında Amazon AWS EC2, Google Kubernetes Engine (GKE), Docker vb. bulunur.

Özellikler; Konteynerlerin uygulanması birçok avantaj sunar ve bunları çeşitli endüstriler için çekici bir teknoloji haline getirmektedir;

Taşınabilirlik ve tutarlılık; Bir kapsayıcıda geliştirilen uygulama veya yazılım, gerçekleştirmek için gereken tüm kaynakları içerir. Bu taşınabilirlik, istemcilerin veya son kullanıcıların çeşitli platformlarda ve özel veya genel bulut ortamlarında bir uygulamayı çalıştırmasına yardımcı olur.

Güvenlik; Kapsayıcıların bağımsız yapısı nedeniyle güvenlik riskleri azalır. Bir uygulama saldırıya uğrarsa veya tehlikeye atılırsa, enfeksiyonları kalan kapsayıcılara yayılmaz.

Yüksek verimlilik ve maliyet etkinliği; Kapsayıcılar, bağımsız işletim sistemlerine ihtiyaç duymadıkları için sanal makinelere kıyasla daha az kaynakla çalışabilirler. Kapsayıcıların çalışması için birkaç megabayt belleğe ihtiyaç vardır ve bu da kullanıcıların tek bir sunucuda birden fazla kapsayıcı çalıştırmasını sağlar. Bu kapsayıcılar bir bulut sunucusunda izole edilir çünkü bir uygulama bir kapsayıcı için kapalıysa, diğer kapsayıcılar teknik aksaklıklar olmadan bunu kullanabilir.

Ölçeklenebilirlik; Kapsayıcılar ölçeklenebilirdir ve abonelerin veya kullanıcıların boyutlarını artırmak için aynı küme altında daha fazla benzer kapsayıcıyı entegre etmelerini sağlar. Akıllı ölçekleme teknolojisi, kullanıcıların sadece amaçlanan konteyneri çalıştırmasını ve istenmeyen konteynerleri beklemeye almasını sağlayarak maliyet açısından etkili hale getirir.

Sağlamlık; Konteynerler işletim sistemlerine ihtiyaç duymadıkları için saniyeler içinde oluşturulabilir, dağıtılabilir ve yok edilebilir. Bu özellik; hızlı geliştirme süreci, artan operasyonel hız, belirtilen süre içinde yeni yazılım sürümlerinin başlatılmasını sağlar. Kullanıcının uygulama ile deneyimini hızlandırarak geliştiricilerin ve kuruluşların hataları hızla gidermesini ve en son özellikleri entegre etmesini kolaylaştırır.

Konteyner Teknolojisi Mimarisi; Beş katmanlı bir mimariye sahiptir ve üç aşamalı yaşam döngüsünden geçer;

1. Katman - Geliştirici makineleri ; Görüntü oluşturma, test etme ve akreditasyon.

2. Katman - Test etme ve akreditasyon sistemleri ; Görüntü içeriklerinin doğrulanması ve onaylanması, görüntülerin imzalanması ve kayıt defterlerine gönderilmesi.

3. Katman - Kayıt defterleri ; Görüntüleri depolamak ve isteklere göre düzenleyicilere dağıtmak.

4. Katman - Düzenleyiciler ; Görüntüleri kapsayıcılara dönüştürmek ve kapsayıcıları host bilgisayarlara dağıtmak.

5. Katman - Host bilgisayarlar ; Düzenleyicinin talimatlarına göre kapsayıcıları işletmek ve yönetmek.

Görüntü Oluşturma, Test Etme ve Akreditasyon; Konteyner teknolojisinin ilk aşaması görüntü oluşturma ve doğrulamadır. Bu aşamada; uygulama veya yazılım bileşenleri geliştirilir ve görüntüye veya görüntülere depolanır. Görüntü; konteyneri çalıştırmak için gereken dosyalardan ve kaynaklardan oluşur. Görüntü oluşturma işlemi geliştiriciler tarafından gerçekleştirilir, uygulamanın temel bileşenlerini entegre etmekten sorumludur. Görüntü oluşturulduktan sonra güvenlik ekipleri görüntü testini ve akreditasyonunu gerçekleştirir.

Görüntü Depolama ve Alma; Görüntüler genelde kayıt defteri olarak bilinen merkezi konumlara yerleştirilir. Kayıt defterleri, geliştiricilere görüntüleri depolamak, etiketlemek ve kolay tanımlama için görüntüleri kataloglamak, kolay keşif ve yeniden kullanım için sürüm kontrolü ve diğer geliştiriciler tarafından oluşturulan görüntüleri getirmek, indirmek gibi çeşitli hizmetler sağlar. Kayıt defterleri bir hizmet olarak sağlanabilir veya kendi kendine barındırılabilir. Popüler kayıt defteri hizmetleri arasında Docker Hub, Amazon Elastic Container Registry (ECR), Docker Trusted Registry (DTR) vb. bulunur.

Konteyner Dağıtımı ve Yönetimi; Orkestratörler, DevOps yöneticilerinin kayıt defterlerinden görüntüleri almalarına, bunları kapsayıcılara dağıtmalarına, kapsayıcı işlemlerini yönetmelerine olanak tanıyan araçlardır. Uygulamanın en son sürümünün dağıtıldığı ve canlı kullanıma/eyleme girdiği kapsayıcı yaşam döngüsünün son aşamasıdır.

Orkestratörler, kapsayıcı kaynak tüketimini ve iş yürütmeyi izlemede, host bilgisayar arızalarını belirlemede, yeni host bilgisayarlarda kapsayıcıları otomatik olarak yeniden başlatmada yardımcı olur. Kaynaklar tükendiğinde, orkestratör kapsayıcılara ek kaynaklar tahsis eder. Kapsayıcıda çalışan bir uygulamanın güncellenmesi gerektiğinde, mevcut kapsayıcılar yok edilir, güncellenen görüntülerden yeni kapsayıcılar oluşturulur. Popüler düzenleyiciler arasında Kubernetes, Docker Swarm, Nomad, Mesos vb. bulunur.

Avantajları: Bir uygulamayı geliştirmek için gereken minimum kaynak sayısına sahiptirler. Yazılım sorunlarının daha hızlı tespiti ve yamaların dağıtımı sağlanır. Maliyet etkinliği ve kolay gönderime sahiptirler. Artan uygulama taşınabilirliği vardır. Ölçeklenebilir kaynaklardır. Hızlı konteyner önyüklemesi bulunur (saniyeler içinde) böylelikle uygulamalar hızlı aşamada geliştirilebilir. Konteynerlerdeki izole uygulamaların kolay yönetimi vardır. Kolay test ve hata ayıklamaya sahiptirler.

Dezavantajları: Artan karmaşıklık vardır. Personel uzmanlığının eksikliği yanlış yapılandırmalara neden olabilir. Paylaşılan kaynaklar nedeniyle artan güvenlik açığı bulunmaktadır. Şüpheli konteyner performansı vardır. Konteynerleri çalıştırmak için platform seçmede zorluk vardır. Hizmet keşfinde farklılıklar bulunmaktadır.

Konteynerler ve Sanal Makineler; Sanallaştırma, bulut bilişimini destekleyen temel bir teknolojidir. Tek bir fiziksel sistemde birden fazla işletim sistemi çalıştırma ve sunucular, depolama aygıtları veya ağlar gibi temel kaynakları paylaşma olanağı sağlar. Sanallaştırma, kuruluşların mevcut bilgisayar donanımlarının üretkenliğini, kullanımını ve esnekliğini artırırken BT maliyetlerini düşürmelerine olanak tanır. Sanallaştırma satıcıları arasında VMware vCloud Suite, VMware vSphere, VirtualBox, Microsoft Hyper-V vb. bulunur. Geleneksel olarak sanallaştırma, uygulama taşınabilirliğini ve bulut BT altyapısının optimizasyonunu kolaylaştırmak için ortaya çıkmıştır. Fakat sanal makinelerin ağırlığı nedeniyle daha yavaş performans, taşınabilirlik sorunları, BT kaynak sağlamada zaman tüketimi gibi çeşitli dezavantajları vardır. Bu sorunları çözmek için endüstriler, tek bir işletim sisteminde çalışan ve yazılım/uygulamayı ölçeklenebilir kaynaklarla her yerde çalıştıran hafif kapsayıcılar biçiminde uygulama kaynakları sağlayan kapsayıcılaştırma teknolojisi benimsiyor.

Kapsayıcılar, fiziksel bir sunucunun ve ana işletim sisteminin üstüne yerleştirilir ve sistem çekirdeği ikili dosyalarını ve kitaplıklarını paylaşarak işletim sistemini yeniden üretme ihtiyacını azaltır. Konteynerleştirme yoluyla, sunucu tek bir işletim sistemini kullanarak birden fazla iş yükünü çalıştırabilir. Bu nedenle, konteynerler hafiftir sadece megabayt boyutundadır ve birkaç dakika süren önyükleme işlemlerinin aksine saniyeler içinde önyükleme yapar.

Docker; Uygulamaları geliştirmek, paketlemek ve çalıştırmak için kullanılan açık kaynaklı bir teknolojidir. Tüm Docker bağımlılıkları, uygulamaların sorunsuz ortamda çalışmasını sağlamak için kapsayıcılar biçimindedir. Docker, işletim sistemi düzeyinde sanallaştırma yoluyla PaaS sağlar ve kapsayıcı yazılım paketleri sunar. Bu teknoloji; uygulamaları daha hızlı yazılım teslimi için temel altyapıdan izole eder. Docker'ın avantajı, bir uygulama bağımlılıklarıyla birlikte Docker kapsayıcısına paketlendiğinde, herhangi bir ortamda çalışabilmesidir. Geliştiriciler Docker kullanarak uygulamalar oluşturduklarında, Docker kapsayıcıları birbirinden izole edildiği ve iyi tanımlanmış kanallar aracılığıyla iletişim kurduğu için aralarında hiçbir müdahale olmayacağından emin olurlar.

Docker Motoru; Şu bileşenleri kullanarak uygulamaları geliştirmeye, dağıtmaya ve çalıştırmaya izin veren host bilgisayara yüklenen istemci/sunucu uygulamasıdır;

Sunucu: Daemon işlemi (dockerd komutu) olarak da bilinen kalıcı arka uç işlemidir.

Rest API: Bu API, görevlerin daemon'a iletilmesini ve atanmasını sağlar.

İstemci CLI: Daemon ile iletişim kurmak için kullanılan ve çeşitli Docker komutlarının başlatıldığı komut satırı arayüzüdür.

Docker Swarm; Docker motoru, Docker platformu içinde birden fazla Docker motorunu yönetmeye olanak tanıyan swarm modunu destekler. Docker CLI, swarm oluşturmak, swarm'a uygulama dağıtmak, etkinliğini veya davranışını yönetmek için kullanılır.

Swarm modu, yöneticilerin ve geliştiricilerin ; Kapsayıcılarla iletişim kurmasını ve işleri farklı kapsayıcılara atamasını sağlar. Yüke göre kapsayıcı sayısını genişletmesini veya azaltmasını sağlar. Sağlık kontrolü gerçekleştirmesini ve farklı kapsayıcıların yaşam döngüsünü yönetmesini sağlar. Düğüm arızası meydana gelse bile bir işlemi sürdürmek için devralma ve yedekliliği dağıtmasını sağlar. Tüm kapsayıcılara zamanında yazılım güncellemeleri gerçekleştirmesini sağlar.

Docker Mimarisi; Docker mimarisi bir istemci/sunucu modeli kullanır ve host bilgisayar, istemci, ağ, kayıt defteri ve diğer depolama birimleri gibi çeşitli bileşenlerden oluşur. Docker istemcisi, kapsayıcıları geliştiren, çalıştıran ve dağıtan Docker daemon'uyla etkileşime girer.

Daemon ve Docker istemcileri aynı host bilgisayarda işlemler gerçekleştirebilir. Alternatif olarak, kullanıcılar Docker istemcisini uzak daemon'lara bağlayabilir. Docker istemcisi ile Docker sunucusu daemon'u arasındaki iletişim REST API aracılığıyla kurulur.

Docker mimarisinin çeşitli bileşenleri;

Docker Daemon: Docker daemon'u (dockerd), API isteklerini işler ve kapsayıcılar, birimler, görüntüler ve ağlar gibi çeşitli Docker nesnelerini işler.

Docker İstemcisi: Kullanıcıların Docker ile iletişim kurduğu birincil arayüzdür. Docker run gibi komutlar başlatıldığında, istemci ilgili komutları dockerd'ye iletir ve dockerd de bunları yürütür. Docker komutları iletişim için Docker API'sini kullanır.

Docker Kayıtları: Docker kayıt defterleri, görüntülerin depolandığı ve çekildiği konumlardır ve özel veya genel olabilir. Docker Cloud ve Docker Hub, iki popüler genel kayıt defteridir. Docker Hub, tüm kullanıcılar tarafından kullanılabilen Docker görüntülerinin önceden tanımlanmış bir konumudur.

Docker Nesneleri: Docker nesneleri bir uygulamayı birleştirmek için kullanılır.

En önemli Docker nesneleri şunlardır;

Görüntüler: Kapsayıcıları depolamak ve dağıtmak için kullanılır. Kapsayıcı oluşturma talimatları içeren salt okunur ikili şablonlardır.

Kapsayıcılar: Uygulama kaynakları kapsayıcıların içinde çalışır. Kapsayıcı, bir uygulama görüntüsünün çalıştırılabilir örneğidir. Docker CLI veya API, bu kapsayıcıları oluşturmak, başlatmak, durdurmak ve yok etmek için kullanılır.

Hizmetler: Kullanıcıların kapsayıcı sayısını daemon'lar arasında genişletmesini sağlar ve birlikte birkaç yönetici, çalışandan oluşan küme görevi görürler. Her küme üyesi bir daemon'dur ve tüm bu daemon'lar Docker API'yi kullanarak birbirleriyle etkileşime girebilir.

Ağ: Tüm izole konteynerlerin iletişim kurduğu bir kanaldır.

Birimler: Docker tarafından oluşturulan ve Docker konteynerleri tarafından kullanılan kalıcı verilerin depolandığı depolama alanıdır.

Docker İşlemleri; Docker görüntüleri tarafından gerçekleştirilen yaygın işlemler şöyledir; Dockerfile'dan yeni görüntü oluşturma. Tüm yerel görüntüleri listeleme. Mevcut bir görüntüyü etiketleme. Docker kayıt defterinden yeni bir görüntü çekme. Yerel bir görüntüyü Docker kayıt defterine itme. Mevcut görüntüleri arama.

Mikroservisler ve Docker; Monolitik uygulamalar, her biri benzersiz bir görevi yerine getiren, birlikte çalışan mikroservisler adı verilen bulutta barındırılan alt uygulamalara ayrılır. Mikroservisler, uygulama iş yükünü böler ve dağıtır, birbirleriyle etkileşime girerek kararlı, sorunsuz ve ölçeklenebilir hizmetler sunar. Monolitik uygulamalar, mikroservisleri geliştirmek, desteklemek ve dağıtmak için çapraz işlevli ekipleri destekleyen iş yetenekleri etrafında ayrıştırılır.

Monolitik uygulamalar tarafından kullanılan geleneksel veri depolama modellerine kıyasla, mikroservisler kendi veri depolarını yöneterek veri depolamasını merkezden uzaklaştırır. Geliştiriciler her mikroservis için bir Docker konteyneri oluşturur. Her mikroservis, gerekli kitaplıklar, çerçeveler ve yapılandırma dosyalarıyla birlikte konteynere paketlendiğinden, tek bir uygulamaya ait mikroservisler birden fazla platform kullanılarak geliştirilebilir ve yönetilebilir.

Docker Ağ Oluşturma; Docker, birden fazla konteyneri ve hizmeti veya diğer Docker dışı iş yüklerini birbirine bağlamaya olanak tanır. Linux ve Windows gibi birden fazla platformda çalışan Docker host bilgisayarlarını platformdan bağımsız şekilde yönetebilir. Docker ağ mimarisi, heterojen altyapılar arasında uygulama taşınabilirliği sağlayan konteyner ağ modeli (CNM) olarak bilinen arayüz kümesi üzerinde geliştirilmiştir.

CNM, birden fazla üst düzey yapı içermektedir;

Sandbox: Konteyner arayüzlerinin, yönlendirme tablolarının, etki alanı adı sistemi (DNS) ayarlarının yönetimi için konteyner ağ yığını yapılandırmasını içerir.

Uç Nokta: Uygulama taşınabilirliğini korumak için, bir uç nokta bir ağa bağlanır ve uygulamadan soyutlanır, böylece hizmetler farklı ağ sürücülerini uygulayabilir.

Ağ: Bir ağ, birbirine bağlı uç noktaların bir koleksiyonudur. Ağ bağlantısı olmayan uç noktalar ağ üzerinden iletişim kuramazlar.

CNM, ağ üzerinde ek işlevsellik ve kontrol sağlamak için iki takılabilir sürücü arayüzü içerir;

Ağ Sürücüleri: Ağ, Docker ağ sürücülerinin uygulanmasıyla çalışır. Bu sürücüler takılabilir, böylelikle aynı ağda birden fazla ağ sürücüsü aynı anda kullanılabilir. İki tür CNM ağ sürücüsü vardır; yerel ve uzak ağ sürücüleri.

IPAM Sürücüleri: IP adresi yönetimi (IPAM) sürücüleri, atanmamışlarsa uç noktalara ve ağlara varsayılan alt ağ ve IP adresleri atar.

Docker motoru, beş yerel ağ sürücüsü içerir;

Host Bilgisayar: Host bilgisayar sürücüsü kullanarak kapsayıcı host bilgisayar ağ yığınını uygular.

Köprü: Bir köprü sürücüsü, Docker tarafından yönetilen host bilgisayarda Linux köprüsü oluşturmak için kullanılır.

Kaplama: Bir kaplama sürücüsü, fiziksel ağ altyapısı üzerinden kapsayıcı iletişimini etkinleştirmek için kullanılır.

MACVLAN: Bir macvlan sürücüsü, Linux MACVLAN köprü modunu kullanarak kapsayıcı arayüzleri ile ana host bilgisayar arayüzü veya alt arayüzleri arasında ağ bağlantısı oluşturmak için kullanılır.

Docker, topluluk veya satıcılar tarafından oluşturulan ve CNM ile uyumlu üç uzak sürücü içerir;

Contiv: Cisco tarafından çok kiracılı mikro hizmet dağıtımları için güvenlik ve altyapı politikaları oluşturmak amacıyla tanıtılan açık kaynaklı ağ eklentisidir.

Weave: Birden fazla buluta yayılmış Docker kapsayıcılarını bağlamak için sanal ağ oluşturmak amacıyla kullanılan ağ eklentisidir.

Kuryr: OpenStack ağ hizmeti olan Neutron'u kullanarak Docker libnetwork uzak sürücüsünü uygulayan ve IPAM sürücüsü içeren ağ eklentisidir.

Konteyner Orkestrasyonu; Yazılım konteynerlerinin ve bunların dinamik ortamlarının yaşam döngülerini yönetmek için otomatik bir işlemdir. Mikroservis tabanlı uygulamalar için ayrı konteynerlerin işini planlamak ve dağıtmak için kullanılır. Konteyner orkestrasyonu, yazılım konteynerlerinin ve bunların dinamik ortamlarının yaşam döngülerini yönetmek için otomatik bir işlemdir. Birden fazla kümeye yayılmış mikroservis tabanlı uygulamalar için ayrı konteynerlerin işini planlamak ve dağıtmak için kullanılır. Konteyner orkestrasyonu kullanılarak çeşitli görevler otomatikleştirilebilir; Konteynerlerin sağlanması ve dağıtımı. Konteynerlerin devralınması ve yedekliliği. Yükü host bilgisayar altyapısına eşit şekilde dağıtmak için konteynerler oluşturma veya yok etme. Kaynak tükenmesi veya host bilgisayar arızası durumunda konteynerleri bir host bilgisayardan diğerine taşıma. Konteynerler arasında otomatik kaynak tahsisi. Çalışan hizmetleri harici ortama açma. Konteynerler arasında yük dengeleme, trafik yönlendirme ve hizmet keşfi gerçekleştirme. Çalışan kapsayıcıların ve host bilgisayarların sağlık kontrolünün gerçekleştirilmesi. Kapsayıcıların kullanılabilirliğinin sağlanması. Uygulamayla ilgili kapsayıcıların yapılandırılması. Kapsayıcıların arasındaki iletişimin güvence altına alınması.

Kubernetes; K8s olarak da bilinir, Google tarafından konteynerleştirilmiş uygulamaları ve mikro hizmetleri yönetmek için geliştirilen açık kaynaklı, taşınabilir, genişletilebilir orkestrasyon platformudur. Konteynerler; uygulamaları paketlemek ve çalıştırmak için verimli bir yol sağlar. Gerçek zamanlı üretim ortamında, kesinti süresini sıfıra indirmek için konteynerler verimli şekilde yönetilmelidir. Bir konteyner arızalanırsa, başka bir konteyner otomatik olarak başlatılır. Bu sorunların üstesinden gelmek için Kubernetes, dağıtılmış konteynerleri yönetmek, dağıtım kalıpları oluşturmak ve uygulamalar için devralma ve yedeklilik gerçekleştirmek üzere dayanıklı bir çerçeve sağlar.

Kubernetes tarafından sağlanan özellikler;

Hizmet keşfi: Kubernetes, bir hizmetin bir DNS adı veya IP adresi aracılığıyla keşfedilmesine olanak tanır.

Yük dengeleme: Bir konteyner yoğun trafik aldığında, Kubernetes trafiği otomatik olarak diğer konteynerlere dağıtır ve yük dengeleme gerçekleştirir.

Depolama orkestrasyonu: Kubernetes, geliştiricilerin yerel ve genel bulut depolama gibi kendi depolama yeteneklerini monte etmelerine olanak tanır.

Otomatik dağıtımlar ve geri almalar: Kubernetes, yeni kapsayıcılar oluşturma, mevcut kapsayıcıları yok etme ve tüm kaynakları bir kapsayıcıdan diğerine taşıma sürecini otomatikleştirir.

Otomatik kutu paketleme: Kubernetes, kapsayıcılaştırılmış uygulamaları çalıştıran bir düğüm kümesini yönetebilir. Kapsayıcıyı çalıştırmak için gereken kaynakları (işlem gücü ve bellek gibi) belirtirseniz, Kubernetes kaynakları kapsayıcılara otomatik olarak tahsis edebilir ve tahsisini kaldırabilir.

Kendi kendini iyileştirme: Kubernetes, kapsayıcıların sağlık kontrolünü otomatik olarak gerçekleştirir, başarısız kapsayıcıları yeni kapsayıcılarla değiştirir, başarısız kapsayıcıları yok eder ve istemcilere kullanılamayan kapsayıcıları duyurmaktan kaçınır.

Gizli ve yapılandırma yönetimi: Kubernetes, kullanıcıların kimlik bilgileri, güvenli kabuk (SSH) anahtarları, OAuth belirteçleri gibi hassas bilgileri depolamasına ve yönetmesine olanak tanır. Uygulama yapılandırması ve hassas bilgiler, kapsayıcı görüntülerini yeniden oluşturmaya gerek kalmadan dağıtılabilir ve güncellenebilir.

Kubernetes Küme Mimarisi; Kubernetes dağıtıldığında kümeler oluşturulur. Küme, Kubernetes tarafından yönetilen kapsayıcıların içindeki uygulamaları yürüten düğümler olarak bilinen bir bilgisayar grubudur. Bir küme, en az bir ana düğüm ve bir çalışan düğümden oluşur. Çalışan düğümler, pod'lar (bir kapsayıcı grubu) içerir ve ana düğüm bunları yönetir.

Ana Bileşenler: Ana düğümün bileşenleri bir küme kontrol paneli sağlar ve küme olaylarını zamanlama, algılama ve işleme gibi çeşitli etkinlikler gerçekleştirir. Bu ana bileşenler kümedeki herhangi bir bilgisayar tarafından yürütülebilir.

Kube-apiserver: API sunucusu, tüm API isteklerine yanıt veren Kubernetes kontrol panelinin ayrılmaz bir parçasıdır. Kontrol paneli için bir ön uç yardımcı programı olarak hizmet eder ve etcd kümesiyle etkileşime giren ve veri depolamasını sağlayan tek bileşendir.

Etcd kümesi: Kubernetes küme verilerinin, hizmet keşif ayrıntılarının, API nesnelerinin vb. depolandığı dağıtılmış ve tutarlı bir anahtar-değer depolama alanıdır.

Kube-scheduler: Yeni oluşturulan pod'ları tarayan ve onlar için bir düğüm tahsis eden bir ana bileşendir. Düğümleri, genel kaynak gereksinimi, veri yerelliği, yazılım/donanım/politika kısıtlamaları ve dahili iş yükü müdahaleleri gibi faktörlere göre atar.

Kube-controller-manager: Denetleyicileri çalıştıran ana bileşendir. Denetleyiciler genelde ayrı süreçlerdir fakat karmaşıklığı azaltmak için tek ikili dosyada birleştirilir ve tek bir süreçte birlikte çalıştırılır.

cloud-controller-manager: Bu, bulut sağlayıcılarıyla iletişim kuran denetleyicileri çalıştırmak için kullanılan ana bileşendir. Cloud-controller-manager, Kubernetes kodunun ve bulut sağlayıcı kodunun ayrı ayrı gelişmesini sağlar.

Düğüm bileşenleri: Düğüm veya çalışan bileşenler kümedeki her düğümde çalışır, çalışan pod'ları yönetir ve Kubernetes çalışma zamanı hizmetlerini sağlar.

Kubelet: Her düğümde çalışan ve bir pod'da çalışan kapsayıcıları sağlayan önemli bir hizmet aracısıdır. Pod'ların ve kapsayıcıların sağlıklı ve beklendiği gibi çalışmasını sağlar. Kubelet, Kubernetes tarafından oluşturulmayan kapsayıcıları işlemez.

Kube-proxy: Her çalışan düğümde çalışan ağ proxy hizmetidir. Bu hizmet, pod'lara ağ bağlantısını sağlayan ağ kurallarını korur.

Kapsayıcı Çalışma Zamanı: Kapsayıcı çalışma zamanı, kapsayıcıları çalıştırmak için tasarlanmış bir yazılımdır.

Kurbernetes, Docker, rktlet, containerd ve cri-o gibi çeşitli kapsayıcı çalışma zamanlarını destekler.

Kubernetes Ve Docker; Docker, tek bir işletim sisteminde konteynerleştirilmiş uygulamaları oluşturmak, dağıtmak ve çalıştırmak için herhangi bir host bilgisayara yüklenebilen açık kaynaklı yazılımdır. Konteynerleştirme, çalışan uygulamaları host bilgisayar işletim sisteminde çalışan diğer hizmetlerden ve uygulamalardan ayırır. Kubernetes, konteynerleri oluşturma, yönetme, güncelleme, ölçekleme ve yok etme sürecini otomatikleştiren konteyner düzenleme platformudur. Hem Dockers hem de Kubernetes, mikro hizmet mimarisine dayanır, küçük hafif ikili dosyaları dağıtmak için Go programlama dili kullanılarak oluşturulur ve uygulama yapılandırmalarını, yığınlarını belirtmek için YAML dosyasını kullanır. Kubernetes ve Docker bir araya getirildiğinde, dağıtılmış bir mimaride konteynerlerin verimli şekilde yönetilmesini ve dağıtılmasını sağlarlar. Docker, farklı işletim sistemlerine sahip birden fazla host bilgisayara yüklendiğinde, bu Docker host bilgisayarlarını konteyner sağlama, yük dengeleme, devralma ve ölçekleme ve güvenlik yoluyla yönetmek için Kubernetes'i kullanabilirsiniz. Kubernetes ve Docker, konteynerleştirilmiş uygulamaları oluşturmak ve çalıştırmak için birlikte çalışırlar.

Kümeler ve Konteynerler ;

Küme; Bir küme, bir görevi tamamlamak için paralel olarak çalışan iki veya daha fazla bağlı düğüm kümesini ifade eder. Ayrı ayrı, paralel hale getirilebilir görevlere sahip iş yükleri düğümler arasında paylaşılır. Bu görevler, bir kümedeki tüm düğümlerin birleşik belleğini ve hesaplama gücünü kullanır. Düğümlerden biri, işi tahsis etmekten, sonuçları almaktan ve bir yanıt vermekten sorumlu olan ana düğüm görevi görür.

Küme Hesaplama Türleri;

Yüksek Kullanılabilirlik (HA) veya Devralma: Bir devralma kümesinde, yüksek kullanılabilirlik (HA) veya sürekli kullanılabilirlik (CA) sunmak için birden fazla düğüm aynı anda çalışır. Bir düğüm başarısız olursa, diğer düğüm minimum veya hiç kesinti olmadan sorumluluğunu üstlenir.

Yük Dengeleme: Yük dengeleme kümesinde, iş yükü tek bir düğümün aşırı zorlanmasını önlemek için düğümler arasında dağıtılır. Yük dengeleyici, düğüm arızalarını belirlemek ve gelen trafiği başka bir düğüme yönlendirmek için her düğümde periyodik sağlık kontrolleri gerçekleştirir. Yük dengeleme kümesi aynı zamanda yüksek kullanılabilirliğe sahip bir kümedir.

Yüksek Performanslı Bilgi İşlem: Yüksek performanslı bilgi işlem (HPC) kümesinde, düğümler görevleri paralel hale getirerek aşırı performans sağlayacak şekilde yapılandırılır.

Ölçekleme performansın en üst düzeye çıkarılmasına yardımcı olur.

Buluttaki Kümeler; Sanal makinelerde barındırılan düğüm kümeleridir ve genelde sanal özel bulutlarla birleştirilir. Bulut kümelemesi, bir küme kurmak için gereken çabayı ve zamanı en aza indirir. Bir bulut ortamında, kümeler ek kaynaklar veya VM'ler gibi örnekler kolayca eklenerek talep üzerine ölçeklenebilir. Bulut, gereksinimlerdeki değişikliklere göre altyapıyı yükseltme esnekliği de sağlar. Bulut birçok kullanılabilirlik bölgesinde düğüm dağıtımı yoluyla gecikmeyi ve dayanıklılığı artırır. Bulut kümelemesi kümenin kullanılabilirliğini, güvenliğini ve sürdürülebilirliğini en üst düzeye çıkarır.

Konteynerler ve Kümelerle İlişkileri; Konteynerler, uygulamaların farklı bilgi işlem ortamlarında güvenilir şekilde çalıştırılmasına yardımcı olur. Kuruluş ön ucu ve arka ucu mikro hizmetler olarak oluşturan web uygulaması geliştirdiklerini düşünelim. Bu web uygulamasını dağıtmak için, konteynerler buluttaki bir VM'e gönderilebilir. VM veya donanım arızalanırsa, trafik devralma sunucusu tarafından işlenene kadar uygulama erişilemez olur. Web uygulamalarının kullanılabilirliğini, ölçeklenebilirliğini ve performansını artırmak için, konteynerleştirilmiş uygulamaları bir kümedeki birkaç düğüme gönderiniz. Sonuç olarak da çeşitli düğümlerde çalışan konteynerler kaynak kullanımını en üst düzeye çıkarır. Tek düğüm arızası riski, bir kümedeki her düğüme bir konteyner örneği yerleştirilerek ortadan kaldırılabilir.

Konteyner Güvenlik Zorlukları; Kuruluşlar, özellikleri nedeniyle konteyner tabanlı platformları yaygın olarak benimsiyorlar. Fakat konteyner teknolojisinin hızlı büyümesi ve yayılması birçok güvenlik zorluğuna yol açmıştır.

Konteyner güvenliğiyle ilgili zorluklardan bazıları şöyledir;

Güvenlik açığı olan kaynak kodunun akışı; Konteynerler, geliştiricilerin görüntüleri bir depoda düzenli olarak güncellemek, depolamak ve kullanmak için kullandıkları açık kaynaklı platform oluşturur. Bu, güvenliği tehlikeye atabilecek güvenlik açıkları içerebilen muazzam bir kontrolsüz kodla sonuçlanır.

Geniş saldırı yüzeyi; Host bilgisayar işletim sistemi, bulutta veya şirket içinde birçok konteyner, uygulama, sanal makine ve veritabanından oluşur. Geniş saldırı yüzeyi, çok sayıda güvenlik açığı ve bunları tespit etmede artan bir zorluk anlamına gelir.

Görünürlük eksikliği; Bir konteyner motoru konteyneri çalıştırır, Linux çekirdeğiyle arayüz oluşturur, konteynerlerin eylemlerini kamufle eden, belirli konteynerlerin veya kullanıcıların etkinliklerini izlemeyi zorlaştıran başka bir soyutlama katmanı oluşturur.

Gizli bilgileri tehlikeye atmak; Kapsayıcıların herhangi bir hizmete erişmek için API anahtarları, kullanıcı adları veya parolalar gibi hassas bilgilere ihtiyacı vardır. Bu hassas bilgilere yasa dışı bir şekilde erişen saldırganlar güvenliği tehlikeye atabilir.

DevOps hızı; Kapsayıcılar derhal yürütülebilir ve yürütüldükten sonra durdurulup kaldırılabilir. Bu kaçaklık saldırganların herhangi bir kötü amaçlı kod yüklemeden saldırılar başlatmasına ve kendilerini gizlemesine yardımcı olur.

Gürültülü komşu kapsayıcılar; Bir kapsayıcı tüm kullanılabilir sistem kaynaklarını tüketebilir ve tüketebilir, bu da doğrudan diğer komşu kapsayıcıların çalışmasını etkileyerek hizmet reddi (DoS) saldırısı oluşturur.

Kapsayıcının host bilgisayara çıkışı; Kök olarak çalışan kapsayıcılar, ayrıcalık yükseltmesi yoluyla sınırlamayı kırabilir ve host bilgisayar işletim sistemine erişim sağlayabilir.

Ağ tabanlı saldırılar; Saldırganlar, çeşitli ağ tabanlı saldırılar başlatmak için etkin ham soketlere ve giden ağ bağlantılarına sahip başarısız kapsayıcıları kullanabilir.

Yalıtımı aşma; Saldırganlar, bir konteynerin güvenliğini tehlikeye attıktan sonra diğer konteynerlere veya ana bilgisayara erişim sağlamak için ayrıcalıkları artırabilir.

Ekosistem karmaşıklığı ; Konteynerler, birden fazla satıcı ve kaynak kullanılarak oluşturulur, dağıtılır ve yönetilir. Bu, farklı depolarından kaynaklandıkları için ayrı bileşenlerin güvenliğini sağlamayı ve güncellemeyi karmaşık hale getirir.

Konteyner Yönetim Platformları;

Amazon Elastic Container Service (Amazon ECS), Microsoft Azure Konteyner Örnekleri (Aci), Red Hat OpenShift Konteyner Platformu, Portainer, Rancher.

Çeşitli konteyner yönetim platformları;

Docker; Geleneksel uygulamalardan en son mikro hizmetlere kadar tüm uygulamaları oluşturmaya, yönetmeye ve güvence altına almaya, bunları bulut ortamlarına dağıtmaya yardımcı olan bağımsız konteyner platformudur. Docker, geliştiricilerin uygulamaları oluşturmasına ve dağıtmasına olanak tanıyan 100.000'den fazla konteyner görüntüsüne sahip en son konteyner içerik kütüphanesini ve ekosistemini içerir. Docker, uygulama yığınlarını kolayca paylaşmak ve yönetmek için Docker Desktop, Docker Engine ve Docker Hub gibi temel yapı taşlarına sahiptir.

Kubernetes Platformları ;

Kubernetes; Kubernetes, konteynerleştirilmiş uygulamaların dağıtımını, ölçeklenmesini ve yönetimini otomatikleştirmek için açık kaynaklı konteyner düzenleme motorudur. Kolay yönetim ve keşif için bir uygulamayı oluşturan farklı konteynerleri birkaç mantıksal birime gruplandırır. Kullanıcıların iş yüklerini bir yerden diğerine taşımak için şirket içi, hibrit veya bulut altyapısından yararlanmalarını sağlar. Kubernetes, konteyner görüntülerini yeniden oluşturmadan ve yığın yapılandırmasındaki sırları ifşa etmeden sırları ve uygulama yapılandırmalarını dağıtabilir ve güncelleyebilir. Örnekler; Amazon Elastic Kubernetes Service (EKS). Docker Kubernetes Service (DKS). Knative. IBM Cloud Kubernetes Service. Google Kubernetes Engine (GKE).

Sunucusuz " Serverless" Bilişim; Sunucusuz bilişim, konteynerler ve mikro hizmetler üzerine kurulu bulut tabanlı kurumsal uygulamaların dağıtımı için ortaya çıkan teknolojidir.

Sunucusuz bilişim, tüketicilere kullanım başına ödeme işlevselliği sunarak sunucuları başlatma ve durdurma yükünü ortadan kaldırır. Bu, geliştiricilerin odaklarını sunuculardan görevlere kaydırmalarına olanak tanır. Sunucusuz bilişim kullanan geliştiriciler, bulut bilişimde üst düzey uzmanlığa ihtiyaç duymadan inanılmaz avantajlar ve ölçeklenebilirlik elde eder.

Sunucusuz bilişim; sunucusuz mimari veya FaaS olarak da bilinir, bulut tabanlı uygulama mimarisine sahiptir. Burada uygulama altyapısı ve destekleyici hizmetler, bulut satıcısı tarafından ihtiyaç duyulduğunda sağlanır. Sunucusuz bilişim, uygulama dağıtım sürecini basitleştirir ve geliştiriciler tarafından sunucunun ve donanımın yönetilmesi ihtiyacını ortadan kaldırır.

Sunucusuz uygulamalar tamamen sunucusuz değildir. Sunucular gereklidir fakat geliştiricilere fiziksel olarak açık değildir. Sunucusuz mimaride, uygulama kodu üçüncü taraf bir hizmet sağlayıcı tarafından yönetilen bulutta barındırılan altyapıda çalışır.

Bulut hizmeti sağlayıcısı, sunucusuz altyapının sağlanması, ölçeklenmesi, yük dengelemesi, güvenliğinin sağlanmasından sorumludur. Bulut hizmeti sağlayıcısı işletim sistemlerinin ve altta yatan yazılım, hizmetlerin yama yönetiminden de sorumludur.

Avantajlar: Yüksek ölçeklenebilirlik ve esneklik. Daha hızlı dağıtım ve güncelleme. Azaltılmış altyapı maliyeti. Sunucu yönetimi yoktur. Kullanım başına ödeme vardır. Azaltılmış gecikme ve ölçekleme maliyeti vardır. Daha hızlı kaynak sağlama bulunmaktadır. Düşük arıza riski vardır. Sistem yönetimi yoktur.

Dezavantajlar: Artan güvenlik açığı vardır. Tedarikçi bağımlılığı bulunmaktadır. Durumsuzluğu yönetmede zorluklar vardır. Karmaşık uçtan uca uygulama testi vardır. Sunucusuz bilgi işlem için uzun süre çalışan süreçlerin uygunsuzluğu vardır.

Sunucusuz ve Konteynerler; Geliştiricinin sadece sunucusuz bilgi işlemi desteklemek için kod geliştirmesi ve yüklemesi gerekir. Tüm sağlama süreci bulut hizmet sağlayıcısı tarafından gerçekleştirilir. Çalışması tamamlandıktan sonra sunucusuz işlev bulut ortamı tarafından otomatik olarak yok edilir. Sunucusuz dağıtım sadece tüketilen kaynaklar için ücret alır. Sunucusuz işlevlerde zaman aşımı etkinleştirilir. Altta yatan host bilgisayar altyapısı geliştiriciler için şeffaftır. Sunucusuz işlevler geçici depolamayı desteklemez, bunun yerine, veriler nesne depolama ortamında saklanır. Sunucusuz işlevler sadece mikro hizmet uygulamaları için uygundur. Sunucusuz işlevler için dil seçimi bulut hizmeti sağlayıcısı tarafından kısıtlanmıştır.

Sunucusuz Bilgi İşlem Çerçeveleri; Arka uç sunucu yönetimi konusunda endişelenmeden kodu çalıştırmayı ve uygulamaları geliştirmeyi kolaylaştırır. Bu sunucusuz bilgi işlem benimsenmesi birçok sektörde hızla artmaktadır. Bazı sunucusuz bulut bilişim sağlayıcıları;

Microsoft Azure Functions; Kullanıcıların sunucuları sağlamadan ve yönetmeden kod çalıştırmasına olanak tanıyan sunucusuz bilişim platformudur. Tamamen otomatiktir ve iş yükü hacmine göre ölçekleme sağlar. Bu özellik, kullanıcıların arka uç sunucu yönetimini düşünmeden daha fazla değer eklemesine olanak tanır.

Diğer sağlayıcılar; AWS Lambda. Google Cloud Functions. IBM Cloud Functions. AWS Fargate. Alibaba Cloud Function Compute.

Bulut Bilişim Tehditleri; Çoğu kuruluş, optimize edilmiş ve verimli bilişim yoluyla maliyeti düşürdüğü için bulut teknolojisini benimser. Sağlam bulut teknolojisi, son kullanıcılara farklı türde hizmetler sunar fakat birçok kişi, saldırganların veri güvenliğini tehlikeye atmak, ağlara yasadışı erişim sağlamak vb. için yararlanabileceği kritik bulut güvenliği riskleri ve tehditleri konusunda endişe duymaktadır.

OWASP'nin En Önemli 10 Bulut Güvenliği Riski;

OWASP'nin En Önemli 10 Sunucusuz Güvenlik Riski; Sunucusuz bilişim, uygulama dağıtım sürecini basitleştirip geliştiricilerin sunucu ve donanımı yönetme ihtiyacını ortadan kaldırsa da, güvenlik tehditlerinin bir kısmını bulut servis sağlayıcılarına da iletir. Sunucusuz uygulamalar yine de bir kodu yürütür ve kod içindeki güvenlik açıkları, XSS, yapılandırılmış sorgu dili (SQL) enjeksiyonu, DoS ve bozuk kimlik doğrulama ve yetkilendirme gibi çeşitli uygulama düzeyindeki saldırılara geçit açabilir yani sunucusuz uygulamalar, geleneksel web uygulamalarıyla aynı tür saldırılara karşı savunmasızdır.

Bulut Bilişim Tehditleri;

Veri İhlali/Kaybı; Birden fazla istemciye sahip, uygunsuz şekilde tasarlanmış bulut bilişim ortamı, bir istemcinin uygulamasındaki kusurun saldırganların diğer istemcinin verilerine erişmesine izin verebilmesi nedeniyle yüksek veri ihlali riski altındadır. Veri kaybı veya sızıntısı büyük ölçüde bulut mimarisine ve işletimine bağlıdır.

Veri kaybı sorunları şunları içerir; Veriler silinir, değiştirilir veya bağlantısı kesilir yani kaybolur. Şifreleme anahtarları kaybolur, yanlış yerleştirilir veya çalınır. Uygunsuz kimlik doğrulama, yetkilendirme ve erişim kontrolleri nedeniyle verilere yasa dışı olarak erişilir. Veriler CSP tarafından kötüye kullanılır.

Alınacak önlemler; Veri bütünlüğünü korumak için bulutta depolanan verileri ve aktarım halindeki verileri şifreleyiniz. Güçlü anahtar oluşturma, depolama ve yönetimi uygulayınız. Hem tasarım hem de çalışma zamanı sırasında veri korumasını kontrol ediniz. Çok faktörlü kimlik doğrulamayı zorunlu kılınız. Veri kaybından kurtarmak için düzenli olarak güvenli veri yedeklemeleri gerçekleştiriniz. Verilere yönelik olası tehditleri tespit etmek için veri kaybı önleme (DLP) yazılımı dağıtınız. Verileri hassasiyet seviyelerine göre sınıflandırarak uygun güvenlik politikalarını uygulayınız. İnternet üzerinden veri dağıtımı gibi işlemleri kısıtlayan bulut erişim güvenlik aracılarını (CASB) dağıtınız. Veri erişimini birkaç ağ düğümüyle sınırlamak için mikro segmentasyon kullanınız. Veri ihlallerini tespit etmek ve azaltmak için ayrıcalıklı hesapları denetleyin ve izleyiniz. Ağa giren ve çıkan veri paketlerini filtrelemek için çevre güvenlik duvarı kullanınız.

Bulut Hizmetlerinin Kötüye Kullanımı ve Kötü Niyetli Kullanımı; Bulut bilişim ortamında zayıf kayıt sistemlerinin varlığı, saldırganların bulut hizmetlerine anonim erişim oluşturmasına, parola ve kritik kırma, gökkuşağı tabloları oluşturma, CAPTCHA çözme çiftlikleri başlatma, dinamik saldırı noktaları başlatma, bulut platformlarında istismarları barındırma, kötü amaçlı verileri barındırma, Botnet komuta veya kontrolü ve DDoS gibi çeşitli saldırılar gerçekleştirmesine olanak tanıyabilir.

Alınacak önlemler; Sağlam kayıt ve doğrulama süreci uygulayınız. Kötü amaçlı faaliyetler için istemci trafiğini izleyiniz. Genel kara listelerdeki kötü amaçlı ağları izleyiniz ve engelleyiniz. Bulut ödeme hizmetleri için gelişmiş kredi kartı dolandırıcılığı izleme ve koordinasyon sistemi kullanınız. Bulut hizmeti kötüye kullanımını önlemek için sürekli çalışan yüksek güvenlikli bulut hizmeti sağlayıcısı (CSP) kullanınız. Kullanıcıları kiracı başına güvenlik duvarları kullanarak aynı bulutta izole ediniz.

Güvensiz Arayüzler ve API'ler; Arayüzler veya API'ler müşterilerin bulut hizmetlerini yönetmesini ve bunlarla etkileşim kurmasını sağlar. Bulut hizmeti modelleri güvenlik açısından entegre olmalı ve kullanıcılar bu tür hizmetlerin kullanımı, uygulanması ve izlenmesindeki güvenlik risklerinin farkında olmalıdır.

Güvensiz arayüzler ve API riskleri şunları içerir; Kullanıcı tanımlı politikaları aşar. Kimlik bilgisi sızdırmazlığı. Kayıt ve izleme tesislerinde ihlal. Bilinmeyen API bağımlılıkları. Yeniden kullanılabilir parolalar/belirteçler. Yetersiz giriş verisi doğrulaması.

Alınacak önlemler; Bulut sağlayıcı arayüzlerinin güvenlik modelini analiz ediniz. Güvenli kimlik doğrulama ve erişim kontrolleri uygulayınız. Verileri aktarım sırasında şifreleyin ve API'lerle ilişkili bağımlılık zincirini anlayınız. Açık Bulut Bilişim Arayüzü (OCCI) ve Bulut Altyapısı Yönetim Arayüzü (CIMI) gibi güvenliğe odaklı API çerçevelerinden yararlanınız. Toplam görünürlük sağlamak ve API güvenlik risklerini belirlemek, azaltmak için ağ izleme ve analizini kullanınız. API anahtarlarını asla yeniden kullanmayınız. Tüm API trafiğinin şifrelendiğinden ve API çağrılarının tüm katmanlarda doğrulandığından emin olunuz.

Yetersiz Durum Tespiti; CSP'nin bulut ortamının bilinmemesi, güvenlik, şifreleme, olay müdahalesi ve sözleşmesel sorunlar, tasarım ve mimari sorunlar gibi operasyonel sorumluluklarda riskler oluşturur.

Alınacak önlemler; Buluta geçmeyi amaçlayan kuruluşlar, riskleri kapsamlı şekilde araştırmalı, CSP durum tespitini yapmalı, yeterli kaynaklara sahip olmalıdır. Tüm çalışanların güvenlik standartları ve kaynak bakımı konusunda eğitildiğinden emin olunuz. CSP'nin herhangi bir olay sırasında ilgili güvenlik önlemlerini uygulamak için uygun ekipleri istihdam ederek bir olay yanıt planı (IRP) sürdürmesini sağlayınız. Felaket kurtarma planları, şifreleme stratejileri, güvenlik politikaları konusunda CSP ile uygun iletişimi sürdürünüz. Şirketin üst düzey yönetimiyle yönetişimde uyulması gereken katı güvenlik politikalarını güçlendiriniz.

Paylaşılan Teknoloji Sorunları; laaS satıcıları, hizmetleri ölçeklenebilir şekilde sunmak için altyapıyı paylaşır. Altta yatan altyapı bileşenlerinin çoğu çok kiracılı bir ortamda önemli izolasyon özellikleri sunmaz. Bu, saldırganların bir istemcinin uygulamalarındaki güvenlik açıklarından yararlanabilmeleri durumunda diğer makinelere saldırmalarını sağlar. Bu boşluğu gidermek için sanallaştırma hipervizörleri, konuk işletim sistemleri ile bilgisayar korsanlarının altta yatan platformlar üzerinde yetkisiz kontrol elde etmelerine olanak tanıyan boşluklar içerebilecek fiziksel kaynaklar arasındaki erişime aracılık eder.

Alınacak önlemler; Kurulum/yapılandırma için en iyi güvenlik uygulamalarını uygulayınız. Yetkisiz değişiklikler/etkinlikler için ortamı izleyiniz. Yönetimsel erişim ve işlemler için güvenli kimlik doğrulama ve erişim denetimini teşvik ediniz. Yama ve güvenlik açığı giderme için hizmet düzeyi anlaşmalarını uygulayınız. Güvenlik açığı taramaları ve yapılandırma denetimleri gerçekleştiriniz. Bulut altyapısının, uygulamasının ve hizmetlerinin her düzeyinde sıkı güvenlik uygulayınız. Bulut ortamındaki her kullanıcı için trafiği izole etmek üzere çevre, host bilgisayar tabanlı, kiracı başına güvenlik duvarlarını kullanınız. Sadece kullanıcıların veya sahiplerin dosyalara erişebilmesini sağlamak için uygun dosya izinlerini ayarlayınız.

Bilinmeyen Risk Profili; Yazılım güncellemeleri, tehdit analizi, saldırı tespiti, güvenlik uygulamaları ve çeşitli diğer bileşenler bir kuruluşun güvenlik duruşunu belirler. Müşteri kuruluşları, bulutta donanım ve yazılım sahipliği ve bakımıyla daha az ilgilendikleri için dahili güvenlik prosedürleri, güvenlik uyumluluğu, yapılandırma sertleştirme, yama, denetim ve günlük kaydı vb. hakkında net bir resim elde edemezler. Fakat kuruluşlar dahili güvenlik prosedürleri, güvenlik uyumluluğu, yapılandırma sertleştirme, yama ve denetim ve günlük kaydı gibi konulardan haberdar olmalıdır.

Alınacak önlemler; Müşterilere geçerli günlüklerin ve verilerin ifşa edilmesi. Altyapı ayrıntılarının (yama seviyeleri, güvenlik duvarları gibi) kısmen/tamamen ifşa edilmesi. Gerekli bilgilerin izlenmesi ve uyarılması.

Eşzamanlanmamış Sistem Saatleri; Son sistemlerde saatlerin eşzamanlanmasındaki başarısızlık, otomatik görevlerin çalışmasını etkileyebilir. Bulut bilişim cihazlarının eşzamanlanmış veya eşleştirilmiş saatleri yoksa, zaman damgası yanlışlığı ağ yöneticisinin günlük dosyalarını herhangi bir kötü amaçlı etkinlik için doğru şekilde analiz edememesine neden olur. Eşzamanlanmamış saatler çeşitli diğer sorunlara neden olabilir. Para işlemleri veya veritabanı yedeklemeleri durumunda, eşleşmeyen zaman damgası önemli sorunlara veya tutarsızlıklara neden olabilir.

Alınacak önlemler; Ağ zaman protokolü (NTP) gibi saat eşzamanlama çözümleri kullanınız. Dışarıdan gelen tehditleri en aza indirmek ve ağdaki zaman doğruluğunu en üst düzeye çıkarmak için kuruluş güvenlik duvarının içine zaman sunucusu kurunuz. Ağ zaman sistemi, saatleri kurumsal ağ sunucusuyla senkronize etmek için de kullanılabilir.

Yetersiz Altyapı Tasarımı ve Planlaması; CSP ile müşteri arasındaki bir anlaşma, CSP'nin sunduğu hizmet kalitesini, örneğin kesinti, fiziksel ve ağ tabanlı yedeklilikler, standart veri yedekleme ve geri yükleme süreçleri, kullanılabilirlik dönemlerini belirtir. Bazen, CSP'ler bilgi işlem kaynaklarının yetersizliği veya zayıf ağ tasarımı nedeniyle talepteki hızlı artışı karşılayamayabilir ve bu da kabul edilemez ağ gecikmesine veya kararlaştırılan hizmet seviyelerini karşılayamamaya yol açabilir.

Alınacak önlemler; Talebi tahmin edin ve buna göre yeterli altyapı hazırlayınız. Bulut kullanımını planlamak için iş yüklerinin güvenilirliğine ve çalışma süresi gereksinimlerine güveniniz.

İstemci Güçlendirme Prosedürleri ile Bulut Ortamı Arasındaki Çakışmalar; Bazı istemci güçlendirme prosedürleri CSP ortamıyla çakışabilir ve istemci tarafından uygulanmasını imkansız hale getirebilir.

Bir bulut çok kiracılı bir ortam olduğundan, birçok müşterinin bir arada bulunması bulut sağlayıcıları için gerçekten de çatışmalara neden olur çünkü iletişim güvenliği gereksinimlerinin müşteriler arasında farklılaşma olasılığı yüksektir.

Alınacak önlemler; Müşterilerin gerçekleştirmesi gereken asgari eylemleri tanımlamak için sorumlulukların net şekilde ayrılmasını sağlayınız. Müşteri kuruluşunun gölge BT sorunundan etkilenen iş yükü, veri ve bulut hesaplarının uygun görünürlüğüne sahip olduğundan emin olunuz. Hem istemci tarafında hem de CSP tarafında periyodik olarak bulut VAPT testi uygulayınız.

Operasyonel ve Güvenlik Günlüklerinin Kaybı; Operasyonel günlüklerin kaybı, operasyonel değişkenlerin değerlendirilmesini zorlaştırır. Analiz için veri bulunmadığında sorunları çözme seçenekleri sınırlıdır. Güvenlik günlüklerinin kaybı, bilgi güvenliği yönetim programının uygulanmasını yönetmek için risk oluşturur. Sağlama altında depolama durumunda güvenlik günlüklerinin kaybı meydana gelebilir.

Alınacak önlemler; Etkili politikalar ve prosedürler uygulayınız. Operasyonel ve güvenlik günlüklerini düzenli olarak izleyiniz. Güvenli günlük yönetim sistemi kurun ve sürdürünüz. Günlük dosyası erişimi kısıtlanmalı ve kullanıcıların günlük dosyalarında dosya düzeyinde işlemler yapmasına izin verilmemelidir. Arşivlenmiş günlük dosyalarını uygun şekilde koruyun ve günlük verilerini sistemden merkezi günlük yönetim sunucularına aktarmak için güvenli protokoller uygulayınız.

Kötü Amaçlı İçeriden Kişiler; Kötü niyetli içeridekiler, bulut kaynaklarına yetkili erişimi olan ve bu erişimi bilerek aşabilecek, kötüye kullanabilecek ve kuruluş bilgilerinin gizliliğini, bütünlüğünü veya kullanılabilirliğini tehlikeye atabilecek hoşnutsuz mevcut/eski çalışanlar, yükleniciler veya diğer iş ortaklarıdır. Bulut kaynaklarına yetkili erişimi olan kötü niyetli içeridekiler, bulutta bulunan bilgileri tehlikeye atmak için erişimlerini kötüye kullanabilirler. Tehditler arasında itibar kaybı, üretkenlik kaybı ve mali hırsızlık yer alır.

Alınacak önlemler; Sıkı tedarik zinciri yönetimi uygulayın ve kapsamlı tedarikçi değerlendirmesi yapınız. Yasal sözleşmelerin bir parçası olarak insan kaynakları gereksinimlerini belirtiniz. Genel bilgi güvenliği ve yönetim uygulamaları ile uyumluluk raporlamasında şeffaflık talep ediniz. Güvenlik ihlali bildirim süreçlerini belirleyiniz.

Buluta Yasadışı Erişim; Zayıf kimlik doğrulama ve yetkilendirme kontrolleri, yasa dışı erişime yol açabilir ve böylece bulutta depolanan gizli ve kritik verileri tehlikeye atabilir.

Alınacak önlemler: Sağlam bilgi güvenliği (IS) politikası uygulayın ve buna uyunuz. Müşterilerin CSP'lerin IS politikasını ve prosedürlerini denetlemesine/incelemesine izin veriniz.

Ortak Kiracı Faaliyetleri Nedeniyle İş İtibarının Kaybı; Bu tehdit, kaynak ve itibar izolasyonunun eksikliği, hipervizörlerdeki güvenlik açıkları vb. nedeniyle ortaya çıkar. Kaynaklar bulutta paylaşılır bu nedenle bir ortak kiracının kötü niyetli faaliyeti diğerinin itibarını etkileyebilir ve bu da zayıf hizmet sunumu, veri kaybı vb. ile sonuçlanarak kuruluşun itibarını düşürebilir.

Alınacak önlemler; Riski azaltmak ve kaynakların izolasyonunu sağlamak için iyi bilinen ve verimli CSP seçiniz. CSP tarafından kullanılan sanallaştırma ve izolasyon tekniklerini kontrol ediniz. Çok kiracılı bir mimaride yer alan riskleri değerlendirin. CSP'ler işlevleri kiracılar arasında ayırmalıdır.

Ayrıcalık Yükseltmesi; Kodlama hataları ve tasarım kusurları gibi erişim tahsis sistemindeki hatalar, müşterinin, üçüncü tarafın veya çalışanın gerekenden daha fazla erişim hakkı elde etmesine neden olabilir. Bu tehdit; kimlik doğrulama, yetkilendirme ve hesap verebilirlik açıkları, kullanıcı sağlama, sağlamayı kaldırma açıkları, hiper yönetici açıkları, belirsiz roller ve sorumluluklar, yanlış yapılandırma vb. nedeniyle ortaya çıkar.

Alınacak önlemler; İyi bir ayrıcalık ayırma şeması kullanınız. Varsa yeni keşfedilen ayrıcalık yükseltme açıklarını düzeltmek için yazılım programlarını düzenli olarak güncelleyiniz.

Bulut hizmeti ortamlarında yapılandırılan tüm kimlik ve erişim yönetimi (IAM) düzenlemelerini ve rollerini düzenli olarak denetleyiniz. Shodan gibi standart ağ tarayıcılarını ve güvenlik sorgu araçlarını kullanarak, ortamı açığa çıkan API'ler açısından tarayın ve bulut hizmetlerini şüpheli ağ trafiği veya kullanıcı davranışları açısından izleyiniz.

Doğal Afetler; Coğrafi konuma ve iklime bağlı olarak, veri merkezleri bulut hizmetlerini etkileyebilecek sel, yıldırım ve deprem gibi doğal afetlere maruz kalabilir.

Alınacak önlemler; Kuruluşun güvenli alanda bulunduğundan emin olunuz. Farklı konumlarda veri yedekleri tutunuz. Doğal afetlerden kaynaklanan uzun vadeli riskinizi azaltmaya veya ortadan kaldırmaya yardımcı olan azaltma önlemlerini uygulayınız. Etkili iş sürekliliği ve felaket kurtarma planı hazırlayınız.

Donanım Arızası; Veri merkezlerindeki anahtarlar, sunucular, yönlendiriciler, erişim noktaları, sabit diskler, ağ kartları ve işlemciler gibi donanım arızaları bulut verilerine erişilemez hale getirebilir. Donanım arızalarının çoğu sabit disk sorunlarından kaynaklanır. Sabit disk arızalarının izlenmesi ve düzeltilmesi düşük düzeydeki karmaşıklıkları nedeniyle çok zaman alır. Donanım arızası, son kullanıcılara düşük performans sunumuna yol açabilir ve işletmeye zarar verebilir.

Alınacak önlemler; Fiziksel güvenlik programlarını uygulayın ve sürdürünüz. Önceden yüklenmiş bekleme donanım aygıtları zorunludur. Gerekli verileri tanımlama ve yedekleme sürecini otomatikleştiriniz. Tek bir arıza noktasından kaçınmak için yedek iş yükü bileşenlerini sağlayınız.

Tedarik Zinciri Arızası; Eksik ve şeffaf olmayan kullanım koşulları, çapraz bulut uygulamaları tarafından oluşturulan gizli bağımlılıklar, uygunsuz CSP seçimi, tedarikçi yedekliliğinin olmaması vb. nedenlerle meydana gelebilir. Bulut sağlayıcıları belirli görevleri üçüncü taraflara dış kaynak olarak verir. Bu nedenle de bulutun güvenliği her bir bağlantının güvenliği ve üçüncü taraflara olan bağımlılığın derecesiyle doğru orantılıdır. Zincirdeki bir kesinti, veri gizliliği ve bütünlüğünün kaybına, hizmetlerin kullanılamamasına, SLA'nın ihlaline, müşteri talebini karşılayamama nedeniyle ekonomik ve itibar kayıplarına ve ardışık arızalara yol açabilir.

Alınacak önlemler; Tedarik zinciri risklerini azaltmak için bir dizi kontrol tanımlayınız. Güvenilir karşı tarafın arızasından kaynaklanan hasarı sınırlamak için sınırlama planı geliştiriniz. Tedarik zincirinin tehlikeye atılmış unsurlarını tespit etmek için görünürlük mekanizmaları oluşturunuz. Karşı tarafların güvenlik duruşu hakkında bilgi sunan üçüncü tarafları tedarik etmeyi düşününüz. Tedarik zinciri arıza saldırılarından bulut ortamını korumak için yetenekli profesyonellerden oluşan özel ekip kullanınız. Herhangi bir değişiklik için tedarik zincirinin güvenilirliğini ve gerçekliğini korumak için blok zinciri teknolojisi, Hyperledger gibi gelişmiş doğrulama teknolojilerini kullanınız. Tedarik zincirindeki kritik finansal işlemler için dijital imzalar, çok faktörlü kimlik doğrulama (MFA), güvenli oturum yönetimi gibi gelişmiş güvenlik politikalarını uygulayınız. Şüpheli faaliyetler için her iletişim bağlantısını izlemek ve tedarik zinciri boyunca uygun güvenliği sağlamak için sıfır güven mimarisini kullanınız.

Ağ Trafiğini Değiştirme; Bulutta ağ trafiği, ağların sağlanması veya kaldırılması sırasındaki kusurlar veya iletişim şifrelemesindeki güvenlik açıkları nedeniyle değiştirilebilir. Ağ trafiğinin değiştirilmesi, gizli verilerin ve iletişimlerin kaybolmasına, değiştirilmesine veya çalınmasına neden olabilir.

Alınacak Önlem; Herhangi bir anormallik varsa onu bulmak için özel araçlar kullanarak ağ trafiği analizi gerçekleştiriniz.

Yalıtım Arızası; Çoklu kiracı ve paylaşılan kaynaklar, bulut bilişimin özellikleridir. Farklı kiracılar arasında depolama, bellek, yönlendirme ve itibarın güçlü izolasyonu veya bölümlendirilmesi eksiktir. İzolasyon başarısızlığı nedeniyle saldırganlar verilere yasadışı erişim elde etmek için diğer bulut müşterilerinin işlemlerini kontrol etmeye çalışır.

Alınacak önlem; Belleği, depolamayı ve ağ erişimini izole tutmak esastır.

Bulut Sağlayıcı Edinimi; CSP edinimi taktiksel kayma olasılığını artırabilir ve bağlayıcı olmayan sözleşmeleri riske atabilir. Bu, güvenlik gereksinimlerinin ele alınmasında bir zorluk oluşturabilir.

Alınacak önlemler; Bir bulut sağlayıcısı seçerken dikkatli olunuz. Riski ortadan kaldırmak için saygın ve popüler CSP tercih ediniz. CSP'ler tarafından sunulan veri politikalarını dikkatlice doğrulayınız. CSP'nin güvenlik yeteneklerini inceleyiniz. Hizmet düzeyi sözleşmelerinin (SLA) görev hedefleri, başarı ölçümleri, veri toplama, ölçümler hakkında bilgi sağladığından emin olunuz.

Yönetim Arayüzü Tehlikesi; Bulut sağlayıcılarının müşteri yönetim arayüzleri, internet üzerinden çok sayıda kaynağa erişimi kolaylaştırır. Bu, özellikle uzaktan erişim ve web tarayıcısı güvenlik açıklarıyla birleştirildiğinde güvenlik risklerini artırır. Yönetim arayüzü ihlali, uygunsuz yapılandırma, sistem ve uygulama güvenlik açıkları, yönetim arayüzüne uzaktan erişim vb. nedeniyle ortaya çıkar.

Alınacak önlemler; Belleği, depolamayı ve ağ erişimini izole tutmak esastır. Uzaktan erişimle ilgili tehditleri azaltmak için güvenli protokoller kullanınız. Web tarayıcısı güvenlik açıklarını önlemek için yamaları düzenli olarak güncelleyiniz. Kurumsal ağdan izole edilmiş yönetim düzeyi arayüzleri için özel sanal yerel alan ağı (VLAN) dağıtınız. Sıkı güvenlik önlemlerini sağlayın ve atlama sunucularını kullanarak güvenilmeyen ağlar üzerinden genel erişim gerektiren arayüzlere odaklanınız.

Ağ Yönetimi Hatası; Zayıf ağ yönetimi, hizmetleri ve güvenliği etkileyen ağ tıkanıklığına, yanlış bağlantıya, yanlış yapılandırmaya, kaynak izolasyonunun eksikliğine vb. yol açar.

Alınacak önlemler; Yeterli güvenlik politikasının uygulandığından emin olunuz. Proaktif ağ yönetimi teknikleri kullanınız. Yeni teknolojileri güncellemeye devam edin ve kuruluşunuz için neyin daha iyi çalışabileceğini analiz ediniz. Ağ tasarımının ve sistem yapılandırmalarının BT yönetimini takip ettiğinden, kuruluşun hizmet ve kapasite gereksinimleriyle eşleştiğinden emin olunuz. Her türlü güvenli ve güvenli olmayan bağlantıdan gelen trafik için sıkı ağ izleme ve analizi uygulayınız. Wi-Fi ile kurumsal ağ arasındaki tüm ağ trafiğinin güvenli VPN ağı üzerinden iletildiğinden emin olunuz. Ağ çevresinin dışında konuşlandırılmış kurumsal bulut ağında daha iyi görünürlük için bulut ağı güvenlik izleme araçlarını kullanınız.

Kimlik Doğrulama Saldırıları; Zayıf kimlik doğrulama mekanizmaları ve tek faktörlü kimlik doğrulama mekanizmalarının içsel sınırlamaları, saldırganların bulut bilişim sistemlerine yetkisiz erişim elde etmesine olanak tanır.

Alınacak önlemler; Parolaları güvenli tutmak için güçlü parola politikaları uygulayınız. Gerektiğinde iki faktörlü kimlik doğrulamayı zorunlu kılınız. Erişimi kontrol ederek ve sınırlayarak yetkisiz erişimi engellemek için IP beyaz listelemeyi kullanınız. Rollere göre belirli kaynaklara erişim için minimum kullanıcı haklarını uygulamak için en az ayrıcalık ilkesini kullanınız. Kullanıcıların bulut kaynaklarına erişimini yönetmek için sağlam kimlik ve erişim yönetimini (IAM) etkinleştiriniz.

VM Düzeyinde Saldırılar; Bulut bilişim, VMware, Xen, Virtual Box ve vSphere dahil olmak üzere çeşitli satıcılar tarafından sunulan sanallaştırma teknolojilerini kapsamlı şekilde kullanır. Bu teknolojilere yönelik tehditler, hipervizörlerdeki güvenlik açıklarından kaynaklanır.

Alınacak önlemler; Saldırıyı kullanın algılama/önleme sistemleri (IDS/IPS) ve bilinen VM düzeyindeki saldırıları azaltmak için güvenlik duvarı uygulayınız. VM düzeyindeki saldırılara karşı koruma sağlamak için yüksek düzeyde yapılandırılmış, güncellenmiş hipervizörler, hipervizörlerin etrafında sanal alanlar kullanınız. Yüksek düzeyde sanal makine izolasyonu sunan Yüksek Güvence Platformu'nu (HAP) kullanınız. Hiçbir geçerli VM kullanıcısının diğer kullanıcılarla donanım paylaşmadığından emin olunuz.

Kilitlenme" Lock In"; Araçların, prosedürlerin, standart veri biçimlerinin, uygulamaların ve hizmet taşınabilirliğinin olmaması nedeniyle istemcinin bir CSP'den diğerine veya şirket içi sistemlere geçiş yapamamasını yansıtır. Bu tehdit, uygunsuz CSP seçimi, eksik ve şeffaf olmayan kullanım koşulları, standart mekanizmaların eksikliği vb. ile ilgilidir.

Alınacak önlemler; Standartlaştırılmış bulut API bulutu kullanmak faydalı olabilir. Tek CSP'ye güvenmek yerine çoklu bulut veya hibrit bulut stratejisi kullanınız. Taşınabilir ve gevşek bağlı uygulamalar tasarlayınız. Tescilli yapılandırmaların neden olduğu risklerden kaçınmak için DevOps araçlarını uygulayınız. İlk anlaşmayı imzalamadan önce net bir çıkış stratejisi oluşturunuz.

Lisanslama Riskleri; CSP bulutta dağıtılan yazılımı örnek başına ücretlendirirse kuruluş önemli lisanslama ücreti ödemek zorunda kalabilir. Bu nedenle kuruluş, bulut sağlayıcı ortamında bulunan yazılım varlıkları üzerinde her zaman mülkiyeti elinde tutmalıdır. Lisanslama riskleri, eksik ve şeffaf olmayan kullanım koşulları nedeniyle ortaya çıkar.

Alınacak önlemler; Etkili lisanslama geliştirmek ve genel maliyetleri belirlemek için CSP'nin mevcut lisanslama durumunu inceleyiniz. Maliyetleri, lisans kullanımını vb. yönetmek için tek bir merkezi platform kullanınız. Kullanılmayan ve bağlanmayan bulut kaynaklarını ortadan kaldırınız.

Yönetim Kaybı; Bulut altyapısını kullanırken, müşteriler güvenliği etkileyebilecek sorunlar konusunda CSP'lere kontrol verir. SLA'lar CSP'yi bu tür hizmetleri sağlamaya mecbur etmeyebilir ve böylece güvenlik savunmalarında boşluk bırakabilir. Bu tehdit; rollerin ve sorumlulukların belirsizliğinden, güvenlik açığı değerlendirme süreçlerinin eksikliğinden, SLA'larda çelişen vaatlerden, sertifika şemalarının ve yargı yetkisinin eksikliğinden ve denetimin bulunmamasından kaynaklanır. Yönetim kaybı; güvenlik gereksinimlerine uyulmaması, verilerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin olmaması, zayıf performans ve hizmet kalitesi vb. ile sonuçlanır.

Alınacak önlemler; SLA'ların yürütülmesi için dikkatli çaba sarf ediniz. Hassas verileri korumak ve performansı iyileştirmek için katı yönetim kurallarını uygulayınız. Şirket içi ve bulut operasyonları için birleşik bir yönetim politikası sürdürünüz. Yönetim politikasına uyumu doğrulamak için otomasyonu kullanınız.

Şifreleme Anahtarlarının Kaybı; Güvenli iletişim veya sistem erişimi için gereken şifreleme anahtarlarının kaybı, potansiyel saldırganlara yetkisiz varlıklara erişme olanağı sağlar. Bu tehdit, zayıf anahtar yönetimi ve oluşturma tekniklerinden kaynaklanır.

Alınacak önlemler; Şifreleme anahtarlarını şifrelenmiş verilerle birlikte saklamayınız. Anahtarları oluşturmak için gelişmiş şifreleme standardı (AES) ve Rivest—Shamir—Adleman (RSA) gibi güçlü algoritmalar kullanınız. Anahtar depolarına erişimi kısıtlayın ve anahtar depolarına erişimi kontrol etmek ve yönetmek için rol ayrımı gibi politikalar uygulayınız. Şifreleme anahtarları için güvenli yedekleme ve kurtarma planı uygulayınız. Anahtarları farklı amaçlar için yeniden kullanmayınız. Şifreleme anahtarlarını güvence altına almak için bir donanım güvenlik modülü (HSM) kullanınız.

Yetki Alanı Değişikliklerinden Kaynaklanan Riskler; Bulutlar, müşteri verilerini bazıları yüksek riskli olabilecek birden fazla yetki alanında depolayabilir. Yüksek riskli ülkelerdeki yerel yetkililer veri merkezlerine baskın düzenleyebilir; veriler veya bilgi sistemleri zorunlu ifşaya veya ele geçirilmeye tabi tutulabilir. Verilerin yetki alanındaki değişiklikler, hükümet veya diğer kuruluşlar tarafından bilgi sisteminin engellenmesine veya el konulmasına yol açabilir. Müşteriler, bulutu benimsemeden önce yetki alanındaki belirsizlikleri göz önünde bulundurmalıdır çünkü veri depolama için yerel yasalar hükümetin özel verilere erişimini sağlayabilir.

Alınacak önlem; Verilerin depolanabileceği ve işlenebileceği yetki alanları hakkında bilgi edinin ve varsa ilgili riskleri değerlendiriniz.

Kötü Amaçlı Araştırmalar veya Taramalar Yapmak; Saldırganların gizlilik ve bütünlüğün kaybına, hizmetlerin ve verilerin kullanılabilirliğinin kaybına yol açabilecek hassas bilgileri toplamasına olanak tanır.

Alınacak önlemler; Güvenlik duvarları ve saldırı tespit sistemleri gibi çeşitli güvenlik mekanizmaları dağıtınız. Hipervizörü ve VM'leri aynı ağa yerleştirmeyiniz. VLAN oluşturarak hipervizör yönetimini ve uzaktan erişim trafiğini ayırınız. Hipervizörün çalıştığı ağdan gelen ping ve traceroute yanıtlarını engelleyiniz. Hipervizörün yönetim arayüzlerini düzgün şekilde yapılandırınız.

Bilgisayar Ekipmanının Çalınması; Girişte akıllı kart erişimi gibi fiziksel parametreler üzerindeki yetersiz kontroller nedeniyle ekipman hırsızlığı meydana gelebilir ve bu da fiziksel ekipman ve hassas verilerin kaybına yol açabilir.

Alınacak önlemler; Güvenlik görevlileri işe almak, kapalı devre televizyon (CCTV) kapsamı, alarmlar, kimlik kartları ve uygun çitleme gibi fiziksel güvenlik önlemlerini uygulayınız. Belirli değişiklikleri yapmak ve en son fiziksel güvenlik önlemlerini sürdürmek için güvenliği düzenli olarak değerlendiriniz. Biyometrik girişler gibi farklı gelişmiş teknolojilerin uygulanmasıyla fiziksel erişimi kontrol ediniz. Saldırıyı önlemek ve güvenlik ekibini en kısa sürede uyarmak için izinsiz giriş alarm sistemleri uygulayınız. Sunucu odasının her zaman kilitli olduğundan ve odaya sadece yetkili personelin girmesine izin verildiğinden emin olunuz. Fiziksel güvenliği artırmak için raf tipi sunucular kullanın, taşınmasını imkansız hale getiriniz. Yedekleme cihazlarını ve sürücülerini tesis dışı bir konumda güvence altına alınız.

Bulut Hizmetinin Sonlandırılması veya Arızalanması; Karlılıksızlık veya anlaşmazlıklar nedeniyle bulut hizmetinin sonlandırılması, son kullanıcılar kendilerini yasal olarak korumadıkları takdirde veri kaybına yol açabilir. Rekabet baskısı, finansal destek eksikliği, yetersiz iş stratejileri gibi birçok faktör bulut hizmetinin sonlandırılmasına veya başarısızlığa uğramasına yol açabilir. Bu tehdit, zayıf teslimat ve hizmet kalitesi, yatırım kaybına neden olur. CSP'ye dış kaynaklı olarak verilen hizmetlerdeki arızalar, CSP'nin müşterilerine karşı görevlerini ve taahhütlerini yerine getirme yeteneğini etkileyebilir.

Alınacak önlemler; Bulut sağlayıcılarının hizmet sonlandırma durumunda net ve denetlenebilir prosedürler tanımlamasını sağlayınız. Bu, anlaşma şartlarına göre verilerin müşteriye güvenli şekilde geri aktarılmasını garanti etmeyi içerir. CSP'nin hizmet sonlandırmadan önce günlük ve denetim dosyaları gibi müşteri verilerinin temizleme işlemini gerçekleştirdiğinden emin olunuz. Veri saklama ve silme çıkış süreciyle ilgili olarak CSP'lerle katı hizmet anlaşmaları yapınız. Anlaşmalar için destekleyici yargı yasalarından yararlanınız. CSP'nin hizmet sonlandırıldıktan sonra herhangi bir veri ihlali veya koklama "sniff" olmadan güvenli veri silme prosedürüne sahip olduğundan emin olunuz.

Mahkeme Celbi ve E-Keşif; Müşteri verileri ve hizmetleri yetkililerden veya üçüncü taraflardan gelen durdurma talebine tabi tutulur. Bu tehdit, uygunsuz kaynak izolasyonu, birden fazla yargı alanında veri depolama ve yargı alanları hakkında bilgi eksikliği nedeniyle oluşur.

Alınacak önlemler; CSP'yi dikkatlice seçin ve uygun güvenliğin sağlandığından emin olunuz. Hizmet sözleşmesini iyice inceleyiniz. Kayıt yönetimi, erişilebilirlik, müşteri desteği, yasal politikalar, hesap verebilirlik, gizlilik, sözleşmenin uzunluğu, fesih prosedürleri vb. konuları ele almalıdır. Koordineli eKeşif planı yürütünüz. Bir çıkış stratejisi düşününüz.

Uygunsuz Veri İşleme ve İmha Bulut altyapısına sınırlı erişim nedeniyle CSP'ler tarafından izlenen veri işleme ve imha prosedürlerini tespit etmek zordur. Müşteriler veri silme talebinde bulunduğunda, veriler gerçekten silinemeyebilir çünkü ; verilerin birden fazla kopyası kullanılmıyor olsa bile saklanır. İmha edilecek diskte diğer müşterilerin verileri de bulunabilir. Buluttaki çoklu kiracı ve donanım kaynaklarının yeniden kullanımı, müşteri verilerini risk altında tutar.

Alınacak önlemler; Müşteri verilerini güvence altına almak ve verilerin tüm kopyalarla birlikte birincil sunuculardan tamamen kaldırıldığından emin olmak için VPN'leri kullanınız. Verileri, silindikten sonra izlere erişilse bile okunamayacak hale getirmek için şifreleyiniz. Verileri eskidikten sonra tüm yedekleme aygıtlarından güvenli şekilde tutmak ve imha etmek için veri depolama süresi ayarlayınız. Kullanılan aygıt ve imha tekniğine karşılık gelen veri imha süreci uygulayınız. Veri temizliğini gerçekleştirmek ve prosedürü standartlaştırmak için strateji uygulayınız. Sağlam denetim izi geliştirmek ve tüm imha sürecini müşterilerle doğrulamak için veri temizliğinin tüm adımlarını belgelendiriniz.

Yedekleme Verilerinin Kaybı/Değiştirilmesi; Saldırganlar, SQL enjeksiyonu ve güvenli olmayan kullanıcı davranışı gibi güvenlik açıklarını kullanarak buluttaki veri yedeklerine yasadışı erişim sağlayabilir. Saldırganlar erişim sağladıktan sonra veritabanlarında depolanan verileri silebilir veya değiştirebilir. Yedekleme verilerinin kaybı durumunda veri geri yükleme prosedürlerinin olmaması hizmet seviyelerini riske atar.

Alınacak önlemler; Kayıp verileri almak için uygun veri geri yükleme prosedürlerini veya araçlarını kullanınız. Yedekleme için tek bir depolama yöntemine veya ortamına güvenmekten kaçınınız. Bunun yerine 3-2-1 modelini uygulayınız.

Uyumluluk Riskleri; CSP'nin gerekliliklere uyum sağladığına dair kanıt sağlayamaması, bulut yönetimini üçüncü taraflara dış kaynak olarak vermesi veya müşteri tarafından denetim yapılmasına izin vermemesi durumunda standartlara ve yasalara uyum sağlamaya çalışan kuruluşlar risk altında olabilir. Uyumluluk riskleri, denetimler ve endüstri standardı değerlendirmeleri üzerindeki yönetişim eksikliğinden kaynaklanır. Bu nedenle, müşteriler erişilebilirlik, kimlik yönetimi ve görevlerin ayrılması konusunda sağlayıcıların süreçlerinden, prosedürlerinden ve uygulamalarından habersizdir.

Alınacak önlemler; Bulut sağlayıcıları, müşteri verilerinin tehlikeye atılmamasını sağlamalıdır. Bulut sağlayıcılarının iç denetim süreçlerini gözden geçiriniz.

Ekonomik Sürdürülebilirlik Reddi (EDoS); Bulut sistemindeki ödeme yöntemi "Kullanım yoksa fatura da yoktur"; müşteriler istekte bulunduğunda, CSP onlardan kaydedilen verilere, isteklerin süresine, ağdaki veri aktarım miktarına ve tüketilen CPU döngüsü sayısına göre ücret alır. Ekonomik hizmet reddi finansal kaynakları yok eder; en kötü durumda, bu müşteri iflasına veya başka ciddi ekonomik etkilere yol açabilir. Bir saldırgan bulut sunucusunu kötü amaçlı bir hizmetle meşgul ederse veya çok fazla hesaplama gücü ve depolama alanı tüketen kötü amaçlı bir kod çalıştırırsa, meşru hesap sahibinden CPU kullanımının birincil nedeni tespit edilene kadar ücret alınır.

Alınacak önlem; Uygulama ve ağ katmanı DDoS saldırılarını azaltmak için istemci bulmacası yaklaşımından yararlanarak, tepkisel/talep üzerine, bulut içi EDoS azaltma hizmeti (temizleme hizmeti) kullanınız.

Güvenlik Mimarisi Eksikliği; Şirketlerin çoğu BT yeteneklerini genel buluta taşıyor, bu nedenle siber tehditlere karşı uygun güvenlik stratejilerini dahil etmek büyük bir zorluktur. BT altyapısını buluta taşımadan önce uygun güvenlik mimarileri ve stratejileri geliştirmek önemlidir.

Alınacak önlemler; Güvenlik mimarinizin iş hedefleriniz ve amaçlarınızla uyumlu olduğundan emin olunuz. Tehdit modelini düzenli olarak güncelleyiniz. Gerçek güvenlik duruşunun periyodik güvenlik değerlendirmesini yapınız.

Hesapların Ele Geçirilmesi; Kuruluşlar için son derece kritik bir tehdit, buluttaki çalışan hesaplarının tehlikeye atılmasıdır. Bir saldırgan, kullanıcı hesabını tehlikeye atarak buluta erişim sağlarsa, bulut sunucularında depolanan tüm bilgilere hiçbir iz bırakmadan erişebilir.

Saldırganlar, kullanıcı kimlik bilgilerini elde etmek için kimlik avı ve parola kırma gibi teknikler kullanır. Bu saldırılar, itibar kaybına, marka değerinin düşmesine, hassas bilgilerin ifşa edilmesine vb. neden olarak işletme operasyonlarını ciddi şekilde etkiler.

Alınacak önlemler; Kullanıcı hesaplarına sadece asgari düzeyde erişim ayrıcalıkları veriniz. Derinlemesine savunma stratejileri uygulayın ve kimlik ve erişim yönetimi (IAM) çözümleri yükleyiniz. Hassas bilgileri bulut sunucularında şifreleyin ve saklayınız. Çok faktörlü kimlik doğrulama gibi güçlü kimlik doğrulama mekanizmaları uygulayınız. Artık gerekli olmayan kimlik bilgilerini ve kullanıcı hesaplarını kaldırınız. Son derece hassas bilgilere gereksiz erişimi tespit edin ve geri çekiniz. Üçüncü taraflar tarafından bulut kaynaklarına erişimi kontrol ediniz. Sadece yetkili kullanıcıların erişim sağlamasını sağlamak için bulut belirteçlemeyi uygulayınız. Tüm kullanıcı hesapları için parola oluşturmak ve yönetmek için parola yöneticisinin kullanıldığından emin olunuz.

Konteyner Güvenlik Açıkları; Konteyner; operasyonel verimlilik, üretkenlik ve tutarlılık sunarak bulut bilişimde daha büyük rol üstlenmiştir. Çeşitli bulut hizmetlerinin benimsenmesi, bulut konteynerlerine yönelik tehditleri ve saldırıları artırmıştır. Konteynerler, başarılı saldırı durumunda daha geniş sonuçlarla karşı karşıya kalır. Saldırı hızla tekrarlanabilir ve bu da saldırganların aşırı sayıda kurbanının avı olmasına yol açabilir.

Kubernetes Güvenlik Açıkları; Kubernetes'in uygulanması, BT liderlerinin şirket içi ve genel bulut ortamları arasında köprü kurmasını kolaylaştırmıştır. Kubernetes, buluttaki konteynerler içinde katmanlama ve uygulama ölçekleme olanağı sağlayarak daha taşınabilir, üretken altyapı sağlar. Kubernetes'in artırılmış kullanımı, temeldeki güvenlik açıklarını hedef alan kritik siber saldırıları kolaylaştırır.

Bulut Saldırıları;

Sosyal Mühendislik Kullanarak Hizmet Gaspı; Hesap veya hizmet gaspında, saldırgan CSP'nin veya istemcinin kimlik bilgilerini kimlik avı, sosyal mühendislik ve yazılım açıklarından yararlanarak çalar. Saldırgan, çalınan kimlik bilgilerini kullanarak bulut bilişim hizmetlerine erişim sağlar ve veri gizliliğini, bütünlüğünü ve kullanılabilirliğini tehlikeye atar. Sosyal mühendislik, büyük ölçüde insan etkileşimine dayanan ve genelde rutin güvenlik prosedürlerini ihlal etmeleri için başkalarını kandırmayı içeren teknik olmayan saldırı türüdür. Saldırganlar, şifreleri sıfırlamaları için CSP'leri veya şifreleri ifşa etmek için bulut hizmetlerine erişmeleri için BT personelini hedef alabilir. Şifreleri elde etmenin diğer yolları arasında şifre tahmini, tuş kaydı kötü amaçlı yazılımları, şifre kırma tekniklerini uygulama, kimlik avı e-postaları gönderme yer alır. Sosyal mühendislik saldırıları, müşteri ve kredi kartı verilerinin, kişisel bilgilerin, iş planlarının, personel verilerinin, kimlik hırsızlığının vb. ifşa edilmesiyle sonuçlanır.

Saldırgan önce sahte bulut hizmeti oturum açma sayfası oluşturur ve bulut hizmeti kullanıcısına kötü amaçlı bir bağlantı gönderir. Kullanıcı, bağlantıyı aldıktan sonra üzerine tıklar ve oturum açma kimlik bilgilerini girer. Bunun sahte oturum açma sayfası olduğunu fark etmezler. Kullanıcı enter tuşuna bastığında, saldırgan kullanıcının oturum açma kimlik bilgilerini alırken, sayfa onu otomatik olarak orijinal bulut hizmeti oturum açma sayfasına yönlendirir. Şimdi, saldırgan çalınan kullanıcı kimlik bilgilerini kullanarak bulut hizmetine oturum açar ve kötü amaçlı etkinlik gerçekleştirir.

Alınacak önlemler; Hesap kimlik bilgilerini kullanıcılar ve hizmetler arasında paylaşmayınız. Mümkün olan her yerde sağlam iki faktörlü veya çok faktörlü kimlik doğrulama mekanizması uygulayınız. Personeli sosyal mühendislik saldırılarını tanımaları için eğitiniz. Çerçevelenen güvenlik politikalarına kesinlikle uyunuz. Verileri internet üzerinden iletmeden önce şifreleyiniz. Hizmetlere erişimi kısıtlamak için "en az ayrıcalık" ilkelerini kullanınız. Sorumlulukları CSP yöneticileri ve yöneticileriniz arasında bölünüz. Bu, diğerlerinin tüm güvenlik katmanlarına ücretsiz erişimini kısıtlar.

Ağ Koklama Kullanarak Hizmet Ele Geçirme; Ağ koklama, iki bulut düğümü arasındaki ağ trafiğinin kesilmesini ve izlenmesini içerir. Şifrelenmemiş hassas veriler ağ üzerinden iletim sırasında yüksek risk altındadır. Saldırganlar, parolalar ve oturum çerezleri gibi hassas verileri, evrensel açıklama keşfi ve bütünlüğü (UDDI), basit nesne erişim protokolü (SOAP) ve web hizmeti açıklama dili (WSDL) dosyaları gibi diğer web hizmetiyle ilgili güvenlik yapılandırma verilerini yakalamak için paket koklayıcıları kullanır.

Kullanıcı bulut hizmetlerine erişmek için oturum açma kimlik bilgilerini girdiğinde, saldırgan, Wireshark ve Capsa Portable Network Analyzer gibi paket koklayıcıları kullanarak ağ üzerinden iletim sırasında kimlik bilgilerini/çerezleri koklayabilir. Saldırgan daha sonra çalınan kimlik bilgileri aracılığıyla bulut hizmetlerine giriş yapar.

Alınacak önlemler; Hassas verileri ağ üzerinden şifreleyiniz. Yapılandırma dosyalarındaki hassas verileri şifreleyiniz. Karışık modda çalışan ağ arabirimi denetleyicilerini (NIC) tespit ediniz. Kimlik bilgilerini içeren web trafiğinin SSL/TLS ile şifrelendiğinden emin olunuz.

Yan Kanal Saldırıları veya Misafirler Arası VM İhlalleri; Saldırganlar, kötü amaçlı sanal makineyi hedef bulut sunucusunun yakınına yerleştirerek bulutu tehlikeye atabilir ve ardından yan kanal saldırısı başlatabilir. Saldırganın kötü amaçlı bir VM'yi hedef bulut sunucusunun yakınına yerleştirerek bulutu tehlikeye atabilir. Saldırgan, VM'yi hedef VM ile aynı fiziksel host bilgisayarda çalıştırır ve paylaşılan fiziksel kaynaklardan (işlemci önbelleği) yararlanır. Daha sonra da kurbanın kimlik bilgilerini çalmak için kriptografik anahtarları/düz metin sırlarını çıkarmak üzere yan kanal saldırıları (zamanlama saldırısı, veri kalıcılığı, akustik kriptoanaliz, güç izleme saldırısı, diferansiyel hata analizi) başlatır. Yan kanal saldırıları; herhangi bir yerleşik kullanıcı tarafından uygulanabilir ve esas olarak paylaşılan teknoloji kaynaklarındaki güvenlik açıklarıyla ilgilidir. Saldırgan çalınan kimlik bilgilerini kurbanı taklit etmek için kullanır.

Yan Kanal Saldırısı için Alınacak Önlemler; Bulut bilişimin bulut sunucusu arka ucunda sanal güvenlik duvarı uygulayınız. Bu, saldırganın kötü amaçlı sanal makineler yerleştirmesini önler. Rastgele şifreleme ve şifre çözme uygulayınız (RSA, 3DES, AES algoritmaları kullanarak verileri şifreler). Erişim sağlayabilecek tehlikeye atan vektörleri önlemek için işletim sistemi görüntülerini ve uygulama örneklerini kilitleyiniz.

Bulut sistemleri için yerel işlem izleme verilerini ve günlüklerini ayarlayarak, toplayarak yerel belleğe, herhangi bir hipervizör işlemine veya paylaşılan donanım önbelleğine tekrarlanan erişim girişimlerini kontrol ediniz. Uygulamaları ve işletim sistemi bileşenlerini, bellek önbelleği gibi paylaşılan kaynaklara tutarlı ve öngörülebilir şekilde erişecek şekilde kodlayınız. Bu kodlama stili, saldırganların zamanlama istatistikleri ve diğer davranışsal nitelikler gibi hassas bilgileri toplamasını önler.

Sarmalama "Wrapping" Saldırısı; Saldırganların mesajın gövdesini kopyalayıp meşru kullanıcı olarak sunucuya gönderdiği TLS katmanındaki SOAP mesajının çevirisi sırasında sarmalama saldırısı gerçekleştirilir. Kullanıcılar tarayıcı aracılığıyla VM'lerinden bir istek gönderdiğinde, istek önce web sunucusuna ulaşır. Ardından, yapısal bilgi içeren bir SOAP mesajı oluşturulur ve mesajın iletilmesi sırasında tarayıcıyla değiştirilir. Mesaj iletilmesi gerçekleşmeden önce tarayıcının XML belgesini imzalaması gerekir. İmza değerlerini belgeye eklemesi gerekir. SOAP başlığı hesaplamadan sonra hedef için gerekli bilgileri içermelidir. Sarmalama saldırısında; saldırgan aldatmacası, SOAP mesajının TLS'ye çevrilmesi sırasında gerçekleşir. Saldırgan, mesajın gövdesini kopyalar ve meşru kullanıcı olarak sunucuya gönderir. Sunucu, imza değeri aracılığıyla kimlik doğrulamasını kontrol eder ve bütünlüğünü doğrular. Saldırgan buluta izinsiz girebilir ve bulut sunucularının olağan işleyişini kesintiye uğratmak için kötü amaçlı kod çalıştırabilir.

Alınacak önlemler; SOAP mesajlarını algılamak için XML şema doğrulamasını kullanınız. XML şifreleme spesifikasyonunda kimliği doğrulanmış şifreleme uygulayınız. İmza doğrulaması ve iş mantığı işlevleri arasındaki arayüzü iyileştiriniz. XPath ifadesini belirtmek için CryptoCoverageChecker kesicisini kullanınız.

Buluttaki Adam (MITC) Saldırısı; MITM saldırılarının gelişmiş bir versiyonudur. MITM saldırılarında, saldırgan iki taraf arasındaki iletişimi kesen ve manipüle eden stismar kullanırken, MITC saldırıları veri ihlali, komuta ve kontrol (C&C), veri sızdırma ve uzaktan erişim için Google Drive veya DropBox gibi bulut dosya senkronizasyon hizmetlerini kötüye kullanarak gerçekleştirilir. Senkronizasyon belirteçleri bulutta uygulama kimlik doğrulaması için kullanılır fakat kötü amaçlı trafiği normal trafikten ayırt edemezler. Saldırganlar, MITC saldırıları gerçekleştirmek için bulut hesaplarındaki bu zayıflığı kötüye kullanır.

Saldırgan kurbanı kandırarak kurbanın sürücüsüne saldırganın senkronizasyon belirtecini yerleştiren kötü amaçlı bir kod yükler. Ardından saldırgan kurbanın senkronizasyon belirtecini çalar ve kurbanın dosyalarına erişmek için kullanır. Daha sonra saldırgan kötü amaçlı belirteci kurbanın orijinal senkronize belirteciyle geri yükler, Drive uygulamasını orijinal durumuna döndürür ve tespit edilemez.

Alınacak önlemler: MITC'lere yol açabilecek sosyal mühendislik saldırılarını tespit etmek için e-posta güvenlik ağ geçidi kullanınız. Belirteç son kullanma tarihi politikalarını güçlendirmek bu tür saldırıları önleyebilir. Kötü amaçlı yazılımları tespit edebilen ve silebilen etkili antivirüs yazılımı kullanınız. Oluşturulan örneklerle ilgili anormallikleri tespit etmek için bulut trafiğini izlemek üzere bulut erişim güvenlik aracısını (CASB) uygulayınız. Bulut senkronizasyon belirteci kötüye kullanımının önemli belirtilerini tespit etmek için çalışan etkinliklerini izleyiniz. Bulutta depolanan verileri şifreleyin ve şifreleme anahtarlarının aynı bulut hizmeti içinde depolanmadığından emin olunuz. İki faktörlü kimlik doğrulamayı uygulayınız.

Bulut Hopper Saldırısı; Yönetilen hizmet sağlayıcıları (MSP) ve müşterileri üzerinde tetiklenir. Saldırı başarıyla uygulandıktan sonra saldırganlar hedef MSP'nin ve küresel kullanıcılarının/müşterilerinin fikri mülkiyetine ve kritik bilgilerine uzaktan erişim sağlayabilir. Saldırganlar, üretim, hükümet organları, sağlık ve finans gibi endüstriyel kuruluşlara ait hassas verilere daha fazla erişim sağlamak için bulut ortamındaki bir sistemden diğerine ağda yatay olarak hareket eder.

Saldırganlar, gizli bilgileri elde etmek için personel üyelerinin veya bulut hizmeti şirketlerinin kullanıcı hesaplarını tehlikeye atmak amacıyla özel yapım kötü amaçlı yazılımlarla hedefli kimlik avı e-postaları başlatır. Saldırganlar, keşif ve bilgi toplama için PowerShell ve PowerSploit komut tabanlı betiklemeyi kullanabilir. Saldırganlar toplanan bilgileri aynı ağa bağlı diğer sistemlere erişmek için kullanır. Bu saldırıyı gerçekleştirmek için saldırganlar meşru etki alanlarını taklit eden sitelere ve bellekte bulunan, buradan çalıştırılan dosyasız kötü amaçlı yazılımlara yönelik C&C'yi kullanır.

Saldırganlar, geçerli bir hizmet sağlayıcıyı taklit ederek güvenlik mekanizmalarını ihlal eder ve kuruluşun ve bağlı müşterilerin kurumsal verilerine tam erişim elde eder. Saldırgan hedef MSP sağlayıcısına sızar ve uzaktan erişim elde etmek için kötü amaçlı yazılım dağıtır. Saldırgan daha sonra hedef müşteri profillerine kendi MSP hesabıyla erişir, müşteri verilerini sıkıştırır ve bunları MSP'de depolar. Saldırgan daha sonra bilgileri MSP'den çıkarır ve bu bilgileri hedef kuruluşa ve kullanıcılara daha fazla saldırı başlatmak için kullanır.

Alınacak önlemler; Kimlik bilgilerinin tehlikeye atılmasını önlemek için çok faktörlü kimlik doğrulamayı uygulayınız. Anormal olaylar veya faaliyetler durumunda müşteriler, CSP'ler arasında karşılıklı koordinasyonu sağlayınız. Müşterilerin farkında olduğundan ve bulut hizmeti politikalarını takip ettiğinden emin olunuz. Saldırının etkisini azaltmak ve herhangi bir veri ihlaline karşı savunma sağlamak için veri kategorizasyonunu kullanınız. Güvenliği artırmak ve bulut atlama saldırılarını önlemek için atlama sunucularını kullanınız.

Bulut Kripto Madenciliği; Kripto Madenciliği, kurbanın bilgisayarının gizlice dijital para madenciliği yapmak için yetkisiz kullanılmasıdır. Kripto madenciliği saldırıları, hem dış saldırganları hem de içteki kötü niyetli kişileri içeren oldukça kazançlıdır. Bu saldırıyı gerçekleştirmek için saldırganlar, bulut yanlış yapılandırmaları, tehlikeye atılmış web siteleri ve istemci veya sunucu tarafı güvenlik açıkları gibi saldırı vektörlerinden yararlanır.

Saldırgan, web sayfasına veya web sayfası tarafından yüklenen üçüncü taraf kitaplığına kötü amaçlı kripto madenciliği yükünü enjekte etmek için yanlış yapılandırılmış bulut örneklerini kullanır. Ardından, saldırgan kurbanı kötü amaçlı web sayfasını ziyaret etmeye ikna eder ve kurban web sayfasını açtığında, JavaScript kullanarak kurbanın tarayıcısında kripto madencisini otomatik olarak çalıştırır.

CoinHive ve Cryptoloot gibi JavaScript tabanlı kripto madencileri kullanarak saldırganlar, CoinHive'a bağlantı kullanarak kötü amaçlı kripto madenciliği betiklerini meşru web sitelerine kolayca yerleştirebilirler. Saldırganlar; kodlama, yönlendirmeler ve karartma gibi çeşitli gizleme teknikleri kullanarak kötü amaçlı kripto madenciliği betiğini gizleyerek bu saldırıyı daha karmaşık hale getirir. Yük için yapılandırma genelde dinamik veya sabit kodludur. Kripto madenciliği saldırıları web siteleri, uç noktalar, tüm bulut altyapısı üzerinde ciddi etkilere neden olabilir.

Bulut kripto madenciliği saldırılarının adımları; İlk adımda saldırgan, kötü amaçlı kripto madenciliği betiği yerleştirerek bulut hizmetini tehlikeye atar. İkinci adımda ise kurban tehlikeye atılan bulut hizmetine bağlandığında, kripto madenciliği betiği otomatik olarak yürütülür. Üçüncü adımda, kurban, saldırgan adına kripto para madenciliğine safça başlar ve blok zincirine yeni bir blok ekler. Dördüncü adımdaysa blok zincirine eklenen her yeni blok için saldırgan, kripto para birimi paraları biçiminde yasadışı şekilde ödül alır.

Alınacak önlemler; Güçlü parola politikası uyguladığınızdan emin olunuz. Verilerin üç farklı kopyasını her zaman farklı yerlerde ve bir kopyasını da site dışında saklayınız. Web sunucularını ve cihazları düzenli olarak yamaladığınızdan emin olunuz. Bulut sunucularına erişimi güvence altına almak için parolalar yerine şifreli SSH anahtar çiftleri kullanınız. Güvenlik duvarında CoinBlocker URL ve IP Kara Listesi/kara delik uygulamasını uygulayınız. Kötü amaçlı etkinlikleri erken aşamada tespit etmek ve azaltmak için web sayfası belge nesne modeli (DOM) ve JavaScript ortamlarının gerçek zamanlı izlenmesini kullanınız. Buluttaki en son antivirüs, kötü amaçlı yazılım önleme ve reklam engelleyici araçlarını kullanınız. CoinHive'ın madencilik betiğine benzer betikleri taramak ve sonlandırmak için tarayıcı uzantıları uygulayınız. Cihazlardaki herhangi bir kötü amaçlı uygulamayı tespit etmek için uç nokta güvenlik yönetimi teknolojisini kullanınız. Şirketin web siteleri tarafından kullanılan tüm üçüncü taraf bileşenlerini inceleyiniz. CPU kaynak kötüye kullanımını, madenciliği ve koklama etkinliklerini tespit edebilen gelişmiş ağ izleme araçlarını kullanınız. Çoğu kripto madencisinin saldırı dağıtımı için rastgele bulut kaynaklarını kullanması nedeniyle bulut kaynak kullanım faturalarındaki ani fiyat artışlarını asla ihmal etmeyiniz. Gün sonunda tüm bulut örneklerinin ve hizmetlerinin başarıyla sonlandırıldığından emin olunuz. Aksi takdirde, kripto korsanları için bir giriş noktası haline gelebilirler.

Cloudborne Saldırısı; Cloudborne, saldırganların kötü amaçlı arka kapıyı yazılımına yerleştirmesini sağlayan çıplak "bare" metal bulut sunucusunda bulunan güvenlik açığıdır. Kurulan arka kapı, sunucu yeni istemcilere veya onu laaS olarak kullanan işletmelere yeniden tahsis edilse bile devam edebilir. Fiziksel sunucular tek bir istemciyle sınırlı değildir ve bir istemciden diğerine taşınabilir. Geri alma işlemi sırasında, yazılım yeniden flaşı (fabrika varsayılan ayarı, belleğin tamamen silinmesi vb.) düzgün şekilde uygulanmazsa, arka kapılar yazılımda etkin kalabilir ve sunucu boyunca seyahat edebilir.

Saldırganlar, fiziksel erişim olmadan sağlama, işletim sistemini yeniden yükleme, akıllı platform yönetim arayüzü (IPMI) aracılığıyla sorun giderme gibi uzaktan yönetim faaliyetleri için kullanılan çıplak metal sunucunun temel yönetim kontrolündeki (BMC) yazılımı üzerine yazmak için süper mikro donanımdaki güvenlik açıklarından yararlanır. BMC sunucuları uzaktan kontrol etme, sistemi yeni müşterilere sağlama gücüne sahip olduğundan, saldırganlar onu birincil hedef olarak seçer. Çıplak metal bulut sunucusundaki güvenlik açıkları ve uygunsuz aygıt yazılımı yeniden flaşlama, saldırganların arka kapı kalıcılığını kurmasının ve sürdürmesinin önünü açabilir. Daha sonra, kötü amaçlı arka kapılar saldırganların donanıma doğrudan erişim sağlamalarına, güvenlik mekanizmalarını atlatarak yeni müşterinin faaliyetlerini izleme, uygulamayı/sunucuyu devre dışı bırakma, verileri ele geçirme gibi faaliyetler gerçekleştirmelerine olanak tanır. Bu faaliyetler saldırganların hedefe fidye yazılımı saldırıları başlatmalarına olanak tanır.

Alınacak önlemler; CSP'ler aygıt yazılımını güncel tutmalıdır. Sunucu aygıt yazılımını yeni müşterilere atanmadan önce temizleyiniz. Sunucuyu dağıtmadan önce implantlar ve arka kapılar açısından doğrulayınız. Düzenli olarak donanım yazılımı güvenlik açıklarını kontrol ediniz. CSP'ler teslimattan önce fiziksel donanımın kurcalanıp kurcalanmadığını doğrulamalıdır.

Örnek Meta Veri Hizmeti (IMDS) Saldırısı; Örnek meta veri hizmeti (IMDS), bir örnek, ilişkili ağı ve örneği çalıştırmak üzere yapılandırılmış yazılım hakkında bilgi sağlar. IMDS bir örnekle ilişkili roller için kimlik bilgileri üretir. Atanan role veya politikaya göre, örnekte yapılandırılmış yazılım bulut depolamasındaki kaynaklara da erişebilir. Saldırganlar, hedef uygulama sunucusundaki sıfır günlük güvenlik açığından yararlanarak veya yöneticiler tarafından uygulanan ters proksi aracılığıyla sızdırılan bilgileri kullanarak IMDS saldırıları gerçekleştirir.

IMDS saldırısı gerçekleştiren saldırganların temel amacı; örnekleri tehlikeye atarak ağ kaynaklarına yetkisiz erişim elde etmektir. Saldırganlar sıfır günlük güvenlik açığından veya ters proksi tarafından sızdırılan kimlik bilgilerinden başarıyla yararlanabilirlerse, bulut örneğine bağlanabilir, kullanıcı verileri ve bu örnekle ilişkili çeşitli roller gibi hassas bilgileri elde edebilirler; bu bilgiler, erişim ve bulut depolamada bulunan kaynakları kötüye kullanma veya değiştirmedir.

Saldırı Nasıl Başlatılır; İlk olarak, saldırgan hedef uygulama sunucusunda uygulanan sıfır günlük güvenlik açığını veya ters proksiyi kullanır. Saldırgan daha sonra sunucuda çalışan bulut örneğini tehlikeye atar ve örneğin meta verilerini edinir. Daha sonra, saldırgan bulut kaynaklarına erişim sağlamak için elde edilen kimlik bilgilerini kullanır.

Alınacak Önlemler: IMDSv1 yerine IMDSv2 kullanınız. Gerekmediğinde IMDS'yi kapatınız. Gerekmiyorsa roller bir örneğe atanmamalıdır; gerekiyorsa rollere en az ayrıcalığı atayınız. Şüpheli kullanıcıların IMDS erişimini kısıtlayınız.

Önbellek Zehirli Hizmet Reddi (CPDoS)/İçerik Dağıtım Ağı (CDN) Önbellek Zehirleme Saldırısı; CPDoS veya CDN önbellek zehirleme saldırısında, saldırganlar kötü amaçlı veya hatalı içerikle yanıt vermesi için orijinal web sunucusunu kandırmak için kötü biçimlendirilmiş veya büyük boyutlu HTTP istekleri oluştururlar; bu içerik dağıtım ağı (CDN) sunucularında önbelleğe alınabilir. Bu nedenle de kötü amaçlı veya hata tabanlı içerik, meşru kullanıcılara iletildiği CDN sunucusunda önbelleğe alınır ve hedef ağda DoS saldırısına neden olur.

CPDoS saldırısı, CDN korumalı sunucuların yanlış yapılandırılması nedeniyle meydana gelebilir ve bu da orijinal sunucudan hata yanıtları içeren web içeriğinin veya sayfalarının depolanmasıyla sonuçlanır. Saldırganlar, kullanıcıların bulut hizmetlerine erişmesini önlemek için önbellek zehirleme tekniklerini kullanabilir.

DoS Saldırısı Gerçekleştirmek İçin CDN Önbellek Zehirlenmesi Adımları; Öncelikle saldırgan, kötü amaçlı HTTP başlığı içeren istek göndererek hedef web sunucusundan kaynak ister. Ardından aracı CDN sunucusunda istenen web sayfasının veya kaynağın önbelleği yoksa, istek kötü amaçlı olduğu için hata döndüren kaynak web sunucusuna iletilir. Üçüncü adım olarka hata sayfası, CDN sunucusundaki gerçek sayfa yerine önbelleğe alınır. Dördüncü adımda artık kullanıcılar, kaynağa erişmeye çalıştıklarında orijinal web sayfası yerine "404 Bulunamadı" gibi önbelleğe alınmış hata sayfası alırlar. Beşinci adımda CDN sunucusu aynı hata sayfasını diğer bağlı kullanıcılara da yayınlayarak meşru hizmetlere onlar için ulaşılamaz hale getirir.

Alınacak önlemler; HTTP hata sayfalarının önbelleğe alınmasını önlemek için CDN'yi yapılandırınız. Web uygulaması güvenlik duvarı (WAF) uygulayınız. Hata sayfalarını önbellekten izleyin ve ortadan kaldırınız.

Cloud Snooper Saldırısı; Hedef sunucuyu tehlikeye atmak ve gizlice hassas verileri çıkarmak için AWS güvenlik gruplarında (SG) tetiklenir. Saldırganlar bu saldırıyı zayıf yapılandırılmış güvenlik duvarından veya herhangi bir temel güvenlik açığından yararlanarak gerçekleştirir. Saldırganlar, güvenlik duvarları gibi güvenlik kontrollerini atlatmak ve hedef sunucu üzerinde uzaktan kontrol elde etmek için çeşitli teknikler kullanır. Saldırganlar, sadece 80 veya 443 hedef portlarına sahip trafiğe izin vermeyi amaçlayan SG'lerdeki bir zayıflıktan yararlanır. Saldırganlar, trafik filtrelerindeki zayıflıkları, tedarik zinciri saldırılarını veya SSH'yi zorla zorlayarak kök araç takımlarını yükler. Saldırganlar, meşru trafik gibi görünen komut ve kontrol (C2) paketlerini iletir. Daha sonra da kurulan kök araç takımı paketleri durdurur ve komutları arka kapı Truva Atı'na yönlendirir. Truva Atı, uzak makineden alınan C2 komutlarına göre kötü amaçlı etkinlikleri yürütür.

Cloud Snooper Saldırısında Yer Alan Adımlar; 1. adım olarak saldırganlar, çevre güvenlik duvarını kandırarak, hedef sunucuya normal trafikle birlikte özel olarak oluşturulmuş C2 paketleri gönderir. 2. Adım olarak güvenlik duvarı gelen tüm paketleri doğrular ve tüm paketler hedef bağlantı noktaları olarak 80 ve 443'ü içerdiğinden geçmelerine izin verir. 3. Adım olarak rootkit'teki dinleyici sunucuya giden trafiği keser ve paketleri kaynak bağlantı noktaları 1010, 2020, 6060, 7070, 8080 veya 9999 olan paketlerle yeniden oluşturur. Daha sonra dinleyici bu paketleri rootkit tarafından kurulan arka kapıya iletir. 4. Adım olarak arka kapı Truva Atı artık C2 komutlarına göre eylemler gerçekleştirir ve verileri hedef sunucudan topladıktan sonra rootkit'e geri gönderir. 5. Adım olarak Rootkit, güvenlik duvarını atlatmak, saldırgana veri sızdırmak için alınan paketleri 80 ve 443 kaynak portlarıyla yeniden yapılandırır. Burada, güvenlik duvarı rootkit tarafından tekrar kandırılır.

Alınacak önlemler; Ağ trafiğinin düzenli olarak analiz edildiğinden emin olunuz. Web sunucularının düzenli olarak yamalandığından emin olunuz. Katmanlı güvenlik modeli kullanınız.

Altın SAML Saldırısı "Golden SAML Attack"; SAML saldırıları, kullanıcıların kimlik doğrulaması ve yetkilendirilmesi için SAML protokolünü kullanan Active Directory Federasyon Hizmeti (ADFS) gibi bulut ağlarındaki kimlik sağlayıcılarını hedeflemek için uygulanır. Saldırganlar başlangıçta kimlik sağlayıcının kullanıcı profiline yönetici erişimi elde eder ve SAML iddialarını manipüle ederek sahte SAML belirteçleri veya yanıtları oluşturmak için belirteç imzalama sertifikalarını kullanır. Bu erişim; oturum ele geçirme, ayrıcalık yükseltme, daha önce istismar edilen güvenlik açıkları veya saldırılar yoluyla yanal hareket yoluyla elde edilebilir.

SAML Saldırı Senaryosu; 1. Adım olarak saldırgan ADFS sunucusuna (kimlik sağlayıcı) erişim sağlar ve doğrulamayı imzalayan sertifikayı ve şifreleme anahtarını çalar.2. adım olarak kullanıcı gerekli hizmete erişmeye çalıştığında, hizmet sağlayıcı isteği kimlik sağlayıcıya yönlendirir. 3. Adım olarak saldırgan yönlendirme isteğini engeller ve çalınan anahtarları kullanarak sahte doğrulama değerleriyle SAML yanıtını geri gönderir. 4. Adım olarak hizmet sağlayıcı saldırganın hedef kullanıcı hesabıyla ilişkili federasyon hizmetlerine erişmesine izin verir.

Alınacak önlemler; Kullanıcı etkinliklerini sürekli olarak izleyiniz. Çok faktörlü kimlik doğrulamayı ve güçlü parolaları kullanınız. En düşük ayrıcalıklı erişimi uygulayınız. Bir saldırının belirtileri için ortamı analiz ediniz. Sertifikaları zamanında güncelleyiniz.

Diğer Bulut Saldırıları;

Cross-Site Scripting (XSS) Saldırısı Kullanarak Oturum Ele Geçirme; Saldırganlar, kullanıcı kimlik doğrulama sürecinde kullanılan çerezleri çalmak için XSS uygular. Bu, web sitesine kötü amaçlı kod enjekte etmeyi içerir ve bu kod daha sonra tarayıcı tarafından yürütülür. Saldırganlar, çalınan çerezleri kullanarak etkin bilgisayar oturumlarını istismar eder ve böylece verilere yetkisiz erişim elde eder. Saldırganlar ayrıca oturum kimliklerini tahmin edebilir veya koklayabilir.

Saldırgan bulut sunucusunda kötü amaçlı betiğin bulunduğu web sayfası barındırır. Bir kullanıcı saldırgan tarafından barındırılan sayfayı görüntülediğinde, kötü amaçlı betiği içeren HTML kullanıcının tarayıcısında çalışır. Kötü amaçlı betik kullanıcının çerezlerini toplar ve gönderir, kullanıcıyı saldırganın sunucusuna yönlendirir.

Alınacak önlemler; Güvenli soket katmanları (SSL), güvenlik duvarları, antivirüsler ve kod tarayıcıları kullanmak, bir bulutu oturum ele geçirmeye karşı koruyabilir.

Session Riding kullanarak Session Hijacking; Saldırganlar, yetkisiz komutları iletmek için siteler arası istek sahteciliği yaparak web sitelerini istismar eder. Session Riding'de saldırganlar, e-posta göndererek veya kullanıcıları gerçek hedef siteye giriş yaparken kötü amaçlı web sayfasını ziyaret etmeye kandırarak etkin bilgisayar oturumunu sürer.

Kullanıcılar kötü amaçlı bağlantıya tıkladığında, web sitesi isteği kullanıcı daha önce kimliğini doğrulamış gibi yürütür. Kullanılan komutlar arasında kullanıcı verilerini değiştirme veya silme, çevrimiçi işlemler gerçekleştirme, parolaları sıfırlama vb. yer alır.

Kullanıcı güvenilir siteye giriş yaparak yeni oturum oluşturur. Sunucu, oturum için oturum tanımlayıcısını web tarayıcısındaki çerezde depolar. Saldırgan, kurbanı kendisi tarafından kurulan kötü amaçlı web sitesini ziyaret etmeye ikna eder. Saldırgan daha sonra çalınan oturum çerezi kullanarak kullanıcının tarayıcısından bulut sunucusuna bir istek gönderir.

Alınacak önlemler: Tarayıcınızın ve web sitelerinizin giriş bilgilerini kaydetmesine izin vermeyiniz. HTTP yönlendirme başlığını kontrol edin ve POST işlerken URL parametrelerini yok sayınız.

Alan Adı Sistemi (DNS) Saldırıları; DNS sunucusu, insan tarafından okunabilen alan adını düğümler arasındaki iletişimleri yönlendiren sayısal IP adresine çevirir. Saldırganlar, internet kullanıcılarından kimlik doğrulama bilgilerini elde etmek için DNS saldırıları gerçekleştirir.

DNS Saldırı Türleri;

DNS Zehirlenmesi: Kullanıcıları, DNS sunucusunu veya kullanıcının sistemindeki DNS önbelleğini zehirleyerek sahte web sitesine yönlendirmeyi içerir.

Siber Çömelme "Cybersquatting": CSP'ye benzer alan adı kaydederek kimlik avı dolandırıcılığı yapmayı içermektedir.

Alan Adı Kaçırma: CSP alan adını çalmayı içermektedir.

Alan Adı Kesme: Süresi dolmuş alan adını kaydetmeyi içermektedir.

Saldırgan DNS önbellek zehirlenmesi gerçekleştirerek kullanıcıları sahte web sitesine yönlendirir. Burada, kullanıcı dahili DNS sunucusundan DNS bilgilerini sorgular. Dahili DNS sunucusu daha sonra ilgili bulut sunucusundan DNS bilgilerini ister. Bu noktada da saldırgan bulut sunucusundan gelen DNS yanıtını engeller, sahte web sitesinin IP'sini içeren DNS yanıtını dahili DNS sunucusuna gönderir. Böylece, dahili DNS sunucusu önbelleği sahte web sitelerinin IP'leriyle kendini günceller ve kullanıcıları otomatik olarak bu web sitelerine yönlendirir.

Alınacak önlemler: Alan adı sistemi güvenlik uzantılarını (DNSSEC) kullanmak, DNS tehditlerinin etkilerini bir dereceye kadar azaltır.

SQL Enjeksiyon Saldırıları; SQL, veritabanı yönetim sistemleri için tasarlanmış programlama dilidir. SQL enjeksiyon saldırısında, saldırganlar savunmasız veritabanı uygulamaları çalıştıran SQL sunucularını hedef alır. Saldırganlar, veritabanına ve diğer gizli bilgilere yetkisiz erişim elde etmek için standart SQL koduna kötü amaçlı kod ekler. Bu tür saldırılar genelde uygulamalar girdiyi dinamik SQL ifadeleri oluşturmak için kullandığında gerçekleştirilir. Dahası, saldırganlar veritabanı içeriklerini manipüle edebilir, hassas verileri alabilir, uzaktan sistem komutlarını yürütebilir, ek suç faaliyetleri için web sunucusunun kontrolünü ele geçirebilir. Saldırgan kullanıcı tarafından erişilen bulut web uygulamasında SQL enjeksiyonu gerçekleştirir ve bulutta barındırılan hassas bilgilere erişim elde eder.

Alınacak önlemler: Kullanıcı girdisini temizlemek için filtreleme teknikleri kullanınız. Giriş uzunluğunu, aralığını, biçimini ve türünü doğrulayınız. Sunucuları ve uygulamaları düzenli olarak güncelleyin ve yamalayınız. Veritabanı izleme teknolojilerini ve saldırı önleme sistemlerini (IPS) kullanınız. Bulut tabanlı web uygulaması güvenlik duvarı uygulayınız.

Kripto Analiz Saldırıları; Güvensiz veya eski şifreleme, bulut hizmetlerini kripto analize karşı savunmasız hale getirmektedir. Bulutta bulunan veriler, kötü niyetli kullanıcılar tarafından erişildiğinde okunmasını önlemek için şifrelenebilir.

Kriptografik algoritma uygulamalarındaki kritik kusurlar güçlü şifrelemeyi zayıf veya bozuk hale getirebilir. Kriptografiyi kırmak için yeni yöntemler mevcuttur. Şifrelenmiş verilerden, istemcilerin sorgu erişim kalıplarını izleyerek, erişilen konumları analiz ederek kısmi bilgiler de elde edilebilir.

Alınacak önlemler: SSH anahtarları ve DNSSEC'ler gibi kriptografik materyallere sağlamlık sağlamak için kriptografik olarak güvenli rastgele sayılar üreten rastgele sayı üreteçleri kullanınız. Hatalı kriptografik algoritmalar kullanmayınız. Tuzlama, hash oluşturma vb. içeren en son ve en güçlü şifreleme prosedürlerini kullanınız.

DoS ve DDoS Saldırıları; CSP'lere DoS saldırıları gerçekleştirmek, kiracıların hesaplarına erişimini engelleyebilir. Bulut altyapısında, birden fazla kiracı CPU, bellek, disk alanı, bant genişliği vb. paylaşır. Bu nedenle, saldırganlar buluta erişim sağlarsa, kaynak istekleri veya meşru kullanıcıların uygulamalarında çalışabilen kod türü olabilecek yanlış veriler üretirler. Bu tür kötü amaçlı yazılım isteklerinin hesaplanması, bir sunucunun CPU'sunu, belleğini ve diğer tüm cihazları meşgul eder. Sunucu eşik sınırına ulaştığında, işlerini başka sunucuya yüklemeye başlar. Aynı şey diğer satır içi sunucularda da olur ve sonunda saldırgan, ysunucunun olağan işlemine müdahale ederek tüm bulut sistemini meşgul etmeyi başarır. Bu da bulut kullanıcılarının hizmetlerine erişememesine neden olur. DoS, sunucuyu tüm kullanılabilir sistem kaynaklarını tüketmek için birden fazla istekle doldurarak, uygulama sürecini çökerten sunucuya kötü amaçlı girdi göndererek, sürekli olarak yanlış parolalar girerek gerçekleştirilebilir. DoS saldırısı, botnet üzerinden başlatılırsa, bu bir DDoS saldırısıdır. DDoS saldırısı, tek bir hedefe saldıran çok sayıda tehlikeye atılmış sistemi içerip hedeflenen sistemin kullanıcılarına hizmet reddi durumu oluşur. Saldırgan internet üzerinden çok sayıda bilgisayarı enfekte eden işleyici ayarlayarak saldırgan bulut sunucusunu birden fazla istekle doldurur ve bu da aşırı kaynak tüketimine neden olur. Böylece, meşru kullanıcılar bulut hizmetlerine erişemez.

Alınacak önlemler: Sunucuya bağlanan kullanıcılar için en düşük ayrıcalık kavramını izleyiniz. DoS ve DDoS saldırılarını azaltmak için bulutun hem fiziksel hem de sanal makinelerine IDS yükleyiniz.

Tarayıcıda Adam Saldırısı; Saldırganların kullanıcının tarayıcısı ile bulut uygulaması arasında paylaşılan bilgileri izlemesine olanak tanıyan karmaşık kötü amaçlı yazılımlar enjekte ederek kullanıcının web tarayıcısını hedef alır. Enjekte edilen kod, kullanıcı adı ve parolalar gibi kullanıcının oturum açma kimlik bilgilerini saldırganlara sızdırır. Daha sonra saldırganlar, bu kimlik bilgilerini bulut sunucusunda doğrulayabilir, kullanıcının farkında olmadan kullanıcı adına kötü amaçlı faaliyetler gerçekleştirebilir.

Alınacak önlemler: Ağı yasadışı erişime karşı korumak için bulut hizmetlerine erişimi sınırlayınız. Anormal kullanıcı etkinliklerini tespit etmek ve bildirmek için bulut tabanlı çözümü kontrollü saldırı tespit sistemleriyle entegre ediniz. IP adresi aralığını sınırlayın ve hizmetleri VPN'ler aracılığıyla sununuz.

Meta Veri Sahteciliği Saldırısı; Bulut hizmeti meta verileri, ağ bileşenlerinin konumu, güvenlik gereksinimleri, veri biçimleri gibi çeşitli hizmetlerin ayrıntılarını açıklar. Meta veri sahteciliği, hizmet örnekleriyle ilgili bilgilerin depolandığı web hizmeti tanımlama dili (WSDL) dosyasında yazılan hizmet meta verilerini değiştirme veya düzenleme işlemidir. Değiştirilen dosya başarıyla dağıtıldığında, bulut kullanıcıları DNS sahteciliği sürecine benzer şekilde bilinmeyen yerlere yönlendirilir.

Alınacak önlemler: Uygulama ve hizmet ayrıntılarını bulutta şifreleyin ve depolayınız. Sahtecilik saldırılarını azaltmak için hash tabanlı bütünlük denetimi uygulayınız. Güvenli olmayan meta veri sürümleriyle birlikte gerekli olmayan meta veri hizmetlerini devre dışı bırakınız. Örnek meta veri API erişimini kısıtlamak için host bilgisayar tabanlı güvenlik duvarlarını uygulayınız.

Bulut Kötü Amaçlı Yazılım Enjeksiyon Saldırısı; Saldırganlar SaaS, PaaS veya laaS olarak çalışan bulut hizmetlerine kötü amaçlı hizmet uygulamaları veya sanal makineler yükler. Bulut başarıyla suistimal edildiğinde, bulut kullanıcısı saldırganların web sitesine yönlendirilir, saldırganlar burada iletişimi dinleme, veri çalma ve değiştirme gibi faaliyetler gerçekleştirebilir.

Bulut Kötü Amaçlı Yazılımı;

Hildegard, Kubernetes kümesindeki yanlış yapılandırılmış kubelet'leri istismar etmek ve Kubernetes ortamında bulunan tüm kapsayıcıları enfekte etmek için tasarlanmış bulut kötü amaçlı yazılımıdır. Hildegard, saldırganların güvenlik çözümlerini atlatmalarına, varlıklarını gizlemek için sistem yapılandırmalarını değiştirmelerine yardımcı olur. Bu kötü amaçlı yazılım; bulut kaynaklarının istismarı için iki önemli araç olan peirates ve BotB'yi bırakır. Saldırganlar bu kötü amaçlı yazılımı kullanarak kaynak ele geçirme, kripto ele geçirme, DoS saldırıları, uygulama patlaması, kripto madenciliği vb. gerçekleştirebilir.

Özellikler; LD_PRELOAD kullanarak kapsayıcılardaki kötü amaçlı işlem yürütmeyi gizler. IRC aracısı kullanarak statik analiz araçlarını atlar. Sistem DNS çözücülerini değiştirerek DNS izleme araçlarını atlar. Kimlik bilgisi keşfi ve keşif işlemleri gerçekleştirir. İki C2 iletişim kanalı olan tmate ve IRC, neredeyse benzer şekilde çalışmaktadır.

Bazı ek bulut kötü amaçlı yazılımları şunlardır: Denonia. LemonDuck. RansomCloud. DBatLoader/ModiLoader. Goldbackdoor.

Bulut Hackleme; Çoğu kuruluş, maliyet açısından etkili çeşitli hizmetler için bulut teknolojilerini benimsesede, paylaşıma bağlı olduğu için güvenlik önemli bir endişe olmaya devam etmektedir. Altta yatan teknolojilerin güvenlik açıkları, saldırganların çeşitli türde bulut saldırıları başlatmasına olanak tanıyarak bulut sistemlerindeki kaynakların ve hizmetlerin gizliliğini, bütünlüğünü, kullanılabilirliğini etkileyebilir. Günümüzde, birçok kuruluş iş süreçlerini ve müşteri verilerini buluta taşımaktadır. Kurumsal ve kişisel verilerin buluta büyük ölçüde taşınması, hem kuruluşlar hem de bireyler için saldırı yüzeylerini ve tehditleri artırmıştır.

Saldırganlar, bulut depolama sistemlerine yönelik çeşitli hedefli yüksek profilli saldırılar gerçekleştirmek, müşteri ve kurumsal verileri tehlikeye atmak için bulut teknolojilerinde bulunan güvenlik açıklarından yararlanmaktadır. Bulut ortamını hacklemenin temel amacı kullanıcı verilerine erişmek, bulut hizmetlerine erişimi engellemektir. Bunun hem son kullanıcılar hem de kurumsal şirketler üzerinde büyük bir etkisi vardır ve bulut hizmetlerinin güvenliğine olan güveni yerle bir eder. Bu nedenle de kuruluşların bulutta depolanan iş süreçlerinin ve müşteri bilgilerinin güvenliğini ve emniyetini sağlaması gerekir.

Saldırgan bulutu hackleyerek nasıl kar elde edebilir? Veri sızdırma ve hassas bilgilerin ifşasını gerçekleştirmek için zayıf güvenlik uygulamalarından faydalanarak gerçekleştirebilir. Bulut uygulamalarına yetkisiz erişim elde ederek yapabilir. Diğer bulut kullanıcılarının kimlik bilgilerini çalmak için meşru erişimi kötüye kullanmakla yapabilir. Hedefin işlem gücüne erişerek yasadışı kripto para üreterek yapabilir. Gelir elde etmek için gizli kripto madenciliği kötü amaçlı yazılımı kullanarak. Meşru kullanıcıların bulut hizmetlerine erişmesini önlemek için DoS saldırıları gerçekleştirerek. Senkronizasyon belirteci sistemlerindeki güvenlik açıklarından yararlanarak bulut hizmetlerini yeniden yapılandırarak. Veri merkezi ağlarında yanal hareket gerçekleştirmek ve ağ trafiğini manipüle ederek.

Trivy kullanarak Konteyner Güvenlik Açığı Taraması ; Konteyner görüntüleri, işletim sistemi, uygulama, çalışma zamanı vb.'nin birlikte paketlenmesinden oluşmaktadır. Bu konteynerler yaygın olarak yeniden kullanılır ve güvenlik açığı sorunları olan açık kaynaklı çerçeveler içerebilir. Bu güvenlik açıkları her konteynerin değil, tüm konteyner motorunun güvenliğini tehlikeye atar. Saldırganlar, konteynerlerdeki güvenlik açıklarını taramak ve belirlemek için Trivy Güvenlik Açığı Tarayıcısı, Clair, Dadga ve synk konteyneri gibi araçları kullanır.

Trivy; Konteyner görüntü güvenlik açığı taraması yapmak için kullanılan otomatik araçtır. Doğru bir tarama işlemi başlatmak için görüntü adını belirtmek gerekir. Trivy, Alpine, RHEL ve CentOS gibi işletim sistemi paketlerinin, Bundler, Composer, npm ve yarn gibi uygulama bağımlılıklarının güvenlik açıklarını tespit etmeye yardımcı olur.

Sysdig Kullanarak Kubernetes Güvenlik Açığı Taraması; Kubernetes, sıklıkla küme yanlış yapılandırmalarından muzdarip olan karmaşık bir ortamdır. Saldırganlar bu yanlış yapılandırmalardan yararlanabilir, Sysdig ve Pipeline gibi çeşitli araçları kullanarak Kubernetes kümelerinde güvenlik açığı taramaları gerçekleştirebilir.

Sysdig; Sürekli entegrasyon (CI) veya sürekli teslimat/dağıtım (CD) boru hatlarını, görüntü kayıt defterini, Kubernetes kabul denetleyicilerini entegre ederek Kubernetes güvenlik açıklarını belirler. Sysdig, Kubernetes kabul denetleyicisi özelliğini kullanarak konteyner görüntülerini düzenleme düzeyinde doğrular. Sysdig, her görüntü içeriğinin envanterini otomatik olarak oluşturarak konteynerlerle ilişkili yeni güvenlik açıkları veya yaygın güvenlik açıkları ve ifşalar (CVE) olup olmadığını sürekli olarak kontrol eder.

Ek Kubernetes güvenlik açığı tarama araçları şunları içerir: kube-hunter. Kube-Scan. Kubesec. KubiScan.

S3 Kovalarını Numaralandırma; Basit depolama hizmeti (S3), dosyaların, klasörlerin ve nesnelerin web API'leri aracılığıyla depolandığı Amazon AWS tarafından kullanılan ölçeklenebilir bulut depolama hizmetidir. Müşteriler ve son kullanıcılar, metin belgelerini, PDF'leri, videoları, görüntüleri vb. depolamak için S3 hizmetlerini kullanır. Tüm bu verileri depolamak için kullanıcının benzersiz ada sahip kova oluşturması gerekir. Saldırganlar, kova uygulamasındaki yanlış yapılandırmalardan yararlanabilir ve veri gizliliğini tehlikeye atmak için güvenlik mekanizmasını ihlal edebilir. S3 kova oturumunu çalışır durumda bırakmak, saldırganların dosyaları değiştirmesine, kova dosyalarına kötü amaçlı yazılım enjekte etmesine olanak tanır. Saldırganlar genelde güvenliğini test etmek ve kova uygulamasındaki güvenlik açıklarını belirlemek için kova konumunu ve adını bulmaya çalışırlar.

Saldırganların AWS S3 kovalarını tanımlamak için kullandıkları birkaç teknik şunlardır:

HTML'yi inceleme; Saldırganlar $3 kovaları hakkında bilgi toplamak için HTML kaynak kodu analizi yapmaya çalışır. Arka planda HTML web sayfalarının kaynak kodunu analiz etmek, saldırganların S3 kovalarını hedefleyecek URL'leri bulmasını sağlar.

URL'yi kaba kuvvetle zorlama; Her S3 kovasına benzersiz tanımlama numarası verildiğinden, saldırganlar doğru kova URL'sini belirlemek için hedef kovaya kaba kuvvet saldırıları gerçekleştirir. Saldırganlar, S3 kovalarına kaba kuvvet saldırıları gerçekleştirmek için Burp Suite gibi araçları kullanır.

Alt alan adlarını bulma; Saldırganlar, hedef kovayla ilgili alt etki alanlarını belirlemek için OWASP Amass ve Robtex gibi araçlar kullanır.

Ters IP Araması ; Saldırganlar, hedef S3 kovalarının etki alanlarını belirlemek için ters IP araması yapmak üzere Bing gibi arama motorlarını kullanır. Saldırganlar, verilen IP adresini çözen hedef kovayla ilgili farklı etki alanlarını elde etmek için Bing arama motorunda, gelişmiş arama operatörü ip:<hedef IP adresi> kullanır.

Gelişmiş Google Hackleme; Saldırganlar, hedef S3 kovalarıyla ilgili URL'leri aramak için "inurl" gibi gelişmiş Google arama operatörlerini kullanır. Saldırganların hedef $3 kovalarının URL'lerini tanımlamak için kullandıkları Google Dork'lardan bazıları şunlardır; inurl: s3.amazonaws.com , inurl: s3.amazonaws.com/audio/ , inurl: s3.amazonaws.com/video/ , inurl: s3.amazonaws.com/backup/ , inurl: s3.amazonaws.com/movie/ , inurl: s3.amazonaws.com/image/

S3Scanner Kullanarak Açık S3 Kovalarını Tanımlama; Saldırganlar, Amazon AWS gibi bulut hizmetlerinin açık S3 kovalarını tanımlamak, kötü amaçlı amaçlar için içeriklerini almak için S3Scanner'ı kullanır. S3 kovaları, metin dosyaları, resimler, videolar ve PDF dosyaları gibi dosyalar, klasörler, nesneler vb. biçiminde bilgi depolar; bazı senaryolarda, yedekleme dosyaları ve kimlik bilgileri bile depolarlar. S3Scanner, saldırganların okuma ve yazma izinleri de dahil olmak üzere nesneleri ve erişim kontrol listesi (ACL) erişim bilgilerini almalarına olanak tanır.

AWS Hesap Kimliklerini Numaralandırma; AWS hesapları, herkese açık alanda ifşa edildiğinde saldırganlar tarafından bulut hizmetlerini hedeflemek için kullanılabilen benzersiz kimlikler aracılığıyla tanımlanır. Bu benzersiz kimliklerin özel olması amaçlanmıştır fakat genelde kullanıcının bilgisi olmadan herkese açıktır. Saldırganlar bu bilgi sızıntısından faydalanabilir ve bunu kötü niyetli amaçlar için kullanabilir.

Saldırganlar AWS hesap kimliklerini şu kaynaklar aracılığıyla sıralar: AWS hata mesajları. GitHub gibi kod depoları. Ekran görüntüleri. İlişkisel veritabanı hizmeti (RDS) genel anlık görüntüleri (RDS > Anlık Görüntüler > Tüm Genel Anlık Görüntüler). Genel elastik blok deposu (EBS) anlık görüntüleri (EC2 > Anlık Görüntüler > Genel Anlık Görüntüler). Genel Amazon makine görüntüleri (AMI'ler) (EC2 > AMI'ler > Genel görüntüler). Çevrimiçi yardım/sorun giderme aramak için kişisel kimliklerini yayınlayan kişiler.

Hesap kimliklerini aldıktan sonra saldırganlar kaynak numaralandırması, IAM rol varsayımı ve Lambda işlevlerinin çağrılması gibi çeşitli etkinlikler gerçekleştirebilir.

IAM Rollerinin Numaralandırılması; Saldırganlar, kullanıcının varlığına ilişkin bilgileri ortaya çıkaran AWS hata mesajlarını analiz ederek IAM rol adlarını sıralar. AWS bulut hizmetlerinde kullanıcıların bir rolü üstlenmek için çok sayıda girişimde bulununuz. Her başarısız girişim için AWS yanıt mesajları rolün varlığı hakkında bilgi verir. AWS birkaç başarısız girişimden sonra bir hesabı engellerse, kaba kuvvet tekniğini uygulamak zor olabilir fakat imkansız değildir. İşlemi parçalanmış bir hesap veya düğüm kümesiyle yürüterek, saldırganlar nihayetinde IP ve hesap filtreleme çözümlerinden kaçınabilir.

Saldırganlar tarafından IAM rol numaralandırması yoluyla toplanan bilgiler şunları içerir: Dahili yazılım/yığınlar. IAM kullanıcı adları (sosyal mühendislik için kullanılır). Kullanımda olan AWS hizmetleri. Kullanımda olan üçüncü taraf yazılımlar (CloudSploit, Datadog, Okta gibi).

Rolleri numaralandırdıktan sonra saldırganlar açık bir rol üstlenmeye ve kimlik bilgilerini çalmaya çalışabilir. Saldırgan izin verilmeyen bir rolü üstlenmeye çalışırsa, AWS hata mesajı üretir. Saldırganlar hata mesajını analiz ederek rolün varlığını doğrulayabilir fakat rol üstlenme politikasındaki kısıtlamalar nedeniyle rolü üstlenemez. Aynı komutu var olmayan bir rolü hedef alarak çalıştırırken AWS hata mesajını üretir. Saldırganlar geçerli herhangi bir hesap kimliği ve iyi filtrelenmiş kelime listesi kullanarak mevcut [AM rollerini sıralayabilir.

S3Inspector Kullanarak Kova İzinlerini Sıralama; Saldırganlar AWS S3 kova izinlerini sıralamak için S3Inspector'ı kullanır. Saldırganlar bu aracı kullanarak bir kovanın herkese açık mı yoksa herkese açık olmayan mı olduğunu doğrulayabilir. Herkese açık kova olması durumunda saldırganlar kova izinlerini ve ona erişmek için URL listesi alabilir. Herkese açık olmayan kovalar erişim reddedildi raporlarıyla yanıt verir.

Kubernetes etcd'yi sayma; Kubernetes dağıtılmış bilgi işlem platformudur. Bu nedenle etcd gibi dağıtılmış veritabanına ihtiyaç duyar. Etcd, Kubernetes küme verilerinin, hizmet keşif ayrıntılarının, API nesnelerinin vb. depolandığı dağıtılmış, tutarlı anahtar-değer depolama alanıdır. API sunucusu, diğer Kubernetes bileşenlerinden gelen isteklere göre bilgileri almak ve depolamak için etcd ile iletişim kurar. Etcd'ye erişim elde etmek, sisteme kök düzeyinde erişim elde etmekle aynıdır. Kubernetes'te, API sunucusunun etcd deposuna erişmesine izin verilir. Saldırganlar, Kubernetes ortamına bağlı uç noktaları tanımlamak için etcd işlemlerini, yapılandırma dosyalarını, açık portları (2379 numaralı portu tanımlayan) vb. numaralandırır.

Saldırganlar etcd sunucusunun konumunu ve PKI bilgilerini numaralandırmak için şu komutu kullanabilir: # ps -ef | grep apiserver

Saldırganlar etcd sunucusunun yerini belirlemek ve sertifikalar ve anahtar dosyaları gibi kritik bilgileri almak için bulut hizmeti tarafından sağlanan meta veri hizmetlerini sıralar. Saldırganlar, etcd sunucusu ve PKI hakkında bilgi topladıktan sonra küme verilerini almak için kayıt defterlerine daha fazla göz atabilir. Saldırganlar, anahtarları çözerek kube yapılandırma dosyasından uç noktaları belirleyebilir. Saldırganlar, etcd'den sıralanan bilgileri ayrıcalık yükseltme saldırıları gerçekleştirmek ve düğüm bilgilerine erişmek için kullanabilir.

Azure Active Directory (AD) Hesaplarını Sıralama; Office 365 gibi bulut platformlarına doğrudan internetten erişilebilir. Bu nedenle de saldırganlar Azure Active Directory (AD) ve Office 365'e farklı saldırılar başlatmak için bu ortamları hedef alır.

Azure AD hesaplarını sıralamak için kullanılan teknikler;

Hesap Sıralaması; Office 365 hizmetlerine erişimi olan Azure AD kullanıcıları, tüm kullanıcı hesaplarını ve yönetici gruplarını sıralayabilir. Office 365 hizmetine erişim olasılığı, saldırganları Azure AD'yi istismar etmeye ve bundan yararlanarak hesap numaralandırması yapmaya motive edebilir. Saldırganlar, Azucar gibi araçları kullanarak Azure AD numaralandırması yapabilir.

Azucar; Kullanıcıların Azure ortamının genel güvenliğini değerlendirmesini sağlar. Windows'da kullanılabilen çok iş parçacıklı eklenti tabanlı güvenlik aracıdır. Araçta kullanılan betik, Azure aboneliğinde uygulanan varlıkları etkilemez.

Parola Püskürtme; Saldırganlar, Azure AD hesaplarında otomatik parola tahmini yapmak için parola püskürtmeyi kullanır. Bu yöntem, tek bir parola kullanılarak aynı anda tüm kullanıcı hesaplarına oturum açma girişimleri gerçekleştirildiğinden hesap kilitlenmelerine yol açmaz. Hem şirket içi hem de bulut hesabı MFA olmadan aynı parolayı kullanıyorsa, saldırganların parola püskürtme yoluyla hedef ağa erişme olasılığı yüksektir. Saldırganlar, Ruler gibi gelişmiş araçları kullanarak parola püskürtme yapabilir.

Ruler; Saldırganların uzaktan yordam çağrısı (RPC)/HTTP veya Mesajlaşma Uygulama Programlama Arayüzü (MAPI)/HTTP gibi herhangi bir protokolü kullanarak uzaktan exchange sunucularıyla iletişim kurmasını sağlar. Araç, istemci tarafının Outlook özelliklerinin kullanılmasını ve uzaktan kabuk erişiminin elde edilmesini kolaylaştırır.

IMDS Saldırısıyla Bulut Anahtarlarının Toplanması; AWS ortamında, bulut erişim anahtarları, IAM kullanıcısı veya AWS hesabı kök kullanıcısı tarafından AWS hizmetlerine erişmek için kullanılan güvenlik kimlik bilgileridir. Erişim anahtarı kimliği ve gizli erişim anahtarı, istekleri doğrulamak için kullanılabilen bulut anahtarlarının ayrılmaz parçalarıdır. Saldırganlar, bulut kaynaklarına erişmek için bu bulut anahtarlarını elde etmek amacıyla IMDS saldırıları başlatır. Saldırgan, IMDS (IMDSv1) aracılığıyla belirli bir IP adresinde çalışan REST API'ye erişebilir, EC2 örnekleri ve güvenlik kimlik bilgileri hakkında bilgi edinebilir. Saldırganlar, Nitro EC2 örnekleri için IPv6 adresi (fd00:ec2::254) kullanabilir.

Saldırgan, IMDSv2 aracılığıyla örnek meta verilerini şu yollarla alabilir;

Nimbostratus Kullanarak Amazon Bulut Altyapısını Kullanma; Nimbostratus, Amazon bulut altyapılarının parmak izini almak ve bunları kullanmak için kullanılan bir araçtır. Ayrıca şu işlemleride gerçekleştirmektedir; mevcut IAM rolü için AWS hizmetlerine erişimi sayma. Yeni AWS kullanıcısı oluşturmak için kötü yapılandırılmış IAM rolü kullanma. Meta verilerden, .boto.cfg dosyalarından, ortam değişkenlerinden vb. mevcut AWS kimlik bilgilerini çıkarma. Anlık görüntüde depolanan bilgilere erişmek için veritabanlarını kopyalama.

Veritabanı anlık görüntüsü oluşturma: Bazı durumlarda saldırganların Amazon kimlik bilgileri vardır ve bu kimlik bilgileri RDS API'sine erişmelerine olanak tanır fakat veritabanının kendisine (MySQL kullanıcısı) erişemezler. create-DB-snapshot aracı, saldırganların anlık görüntü oluşturarak, geri yükleyerek veritabanında depolanan bilgilere erişmesini sağlar.

Alınacak önlemler: Doğrudan kök erişimine izin vermek yerine her zaman IAM kullanınız. Her bulut örneği profili ve kullanıcısı için mümkün olan en az ayrıcalıkları atayınız. Kullanıcı grupları oluşturup her grup için ayrıntılı izinler tahsis ediniz. Bulut örneği profillerini kullandığınızdan emin olunuz. Her kullanıcıya veya kullanıcı grubuna atanan izinleri periyodik olarak denetleyiniz.

AWS IAM Kimlik Bilgilerinin Tehlikeye Atılması; AWS IAM, AWS müşterilerine kimlik yönetimi yetenekleri sağlamak için kullanılır. AWS IAM, BT yöneticilerinin AWS kullanıcı kimliklerini ve AWS kaynaklarına erişimlerinin değişen seviyelerini yönetmelerine yardımcı olur. Saldırganlar, bulut ortamındaki çeşitli güvenlik açıklarını ve güvenlik kusurlarını tespit ederek AWS IAM kullanıcı kimlik bilgilerini kolayca tehlikeye atabilir. AWS IAM'yi tehlikeye atmak için saldırganlar Pacu gibi istismar araçlarını kullanır.

Saldırganların AWS IAM kimlik bilgilerini tehlikeye atmak için kullandıkları çeşitli güvenlik açıkları şöyledir;

Depo Yanlış Yapılandırmaları; Çoğu kuruluş, geliştiricilerin ve mühendislerin gerektiğinde anahtarlara kolayca erişebilmesi için AWS anahtarlarını Git deposu gibi dahili bir ağdaki paylaşımlı depolama alanında barındırır. İçeridekiler AWS anahtarlarını kötüye kullanabilir. Geliştiriciler kişisel AWS anahtarlarını bilmeden paylaşımlı depoya paylaşırsa AWS anahtarları da tehlikeye atılabilir. GitHub'daki farkında olmadan herkese açık hale getirilen ortam değişkenleri dosyası, AWS API anahtarlarını internet üzerinden ifşa eder. Kullanıcılar bu dosyayı "güncellenmiş .gitignore" olarak yüklerken commit mesajını görebilir. AWS, AWS API anahtarlarını aramak için GitHub commit mesajlarını tarayarak depolarında yayınlandığında kullanıcıyı bilgilendirir, böylece kullanıcının uygun şekilde hareket etmesini sağlar. Yine de saldırganlar bulut kaynaklarına erişmek için aynı tekniği kullanabilir.

Sosyal Mühendislik; Saldırganlar, kullanıcıları AWS IAM kimlik bilgilerini ifşa etmeleri için kandırmak amacıyla sahte e-postalar, aramalar ve SMS'ler gibi sosyal mühendislik tekniklerini kullanır. Kullanıcı AWS'yi doğrulamak için API anahtarlarını girerse, saldırgan API anahtarlarını çalmak ve kullanıcı hesabını tehlikeye atmak için basit kimlik avı tekniği kullanabilir.

Parola Yeniden Kullanımı; Ciddi güvenlik açıklarına neden olabilen çok yaygın hatadır. Çoğu kullanıcı aynı parolayı birden fazla hizmet için tekrar kullanır. Saldırgan parolayı ele geçirebilirse, aynı kimlik bilgileriyle diğer bulut hizmetlerine erişim sağlayabilir. Bazı senaryolarda web sitesi tehlikeye atılırsa, saldırgan arka uç veritabanına erişebilir, veritabanında depolanan parola karmalarını veya açık metin parolalarını alabilir.

AWS Tarafından Barındırılan Uygulamalarda Güvenlik Açıkları;

Sunucu Tarafı İstek Sahteciliği; Saldırganların tehlikeye atılmış web sunucusundan kurbanlara rastgele web istekleri göndermek için kullandıkları yaygın web uygulaması güvenlik açığıdır. Saldırganlar, web uygulamasında herhangi bir güvenlik açığı bulunursa dahili EC2 meta veri API'sini hedef alarak EC2 örneğinden istekler yapar. Uygulama AWS API'sinden erişime ihtiyaç duyduğunda, geçici AWS kimlik bilgilerini istemek için EC2 örneğine IAM örneği profili eklenir. Tüm bu süreç EC2 meta veri API'si aracılığıyla yapıldığından, saldırgan meta veri URL'sine HTTP istekleri gönderir ve uygulama tarafından kullanılan geçici kimlik bilgilerine kolayca erişebilir.

Yerel Dosyayı Okumak; AWS anahtarları bir işletim sisteminde yapılandırma ve günlük dosyaları gibi çeşitli konumlarda saklanır. Kullanıcı AWS komut satırı arayüzü aws-cli'yi kullanıyorsa, kimlik bilgileri ana dizinde saklanır ve anahtarlar ortam değişkeni dosyasında saklanır. Bir saldırgan işletim sistemine zaten erişim sağladıysa, daha fazla istismar gerçekleştirmek için işletim sisteminde saklanan kimlik bilgilerini ve anahtarları okuyabilir.

Üçüncü Taraf Yazılımını İstismar Etmek; Birçok çevrimiçi hizmet, yazılımlarının veya uygulamalarının düzgün çalışabilmesi için AWS ortamına erişim gerektirir. Bazı kuruluşlar bulut hizmetlerini kolayca yönetmek veya güvenliğini sağlamak için üçüncü taraf yazılımları veya uygulamaları dağıtır. Saldırgan üçüncü taraf yazılımını tehlikeye atarsa, bulut ortamında saklanan verilere erişebilir. Kuruluş çeşitli bulut hizmetlerini yönetmek için üçüncü taraf parola yöneticisi kullanabilir. Bir saldırgan parola yöneticisini tehlikeye atarsa, bulut ortamına kolayca üst düzey erişim elde edebilir.

İçeriden Tehdit; İçeriden gelen tehdit çoğunlukla ortama güvenilir erişimi olan, kötü amaçlı faaliyetler gerçekleştirmek için kimlik bilgilerini ayrı ayrı tehlikeye atması gerekmeyen iş ortaklarından ve mevcut, eski çalışanlardan kaynaklanır. Bu tür içeriden gelenler kuruluş ve AWS ortamı için ciddi tehdit oluşturur. Şirketin itibarını zedelemek isteyen hoşnutsuz bir çalışan, kimlik bilgilerini kullanarak bulut hizmetlerini istismar etmeye çalışır ve bilgilerin kamuoyuna açıklanmasına yol açan doğrudan kod değişiklikleri gerçekleştirir.

Pacu Kullanarak Yanlış Yapılandırılmış IAM Rollerini Ele Geçirme; AssumeRole izinleri gibi AWS IAM politikaları esnektir fakat rol izinlerindeki yanlış yapılandırmalar çeşitli saldırılara kapı açabilir. Saldırganlar, IAM rollerini saymak ve ele geçirmek için açık kaynaklı AWS istismar çerçevesi olan Pacu gibi araçlar kullanır. Araç, yaygın olarak kullanılan rol adlarından oluşan 1100'den fazla kelime listesi içerir. Komut dosyası, rol tanımlandığında saldırganı otomatik olarak uyarır. Yanlış yapılandırılmış rolleri belirleyebilir ve tanımlanan rolleri otomatik olarak üstlenebilir, ardından rol kimlik bilgilerini açığa çıkarabilir. Saldırganlar, bir rolü üstlenmek için Pacu komut dosyasını çalıştırabilir. Komut dosyasını çalıştırmadan önce saldırganların bir rolü üstlenmek için hedef hesap kimliği edinmeleri gerekir.

DumpsterDiver Kullanarak AWS Erişim Anahtarlarını Kırma; Saldırganların AWS erişimi, SSL ve Microsoft Azure anahtarları gibi sabit kodlanmış gizli anahtarları tararken büyük miktarda dosya türünü incelemelerine olanak tanır. Saldırganların basit koşula dayalı arama kuralları oluşturmasına da olanak tanır. Saldırganlar bu aracı hedef bulut hizmetlerindeki olası gizli sızıntıları ve sabit kodlanmış parolaları belirlemek için kullanır.

Bulut Kapsayıcı Saldırı Aracı (CCAT) kullanarak AWS'de Docker Kapsayıcılarını Kullanma; Saldırganlar, Amazon ECS ve ECR'de daha fazla istismar gerçekleştirmek için tehlikeye atılmış AWS kimlik bilgilerini kullanır.

AWS Docker kapsayıcılarını istismar etmede yer alan adımlar:

1. Adım - AWS kimlik bilgilerini kötüye kullanma; Saldırganlar, AWS bulutuna göz atmak ve kullanılabilir ECR depolarını belirlemek için daha önce elde edilen AWS kimlik bilgilerini kötüye kullanır. CCAT, kullanılabilir ECR depolarının ayrıntılarını listelemek için "ECR'yi Listele" modülünü sağlar.

2. Adım - Hedef Docker görüntüsünü çekme; Saldırganlar ECR depolarının listesi hedef organizasyona ait Docker imajını algılar ve çeker. Saldırgan hedef depoyu çekmek için CCAT "Pull Repos from ECR" modülünü kullanabilir.

3. Adım - Arka kapı imajı oluşturma; Saldırganlar, Docker imajını ECR deposundan çektikten sonra hedef Docker imajında ters kabuk için arka kapı oluşturur ve gömer. Saldırgan, varsayılan CMD komutunun yerini alan ters kabuk arka kapısı oluşturmak için "Docker Backdoor" modülünü kullanabilir.

4. Adım - Arka kapı Docker imajını itiniz; Saldırganlar, arka kapı ile gömülmüş hedef Docker imajını ECR deposuna geri iter. CCAT, değiştirilmiş Docker imajını ECR deposuna yüklemek için "Push Repos to ECR" modülünü sağlar.

AWS Lambda'da Sunucusuz Tabanlı Saldırılar; Sunucusuz işlevler yönetilen sunucu olmadan çalışabildiğinden, DDoS, komut enjeksiyonu ve siteler arası betik çalıştırma (XSS) gibi farklı uygulama düzeyindeki saldırılara karşı savunmasızdır. Saldırganlar ayrıcalıklar elde etmek ve bir hesabın gizliliğini tehlikeye atmak için AWS Lambda işlevlerini kötüye kullanabilir.

Saldırganlar Lambda işlevlerini kötüye kullanmak için iki senaryo kullanabilir;

Kara Kutu Senaryosu; Saldırganlar dahili çalışma sistemleri veya ortam hakkında önceden bilgi sahibi olmadıkları için belirli özellik hakkında belirli varsayımlarda bulunurlar.

Kara kutu senaryosu yaklaşımını kullanarak saldırı gerçekleştirme adımları şöyledir; Saldırgan, herhangi bir kimlik bilgisi ile uygulanmamış yanlış yapılandırılmış $3 kovasına erişir. Saldırganın erişim sağladığı yanlış yapılandırılmış kovalar çeşitli organizasyon dosyaları içerebilir. Saldırgan dosyaları S3'e yükler ve ardından yapılandırmalarını yeniden kontrol eder. Dosyalar yüklendikten sonra, tek tek dosyaların etiketleri Lambda işlevi kullanılarak hesaplanabilir. Ardından, saldırgan bir hesabın bulut kimlik bilgilerini sızdırır ve edinilen AWS kimlik bilgileriyle daha yüksek ayrıcalıklar için numaralandırmaya başlar. Saldırganlar saldırıyı gerçekleştirmek için AWS CLI komutlarını kullanabilir.

Beyaz Kutu Senaryosu; Saldırganlar hedeflerine ulaşmalarına yardımcı olan ortam hakkında önceden bilgi tutarlar.

Beyaz kutu senaryosu yaklaşımını kullanarak saldırı gerçekleştirme adımları şöyledir; Saldırgan, kimlik avı veya diğer sosyal mühendislik yöntemleri yoluyla kullanıcı kimlik bilgileri gibi hassas bilgileri elde eder. Saldırgan, tehlikeye atılan bulut hesabıyla ilişkili roller ve diğer politikalar hakkında bilgi elde eder. Burada, saldırgan kesinlikle belirli yanlış yapılandırılmış S3 kovasına odaklanır. Saldırgan artık Lambda işlevlerini listeleyebilir ve herhangi bir işlev hakkında ek bilgi elde edebilir. Ek bilgiler ve elde edilen kullanıcı kimlik bilgileriyle saldırgan, olası güvenlik açıklarının tespiti ve istismarı için ilişkili Lambda kodunu indirir. Saldırgan artık Lambda işlevini daha fazla saldırı başlatmak için kullanabilir.

AWS'de Gölge Yöneticilerini İstismar Etme; Gölge yöneticiler, saldırganların hedef bulut ağına girmesine izin veren belirli izinlere sahip kullanıcı hesaplarıdır. Saldırganlar, hedef ortama bir tür erişim elde ettikten sonra gölge yöneticileri istismar edebilir. Saldırganlar, ayrıcalıkları artırmak ve hedef bulut ortamı üzerinde kontrol elde etmek için gölge yönetici izinlerini kötüye kullanır. Saldırganların gölge yönetici izinlerini kötüye kullanmak için kullandıkları tekniklerden bazıları şöyledir;

Erişim İzinlerini Yükseltme; Saldırganlar, ayrıcalıklarını yönetici hesabının ayrıcalıklarına yükseltmek için Microsoft .Authorization/elevateAccess/Action izinlerini kötüye kullanır.

Mevcut Rolleri Değiştirme; Saldırganlar, mevcut rolü değiştirmek ve yeni yönetici hesapları oluşturmak için Microsoft.Authorization/roleDefinitions/write izinlerini kötüye kullanır.

Yeni Hesaplar Oluşturma; Microsoft.Authorization/roleAssignments/write iznine sahip saldırganlar, ayrıcalıklı hesaplar için yeni roller atayabilir.

Saldırganlar yeni gölge yönetici hesapları oluşturmak için özel rollerden de yararlanabilir. "Depolama Ekibi Lideri" özel rolü tam abonelik yöneticisidir. Saldırganlar, bir hesap için ek izinler atamak üzere AssignableScopes aboneliğini kullanarak Microsoft.Authorization/roleAssignments/* gibi izinleri kötüye kullanabilir.

Gölge Yönetici Tarama Araçları;

SkyArk; AWStealth ve AzureStealth olmak üzere iki ana tarama modülü içerir. SkyArk'tan gelen tarama sonuçlarıyla saldırganlar en hassas ve riskli izinlere sahip varlıkları keşfedebilir.

Gölge yönetici hesaplarını tanımlamak için bazı ek araçlar şunlardır; Red-Shadow. ACLight2.

Docker Remote API'sini Kullanma; Hedef Docker host bilgisayarına erişim sağladıktan sonra saldırganlar, kripto para madenciliği, IP'leri maskeleyerek saldırı başlatma, DoS saldırıları gerçekleştirmek için botnet'ler oluşturma, kimlik avı kampanyaları için hizmetler yükleme, hassas bilgileri alma ve dahili ağın güvenliğini tehlikeye atma gibi daha fazla saldırı başlatmak için Docker uzak API'sini kullanır.

Docker host bilgisayarından dosyaları alma; Saldırganlar yeni kapsayıcı oluşturarak diğer dosyalara erişmek için bunu Docker host bilgisayarındaki klasöre bağlar.

Saldırganlar kapsayıcıya bağlanmış birimleri tanımlayarak host bilgisayarın dışında depolanan verilere erişebilir. $3 ve ağ dosya sistemi (NFS) gibi harici depolama bağlamalarını tespit etmek için Docker inspect komutunu kullanabilirsiniz. Bağlama yazma erişimine sahipse, saldırganlar harici depolamada depolanan dosyaları değiştirebilir.

Dahili ağ taraması; Saldırgan mevcut Docker ağ köprüsünde kapsayıcı oluştururursa, ana Docker host bilgisayarının dahili ağ içinde erişebildiği tüm host bilgisayarlara erişebilir. Ana bilgisayarın dahili ağını taramak ve çalışan hizmetleri belirlemek için Nmap'i kullanabilirsiniz.

Kimlik bilgilerini alma; Ortam değişkenleri, kapsayıcıları çalıştırırken kimlik bilgilerini argüman olarak geçirmek için Docker'da yaygın olarak kullanılır. Saldırganlar, Docker ana bilgisayarında kullanılabilir ortam değişkenlerini belirlemek için Docker inspect komutunu kullanır. Bir kapsayıcıda "env" komutunu çalıştırmak, kapsayıcıları başlatmak için kullanılan kimlik bilgileri dahil olmak üzere tüm ayrıntıları döndürür.

Kimlik bilgilerini almak için şu komutları çalıştırınız:

$ docker -H [docker uzak ana bilgisayarı] inspect [konteyner adı]

$ docker -H [docker uzak ana bilgisayarı] exec -i [konteyner adı] env

Veritabanlarını sorgulama; Kimlik bilgilerini aldıktan sonra saldırganlar, veritabanı tablolarında depolanan hassas bilgileri almak için MySQL kapsayıcılarında sorgular yürütebilir.

Hedef Docker ana bilgisayarındaki MySQL kapsayıcılarını bulmak için şu komutu çalıştırın:

$ docker -H [docker uzak ana bilgisayarı] ps | grep mysql

Akabinde, MySQL kimlik bilgilerini almak için şu komutu çalıştırın: $ docker -H [docker uzak ana bilgisayarı] exec -i some-mysql env

Alınan kimlik bilgilerini kullanarak MySQL kapsayıcısı altındaki veritabanlarını bulun:

$ docker -H [docker ana bilgisayarı] exec -i some-mysql mysql -u root -p

<şifre> -e “show databases”

Kapsayıcı Birimlerini Hacklemek; Kubernetes'te, kapsayıcılar dosya sistemlerini paylaşmak ve kapsayıcı dosyalarını işlemek için birimler kullanır. Bir birim, dosyaları depolayan ve pod'daki tüm kapsayıcılar tarafından erişilebilen bir dizine benzer. Kubernetes, çeşitli protokolleri kullanarak NFS ve İnternet küçük bilgisayar sistemleri arayüzü (iSCSI) gibi farklı birim türlerini destekler. Bu birimlerdeki zayıf ve varsayılan yapılandırmalar, saldırganlar tarafından ayrıcalık yükseltme saldırıları başlatmak, dahili ağda yanal hareket gerçekleştirmek için kullanılabilir.

Ana Düğümlere Erişim: iSCSI gibi birim yapılandırmaları, yapılandırma ayrıntılarını sırlar biçiminde depolar. Saldırganlar API'ye veya etcd'ye erişim sağlarsa, bu birimlerin yapılandırma ayrıntılarını kolayca alabilirler.

Düğümlere Erişim: Kubelet, pod'ları yönetir, bu nedenle saldırganlar pod'daki bir düğüme erişim sağlarsa, pod içinde kullanılan tüm birimlere kolayca erişebilirler. Saldırganlar günlükleri görüntülemek için dosya sistemi araçlarını kullanırsa, bir düğüm hakkında yararlı bilgiler elde edebilirler. Saldırganlar NFS kullanarak birimlerin yapılandırma ayrıntılarını almak için "df" komutunu kullanabilir.

Konteynere Erişim: Düğümlere erişime benzer şekilde, saldırganlar aynı bilgileri konteynerin kendisinden de alabilir. Bir konteynerden birimlere saldırarak, saldırganlar hostpath birim türünü bir düğümden hassas bilgileri alacak şekilde yapılandırabilir. Saldırganlar tüm bağlı birimlere göz atmak için dosya sistemi araçlarını kullanabilir.

CloudGoat 2 - Tasarıma Göre Savunmasız AWS Dağıtım Aracı; CloudGoat 2, Rhino Security Labs tarafından geliştirilen "Tasarıma Göre Savunmasız" AWS dağıtım aracıdır. Birkaç "bayrağı yakala" tarzı senaryo oluşturarak ve tamamlayarak bulut siber güvenlik becerilerinizi geliştirmenize olanak tanır. Her senaryo, yapılandırılmış öğrenme deneyimi oluşturmak için bir araya getirilmiş AWS kaynaklarından oluşur. Bazı senaryolar kolaydır, bazıları zordur ve çoğu zafere giden birden fazla yol sunar. Saldırgan olarak, ortamı keşfetmek, güvenlik açıklarını belirlemek ve senaryonun hedeflerine ulaşmak için kendi yolunuzu bulmak sizin görevinizdir.

Lansmanda yer alan senaryolar şunlardır:

" rce_web_app - Gizli uç noktayı bulun ve sanal özel bulut (VPC) içinde kök EC2 erişimi elde etmek için bir web uygulaması uzaktan kod yürütme güvenlik açığını kullanın.

jam_privesc_by_attachment — Ayrıcalıkları yükseltmek için mevcut örnek profillerini keşfedin ve ekleyiniz.

jam_privesc_by_rollback — IAM politika sürümlerini numaralandırın ve daha yüksek ayrıcalıklara sahip önceki bir sürüme geri dönünüz.

codebuild_secrets — Güvenli bir veritabanında düz metin sırlarını keşfetmek için CodeBuild ve SSM'yi keşfedin.

ec2_ssrf — Web uygulamasında sunucu tarafı istek sahteciliği (SSRF) güvenlik açığını kullanarak anahtarları almak için EC2 meta veri hizmetini bulun ve kullanınız.

SSRF Güvenlik Açıklarından Yararlanarak Erişim Elde Etme; Saldırganlar, rol için AWS kimlik bilgilerini almak, alınan kimlik bilgilerini yerel aws-cli'ye eklemek, S3 kovalarından kullanıcı hesabı ayrıntılarını almak, bu hesapla ilgili tüm kovalarda depolanan verilere erişmek, bunları sızdırmak için bulut hizmetini barındıran web uygulamasındaki SSRF güvenlik açıklarından yararlanabilir.

AWS IAM kimlik bilgilerini almak için SSRF güvenlik açıklarından yararlanma; Saldırganlar, AWS EC2 gibi bulut meta veri hizmetlerine erişmek ve rol için AWS erişim anahtarlarını almak için web uygulamalarındaki SSRF güvenlik açıklarından yararlanabilir. Bu anahtarlar, saldırganların S3 kovalarını bulup yerel host bilgisayara senkronize etmelerine ve böylelikle bu kovalarda depolanan verilere erişmelerine olanak tanır. Saldırganlar bu saldırıyı gerçekleştirebilir

Yerel aws-cli'ye kimlik bilgileri ekleme; Bir rol için AWS kimlik bilgilerine eriştikten sonra kimlik bilgilerini "aws configure" komutunu kullanarak yerel aws-cli'ye ekleyiniz.

Ş3 kovalarında depolanan verilere erişim sağlama; Kimlik bilgilerini ekledikten sonra her şeyin düzgün şekilde ayarlanıp ayarlanmadığını kontrol etmek için şu komutu çalıştırın; " aws sts get-caller-identity --profile stolen_profile " Bu komut, rol için kullanıcı kimliğini, hesap numarasını, Amazon kaynak numarasını (ARN) alır.

Şimdi, hesap için kullanılabilir tüm kovaları almak için şu komutu çalıştırın; " aws s3 ls --profile stolen_profile ". Bu komut, IAM rolü tarafından erişilebilen belirli hesap için tüm $3 kovalarını listeler.

Son olaraksa yerel sisteme kovalarda depolanan verileri senkronize etmek ve indirmek için şu komutu çalıştırın; " aws s3 sync s3://kova-adı "

AWS IAM Ayrıcalık Yükseltme Teknikleri; Hedef bulut hizmetlerine erişim sağladıktan sonra saldırganlar saldırı yüzeylerini genişletmek ve daha fazla istismar gerçekleştirmek için ayrıcalıklarını istismar etmeye çalışır.

Saldırganların AWS IAM ayrıcalıklarını yükseltmek için kullandıkları çeşitli teknikler şöyledir;

Yeni politika sürümü oluşturunuz; iam: CreatePolicyVersion'a erişim izinlerine sahip saldırganlar, özel izinlerle IAM politikasının yeni bir sürümünü oluşturabilir. Saldırganlar, iam: SetDefaultPolicyVersion'ı kullanmak için izin gerektirmeden politikayı oluştururken "--set-as-default" bayrağını ekleyerek yeni politikayı varsayılan sürüm olarak ayarlar. Bu teknik, saldırganların AWS hesabına üst düzey yönetici erişimi elde etmelerini sağlar.

Varsayılan politika sürümünü mevcut sürüme atayınız; Saldırganlar, iam'a erişim izinleri varsa, mevcut kullanılmayan politikaları kötüye kullanarak ayrıcalıklarını artırabilirler: Bir politika saldırganlar tarafından erişilebilirse ve varsayılan olmayan sürümlere sahipse, saldırganlar varsayılan sürümü başka bir mevcut sürüme değiştirebilirler. Bu teknik, saldırganın ayrıcalıklarını kullanılmayan politikaya atanan izin düzeyine yükseltmesine olanak tanır.

Mevcut örnek profiliyle EC2 örneği oluşturunuz; iam: PassRole ve ec2:RunInstances'a erişim izinleri olan saldırganlar işletim sistemine erişmek için halihazırda mevcut örnek profiliyle yeni EC2 örneği oluşturabilir. Daha sonra, yeni EC2 örneğini kötüye kullanarak oturum açabilir ve EC2 örneği meta verilerinden ilişkili AWS anahtarlarına erişebilirler. Bu onlara mevcut örnek profilinin tüm erişim izinlerini verir.

Yeni kullanıcı erişim anahtarı oluşturunuz; iam: CreateAccessKey'e erişim izinleri olan saldırganlar diğer kullanıcılar için erişim anahtarı kimlikleri ve gizli erişim anahtarları oluşturabilir. Bu, saldırganlara kullanıcının sahip olduğu erişim izinlerinin aynı düzeyini verir.

Oturum açma profili oluşturun/güncelleyiniz; Saldırganlar iam: CreateLoginProfile'a erişim izinleri edinirse, AWS konsolu için yeni oturum açma profilleri oluşturabilirler. Benzer şekilde de saldırganlar iam: UpdateLoginProfile'a erişim izinleri edinirse, diğer kullanıcıların oturum açma profillerini değiştirebilirler. Her iki durumda da saldırganlar belirli kullanıcı profilinin ayrıcalıklarına yükseltilir.

Bir kullanıcıya/gruba/role politika ekleyiniz; iam:AttachUserPolicy erişim izinlerine sahip saldırganlar, kullanıcıya politika ekleyerek ve bu politikanın izinlerini saldırganın politikasına ekleyerek ayrıcalıklarını artırabilir. Benzer şekilde de iam:AttachGroupPolicy ve iam: AttachRolePolicy erişim izinlerine sahip saldırganlar, politikaları manipüle edebilir ve ayrıcalıklarını ilgili grup veya rolün düzeyine yükseltebilir.

Kullanıcı/grup/rol için satır içi politika oluşturun/güncelleyiniz; iam: PutUserPolicy, iam: PutGroupPolicy ve iam: PutRolePolicy erişim izinlerine sahip saldırganlar, sırasıyla bir kullanıcı, grup ve rol için satır içi politika oluşturabilir veya güncelleyebilir. Bu teknik, saldırganların AWS ortamında tam yönetici ayrıcalıkları elde etmelerini sağlar.

Bir gruba kullanıcı ekleyiniz; iam: AddUserToGroup erişim izinlerine sahip saldırganlar, AWS ortamında mevcut IAM kullanıcı grubuna kendilerini ekleyebilirler. Bu teknik, saldırganların mevcut grupların ayrıcalıklarını elde etmelerine olanak tanır.

GCPBucketBrute kullanarak Google Storage Kovalarının Ayrıcalıklarını Yükseltme; Amazon AWS S3 kovalarına benzer şekilde Google Storage kovaları statik dosya depolaması için kullanır. Kova izin politikalarındaki güvenlik açıkları, kovaları tüm GCP kullanıcılarına veya genel internete maruz bırakabilir. AWS S3 kovaları gibi Google Storage kovaları da yanlış yapılandırılmış kova ACL'leri aracılığıyla ayrıcalık yükseltme saldırılarına karşı savunmasızdır. GCPBucketBrute, saldırganların Google depolama kovalarını saymalarına, bunlara ne tür erişimleri olduğunu belirlemelerine, ayrıcalık yükseltilebilir olup olmadıklarını kontrol etmelerine olanak tanıyan betik tabanlı araçtır.

"allUsers" veya "allAuthenticatedUsers" kova politikasını okuyabiliyorsa, saldırganlar geçerli bir yanıt alır, aksi takdirde, erişim reddedildi mesajı görüntülenir. Saldırganlar, kova izinlerini almak için kova adı ve Google depolama izinleri listesi vererek Google depolama "TestIamPermissions" API'sini kullanabilirler.

Saldırganlar, keşfedilen kovalarda kendilerine hangi ayrıcalıkların verildiğini kontrol etmek için GCPBucketBrute aracını kullanırlar. Saldırganların kovalara sınırlı erişimi varsa, GCPBucketBrute sahip olunan izinlerin bir listesini görüntüler. Saldırganlar, kovaya ayrıcalıkları yükseltmek için yeterli erişime sahipse, araç kovanın ayrıcalık yükseltmeye karşı savunmasız olduğunu gösteren bir mesaj görüntüler. Bu şekilde, saldırganlar izinlerini yönetici düzeyine yükseltebilirler.

Azure AD'de Yanlış Yapılandırılmış Kullanıcı Hesaplarını Kullanarak Ayrıcalık Yükseltme; Azure AD ortamında yanlış yapılandırılmış kullanıcı hesaplarını istismar etme adımları ele alınmıştır.

Öncelikle saldırgan, Bloodhound veya AzureHound gibi araçları kullanarak Azure AD'de normal bir kullanıcı hesabı keşfeder. İkinci adım olaraksa saldırgan, Azure AD PowerShell modülünü kurmak ve normal kullanıcı hesabı kullanarak Azure AD'de oturum açmak için şu komutu çalıştırır: Connect -AzureAD

Üçüncü adımdaysa saldırgan, uygulama için yeni anahtar kimlik bilgisi oluşturmak ve bunu yerel makinede depolamak için ilgili komutları yürütür. Dördüncü adımda saldırgan, kendi kendine imzalanmış sertifikayı kayıtlı uygulamanın sertifika bölümündeki Azure AD'ye yükler. Beşinci adımda saldırgan yeni oluşturulan sertifikayla Azure AD'yi doğruladıktan sonra normal kullanıcı hesabının ayrıcalıklarını Genel Yönetici'ye yükseltmek için ilgili komut çalıştırır. Altıncı adımda ayrıcalıkları yükselttikten sonra saldırgan Azure AD'yi açar ve normal kullanıcıya atanan rolün Global Administrator olduğunu doğrular. Şimdi saldırgan yükseltilmiş ayrıcalıkları kullanarak hedef Azure AD'yi daha fazla istismar edebilir.

AWS'de Arka Kapı Hesapları Oluşturma; Saldırganlar, sahte AWS hesabı oluşturarak AWS bulut platformunda arka kapı hesapları oluşturabilir. Saldırganlar, mevcut politikaları değiştirerek veya API'ler ve AWS Kaynak Erişim Yöneticisi (RAM) aracılığıyla kaynakları istismar ederek bulut platformundaki mevcut kaynakları kötüye kullanır. Saldırganlar, AWS bulut platformunda arka kapı hesapları oluşturmak için Endgame ve Pacu gibi araçları kullanır.

Endgame; Saldırganların sahte hesap aracılığıyla mevcut AWS bulut platformu üzerinde kontrol sahibi olmalarına ve içinde arka kapı hesabı oluşturmalarına yardımcı olan istismar çerçevesidir. Saldırgan, aracın tam uzunluktaki yeteneklerini kullanarak hedeflenen AWS bulut platformunda arka kapı hesapları listesi oluşturabilir. Kaynak politikalarını değiştirme ayrıcalığına sahip bir hedef kullanıcı hesabı için AWS API kimlik bilgilerine erişim gerektiren istismar sonrası araçtır.

Kullanıcı hesabıyla IAM kaynaklarını listelemek için şu komutu çalıştırın: endgame list-resources -s iam

$3 kovalarını listelemek için aşağıdaki komutu çalıştırın: endgame list-resources --service s3

Hizmetler genelinde kaynakları listelemek için şu komutu çalıştırın: endgame list-resources --service all

Belirli bir kaynağa arka kapı oluşturmak için şu komutu çalıştırın: endgame expose --service iam --name test-resource-exposure

Docker Görüntülerini Dockerscan Kullanarak Arka Kapı Haline Getirme; Dockerscan, saldırganların şu kötü amaçlı etkinlikleri gerçekleştirmesine olanak tanıyan Docker analiz ve saldırı aracıdır; Docker kayıtlarını belirlemek için ağları tarayınız. Görüntü/etiketi kaldırarak, arka kapılı görüntü göndererek ve kötü amaçlı dosya yükleyerek kayıt defterlerini değiştiriniz. Ortam değişkenlerinden parolalara erişim, ortam değişkenlerindeki URL'leri/IP'leri belirleme, yazılımı dahili olarak çalıştırmak için kullanılan kullanıcı kimlik bilgilerini belirleme dahil olmak üzere Docker görüntüsünden hassas bilgileri almak için görüntüleri analiz ediniz. Docker görüntülerini ayıklayın ve değiştiriniz; buna Docker'daki giriş noktasını değiştirme, içine ters bir kabuk enjekte ederek Docker görüntüsünü truva atı haline getirme, Docker görüntüsünde çalışan kullanıcıyı değiştirme de dahildir.

AWS Bulut Ortamında Erişimi Koruma ve İzleri Kapatma;

CloudTrial Hizmetini Manipüle Etme; Saldırganlar bulut kaynaklarına yönetici düzeyinde erişim elde ettikten sonra bulut denemelerini algılanmadan kalmak ve tehlikeye atılmış ortama kalıcı erişim elde etmek için manipüle eder. AWS bulut ortamında, kullanıcı etkinlikleri CloudTrial hizmeti aracılığıyla izlenir. Saldırganın tehlikeye atılmış ortama üst düzey erişim elde ettikten sonra gerçekleştirdiği ilk adım izleri gizlemektir. Varsayılan olarak, CloudTrail hizmeti devre dışıdır. Bir yöneticinin CloudTrial hizmetini etkinleştirmek ve kullanıcı etkinliklerini izlemek için denemeleri yapılandırmak üzere açıkça yapılandırması gerekir. Saldırganlar, CloudTrial hizmetini duraklatarak ve saldırıyı gerçekleştirdikten sonra hizmeti devam ettirerek günlük kaydı işlevini devre dışı bırakır.

CloudTrials üzerinden günlük kaydını durdurmak için şu komutu çalıştırın: $ aws cloudtrial stop-logging --name targetcloud_ trail --profile

administrator

Deneme durumunu edinmek için aşağıdaki komutu çalıştırın:$ aws cloudtrial get-trial-status --name targetcloud_trail --profile

administrator

CloudTrial hizmetini devre dışı bıraktıktan sonra saldırganlar arka kapı IAM kullanıcıları oluşturma, veri sızdırma ve kripto madenciliği betiği çalıştırma gibi çeşitli kötü amaçlı etkinlikler gerçekleştirebilir.

Saldırının yürütülmesi tamamlandıktan sonra saldırganlar, şu komutu çalıştırarak izlerin günlüğe kaydedilmesini tekrar etkinleştirecektir:

$ aws cloudtrail start-logging --name targetcloud_trail --profile

administrator

Bazı senaryolarda, saldırganlar şu komutu çalıştırarak izleri kalıcı olarak kaldırabilir:

$ aws cloudtrail delete-trail --name targetcloud_ trail --profile

administrator

Alternatif olarak, saldırganlar şu komutu çalıştırarak denemeleri depolayan kovanın içeriğini silebilir:

$ aws s3 rb s3://<Bucket_Name or Bucket _Reference> --force --profile

administrator

Saldırganların izleri örtmek için kullandıkları teknikler şunlardır; Bulut denemelerini yeni bir anahtar kullanarak şifrelemek. İzleri yeni S3 kovasına taşımak. Yeni iz girişlerini silmek için AWS Lambda işlevini kullanmak.

Günlükleri temizledikten sonra saldırganlar bulut altyapısına kalıcı erişimi sürdürmek için daha fazla istismar gerçekleştirir. Sonuç olarak saldırganlar şu teknikleri kullanarak AWS altyapısına arka kapılar kurar; ayrıcalıklı erişim haklarına sahip EC2 örneğiyle ilişkili kullanıcı verilerini manipüle etmek. Ayrıcalıklı rol atayarak AMI'ye bağlı olarak yeni EC2 örnekleri oluşturmak. Mevcut Lambda işlevine arka kapı eklemek. Rabbit lambda, cli_lambda ve backdoor_created_users_ lambda gibi Lambda işlevlerini kullanarak erişim anahtarlarını manipüle etmek.

AWS Hacking Aracı;

AWS pwn;

Erişimi Sürdürme;

rabbit_lambda ; Silinen kullanıcının daha fazla kopyasını oluşturarak kullanıcı silme olaylarına yanıt verir.

backdoor_created_users lambda ; Her yeni oluşturulan kullanıcıya bir erişim anahtarı ekler.

backdoor_created_roles_lambda ; Her yeni oluşturulan role bir trustrelationship ekler.

backdoor_created_security_groups_lambda ; Her yeni oluşturulan güvenlik grubuna belirli bir gelen erişim kuralı ekler.

./disrupt_cloudtrail.py -s ; Cloudtrail'i kesintiye uğratma girişimleri.

Keşif; AWS kullanıcıları ve hesap bilgileri hakkında bilgi toplamak için şu betikleri çalıştırın:

validate_iam_access_keys.py ; Erişim anahtarı + gizli [+oturum] kombinasyonlarının bir TSV dosyası verildiğinde, bu betik erişim geçerliliğini kontrol eder ve sorumluların kimlik bilgilerini döndürür.

validate_s3_buckets.py ; Satır başına bir kelime içeren bir metin dosyası verildiğinde, betik kovaların var olup olmadığını kontrol eder ve temel tanımlama bilgilerini döndürür.

validate_iam principals.py ; Yöneticilerin bir metin dosyası verildiğinde betik yöneticilerin belirli bir hesapta olup olmadığını kontrol eder.

validate_accounts.py ; Hesap kimlikleri ve takma adların bir metin dosyası verildiğinde, betik hesapların olup olmadığını kontrol eder.

Ayrıcalık Yükseltme; Farklı erişim düzeyleri almak ve ayrıcalıkları yükseltmek için aşağıdaki betikleri çalıştırınız.

dump instance attributes.py ; Hesaptaki her EC2 örneğini inceler ve belirtilen örnek özniteliklerini alır. Genelde gizli bilgiler içeren kullanıcı verilerini almak için kullanılır.

dump _cloudformation_ stack descriptions.py ; Her mevcut yığın ve son 90 günde silinen her yığın için yığın açıklamalarını alır.

assume_roles.py ; Bir dosyadaki veya liste rolleri API'si tarafından sağlanan tüm ARN'leri varsaymaya çalışır.

./assume_roles.py -o /tmp/out.json add_iam_policy.py ; Yöneticiyi ve tüm eylem politikasını belirli bir kullanıcıya, role veya gruba ekler. IAM putPolicy veya attachPolicy ayrıcalıkları gerektirir.

bouncy bouncy cloudy cloud.py ; Belirli bir EC2 örneğini geri döndürür ve kullanıcı verilerini yeniden yazar, böylece rastgele kodlar çalıştırılabilir veya geçici örnek profili kimlik bilgileri çalınabilir.

Erişimi Koruma ; Bir hesaba erişimi korumak için şu betikleri çalıştırınız.

rabbit_lambda ; Silinen kullanıcının daha fazla kopyasını oluşturarak kullanıcı silme olaylarına yanıt veren Lambda işlevi örneğidir.

eli lambda ; AWS cli proksi'si olarak hareket eden ve kimlik bilgisi gerektirmeyen Lambda işlevidir.

backdoor _created_users_lambda ; Her yeni oluşturulan kullanıcıya bir erişim anahtarı ekleyen Lambda işlevidir.

backdoor _created_roles_ lambda ; Her yeni oluşturulan role bir güven ilişkisi ekleyen Lambda işlevidir.

backdoor _created_security_groups_lambda ; Her yeni oluşturulan güvenlik grubuna belirli bir gelen erişim kuralı ekleyen Lambda işlevidir.

backdoor _all_users.py ; Hesaptaki her kullanıcıya bir erişim anahtarı ekler.

backdoor_all_roles.py ; Hesaptaki her role bir güven ilişkisi ekler.

backdoor _all_ security groups.py ; Hesaptaki her güvenlik grubuna belirli bir gelen erişim kuralı ekler.

İzleri temizleme; Bir saldırının izlerini gizlemek için şu betiği çalıştırınız.

interrupt_cloudtrail.py ; Belirtilen şekilde cloudtrail günlüğünü bozmaya çalışır.

Bulut Güvenliği; Bulut hizmetinin benimsenmesi ve iş açısından kritik verilerin üçüncü taraf sistemlere taşınmasıyla ilişkili çeşitli riskler ve tehditler vardır. Fakat güvenlik yönergelerini ve karşı önlemleri izlemek bulut benimsemesi için iş durumunu güçlendirir.

Bulut Güvenliği Kontrol Katmanları;

Uygulama Katmanı; Uygulama katmanını güçlendirmek için endüstri benimseme güvenlik standartlarıyla eşleşen politikaları belirleyiniz. Uygun düzenleyici ve iş gereksinimlerini karşılamalı ve bunlara uymalıdır. Uygulama katmanı kontrolleri arasında yazılım geliştirme yaşam döngüsü, ikili analiz, tarayıcılar, web uygulaması _ güvenlik duvarları, işlemsel güvenlik vb. bulunur.

Bilgi Katmanı; Bilgileri yetkisiz erişime, değişikliğe veya silinmeye karşı korumak için idari, teknik ve fiziksel güvenlik önlemleri içeren bilgi güvenliği yönetim programı geliştirin ve belgelendiriniz. Bilgi katmanı güvenlik kontrollerinden bazıları veri kaybı önleme (DLP), içerik izleme ve filtreleme, veritabanı etkinlik izleme, şifreleme vb. içermektedir.

Yönetim Katmanı; Bulutun sürekli, kesintisiz ve etkili hizmetlerini kolaylaştırabilen bulut güvenliği yönetim görevlerini kapsar. Bulut tüketicileri daha iyi hizmetlerden yararlanmak için yukarıda belirtilen politikaları aramalıdır. Yönetim katmanı güvenlik kontrollerinden bazıları yönetişim riski uyumluluğu (GRC), IAM, VA/VM, yama yönetimi, yapılandırma yönetimi, izleme vb. içerir.

Ağ Katmanı; Ağ yöneticisi tarafından ağa erişilebilen kaynakların yasadışı erişimini, kötüye kullanımını, değiştirilmesini veya reddedilmesini izlemek ve önlemek için benimsenen çeşitli önlemler ve politikalarla ilgilenir. Ağ katmanı güvenlik kontrolleri arasında ağ saldırı önleme/tespit hizmetleri, güvenlik duvarları, derin paket denetimi, DDoS önleme, hizmet kalitesi (QoS), DNSSEC ve OAuth bulunur.

Güvenilir Bilgi İşlem; Bulut işlemlerinin kullanılabilirliğini ve bütünlüğünü sağlamak için dahili kontrol, denetlenebilirlik ve bakım uygulayan güvenli hesaplama ortamını tanımlar. Donanım ve yazılım RoT ve API, güvenilir bilgi işlem için birkaç güvenlik kontrolüdür.

Hesaplama ve Depolama; Bulutta, verilerin ve makinenin fiziksel kontrolünün olmaması nedeniyle, hizmet sağlayıcı verileri ve hesaplamayı yönetemeyebilir, bulut tüketicilerinin güvenini kaybedebilir. CSP'ler, yasal, düzenleyici, sözleşmesel veya iş gereksinimleri, uyumluluğu karşılayan hizmetlerin kullanılabilirliğini, sürekliliğini sağlamak için veri depolama ve saklama politikaları, prosedürleri oluşturmalı, uygun yedekleme mekanizmaları uygulamalıdır. Host bilgisayar tabanlı güvenlik duvarları, host bilgisayar tabanlı saldırı tespit/önleme sistemleri, bütünlük ve dosya/günlük yönetimi, şifreleme ve maskeleme, hesaplama ve depolamada bazı güvenlik kontrolleridir.

Fiziksel Katman; Bulut altyapısı, veri merkezleri ve fiziksel kaynaklar için güvenlik önlemlerini içermektedir. Bu çevre altına giren güvenlik varlıkları fiziksel tesis güvenliği, çitler, duvarlar, bariyerler, muhafızlar, kapılar, elektronik gözetim, CCTV, fiziksel kimlik doğrulama mekanizmaları, güvenlik devriyeleri vb.'dir.

Bulut Güvenliği Hem Bulut Sağlayıcısının Hem de Tüketicinin Sorumluluğundadır; Güvenlik, hem bulut tüketicilerinin hem de CSP'lerin mevcut bilgi işlem kaynakları üzerinde farklı düzeylerde kontrole sahip olduğu bulut sistemlerinde paylaşılan sorumluluktur. Tek bir kuruluşun bilgi işlem kaynaklarının tamamı ve sistemlerin tüm yaşam döngüsü üzerinde yetkiye sahip olduğu geleneksel BT sistemleriyle karşılaştırıldığında, CSP'ler ve tüketiciler bulut tabanlı sistemleri tasarlamak, oluşturmak, dağıtmak ve işletmek için birlikte çalışırlar. Bu nedenle, her iki taraf da bu sistemler için yeterli güvenliği sağlama sorumluluğunu paylaşır. Farklı bulut hizmeti modelleri (laaS, PaaS ve SaaS), CSP'ler ve bulut tüketicileri arasında farklı düzeylerde kontrol anlamına gelir.

laaS platform sağlayıcısı genelde başlangıçtaki sistem ayrıcalıklı kullanıcıları için hesap yönetimi kontrolleri gerçekleştirirken, bir bulut tüketicisi laasS'de dağıtılan uygulamalar için kullanıcı hesap yönetimini kontrol eder.

Bazı bulut güvenlik kontrolleri şöyledir; PKI (Genel anahtar altyapısı), SDL (Güvenlik geliştirme yaşam döngüsü), WAF (Web uygulama güvenlik duvarı), FW (Güvenlik duvarı), RTG (Gerçek trafik yakalayıcı), IAM (Kimlik ve Erişim Yönetimi), ENC (Şifreleme), DLP (Veri kaybı önleme), IPS (Saldırı önleme sistemi), SWG (Güvenli web ağ geçidi), VA/VM (Sanal uygulama/Sanal makine), App Sec (Uygulama güvenliği), AV (Virüsten koruma), VPN (Sanal özel ağ), LB (Yük dengeleyici), GRC (Yönetim, risk ve uyumluluk), Config Control (Yapılandırma denetimi), CoS/QoS (Hizmet sınıfı/Hizmet kalitesi), DDoS (Dağıtılmış hizmet reddi), TPM (Güvenilir platform modülü), Netflow (Cisco tarafından sağlanan ağ protokolü).

Bulut Bilişim Güvenlik Hususları; Bulut bilişim hizmetleri, müşterilerin verilen güvenlik gereksinimlerine göre satıcı tarafından özel olarak yapılmalıdır. CSP'ler, bulut kaynaklarının optimum kullanımını sağlayan yüksek çoklu kiracı sağlamalı, verileri ve uygulamaları güvenli hale getirmelidir. Bulut hizmetleri, beklenmeyen durumlarda bilgi alınmasını sağlayan depolanan veriler için felaket kurtarma planı uygulamalıdır. Tüketiciler ve hizmet sağlayıcılar arasındaki hizmet seviyesi anlaşmalarını sürdürmek için QoS'nin sürekli izlenmesi gerekir. Veri bütünlüğünü sağlamak için bulut hizmetlerinde depolanan veriler güvenli şekilde uygulanmalıdır. Bulut bilişim hizmeti hızlı, güvenilir olmalı ve yeni isteklere hızlı yanıt süreleri sağlayabilmelidir. Bulut bilişimde optimum veri güvenliği için simetrik ve asimetrik kriptografik algoritmalar uygulanmalıdır. Bulut tabanlı hizmetlerin operasyonel süreci, kurumsal güvenlik yönetimine güvenli bir şekilde tasarlanmalı, işletilmeli ve entegre edilmelidir. Yük dengeleme, işin yanıt süresini maksimum verimle iyileştirmek için ağları ve kaynakları kolaylaştırmak amacıyla bulut hizmetlerine dahil edilmelidir. CSP'ler fiziksel tehditlere karşı daha iyi dayanıklılık ve gelişmiş koruma sağlamalıdır. Genel bulut hizmetleri, taşıyıcı sınıfı ağ ve özel VPN gibi gelişmiş ağ seçenekleri kullanmalıdır. CSP'ler uygun olay işleme ve yanıt planlarını dahil etmelidir. CSP'ler, rol ataması, rol yetkilendirmesi, işlem yetkilendirmesi gibi rol tabanlı korumaların uygulanmasını destekleyen hizmetlerden yararlanmalıdır. Bulut hizmetleri, güvenlik bilgilerinin büyük bir veritabanından oluşan küresel tehdit istihbarat veritabanından yararlanmalıdır. Bulut sağlayıcıları, DLP yeteneklerine sahip güvenli web ağ geçidi sağlamak için CASB çözümünü dahil etmelidir İş uygulamalarını segmentlere ayırmak için sıfır güven ilkelerini kullanınız.

Bulutta Güvenlik Kontrollerinin Yerleştirilmesi; Bilgi güvenliği kontrollerini seçmek ve bunları genelde tehditleri, güvenlik açıklarını ve etkileri değerlendirerek risklere orantılı olarak uygulamak en iyi uygulamadır. Bulut güvenlik mimarisinin verimli olması için uygun savunma uygulamasının yerinde olduğundan emin olunmalıdır. Birçok güvenlik kontrolü, uygun bir yerde tutulduğunda sistemdeki herhangi bir açığı koruyabilir ve bir saldırının etkilerini azaltabilir.

Güvenlik kontrollerinin kategorileri;

Caydırıcı kontroller; Bu kontroller bulut sistemine yapılan saldırıları azaltır.

Önleyici kontroller; Bu kontroller, güvenlik açıklarını en aza indirerek veya ortadan kaldırarak sistemi olaylara karşı güçlendirir.

Tespit edici kontroller; Bu kontroller meydana gelen olayları tespit eder ve uygun şekilde tepki verir.

Düzeltici kontroller; Bu kontroller, hasarı sınırlayarak bir olayın sonuçlarını en aza indirir.

Bulutu Güvence Altına Almak İçin En İyi Uygulamalar; Veri koruma, yedekleme ve saklama mekanizmalarını uygulayınız. Yama ve güvenlik açığı giderme için SLA'ları uygulayınız. Tedarikçiler düzenli olarak AICPA SAS 70 Tip II denetimlerinden geçmelidir. Bulutunuzu kamuya açık kara listelerde olmadığını doğrulayınız. Çalışan davranış politikasında yasal sözleşmeleri uygulayınız. Kullanıcı kimlik bilgilerinin kullanıcılar, uygulamalar ve hizmetler arasında paylaşılmasını yasaklayınız. Güvenli kimlik doğrulama, yetkilendirme ve denetim kontrollerini uygulayınız. Hem tasarım hem de çalışma zamanında veri korumasını kontrol ediniz. Güçlü anahtar oluşturma, depolama, yönetim ve imha uygulamalarını uygulayınız. İstemcinin trafiğini kötü amaçlı etkinlikler açısından izleyiniz. Güvenlik kontrol noktalarını kullanarak yetkisiz sunucu erişimini önleyiniz. Müşterilere geçerli günlükleri ve verileri ifşa ediniz. Bulut sağlayıcı güvenlik politikalarını ve SLA'larını analiz ediniz. Bulut API'lerinin güvenliğini değerlendirin ve müşteri ağ trafiğini kaydediniz. Bulutun düzenli güvenlik kontrolleri ve güncellemelerinden geçtiğinden emin olunuz. Fiziksel güvenliğin 7 gün 24 saat açık olduğundan emin olunuz. Kurulum/yapılandırmada güvenlik standartlarını uygulayınız. Belleğin, depolamanın ve ağ erişiminin izole edildiğinden emin olunuz. Mümkün olduğunda güçlü iki faktörlü kimlik doğrulama tekniklerinden yararlanınız. Temel güvenlik ihlali bildirim süreci uygulayınız. API bağımlılık zinciri yazılım modüllerini analiz ediniz. Sıkı kayıt ve doğrulama sürecini uygulayınız. Güvenlik açığı ve yapılandırma risk değerlendirmesi gerçekleştiriniz. Altyapı bilgilerini, güvenlik yamalarını ve güvenlik duvarı ayrıntılarını müşterilere açıklayınız. Sıkı bulut güvenliği uyumluluğunu, yazılım yapılandırma yönetimini (SCM) ve yönetim uygulaması şeffaflığını uygulayınız. Bulutta depolanan verilere yetkisiz erişimi korumak ve durdurmak için IDS, IPS ve güvenlik duvarı gibi güvenlik aygıtlarını kullanınız. Sıkı tedarik zinciri yönetimini uygulayın ve kapsamlı tedarikçi değerlendirmesi yapınız. Erişim kontrol politikası, bilgi güvenliği yönetim politikası, sözleşme politikası gibi sıkı güvenlik politikalarını ve prosedürlerini uygulayınız. Uygun yönetim ve izleme, kullanılabilirlik, güvenli VM ayırma ve hizmet güvencesi yoluyla altyapı güvenliğini sağlayınız. İstemci verilerini güvence altına almak için VPN'leri kullanın ve veri imhası talep edildiğinde bunların birincil sunuculardan ve replikalarından tamamen silindiğinden emin olunuz. Hassas ve gizli veri iletimi için SSL kullanıldığından emin olunuz. Bulut sağlayıcı arayüzlerinin güvenlik modelini analiz ediniz. Minimum çalışma süresi düzeyi ve kararlaştırılan düzeye uyulmaması durumunda cezalar gibi SLA'daki hüküm ve koşulları anlayınız. Temel bilgi güvenliği uygulamalarını uygulayınız. (güçlü parola politikası, fiziksel güvenlik, cihaz güvenliği, şifreleme, veri güvenliği, ağ güvenliği gibi) Kaynak yapılandırmasında tutarlılığı sağlayın ve katılım ile kurtarma uygulamalarını uygulayınız. En az müdahaleci politikaları oluşturmak için kurumsal risk tolerans seviyesini değerlendiriniz. Altyapı bilgilerini, güvenlik yamalarını, güvenlik duvarı ayrıntılarını müşterilere açıklayınız. Bulut hizmetleri genelinde kimlik yönetimi için tutarlı çerçeve uygulayınız.

Tehditleri hızla belirlemek, analiz etmek ve ortadan kaldırmak için otomasyon ve AI/ML teknolojilerini uygulayınız. Anormallikleri izlemek ve hem dahili hem de harici veri kaybını azaltmak için kullanıcı davranış analitiği gibi teknolojilerden yararlanınız. Tek amaçlı iş yükleri için uygulama beyaz listeleme ve bellek istismarı önlemeyi dağıtınız. LaaS veya PaaS kullanırken gelişmiş uç nokta güvenlik çözümleri ve kötü amaçlı yazılım önleme teknolojisi uygulayınız. Mevcut bulut güvenlik çabalarının verileri ve uygulamaları korumak için yeterli olup olmadığını kontrol etmek için penetrasyon testleri gerçekleştiriniz. Bulutta optimum güvenlik kontrollerinin kullanıldığından emin olmak için bulut erişim güvenlik aracısı (CASB) uygulayınız. Buluttan hassas verileri uyumlu şekilde güvenli şekilde silmek için bulut veri silme politikası ayarlayınız.

Bulut Güvenliği için NIST Önerileri; Müşterinin verilerine, yazılımlarına ve altyapısına yönelik riski değerlendiriniz. İhtiyaçlara göre uygun dağıtım modeli seçiniz. Veri koruması ve yazılım izolasyonu için denetim prosedürlerinin yerinde olduğundan emin olunuz. Kuruluşun güvenlik gereksinimleri ile bulut sağlayıcısının standartları arasında güvenlik boşlukları olması durumunda SLA'ları yenileyiniz. Uygun olay algılama ve raporlama mekanizmaları oluşturunuz. Kuruluşun güvenlik hedeflerini analiz ediniz. Buluttaki veri gizliliği ve güvenlik sorunlarından kimin sorumlu olduğunu sorunuz.

Güvenlik İddiası İşaretleme Dili (SAML); İki iletişim kuran varlık arasında kimlik doğrulama ve yetkilendirme için kullanılan popüler açık standart protokoldür. Kullanıcıların ortak kimlik bilgileri kümesiyle birden fazla uygulama veya hizmetle etkileşim kurması için tek oturum açma (SSO) olanağı sağlar. SAML, hizmet sağlayıcıya (SP) ve kimlik sağlayıcıya (IdP) kurulabilen, kullanıcılar için federasyon yetkilendirme ve kimlik doğrulama mekanizmalarını basitleştiren hizmet olarak yazılım olarak sunulabilir. SAML protokolü üç varlıktan oluşur;

İstemci veya kullanıcı: Web tarayıcısı aracılığıyla hizmet veya kaynak talep eden geçerli bir hesaba sahip varlıktır.

Hizmet sağlayıcı (SP): Kullanıcılar için uygulamaları veya hizmetleri barındıran bir sunucudur.

Kimlik sağlayıcı (IdP): Kullanıcı dizinlerini ve doğrulama mekanizmalarını depolayan sistem içindeki varlıktır.

SAML federasyon yazılımı kurulduğunda veya yapılandırıldığında, SP ve IdP arasında güvenli iletişimi sağlayan bir güven ilişkisi kurar. Bir kullanıcı herhangi bir hizmete veya kaynağa erişmek istediğinde, kimlik sağlayıcısı tarafından kimliği doğrulanmalıdır. Kullanıcıdan bir hizmet isteği başlatıldıktan kısa bir süre sonra, SP kullanıcıyı doğrulamak için kimlik sağlayıcısına SAML isteği gönderir. Ardından kimlik sağlayıcısı, başlatılan oturum açma girişiminin türünü (şifre, iki faktörlü, vb.) açıklayan XML tabanlı SAML kimlik doğrulama doğrulaması oluşturur; kullanıcı hakkında belirli ayrıntıları içeren SAML öznitelik doğrulaması ve kullanıcının hizmete erişmesine izin verilip verilmeyeceğini açıklayan yetkilendirme doğrulamasıdır. Daha sonra XML tabanlı doğrulamalar SP'ye iletilir. Kimlik doğrulama işlemi başarıyla tamamlandıktan sonra kullanıcı korunan kaynaklara veya hizmetlere erişmekte özgürdür.

Bulut Ağ Güvenliği; Bulut ağı, bulut hizmet sağlayıcıları (CSP) tarafından yönetilen sanal BT altyapısıdır. Burada ağ kaynakları özel ve genel bulutlar biçiminde talep üzerine sağlanır. Mevcut bir fiziksel ağ aracılığıyla bulut içinde sanal ortam oluşturarak, CSP'ler bireysel istemci hesaplarını kullanarak genel bulutta ağ işlemleri gerçekleştirebilir.

Bulut ağ güvenliği şu yollarla sağlanabilir;

Sanal özel bulut (VPC); Genel bulut içerisinde bulunan güvenli ve bağımsız özel bulut ortamıdır. VPC istemcileri, kendi bireysel hesaplarını kullanarak özel ağ üzerinde programları yürütebilir, uygulamaları barındırabilir, verileri kaydedebilir ve istedikleri her şeyi gerçekleştirebilir fakat özel bulut genel bulut sağlayıcısı tarafından barındırılır. VPC genelde aynı hesapla çalışan diğer VPC'lerden bağımsızdır; dolayısıyla bir VPC istemcisi, başka bir istemcinin VPC'lerine yönlendirilen trafiği görüntüleyemez. İstemci ayrıca bir IPv6 bloğu oluşturabilir ve bu blok içerisinde birden fazla alt ağ ekleyebilir. VPC, genel bulut bilişiminin ölçeklenebilirliğini ve diğer optimum özelliklerini özel bulut bilişiminin veri ayrımıyla birleştirebilir. VPC kaynakları talep üzerine kullanılabilir ve gereksinime göre genişletilebilir ve yapılandırılabilir.

Genel ve özel alt ağlar: VPC'deki alt ağlar genel veya özel olabilir. Genel alt ağda bulunan sanal makineler, veri paketlerini doğrudan web üzerinden iletebilirken, özel bir alt ağdaki VM'ler iletemez. Genel bir alt ağ, bant genişliği üzerinde herhangi bir koşul olmaksızın VPC'den IPv4 ve IPv6 trafiğine izin veren İnternet Ağ Geçidi (IGW) aracılığıyla iletileri ileten bir dışa doğru yoldan oluşur. Genel alt ağdaki sanal makineler, ağ ACL'leri ve güvenlik grupları izin verdiği sürece IGW aracılığıyla gelen trafiği de alabilir.

Özel alt ağ, genel ağ adresi çevirisi (NAT) ağ geçidi aracılığıyla harici web'e bağlanabilir. Yönlendirme aygıtının kendisi NAT gerçekleştirir. NAT web'den gelen trafiğe doğrudan izin vermez, bu da alt ağı özel hale getirir. Özel alt ağ için harici bağlantı, VPN hizmetleri kullanılarak da oluşturulabilir.

Geçiş ağ geçitleri: Şirket içi tüketici ağı ile VPC'ler arasında merkezi bir birim aracılığıyla iletişim kuran ve yöneten ağ yönlendirme çözümüdür. Bu yaklaşım; ağ topolojisini basitleştirerek karmaşık eşleme bağlantılarını ortadan kaldırır. Fakat bu iletişimlere, host bilgisayarların bağlantı noktası numaralarına, IP adreslerine bağlı olarak buluta özgü ACL'ler tarafından izin verilebilir veya engellenebilir. Merkezi birim sayesinde, yönetici veya ağ yöneticisi, cihaz bağlantıları yazılım tanımlı geniş alan ağı (SD-WAN) üzerinden yapılsa bile, tüm ağın net bir resmine sahip olabilir.

VPC uç noktası; İnternete, harici ağ geçitlerine, NAT çözümlerine, VPN bağlantılarına veya genel adreslere erişim olmadan VPC ile başka bir bulut hizmeti arasında özel bir bağlantı kurar. Bu nedenle de uç noktalar arasındaki trafik kuruluşun ağından çıkmaz. Buradaki uç noktalar sanal bilgi işlem cihazlarıdır. Bunlar; herhangi bir bant genişliği kısıtlaması veya kullanılabilirlik arızası olmadan VPC'deki sanal makineler ile bulut hizmetleri arasında etkileşime izin veren yedekli, ölçeklenebilir ve yüksek düzeyde kullanılabilir VPC öğeleridir. İki tür VPC uç noktası bulunmaktadır;

Arayüz uç noktası; Tanımlı bir alt ağın sınırı içinde özel IP adresine sahip elastik ağ arabirimidir (ENI). Bir VPC'ye veya desteklenen bulut hizmetlerine giden trafik için ilk kaynak noktası olarak çalışmaktadır.

Ağ geçidi yük dengeleyici uç noktası:; Aynı zamanda bir ENI'dir ve trafik akışını engellemek, bunu daha sonra güvenlik denetimi için kullanılan ağ geçidi yük dengeleyici aracılığıyla yapılandırılmış bir hizmete yönlendirmek için ilk kaynak noktası olarak çalışmaktadır.

Bulut Güvenlik Kontrolleri; Bulut ortamını her türlü güvenlik açığından koruyarak siber saldırıların etkilerini en aza indirmektedir. Bu kontroller,İ bulut altyapısını güvence altına almak için uygulanan uygulamaları, prosedürleri, yönergeleri ve politikaları içerebilir.

Bulut Uygulama Güvenliği; Box, Google G Suite, Slack ve Microsoft Office 365 gibi işbirlikçi bulut platformları arasındaki tüm veri alışverişini yöneten bir dizi kural, süreç, politika, kontrol ve tekniktir. Çalışanlar veya kullanıcılar uzun vadede bulut platformlarında veri depolar ve gönderirse, sıfır güven güvenlik uygulamasında "güvenlik ağı" olarak bilinen bulut tabanlı bir çözümün dahil edilmesi zorunludur. Bulut uygulama güvenliği sadece SaaS, laaS ve PaaS uygulama katmanlarına uygulanır. Bulut uygulama güvenliğinin uygulanması; siteler arası betik çalıştırma (XSS), siteler arası istek sahteciliği (CSRF), oturum ele geçirme, SQL enjeksiyonu ve zayıf kimlik doğrulama gibi istismarları önler.

Bölgeler Arası Yüksek Kullanılabilirlik; Bir uygulama için bulut ortamı, uygulamanın hizmetleri kasıtlı veya kasıtsız ağ kesintileri sırasında devam ederse yüksek kullanılabilirliğe sahiptir. Yüksek kullanılabilirlik, sunucuları bölgelere ayırarak ve bunlar arasında ağ tutarlılığını koruyarak elde edilebilir. Ortamın, veri kaybetmeden bireysel kullanılabilirlik bölgelerindeki veya ağdaki arızaları ele almasını sağlar. Ağ işlemlerini ve kaynak kullanımını izlemek için merkezi yönetim sağlar.

Yüksek kullanılabilirliğe sahip bir bulut ortamı iki düğümden oluşur; ana düğüm ve ikincil düğüm. İlk sunucu ilk kullanılabilirlik bölgesinde, ikinci sunucu ise ikincil kullanılabilirlik bölgesinde çalışır. Bu ortam; disk arızası, birim arızası, ağ arızası ve bölge arızası gibi çeşitli hizmet kesintilerinden korunur. Bu kısımda her düğüm bağımsızdır ve ayrı bölgelere sahiptir. Herhangi bir düğüm arızalanırsa, verilerinin bir kopyasının diğer düğümde bulunması sağlanarak tüm bilgilere erişim sağlar. Diğer düğüm aktif olarak hizmetleri sağlarken bir düğüm yükseltilmek üzere kapatılabilir.

Bulut Entegrasyonu ve Denetimi; Bulut entegrasyonu, yöneticilerin sistemlere, hizmetlere, verilere ve uygulamalara sürekli olarak erişmesini ve bunları yönetmesini sağlayan genel veya karma bulut biçiminde birden fazla bulut ortamını bir araya getirme sürecidir. Bir bulut ortamını şirket içi ortamla birleştirir. Bulut entegrasyonu olmadan, yöneticilerin her entegrasyon görevini bağımsız ve manuel olarak gerçekleştirmesi gerekir. Bu da zaman alıcı ve hataya açık bir işlemdir. Şirket içi ağlar için risk göstergeleri genelde ağ veya uygulama günlüklerinde tespit edilirken, bulut tabanlı risk göstergeleri API günlüklerinden elde edilir. Bu nedenle, tüm hizmetler tanımlanmış güvenlik politikalarına veya yönergelerine göre entegre edilmeli, güvenlik uyumluluğunu sağlamak için daha fazla denetlenmelidir. Bulut entegrasyon mekanizmaları, kuruluşun tüm verilerine kapsamlı bir görünüm sağlar, bağlantıyı geliştirir ve değerlendirme için tüm risk göstergelerinin toplanmasına yardımcı olur.

Bulut denetimi, bulut sağlayıcıları tarafından sunulan hizmetleri analiz etme ve bulut ortamı için gizlilik, güvenlik ve performans gereksinimlerine uygunluğu doğrulama sürecidir. Bulut güvenlik denetimleri, hem geleneksel hem de bulut altyapısıyla ilişkili sorunları ele almalıdır. Uygun bir denetim, müşterilere her koşulda düzenli ve kapsamlı bir şekilde hizmet sunulmasını sağlayabilir. Sistematik değerlendirme ve karşılaştırma için güvenlik ve operasyonlar hakkında otomatik veri toplama sunar. Hem büyük hem de küçük işletmeler için zamandan tasarruf sağlayan uygun maliyetli bir yaklaşımdır çünkü bir kez sağlanan bilgiler, değişiklikler uygulandığında dinamik olarak güncellenebilir.

Güvenlik Grupları; Bir güvenlik grubu, sanal örneklere güvenlik sağlamak için bulut altyapısında uygulanan temel bir güvenlik önlemidir. Sanal makineler için güvenlik çözümü görevi görür. Güvenlik grubu, internet ve sanal örnekler arasında yer alarak gelen ve giden trafiği kontrol eder. Düzgün yapılandırılmış bir güvenlik grubu, hizmet reddi (DoS) saldırılarını ve BT kaynaklarına yetkisiz erişimi önler.

Örnek Farkındalığı; Bulut tabanlı öldürme zinciri modeli, bulut ortamından veri sızdırmak için komut ve kontrol için sahte bulut örnekleri kullanma olasılıklarını açıklar. Güvenlik duvarları, ağ geçitleri ve diğer bulut güvenlik araçları gibi birçok güvenlik çözümü, bulut uygulamalarının örnekleri arasındaki farkları izleyemedikleri için bu tehditlerle mücadele edemez. Saldırganlar genellikle bulut ağlarını hedef alırken bu yetersizlikten yararlanır. Bu nedenle, veri sızdırma ve SaaS kimlik avı gibi bulut tabanlı tehditlere karşı koruma sağlamak için Google Drive ve OneDrive gibi bulut örneklerini fark eden veya ayırt edebilen araçları kullanmak gerekir.

Kubernetes Güvenlik Açıkları ve Çözümleri; En iyi genel bulut sağlayıcıları da dahil olmak üzere çeşitli kuruluşlarda Kubernetes teknolojilerinin artan popülaritesi ve kabulünün sonucunda kritik güvenlik açıkları artmıştır. Güvenlik uzmanlarının güvenlik açıklarını tespit etmesi ve gelişmiş güvenlik çözümleri uygulaması zorunlu hale gelmiştir.

Sunucusuz Güvenlik Riskleri ve Çözümleri; Sunucusuz bilişim; sıfır yönetim, kullanım başına ödeme hizmeti ve kendi kendine ölçeklenebilirlik gibi dikkat çekici özellikleri nedeniyle popüler hale gelmiştir. Sunucusuz teknolojinin birçok avantajı olmasına rağmen aynı zamanda azaltılması gereken yeni riskler de ortaya çıkarmıştır.

Konteyner Güvenliği için En İyi Uygulamalar; Konteyner çalışma zamanının CVE'lerini düzenli olarak izleyin ve güvenlik açıkları tespit edilirse bunları düzeltiniz. Konteyner ağ arayüzlerini, ağ trafiğini ve ağ anormalliklerini izlemek için uygulama farkındalı araçları kullanınız. Ayrıcalık yükseltmesini önlemek için uygulamaları normal kullanıcılar olarak çalışacak şekilde yapılandırınız. Yazma erişimini kısıtlamak ve kötü amaçlı yazılım enjeksiyon saldırılarını önlemek için host bilgisayarın kök dosya sistemini salt okunur modunda yapılandırınız. Üçüncü taraf yazılım kullanmaktan kaçınarak konteynerleri kötü amaçlı yazılımlardan korumak için uygulama güvenliği tarama araçlarını kullanınız.

Güvenlik açıklarını veya yanlış yapılandırmaları belirlemek için depodaki görüntüleri düzenli olarak tarayınız. Konteyner güvenliğini artırmak ve tehditlerin ortama girmesini önlemek için uygulama güvenlik duvarları dağıtınız. Hassas görüntüler ve veriler dahil olmak üzere kayıtlara kimlik doğrulamalı erişimi sağlayınız. Bireysel uygulamaların daha iyi görünürlüğü ve gelişmiş veri yönetimi için her uygulama için ayrı bir veritabanı kullanınız. Host bilgisayar işletim sistemini ve çekirdeği düzenli olarak en son güvenlik yamalarına güncelleyiniz. Orkestratörleri, duyarlılık seviyelerine göre bir dizi host bilgisayarı ayrı ayrı dağıtmak üzere yapılandırınız. Konteyner çalışma zamanı yapılandırma standartlarına uyumu otomatikleştiriniz. Gömülü kötü amaçlı yazılımlar için görüntülerin sürekli izlenmesini gerçekleştiriniz. Hassas verileri harici olarak depolayın ve çalışma zamanında dinamik erişime izin veriniz. Güvenilir kayıt defterleri ve görüntüler kümesini koruyun ve yalnızca bu kümeden görüntülerin kapsayıcı ortamında çalışmasına izin verildiğinden emin olunuz. Uygulamalara ve sistem hizmetlerine yönelik saldırıları önlemek için SELinux ve AppArmor gibi zorunlu erişim kontrol araçlarını kullanınız. Gerçek zamanlı tehdit algılama çözümleri kullanın ve güvenlik olaylarını ele almak için olay yanıtlama yetenekleri geliştiriniz. Dağıtımdan sonra kapsayıcı değişikliğine izin vermeyen değiştirilemez kapsayıcılar uygulayınız.Kullanıcıların varsayılan ayrıcalıklarını kökten kök olmayana değiştirin ve rol tabanlı erişim kontrolü (RBAC) kullanarak izinleri yapılandırınız. Hassas bilgileri kod ve yapılandırma dosyalarına yazmaktan kaçınınız. Kritik olmayan yerel hizmetleri kaldırarak host bilgisayar ortamını güçlendirmenin yanında tüm yığını güçlendiriniz. Bileşen sayısını azaltarak kapsayıcıları her zaman hafif tutunuz. Bulut kaynaklarını yönetmek ve dağıtımdan önce yapılandırmayı doğrulamak için Altyapı-Kod Olarak (laC)'yi kullanınız.

Docker Güvenliği için En İyi Uygulamalar; Docker daemon soketini açığa çıkartmaktan kaçının çünkü burası Docker API için temel giriş noktasıdır. Kötü niyetli kullanıcılar tarafından oluşturulan Docker imajlarına arka kapılar enjekte edilebileceğinden sadece güvenilir Docker imajları kullanınız. Host bilgisayar işletim sistemini ve Docker'ı en son güvenlik güncellemeleriyle düzenli olarak yamalayınız. Sadece konteyner tarafından gerekli olan özelliklere erişime izin vererek yetenekleri sınırlayınız. Konteynere atanmış tüm yetenekleri bırakmak ve ardından sadece gerekli yetenekleri atamak için --cap-drop all komutunu kullanabilirsiniz. Setuid veya setgid ikili dosyalarını kullanarak ayrıcalık yükseltme saldırılarını önlemek için Docker imajlarını her zaman --security-opt=no-new-privileges ile çalıştırınız. --icc=false kullanarak Docker demon'u çalıştırırken konteynerler arası iletişim özelliğini devre dışı bırakınız. Diğer konteynerlerle iletişim kurmak için --link=CONTAINER_NAME veya _ID:ALIAS seçeneğini kullanabilirsiniz. Seccomp, AppArmor ve SELinux gibi Linux güvenlik modüllerini kullanarak işlemler yapınız. Bellek, CPU, maksimum dosya tanımlayıcı sayısı, maksimum işlem sayısı ve DoS saldırılarını önlemek için yeniden başlatmalar gibi kaynakları sınırlayınız. - read-on1ly bayrağını ayarlayarak dosya sistemlerinde ve birimlerde salt okunur modunu etkinleştiriniz. Docker daemon günlük düzeyini 'info' olarak ayarlayınız ve Docker daemon'u 'debug' günlük düzeyini kullanarak çalıştırmaktan kaçınınız .Docker imajı için varsayılan kullanıcı ayarı köktür; ayrıcalık yükseltme saldırılarını önlemek için kapsayıcı uygulamasını ayrıcalıksız kullanıcı olarak çalışacak şekilde yapılandırınız. Saldırı yüzeyini azaltmak için sadece gerekli paketleri yükleyiniz. Uzak kayıt defterindeki Docker görüntülerinin Docker içerik güvenini kullanarak dijital olarak imzalandığını kontrol ediniz. Hassas bilgiler için çevresel değişkenleri kullanmaktan kaçının ve gizli bilgileri aktarım sırasında şifrelemek için Docker gizli bilgileri yönetimini kullanınız. RESTful API'yi açığa çıkarırken API uç noktalarını HTTPS ile güvenceye alınız. Ağ ile tek host bilgisayar uygulamasını kullanırken varsayılan köprü ağını kullanmaktan kaçınınız. Gelişmiş veri güvenliği, veri kalıcılığı ve veri şifrelemesi için hassas verileri her zaman Docker birimlerinde saklayınız. Docker istemcisi ile daemon arasında HTTPS üzerinden güvenli iletişim için TLS'yi etkinleştirerek temel kimlik doğrulamasını oluşturunuz. Docker güvenlik açıklarını tespit etmek için InSpec ve DevSec gibi araçları kullanınız. Test ve sorun giderme gibi yönetimsel işlemleri gerçekleştirirken konteynerlerin günlük dosyalarını işlemek için SSH oturum açma bağlantılarını yöneticiyle sınırlayınız. Konteynerlere erişirken tutarsızlığı önlemek için otomatik konteyner etiketleme mekanizmasını kullanınız. Daha sağlıklı ve güvenli dosyalar sağlamak için mümkün olan her yerde HEALTHCHECK komutunu docker dosyalarına dahil ediniz.

Kubernetes Güvenliği için En İyi Uygulamalar; İşlemin her aşamasında dosya içeriklerinin ve yollarının doğru şekilde doğrulandığından emin olunuz. Kimlik bilgileri yolları için yapılandırma yöntemini uygulayın ve sabit kodlanmış yollara bağlı kalmayınız. Bileşik bir işlemin her adımından sonra hataları açıkça yükseltiniz. Kubelet yeniden başlatıldığında günlüklerin kaybolmamasını sağlamak için günlük döndürme için kopyala-sonra-yeniden adlandır yöntemini kullanınız. JSON nesneleri oluşturmak için iyi test edilmiş JSON kitaplığını ve tür yapılarını kullanınız. Sistem durumunu etkiledikleri için uygun doğrulamalar olmadan asla bileşik kabuk komutlarını kullanmayınız. PID'nin bir çekirdek işlemi olup olmadığını belirlemek için os.Readlink /proc/<pid>/exe'nin döndürülen hata değerini açıkça kontrol ediniz. Kod okunabilirliğini artırmak için kod tabanında ortak görevleri gerçekleştirmek, ParsePort gibi ortak ayrıştırma işlevlerini kullanmak için merkezi kitaplıkları kullanınız. Günlük rotasyonu yerine kalıcı günlükler kullanarak günlükleri doğrusal sırada yazabilir ve rotasyon gerektiğinde yeni günlükler oluşturulabilirsiniz. Merkezi doğrulamayı desteklediği için tüm yapılandırma görevleri için tek kodlama biçimi kullanınız. Kubelet'te bellek dışı hatalarını önlemek için manifest dosyalarının boyutunu sınırlayınız. Sunulan sertifikaları kontrol etmek için CRL'leri koruyan kube-apiserver örneklerini kullanınız. Gizli veri şifrelemesini etkinleştirmek ve şifreleme için AES Galois/Counter modunu veya şifreli blok zincirlemesini kullanmaktan kaçınmak için anahtar yönetim hizmetlerini kullanınız. Sertifikaların CA tarafından verildiğinden emin olmak ve MITM saldırılarını önlemek için tüm HTTPS bağlantılarını varsayılan olarak doğrulayınız. Sunucu IP adreslerinin doğruluğunu düzgün şekilde doğrulamadıkları için eski SSH tünellerini kullanmaktan kaçınınız. Sertifikaların iptal durumunu kontrol etmek için çevrimiçi sertifika durumu protokolü (OSCP) zımbalama kullanınız. Yanlış yapılandırmadan kaynaklanan güvenlik açıklarını azaltmak için geliştirme ve üretim yapılandırmalarında varsayılan olarak güvenli TLS kullanınız. Dosya erişim izinlerini yönetmek ve yetkisiz erişimi önlemek için ACL'leri kullanınız. Taşıyıcı belirteçleri ve diğer hassas bilgiler gibi temel kimlik doğrulamasını günlük verilerinden kaldırmak için günlük filtrelemeyi kullanınız.

Sunucusuz Güvenlik İçin En İyi Uygulamalar; Saldırı yüzey alanını azaltmak için geliştirme aşamasında sunucusuz izinleri en aza indiriniz. Kötü amaçlı kod enjeksiyonu ve diğer web sunucusu saldırılarının girişimlerini belirlemek için işlev katmanlarını düzenli olarak izleyiniz. Ek görünürlük ve kontrol katmanları sağladıkları için üçüncü taraf güvenlik araçlarını kullanınız. İşlev bağımlılıklarını ve uygulamalarını düzenli olarak yamalayın ve güncelleyiniz. Bilinen güvenlik açıkları için sunucusuz uygulamaları taramak üzere Snyk gibi araçları kullanınız.

İzole işlev çevrelerini koruyun ve işlev erişimi ve çağrı sıralamasına güvenmekten kaçınınız. Kod enjeksiyon saldırılarını önlemek için olay girişini uygun şekilde temizleyiniz. Kaynaklara erişimi devre dışı bırakan ve çalışma zamanı en az ayrıcalıklarını uygulayan güvenlik kitaplıklarını kullanınız. Ayrıntı düzeyini en aza indirmek ve örtük genel rolleri önlemek için işlevleri en düşük ayrıntı düzeyinde dağıtınız. Veri serileştirmeyi kaldırmak yerine şemalarda ve veri aktarım nesnelerinde veri doğrulama tekniğini kullanınız. Giriş veri filtreleme, trafik kısıtlama, hız sınırlaması gerçekleştirmek, DDoS saldırılarına karşı koruma sağlamak için API ağ geçidi yeteneklerinden yararlanınız. Daha iyi gözlemlenebilirlik elde etmek için işlev olaylarının ayrıntılı ve güvenli şekilde günlüğe kaydedilmesini zorunlu kılarak işlevleri denetleyin ve izleyiniz. Güvenlik açığı olan uygulama kodlarını düzeltmek için güvenli kodlama uygulamalarını kullanın ve kod inceleme oturumları gerçekleştirin, paylaşılan güvenlik kitaplıklarını kullanınız. Güvenli iletişim için TLS/HTTPS kullanın, kimlik bilgilerini şifrelemek için kriptografik algoritmalar kullanınız. Uzak kimlikle iletişimi tanımak ve doğrulama başarısız olursa iletişimin durmasını sağlamak için SSL sertifikalarını doğrulayınız. Aktarım sırasında verileri korumak ve HTTP'yi önlemek için bulut satıcıları için imzalı istekleri etkinleştiriniz. Hem çalışma zamanı erişimi hem de anahtar rotasyonu sağlayan hassas bilgiler için gizli depolama kullanınız. Sunucusuz işlevlerin ne kadar uzun süre yürütülebileceğini sınırlamak için zaman aşımı kullanınız.

Sıfır Güven Ağları; Sıfır Güven modeli, varsayılan olarak ağa erişmeye çalışan her kullanıcının güvenilir bir varlık olmadığını varsayan ve ağa erişime izin vermeden önce gelen her bağlantıyı doğrulayan güvenlik uygulamasıdır. "Kimseye güvenmeyin ve bir bulut hizmeti sağlamadan veya erişim izni vermeden önce doğrulayın" ilkesine sıkı sıkıya uyar. Bu aslında şirketin çalışanlarının zarar vereceği anlamına gelmez fakat ağ tehlikeye girebilir veya ağı kullanmaya çalışan bir kişi güvenilir olmayabilir. Bu güven modeli; kullanıcıların/çalışanların doğrulanmadan bir ağa erişmesini önler. Şirketlerin, çalışanların sadece iş rolleri için gereken uygun kaynaklara erişmesine izin vermek gibi koşullar koymasına olanak tanır.

Bulut kontrol düzlemi, veri düzlemini (ağdaki diğer tüm bileşenleri) koordine eden ve yönetebilen bir destek sistemidir. Kontrol düzlemi, sadece meşru ve doğrulanmış kullanıcılardan veya cihazlardan gelen ağ erişim isteklerine izin verir. Bu katmanda; kuruluştaki role, günün saatine ve cihaz türüne göre ayrıntılı politikalar uygulanır. Daha güvenli İnternet kaynaklarına erişmek için kullanıcıların daha güçlü kimlik doğrulamasına ihtiyacı vardır. Erişim isteği kontrol paneli tarafından onaylandıktan sonra, veri düzlemi yalnızca o belirli istemciden gelen trafiği kabul edecek şekilde yapılandırılır.

Bu modeli uygulamanın arkasındaki fikir; kaynaklara erişimin güvenli bir yolunu sağlamak, sıkı erişim denetimi uygulamak ve ağ trafiği akışını izlemektir.

Sıfır Güven; şifreleme, çok faktörlü kimlik doğrulama, ayrıcalıklı erişim yönetimi (PAM) gibi tekniklerle entegre edilebilir. Bu güven ağı; ağın belirli bölümlerine ayrı erişim sağlamak için ağ bölgesini daha küçük parçalara bölmek için mikro segmentasyon yöntemini izler. Herhangi bir çevre ihlali belirlenirse, mikro segmentasyon ağın daha fazla istismar edilmesini önler.

Kuruluş/Sağlayıcı Bulut Güvenliği Uyumluluk Kontrol Listesi;

Uluslararası Bulut Güvenlik Örgütleri; Bazı uluslararası bulut güvenlik örgütleri, güvenlik uzmanlarına en iyi uygulamalar, güvenlik farkındalığı ve daha iyi siber güvenlik dayanıklılığı, güvenilir bulut ekosistemi sağlayan güçlü güvenlik politikaları konusunda yardımcı olmaya adanmıştır.

Bulut Güvenlik İttifakı (CSA) ; Artan farkındalık sağlayan ve bulut ortamına yardımcı olmak, güvenliğini sağlamak için en iyi uygulamaları ve güvenlik politikalarını teşvik eden kar amacı gütmeyen küresel bir örgüttür. Bulut bilişimin kullanımları hakkında eğitim ve bilgi sağlayıp her türlü bilişimin güvenliğini sağlamaya yardımcı olurlar. Bulut tabanlı araştırma, eğitim, sertifikasyon ve ürünler sağlamak için endüstrilerin, hükümetlerin ve kurumsal üyelerin konu uzmanlığını birbirine bağlamak için kullanılabilir.

Bulut Güvenlik Araçları ; Buluta geçişin muazzam faydaları olmasına rağmen, güvenlik sorunları öncelikli endişe kaynağıdır. Bulutta barındırılan verilerin gizliliğini, bütünlüğünü ve güvenliğini sağlamak için bulut penetrasyon testi sürecini otomatikleştirmek için birçok mevcut güvenlik hizmeti veya aracı kullanılabilir.

Gölge Bulut Varlık Keşif Araçları ; Gölge bulut varlıkları, BT departmanının gözlemi dışında kurumsal ortamda kullanılan bulut uygulamaları veya hizmetleridir. Bu tür varlıklar; veri kaybı, hesap kötüye kullanımı, kötü amaçlı yazılım bulaşması/dağıtımı gibi risk faktörlerini artırabilir. Bu güvenlik sorunlarının üstesinden gelmek için kuruluş, uygulama kullanımında tam görünürlük sağlayan Cisco Umbrella ve Microsoft Defender for Cloud Apps gibi araçları kullanabilir. Bu araçlar, yöneticilerin kuruluşun bulut ağındaki ağ etkinliklerini izlemesine ve denetlemesine olanak tanır.

Cisco Umbrella ; Cisco Umbrella, bulut uygulamalarını güvenli ve düzenli şekilde yönetmek için tam görünürlük ve risk bilgisi sağlayan uygulama keşif aracıdır. Pano, gölge bulut hizmetlerinin risk düzeyini görüntüleyerek risk düzeylerine göre sıralanmış uygulama kategorilerine dayalı özet sunar. Gözden Geçirilmemiş, Denetim Altında, Onaylanmış ve Onaylanmamış gibi etiketlere sahip uygulamaların listesini izleme için sağlar. Yöneticilerin bir kullanıcının veya grubun bulut uygulamalarına erişimini engellemesine veya izin vermesine olanak tanır.

Diğer gölge bulut varlık keşif araçları şunlardır; Securiti, Microsoft Defender for Cloud Apps, FireCompass, Data Theorem, CloudCodes.

Bulut Güvenlik Araçları ;

Bulut ortamını güvence altına almak için bazı araçlar şunlardır:

Qualys Cloud Platform; Tüm BT varlıklarının nerede bulunduğuna bakılmaksızın görünürlük sağlayan, küresel güvenlik ve uyumluluk duruşunun sürekli, her zaman açık bir değerlendirmesini sağlayan uçtan uca bir BT güvenlik çözümüdür. Sürekli görünürlük sağlayan sensörler içererek tüm bulut verileri gerçek zamanlı olarak analiz edilebilir. Tehditlere anında yanıt verir, internet kontrol mesajı protokolü zaman damgası isteğinde etkin güvenlik açığı gerçekleştirir, sonuçları AssetView ile tek bir yerde görselleştirir.

Fidelis CloudPassage Halo; Genel bulut altyapısı için kapsamlı güvenlik görünürlüğü ve sürekli uyumluluk sağlar. Siber güvenlik risklerini azaltmak için kapsamlı görünürlük, koruma ve sürekli uyumluluk izleme sağlayan güvenlik otomasyon platformudur. Tüm bulut varlıklarını keşfetme, genel bulut saldırı yüzeyini azaltma, kritik riskleri belirleme ve sürekli uyumluluğu sürdürme gibi özellikler sunar.

Lookout CipherCloud; CASB, sıfır güven ağ erişimi (ZTNA), güvenli web ağ geçidi (SWG), veri kaybı önleme (DLP) dahil olmak üzere çeşitli gelişen güvenli erişim hizmeti kenarı (SASE) kategorilerini kapsar. Bu çözümler birlikte, bulut tabanlı uygulamalar için kapsamlı görünürlük, veri güvenliği, tehdit koruması ve uyumluluk sağlar.

Ek bulut güvenlik araçları şunlardır; Veri Farkında Bulut Güvenliği. Netskope Güvenlik Bulutu.Prisma Bulutu. ForgeRock Kimlik Bulutu. Derin Güvenlik.

Konteyner Güvenlik Araçları; Konteynerler bulut ortamlarında sürekli olarak dağıtıldığından, daha yüksek güvenlik standartlarıyla korunmaları gerekir. Güvenlik uzmanları, konteynerleri çeşitli güvenlik ihlallerine karşı korumak için Aqua, Sysdig Falco, Anchore, NeuVector ve Lacework gibi araçlar kullanır.

Aqua; Bilinen güvenlik açıkları, gömülü sırlar, yapılandırma ve izin sorunları, kötü amaçlı yazılımlar ve açık kaynaklı lisanslama açısından konteyner görüntülerini, sanal makineleri ve sunucusuz işlevleri tarar. Bu araç, güvenilmeyen kodun çalışmasını kısıtlar ve işlevlerin, konteynerlerin ve sanal makinelerin değiştirilemez kalmasını sağlayarak, kaynak görüntüleriyle karşılaştırıldığında çalışan iş yüklerinde herhangi bir değişiklik yapılmasını önler. Mevcut altyapıya entegre olabilir, böylelikle DevSecOps işbirliğini, günlük kaydını ve raporlamayı, olay yanıtını ve olay izlemeyi yönetmeyi kolaylaştırır.

Konteynerleri güvence altına almak için ek araçlar şöyledir; Sysdig Falco. Anchore. NeuVector. Lacework. Tenable.io Konteyner Güvenliği.

Kubernetes Güvenlik Araçları ; Kubernetes fiili bir konteyner dağıtım ve yönetim aracı olduğundan, iş yüklerinin düzenli olarak izlenmesi ve uygun güvenlik uygulamalarıyla güvence altına alınması gerekir. Güvenlik uzmanları, Kubernetes ortamını güvence altına almak için Kube-bench, Alcide Advisor, Advanced Cluster Security for Kubernetes gibi araçları kullanır.

Kube-bench; Kubernetes'in internet güvenliği merkezi Kubernetes kıyaslama belgelerine göre kontroller çalıştırarak güvenli şekilde dağıtılıp dağıtılmadığını kontrol etmek için kullanılan bir Go uygulamasıdır. Kubernetes kümeleri arasında izin, kimlik doğrulama, güvenlik kontrolleri gerçekleştirir ve kapsayıcı verilerini güvence altına alır.

Kubernetes ortamının güvenliği için ek araçlar şöyledir; Alcide Advisor. Kubernetes için Gelişmiş Küme Güvenliği. Aqua Kubernetes Güvenliği. KubexXray. Sumo Logic.

Sunucusuz Uygulama Güvenliği Çözümleri; Sunucusuz bulut bilişim son birkaç yılda muazzam bir büyümeye tanık olmuştur. Gelişen bulut tabanlı altyapı, işlev olayı veri enjeksiyonu, bozuk kimlik doğrulama, aşırı ayrıcalıklı işlev izinleri gibi çeşitli güvenlik risklerini de beraberinde getirmektedir. Bu nedenle, düzenli aralıklarla güvenlik denetimleri yapmak zorunludur. Güvenlik profesyonelleri, sunucusuz altyapıda güvenlik testleri yürütmek için CloudGuard, Synk ve Aqua Security for Serverless Functions (FaaS) gibi çeşitli araçlar kullanmaktadır.

CloudGuard; Sunucusuz uygulamalar için kapsamlı bir güvenlik çözümüdür. İşlevler, günlükler ve veritabanları için otomatik en az ayrıcalıklı koruma sağlar. Dahili makine tabanlı analiz mekanizmaları ve derin öğrenme algoritmalarıyla CloudGuard uygulama katmanı saldırılarını önceden tespit etmek ve engellemek için normal uygulama ve işlev davranışının bir modelini oluşturmaktadır.

Sunucusuz bilgi işlem ortamını güvence altına almak için ek araçlar şöyledir; Synk. Aqua Security for Serverless Functions (FaaS). Prisma Cloud. Dashbird. Thundra.

Bulut Erişim Güvenlik Aracısı (CASB); Şirket içi veya bulutta barındırılan çözümlerdir. Bulut uygulamalarında güvenlik, uyumluluk ve yönetişim politikalarını uygulamaktan sorumludurlar. Kuruluşun şirket içi altyapısı ile bulut sağlayıcısının altyapısı arasında yer alır. Kuruluşların güvenlik politikalarını kendi altyapılarının ötesine uzatmalarını sağlayan bekçi görevi görmektedirler.

CASB'nin Özellikleri;

Bulut kullanımına görünürlük; Gölge BT bulut hizmetlerini bulur ve izin verilen bulut uygulamalarıyla kullanıcı etkinliklerine görünürlük sağlar.

Veri güvenliği; Veri merkezli güvenlik şifrelemesini, belirteçlemeyi, erişim denetimini ve bilgi hakları yönetimini uygular.

Tehdit koruması; Kötü niyetli içeriden gelen tehditleri, ayrıcalıklı kullanıcı tehditlerini, tehlikeye atılmış hesapları algılar ve bunlara yanıt verir.

Uyumluluk ; Buluttaki kritik verileri keşfeder ve veri ikametgahı, uyumluluk gereksinimlerini karşılamak için DLP politikalarını uygular.

CASB'ler şunları sunar; Kötü amaçlı yazılımları tespit etmek için güvenlik duvarlarını kullanarak kötü amaçlı yazılımların kurumsal ağa girmesini önler.

Kullanıcı kimlik bilgileri için kimlik doğrulama yaparak sadece izin verilen kullanıcıların gerekli kurumsal kaynaklara erişebilmesini sağlar. Kötü amaçlı yazılımların ağ düzeyi yerine uygulama düzeyinde güvenliği ihlal etmesini önlemek için WAF'ler kullanılır. DLP, kullanıcıların kritik bilgileri kuruluş dışına aktarmasını önler.

CASB'ler nasıl çalışır: Şirket içi cihazlar ile bulut sağlayıcısı arasındaki ağ trafiğinin kurumsal güvenlik politikalarına uymasını sağlayarak çalışır. Bulut platformları genelinde bulut uygulamalarının kullanımına ilişkin öngörüler sağlayarak izinsiz kullanımı belirler. Otomatik keşfi kullanma, kullanımdaki bulut uygulamaları bulma, yüksek riskli uygulamaları bulma, yüksek riskli kullanıcıları bulma, şifreleme ve cihaz profili gibi farklı güvenlik erişim kontrollerini uygulamai SSO mevcut olmadığında kimlik bilgisi eşleme gibi hizmetler sağlamaktadır.

CASB Çözümleri;

Forcepoint CASB; Tüm bulut uygulamaları için eksiksiz güvenlik sağlar. Temel özellikleri arasında bulut uygulaması keşfi, bulut uygulaması risk puanlaması, veri sınıflandırması, kullanıcı ve uygulama yönetimi, gerçek zamanlı etkinlik izleme/analitiği, otomatik anormallik tespiti, veri kaybı önleme ve üçüncü taraf çözümlerle entegrasyon bulunur.

Ek CASB çözümleri şunlardır; CloudCodes. Cisco Cloudlock. Microsoft Cloud App Security. FortiCASB.

Yeni Nesil Güvenli Web Ağ Geçidi (NG SWG); Bir kuruluşun ağını bulut tabanlı tehditlerden, kötü amaçlı yazılım enfeksiyonlarından ve çevrimiçi veri hırsızlığından koruyan bulut tabanlı güvenlik çözümüdür. İstemcilerin bulut hizmetlerine güvenli şekilde erişmesini sağlar. Bulut tabanlı tehditleri önceden algılar, risklerine göre öncelik sırasına koyar, farklı kullanıcılar ve istemciler tarafından kullanılan uygulamayı yönetir. Modern bulut görünürlük yeteneklerinden ve özelliklerinden bazıları; URL filtreleme. Sertifika (TLS/SSL) şifre çözme. Tanımlama, şifre çözme, analiz etme ve trafiği güvence altına alma. Gelişmiş tehdit koruması (ATP), sanal alan ve makine öğrenimi (ML) odaklı anormallik tespiti. Web trafiği ve bulut uygulamaları için veri kaybı önleme (DLP) desteği. Web denetimi ve raporlaması için nitel meta veri bağlamları

NG SWG çözümlerinden bazıları şunlardır; Netskope Next Gen Secure Web Gateway. Cloudflare Gateway. Quantum Next Generation Firewall Security Gateways.