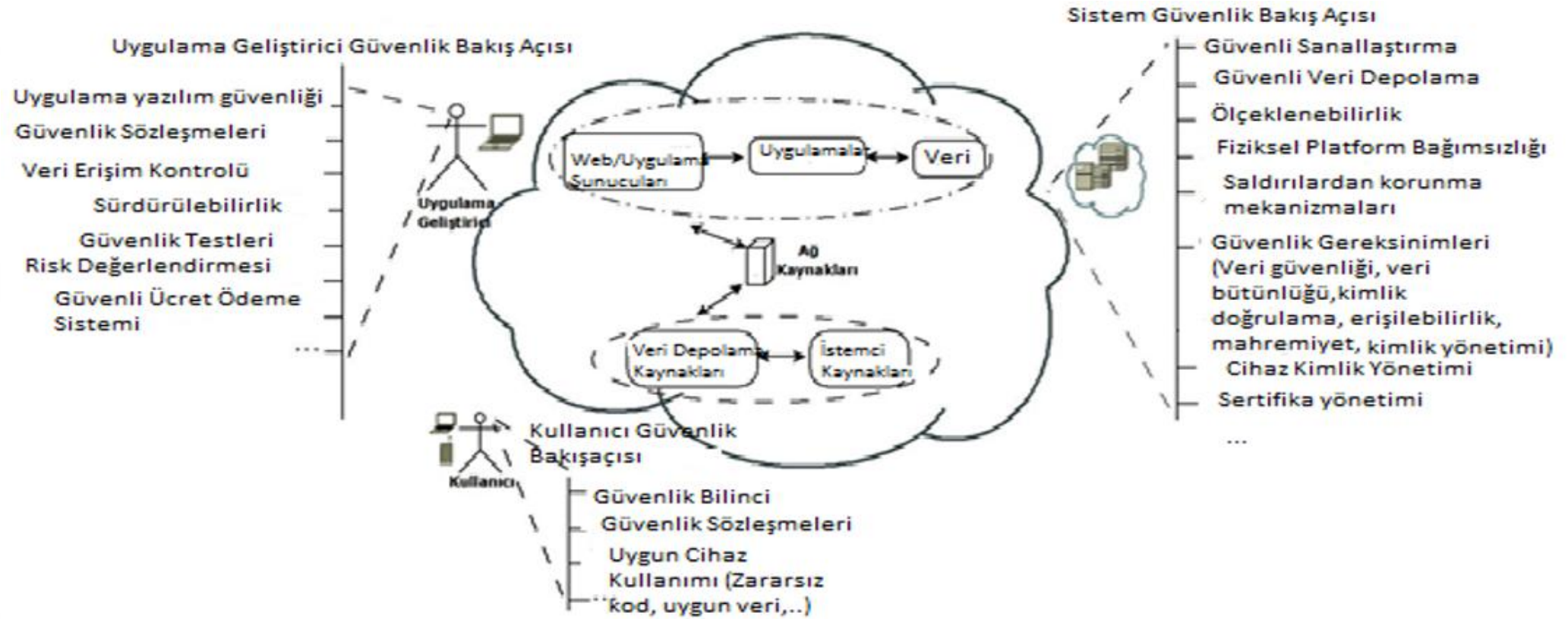


Bulut Sistem Güvenliđi: Saldırılar, Saldırılardan Korunma Yöntemleri

Dr. Fatih KALEMKUŞ

Kafkas Üniversitesi

Bulut Mimarisi Güvenliđi



Sistem Bakış Açısından Güvenlik

- Sistem her bileşenini güvenli biçimde yönetmek istemektedir.
- Öne çıkan başlıklar:
 - Güvenli sanallaştırma
 - Güvenli veri depolama
 - Saldırılardan korunma mekanizmaları
 - Güvenlik gereksinimleri
 - Cihaz kimlik yönetimi


Uygulama Geliřtirici Bakıř Aısından Gvenlik

- Bulut zerindeki uygulama, kullanıcıların ihtiya duyduėu grevleri gerekleřtirirken gerekli ek gvenlik gereksinimlerini de saėlamalıdır.
- PaaS zerinde sıklıkla gncellemeler yapılıp yeni srmler geldiėinden dolayı, uygulamalar da bu srmlere kolaylıkla uyarlanabilir olmalıdır.
- Yazılımların esnek olması sayesinde bilgi gvenliėi artırılmaktadır.

Uygulama Yazılım Güvenliđi - Güvenlik Testleri

- Güvenli yazılım, güvenliđi göz ardı etmeden tasarlanmış, güvenlik kontrolleri ile geliştirilmiş ve güvenli bir durumda kullanıma sunulmuş yazılım demektir.
 - Çalıştırılmayan yazılımlar dışında **%100 güvenli yazılım diye bir şey yoktur.** 😊
- Sızma Testleri
 - Belirlenmiş sistemlere her yol denenerek sızmaya çalışmak.
 - **Amaç:** Güvenlik açıklarını tespit etmek ve olası saldırılara karşı önlemler alabilmek.
 - *Örneđin, yetkiyle ilgili bir sorun tespit ettiysek, tüm erişim yetkilerini yazılımsal ve donanımsal olarak gözden geçirir ve bu delikleri kapatırız.*

Kullanıcı Bakış Açısından Güvenlik

- Kullanıcılar, verilerinin **kendi kontrolleri dışındaki bir ortamda** tutulmasından ve **kendi kontrol edemedikleri bir zaman dilimi içerisinde** işlenmesinden endişe duymaktadırlar.
- Kullanıcılara ait sorumluluklar: 
 - Bencil olmamak. 😊
 - Yalnızca kendi mahremiyetine değil, sisteme gelebilecek olası tehditlerin bilincinde olmak,
 - Güvenlik sözleşmelerini incelemek ve bu sözleşmelere uygun hareket etmek.

Bulut Mimarileri Üzerindeki Güvenlik Riskleri

○ AVANTAJLAR:

- Güvenliğin merkezileştirilmesi,
- Veri ve süreç bölünmesinin sağlanması

○ SORUNLAR:

- Yerel veya bölgesel düzenlemelere uyumlu olma,
- Erişim yetkisine sahip olunmayan alanlarda onay alınması,
- Denetim açısından ek karmaşıklıklar getirmesi,
- Bulut servislerindeki güven eksiklikleri

Gizlilik Riskleri

- Bulut servisleri eęer kişisel bilgileri ele almaktaysa, bulut mimarisinde mahremiyet kavramı da dikkate alınmalıdır.
 - Kişinin bulunduğu yere, tercihlere, sosyal ağlara ve bu gibi dinamik bilgilere göre kişiselleştirilen bulut servisleri için yüksek bir mahremiyet tehdidi öngörülebilmektedir.
- Kişisel bilgilere ek olarak, kurumsal bilgilerin ve ticari sırların da ağ üzerinde paylaşımı dikkate alındığında gizlilik de önemsenmelidir.

Veri Bütünlüğü Riskleri

- Veri bütünlüğü, veri üzerinde istenmeyen değişikliklerin önüne geçerek tutarsızlıkların oluşmasını engellemektir.
- Geleneksel veri tabanlarında **ACID (Atomicity, Consistency, Isolation and Durability)** ilkesi kullanılmaktadır ve tek bir veri tabanı üzerinde işlemler yapıldığından kolaydır.

A C I D
ATOMICITY CONSISTENCY ISOLATION DURABILITY

Veri Bütünlüğü Riskleri

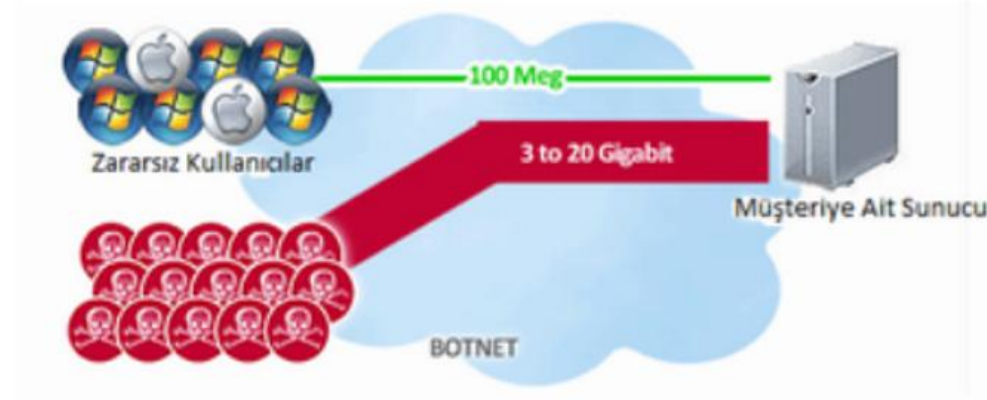
- Bulut ise, dağıtık bir sistemdir, birçok veri tabanı, birçok sistem ve birçok uygulama bulunmaktadır.
- Veri tabanları arası ya da sistemler arası erişimler ve yapılan işlemler dikkatli bir şekilde ele alınmalı ve yönetilmelidir.
- Bunu sağlamak için, **merkezi veritabanı hareket yöneticisi** (central global transaction manager) kullanılmaktadır.

Bulut Sistemlerine Yönelik Saldırıları

- Bulut birçok kullanıcı tarafından erişilebilir olduğundan ataklara daha açıktır.
 - **Dağıtık Hizmet Engelleme Saldırıları** (Distributed Denial of Service Attacks, DDoS)
 - **Yan Kanal Saldırıları** (Side Channel Attacks)
 - **Ortadaki Adam Saldırıları** (Man In The Middle Attacks)

Dağıtık Hizmet Engelleme Saldırıları - DDoS

- Bilgi güvenliği unsurlarından «erişilebilirliği» hedef almaktadır.
- Sistemin kaldırabileceği yükün çok üzerinde anlık istek sonucunda sistem yorulmakta ve cevap veremez hale getirilmektedir.



Dağıtık Hizmet Engelleme Saldırıları - DDoS

- Saldırganlar DDoS saldırıları düzenleyip, tehdit ile hizmet sağlayıcı firmalardan para talep edebilirler.
- Bulut bilişim hizmet sağlayıcıları;
 - Bu tür saldırılara karşı koyacak koruma düzeneklerini oluşturma yoluna gidebilir.
 - İhtiyaç anında hızlı ve dinamik kaynak ayırabilir.
 - Saldırının geldiği noktaları tespit edip engelleyebilir.



Yan Kanal Saldırıları

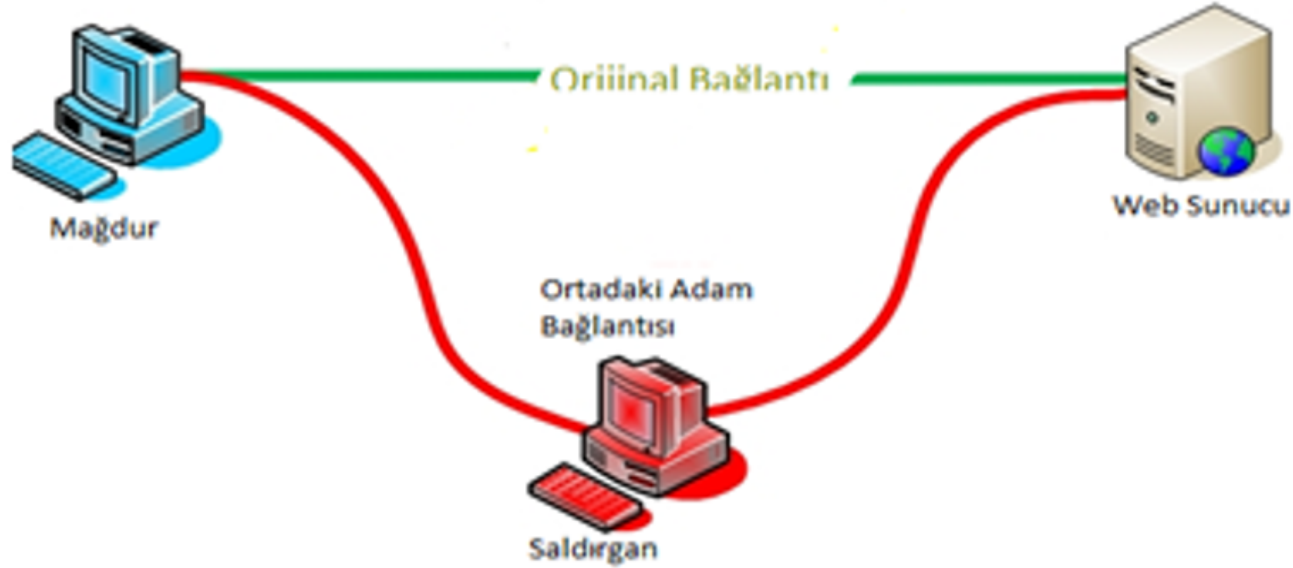
- Bulut mimarisindeki IAAS modeli, bulut altyapısını oluşturmaktadır. Bulut altyapısında;
 - Bilgisayar toplulukları,
 - Sanal makineler,
 - Uygulamalar,
 - Dosyalar,
 - Dokümanlar gibi genel kaynaklar bulunmaktadır.
- Saldırgan bulut sunucusu içerisindeki kötü niyetli bir **sanal makine içerisinde** konumlanır ve bu sanal makine aracılığı ile de gizli bilgilere erişebilir.

Yan Kanal Saldırıları

- Saldırı iki aşamada gerçekleşmektedir:
 - Yerleşme
 - Verinin Dışa Aktarımı
- Verilerin şifreli bir şekilde tutulmasının önemi bu saldırılarda ortaya çıkmaktadır.
 - Saldırgan veriye erişmiş olsa bile, veri şifreli olduğunda çözememekte ve amacına ulaşamamaktadır.

Ortadaki Adam Saldırıları

- Bu saldırıda, saldırgan kendisini iki kullanıcı arasında konumlandırmaktadır.



Bulut Saldırılarından Korunmak için Geliştirilen Yöntemler

- Bulut bilişim, çoklu kullanım desteği ve sanallaştırma özelliklerinden dolayı ölçeklenebilirliği sağlamaktadır.
 - Bir yazılımı bir kişiyle paylaşmak yerine, bir yazılımı birçok kullanıcı tarafından erişebilir kılmayı amaçlar.
- Bulutta gerekli kontrolleri sağlamak için geleneksel yöntemler işe yaramamaktadır. Çünkü erişim kontrol düzenekleri farklılık göstermektedir:
 - Geleneksel yöntemler → Uygulama merkezli erişim kontrolüne sahipler.
 - Sunucular → Aynı güvenilir alt birim içindeki erişim kontrol düzeneklerinden sorumludurlar.

Bulut Saldırılarından Korunmak için Geliştirilen Yöntemler

1. Kimlik Yönetimi ve Kullanıcı Doğrulama

- Bulut üzerinde her bilgi, kişilerin ya da kurumların bulut üzerinde kiraladıkları yerlerde saklanmaktadır.
- Kullanıcılar kendi kişisel bilgilerine internet olan herhangi bir ortamdan erişebilmektedir ve bu erişim kimlik yönetim sistemi ile sağlanmaktadır.
 - Bu mekanizma, kullanıcıların servis tabanlı hizmetler aracılığı ile kullanıcı adı ve şifrelerini doğrulayarak, kullanıcıya kendi kişisel bilgilerine erişme izni vermektedir.
 - Geliştirilen sistem :
Kimlik yönetim sistemi (Identity Management, IDM)



Bulut Saldırılarından Korunmak için Geliştirilen Yöntemler

1. Kimlik Yönetimi ve Kullanıcı Doğrulama

- Kullanıcı doğrulama servisleri, üçüncü parti sistemler ile bütünleştirilmek istendiğinde **gizlilik protokolleri** kullanılmaktadır.
- LDAP(Lightweight Directory Access Protocol) & AD(Active Directory)→
 - LDAP/AD sunucuları, bulut hizmeti dışında bırakılabilmekte ve erişim gerektiği zamanlarda bu sunucularla iletişime geçerek çözüm sağlanmaktadır.

Bulut Saldırılarından Korunmak için Geliştirilen Yöntemler

2. Erişim Kontrolü

- Sistem güvenliğinin, kaynakların ve verinin korunmasının ilk yolu, sistemin kendine gelen erişimleri kontrol altında tutmasıdır.
- Bulut sistemlerinde yaygınlıkla kullanılan erişim kontrol mekanizması **RBAC**'tir. (Role Temelli Erişim Kontrolü, Role Based Access Control)
 - RBAC'in kullanım kolaylığı,
 - Dinamik gereksinimlere ayak uydurabilme özelliği
 - En az yetki prensibine dayanması
 - Ayrıcalıkların dinamik kontrolü

Bulut Saldırılarından Korunmak için Geliştirilen Yöntemler

2. Erişim Kontrolü

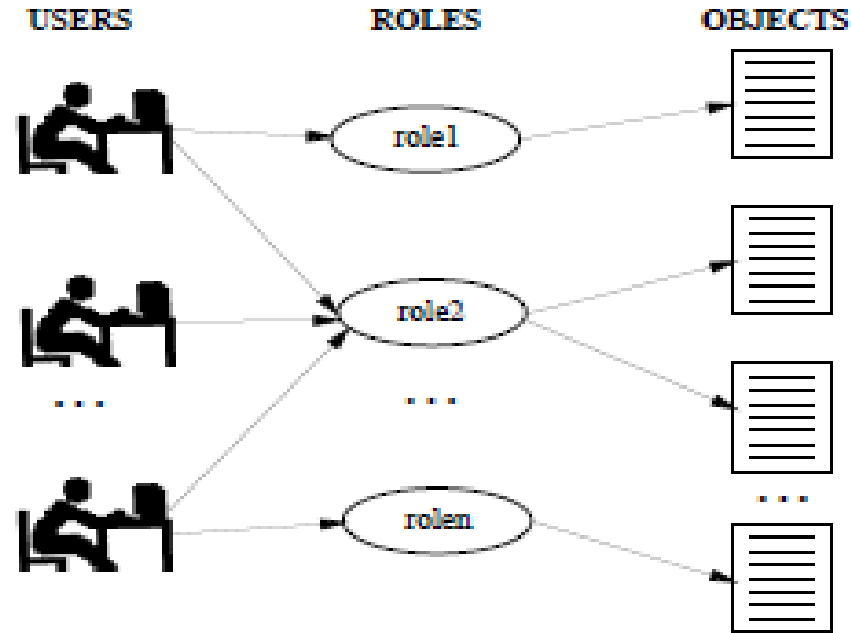


Fig. 20. Role-based access control

Bulut Saldırılarından Korunmak için Geliştirilen Yöntemler

3. Veri Şifreleme

- Şifrelemenin etkinliğinden emin olmak için şifreleme algoritmaları ile birlikte şifreyi açacak anahtarın da dayanıklılığı önem kazanmaktadır.
- Bulut ortamlarında çok büyük veri aktarımları, veri üzerinde işlemler, veri depolama ve yönetme işlemleri olduğundan, işlem hızı da şifreleme algoritmaları tasarlanırken önem kazanmaktadır.
 - Bulut sistemlerinde bu nedenle asimetrik şifreleme algoritmaları yerine simetrik şifreleme algoritmaları kullanılması daha uygundur.



Bulut Saldırılarından Korunmak için Geliştirilen Yöntemler

3. Veri Şifreleme

- Bu algoritmaları çözecek anahtarın yönetimi zayıf olduğunda veri güvenliği sağlanamamaktadır.
 - Anahtar verisinin korunması da veri güvenliği kapsamında değerlendirilmektedir.
- Bulut üzerinde anahtar yönetimi, kullanıcı sayısının çok olması ve sistemin karmaşık olmasından dolayı karmaşık ve zordur.
 - Mobil bulut sistemlerinde hesabın çalınmasına önlem olarak, dinamik şifre belirleme algoritmaları kullanılmaktadır.
 - Bu algoritmada; kullanıcı, yer değiştirdiğinde ya da belirli sayıda veri paketi alışverişi yaptığında, dinamik olarak şifre de değişmektedir.

Bulut Saldırılarından Korunmak için Geliştirilen Yöntemler

4. Veri Aktarımı

- Veri güvenliği ve bütünlüğünü sağlama yöntemlerinden bir tanesi veri aktarımlarının belirli protokoller üzerinden yapılmasıdır.
- Güvenliğin artırılması için izlenmesi gerekli adımlar:
 - Yalıtım,
 - Yedekleme ağının ana trafikten ayrılması,
 - Yedeklerin güvenli yerde tutulması,
 - Yeterli log kayıtları ve denetleme sağlanması,
 - Profesyonel olmayan son kullanıcılara eğitimler sağlanması

Bulut Bilişim Güvenliği Konusundaki Son Gelişmeler

1. Bulut Güvenliği Duruş Yönetimi (Cloud Security Posture Management -CSPM)

- Yönetim veya CSPM, bulut platformu hesaplarının yapılandırmasına bakarak veri ihlallerine ve sızıntılara yol açan olası yanlış yapılandırmaları belirler.
- CSPM, işletmelerin emniyet ve güvenlik açısından kullanıcılarıyla güven geliştirmesine yardımcı olur.
- Güvenliği otomatikleştirir ve bulutta uyumluluk güvencesi sağlar

Bulut Bilişim Güvenliği Konusundaki Son Gelişmeler

2. Buluta Ulaşmadan Önce Müşteri Verilerinin Korunmasını Sağlama

- Bulut bilişimin sayısız faydası vardır ancak güvenlik her zaman risk altındadır.
- Bulut veriler, sahibinin doğrudan kontrolü dışındadır ve bu nedenle veri güvenliği en önemli konu hâline gelmektedir.
- Artan veri ihlalleri, işletmeleri önceki veri koruma formatlarını iyileştirmeye yöneltmektedir.
- Bu amaçla geliştirilen şifreleme teknikleri verilerin bulut ile kullanıcı arasındaki hareketlerinde koruma altına alınmaktadır.

Bulut Bilişim Güvenliği Konusundaki Son Gelişmeler

3. Sıfır Güven Modeli (Zero Trust Model)

- Sıfır güven; ağları, uygulamaları ve verileri korumak için güven kavramını ortadan kaldıran bir BT güvenlik modelidir.
- Bu model, kötü aktörlerin her zaman ağın güvenilmeyen tarafında olduğunu ve güvenilir kullanıcıların her zaman güvenilen tarafta olduğunu varsayan geleneksel çevre güvenlik modelinin tam tersidir.
- Sıfır güven ile bu varsayımlar geçersiz kılınır ve tüm kullanıcıların güvenilmez olduğu varsayılır.

Bulut Bilişim Güvenliği Konusundaki Son Gelişmeler

4. Bulut İçinde Yazılım Yaşam Döngüsü (SDLC) ve DevSecOps

- DevOps ve bulut güvenliği, modern uygulama geliştirmenin en önemli alanlarından ikisidir.
- Farklı sistemler olsalar da bunlar birbirlerini tamamlamaktadır.
- Bu nedenle, DevSecOps'tan en iyi şekilde yararlanmak ve DevSecOps'un bulut güvenliğinin anlamını ve önemini gerçekten anlamak için güvenli bir yazılım geliştirme yaşam döngüsünün kavranması çok önemlidir.
- DevOps, yazılım geliştirme yaşam döngüsünü optimize etmeye yönelik en iyi uygulamaları içermektedir.

Bulut Bilişim Güvenliđi Konusundaki Son Gelişmeler

5. Akıllı Bulut Bilişim Güvenliđi

- Yapay zekâ ve makine öğrenmesinde yaşanan gelişmeler işletmelerin güvenlik tekniklerini yeniden değerlendirmelerini gerektirmektedir.
- Yeni teknoloji teknik gelişmeler, verilerin tam olarak korunmasını sağlayarak işletmeleri ciddi siber hırsızlıklardan kurtarabilir.
- Tespit edilmeyen hırsızlıklar, iyileşmesi zaman alan ciddi hasarlara neden olabileceğinden çok önemlidir.
- Yapay zekâ gibi akıllı teknolojiler siber tehditlere karşı çok daha verimli ve hızlı bir savunma çözümü yaratmaktadır.

Sonu

- Mevcut sistemleri bulut iine yerleřtirmek kolay bir iř olmamakla birlikte, dikkatli planlama ve ykleme ile maliyetleri nemli lde dřren bir yntemdir.
- Bulut sistemler, yapısı gereęi, paylařılan kaynak kullanılmalıdır.
 - *Aę, sunucular, depolama birimleri, uygulamalar veya servisler gibi.*
- Bu paylařımlı altyapı sunumu, birok gvenlik tehdidini de beraberinde getirmektedir.
 - Bu gvenlik tehditlerini en aza indirmek iin yntemler geliřtirilmeli,
 - Yazılımlar birbirinden soyutlanmalı ,
 - Srekli geliřtirilebilir olmalıdır.

Sorular



Dr. Fatih KALEMKUŞ

TEŐEKKÜRLER

Dr. Fatih KALEMKUŐ