**Bulut Bilişime Geçişin Zorlukları**

- Kuruluşlar, bulut tabanlı araçlar (cloud-based tools) ve teknolojiler (technologies) kullanarak altyapılarını değiştiriyor.
- Güvenli kullanılmadığında, bulut tabanlı teknolojiler dış tehditlere (external threats) maruz kalabilir.

**Veri Güvenliği Zorlukları**

- Üçüncü taraf bulut sağlayıcıları (cloud providers) güvenlik en iyi uygulamalarını takip etse de, veri varlık yönetimi (data asset management) hala kuruluşun sorumluluğundadır.
- Bulut ortamında (cloud environment) veri güvenliği ile ilgili zorluklar arasında görünürlük eksikliği (lack of visibility) ve çok kiracılılık (multitenancy) yer alır.

**Gelişen Tehditler ve Riskler**

- İç tehditler (insider threats), mevcut veya eski çalışanlar tarafından oluşturulabilir ve dış güvenlik sistemleri tarafından görünmezdir.
- Dağıtık hizmet reddi (DDoS) saldırıları, sunucuları aşırı trafikle hedef alarak çalışır.

**Paylaşılan Sorumluluk Modeli**

- Paylaşılan sorumluluk modeli (shared responsibility model), bulut sağlayıcısı ve kullanıcı arasında güvenlik sorumluluklarının paylaşıldığı bir çerçevedir.
- IaaS, PaaS ve SaaS (Infrastructure as a Service, Platform as a Service, Software as a Service) için farklı güvenlik sorumlulukları vardır.

**Veri Güvenliği Yetenekleri**

- Kritik veri varlıklarınızı (critical data assets) tanımlayın ve kimlerin erişim sağladığını (access) belirleyin.
- Veri kaybını (data loss) önlemek için politika ihlallerini (policy violations) tespit edin ve engelleyin.

**Erişim Kontrolleri ve Kimlik Yönetimi**

- Bulut kimlik ve erişim yönetimi (Cloud IAM) stratejileri geliştirin; sıfır güven mimarisi (zero trust architecture) uygulayın.
- Kullanıcıların her kaynağa (resource) sürekli olarak kimlik doğrulamasını (authentication) sağlayın.

**Ağ Güvenliği**

- Bulut ağ güvenliği (cloud network security) ile veri koruma ve uyumluluk politikalarını (compliance policies) uygulayın.
- Merkezi güvenlik izleme (centralized security monitoring) ve yönetimi sağlayın.

**En İyi Uygulamalar**

- Bulut kullanım durumunuzu (cloud usage state) ve risklerinizi (risks) belirleyin.
- Bulut sisteminizi korumak için şifreleme (encryption) ve veri paylaşım politikaları (data sharing policies) oluşturun.

**NIST Güvenlik Çerçevesi**

- NIST'in beş sütunlu güvenlik çerçevesi (cybersecurity framework): Tanımlama (Identify), Koruma (Protect), Tespit (Detect), Yanıt (Respond), Kurtarma (Recover).

**Coach**

Bu video, Kimlik ve Erişim Yönetimi (Identity and Access Management - IAM) konusunu ele alıyor ve bulut güvenliğinin (cloud security) ilk savunma hattı olarak nasıl çalıştığını açıklıyor.

**Kullanıcı Türleri**

- **Yönetici Kullanıcılar (Administrative Users)**: Bulut platformu yöneticileri, uygulama ve hizmet örneklerini (service instances) oluşturur, günceller ve siler.
- **Geliştirici Kullanıcılar (Developer Users)**: Uygulama geliştiricileri, hassas bilgilere erişim sağlar ve uygulamaları oluşturup günceller.
- **Uygulama Kullanıcıları (Application Users)**: Bulut tabanlı uygulamaların (cloud-hosted applications) son kullanıcılarıdır.

**Kimlik Doğrulama ve Erişim Kontrolü**

- **Kimlik Doğrulama (Authentication)**: Kullanıcıların kimliğini doğrulamak için çeşitli kimlik sağlayıcıları (identity providers) kullanılır.
- **Çok Faktörlü Kimlik Doğrulama (Multifactor Authentication)**: Kullanıcıların kimlik hırsızlığına karşı korunması için ek bir güvenlik katmanı sağlar.

**Kullanıcı ve Hizmet Erişimi Yönetimi**

- **Erişim Grupları (Access Groups)**: Kullanıcılar ve hizmet kimlikleri (service IDs) için erişim politikalarının (access policies) yönetimini kolaylaştırır.
- **Politikalar (Policies)**: Kullanıcıların ve hizmetlerin kaynaklara erişim izinlerini tanımlar.

**Raporlama ve Denetim**

- **Raporlama (Reporting)**: Kullanıcıların kaynaklara erişimlerini ve erişim haklarındaki değişiklikleri izler.
- **Denetim ve Uyum (Audit and Compliance)**: Uygulanan kontrollerin (controls) güvenlik politikalarına ve uyumluluk gereksinimlerine uygunluğunu doğrular.

Bu özet, Kimlik ve Erişim Yönetimi'nin bulut güvenliğindeki rolünü ve kullanıcıların erişim kontrolü süreçlerini anlamak için temel bilgileri sunmaktadır.

Şifreleme Sisteminin Temel Bileşenleri

- **Şifreleme algoritması (encryption algorithm)**, verilerin okunamaz hale getirilmesi için kuralları tanımlar.
- **Şifre çözme anahtarı (decryption key)**, şifrelenmiş verilerin tekrar okunabilir hale getirilmesini sağlar.

Veri Koruma Yöntemleri

- **Veri dinlenme (data at rest)**: Verilerin fiziksel olarak depolandığı yerlerde korunmasını sağlar.
- **Veri iletimi (data in transit)**: Verilerin bir yerden başka bir yere iletilirken korunmasını sağlar; genellikle SSL (Secure Sockets Layer) ve TLS (Transport Layer Security) protokolleri kullanılır.
- **Kullanımda veri (data in use)**: Verilerin bellek içinde kullanılırken korunmasını sağlar.

Şifreleme Türleri

- **Sunucu tarafı şifreleme (server-side encryption)**: Veriler bulut depolama hizmetine alındıktan sonra şifrelenir.
- **İstemci tarafı şifreleme (client-side encryption)**: Veriler bulut depolama hizmetine gönderilmeden önce şifrelenir, bu sayede bulut sağlayıcısı verileri deşifre edemez.

Anahtar Yönetimi

- Anahtarların güvenli bir şekilde yönetilmesi gerekmektedir; kaybedilen anahtarlar, verilerin okunamaz hale gelmesine neden olur.
- Anahtar yönetim hizmetleri (key management services), şifreleme anahtarlarının yaşam döngüsünü yönetmeye yardımcı olur.

En İyi Uygulamalar

- Şifreleme anahtarlarını şifrelenmiş verilerden ayrı bir yerde saklamak.
- Anahtar yedeklerini düzenli olarak denetlemek ve güncellemek.
- Çok faktörlü kimlik doğrulama (multi-factor authentication) uygulamak.

**Coach**

Bu video, bulut (cloud) tabanlı dağıtımların (deployments) izlenmesi (monitoring) ve yönetilmesi (management) konusunu ele almaktadır. Bulut izleme çözümleri, uygulama (application) ve altyapı (infrastructure) davranışlarını değerlendirerek performans (performance), kaynak tahsisi (resource allocation), ağ (network) kullanılabilirliği (availability), uyumluluk (compliance) ve güvenlik risklerini (security risks) analiz eder.

Bulut İzlemenin Temel Faydaları

- Performans olaylarının (performance incidents) tanı ve çözümünü hızlandırır.
- İzleme altyapısının (monitoring infrastructure) maliyetini kontrol etmeye yardımcı olur.

- Proaktif bildirimlerle (proactive notifications) anormal durumların etkisini azaltır.

Bulut İzleme Çözümleri

- Gerçek zamanlı veri (real-time data) ile sanal makinelerin (virtual machines), hizmetlerin (services), veritabanlarının (databases) ve uygulamaların izlenmesini sağlar.
- Çok katmanlı görünürlük (multilayer visibility) sunarak tüm bulut tabanlı uygulama ve hizmetlerde kullanıcı ve dosya erişim davranışlarını analiz eder.
- Gelişmiş raporlama (reporting) ve denetim (auditing) yetenekleri ile düzenleyici standartların (regulatory standards) karşılandığından emin olur.

Bulut İzleme Araçları Kategorileri

- **Altyapı İzleme (Infrastructure Monitoring)**: Donanım arızalarını (hardware failures) ve güvenlik açıklarını (security gaps) tespit eder.
- **Veritabanı İzleme (Database Monitoring)**: Süreçleri, sorguları (queries) ve hizmetlerin kullanılabilirliğini takip eder.
- **Uygulama Performans İzleme (Application Performance Monitoring - APM)**: Uygulama kullanılabilirliğini ve performansını ölçer, sorunları çözmek için gerekli araçları sağlar.

En İyi Uygulamalar

- Kullanıcı deneyimi izleme (end-user experience monitoring) çözümlerini kullanarak uygulama performansını izlemek.
- Tüm altyapıyı tek bir izleme platformunda birleştirmek.
- Bulut kaynaklarının (cloud resources) kullanımını ve maliyetini takip eden izleme araçları kullanmak.
- İzleme otomasyonunu (monitoring automation) artırmak ve arızaları simüle ederek izleme araçlarının etkinliğini değerlendirmek.

Bulut Teknolojilerinin Faydaları

- **The Weather Company**: Buluta geçiş yaparak kritik hava verilerini (weather data) yüksek hızda güvenilir bir şekilde sunmaktadır, özellikle büyük hava olayları (weather events) sırasında.
- **American Airlines**: Bulut platformu (cloud platform) ve teknolojilerini kullanarak dijital öz hizmet araçları (digital self-service tools) ve müşteri değerini (customer value) daha hızlı bir şekilde sunmaktadır.

Bulut Hizmetleri ve İşletmeler

- **Cementos Pacasmayo**: Bulut hizmetlerini (cloud services) kullanarak operasyonel mükemmeliyet (operational excellence) elde etmekte ve stratejik dönüşüm (strategic transformation) ile yeni pazarlara ulaşmaktadır.

- **Welch**: İş değeri (business value) sağlamak için hibrit bulut (hybrid cloud) depolama (storage) seçmektedir.

Kariyer Fırsatları

- Bulut hizmetleri endüstrisinin (cloud services industry) pazar büyüklüğü, genel IT hizmetlerinin (IT services) neredeyse üç katı kadar büyümektedir.
- Bu alanda mevcut olan bazı iş rolleri (job roles) arasında Bulut Yazılım Mühendisleri (Cloud Software Engineers), Bulut Entegrasyon Uzmanları (Cloud Integration Specialists), Bulut Veri Mühendisleri (Cloud Data Engineers), Bulut Güvenlik Mühendisleri (Cloud Security Engineers), Bulut DevOps Mühendisleri (Cloud DevOps Engineers) ve Bulut Çözüm Mimarları (Cloud Solution Architects) bulunmaktadır.