TR CYBERSECURITY ALLIANCE

Bulut Güvenliğinde En iyi 7 Uygulama

Bulut bilişim, modern iş dünyasında esneklik, ölçeklenebilirlik ve maliyet avantajları sunarak hızla benimsenen bir teknoloji olmuştur. Ancak, bulut hizmetlerinin yaygınlaşmasıyla birlikte, güvenlik riskleri ve tehditler de artış göstermektedir. İşletmelerin verilerini ve sistemlerini korumak için bulut güvenliği en iyi uygulamalarına uyum sağlamaları gerekmektedir. Bu belge **30 Mayıs 2024** tarihinde gerçekleşen **TR Cybersecurity Alliance çalıştayı** sonucunda elde edilen bulut güvenliği konusunda işletmelere rehberlik edecek temel prensipleri ve stratejileri içermektedir. Belirtilen yedi ana başlık altında, bulut güvenliğini sağlamak için dikkat edilmesi gereken önemli noktalar ve bu noktaların nasıl uygulanacağı hakkında kısa açıklamalar sunulmuştur.

1. Başlamadan Önce Uyumluluk Kontrolü Yapın ve Bir Çıkış Planı Belirleyin

Bulut sistemlerini kullanmaya karar vermeden önce, yerel ve sektörel kanunlar, yönetmelikler ve standartlar açısından uyumluluğu sağladığınızdan emin olun. Özellikle bulut kullanımının veya yurtdışında veri depolamanın yasal sınırlamaları olup olmadığını dikkatlice inceleyin. Ayrıca, teknik veya ticari tercihlerin gelecekte değişebileceğini ve yasal zorunlulukların bulut kullanımını kısıtlayabileceğini göz önünde bulundurarak, bulut hizmetlerinden hızlı ve sorunsuz bir şekilde çıkmanızı sağlayacak bir plan hazırlayın. Bu plan, veri taşınabilirliği, veri kurtarma ve hizmet sağlayıcı değişimi gibi unsurları içermelidir. Bulut kullanımına başlamadan önce bu tür bir çıkış planının oluşturulması, olası riskleri minimize eder ve iş sürekliliğini sağlar.

2. Cloud Security Alliance (CSA) Tarafından Yayınlanmış Olan Cloud Control Matrix (CCM) ve Consensus Assessment Initiative Questionnaire (CAIQ) Belgelerinin Öneriler ve Denetimlerini Uygulayın

CSA'nın CCM ve CAIQ belgeleri, bulut güvenliği için en iyi uygulamaları ve kontrol çerçevelerini sunar. CCM, bulut hizmetleri için güvenlik kontrol standartlarını belirlerken, CAIQ bulut sağlayıcılarının güvenlik kontrollerini değerlendirmek için soru setleri sunar. Bu belgeleri kullanarak, güvenlik politikalarınızı CSA'nın önerdiği standartlarla hizalayabilir ve denetim süreçlerinizi yapılandırabilirsiniz.

3. Denetim Günlüklerinin Tutarlı ve Doğru Yönetimini Sağlayın

Denetim günlükleri, bulut ortamında yapılan tüm aktivitelerin kaydını tutar. Bu günlüklerin doğru ve tutarlı bir şekilde yönetilmesi, güvenlik olaylarının izlenmesi ve incelenmesi için kritik öneme sahiptir. Günlüklerin düzenli olarak gözden geçirilmesi, güvenlik açıklarının hızlıca tespit edilmesine ve gerekli önlemlerin alınmasına yardımcı olur.

4. Tutarlı Veri Şifrelemesini ve Uygun Anahtar Yönetimini Sağlayın

Bulut ortamında veri güvenliğini sağlamak için verilerin hem aktarım sırasında hem de depolama alanında şifrelenmesi gereklidir. Şifreleme anahtarlarının güvenli bir şekilde yönetilmesi de bu sürecin bir parçasıdır. Anahtar yönetim politikaları oluşturmak ve uygulamak, verilerin yetkisiz erişimlere karşı korunmasını sağlar.

5. IAM İzinlerini Etkili Bir Şekilde Yönetin ve En Az Ayrıcalıklı Erişime (LPA) Uyun

Kimlik ve Erişim Yönetimi (IAM) sistemleri, kullanıcıların ve servislerin bulut kaynaklarına erişimlerini kontrol eder. IAM izinlerini etkili bir şekilde yönetmek, yalnızca gerekli yetkilere sahip kullanıcıların belirli kaynaklara erişimini sağlar. En Az Ayrıcalıklı Erişim prensibi, kullanıcıların görevlerini yerine getirmek için minimum düzeyde erişim hakkına sahip olmalarını sağlar ve böylece güvenlik risklerini azaltır.

6. Güvenlik Açıklarını Yönetmek için Bir Süreç Oluşturun ve Takip Edin

Güvenlik açıkları, bulut ortamındaki potansiyel zayıflıkları ve tehditleri temsil eder. Bu açıkların yönetimi için bir süreç oluşturmak, düzenli olarak zafiyet taramaları yapmak, yamaları zamanında uygulamak ve güvenlik ihlallerine karşı hızlıca yanıt vermek bulut güvenliğini sağlamak açısından kritiktir. Sürekli izleme ve güncelleme yeni tehditlere karşı hazırlıklı olmayı sağlar.

7. Bulut Ortamlarına BYOD Erişimleri ve Bulut Üzerinde Yazılım Geliştirme Bulunması Halinde SDLC Güvenli Yazılım Süreçlerini Uygulayın

Kendi Cihazını Getir (BYOD) politikaları ve bulut üzerinde yazılım geliştirme süreçleri ek güvenlik zorlukları getirir. BYOD cihazlarının güvenliğini sağlamak için güçlü erişim kontrolleri ve cihaz yönetim politikaları uygulanmalıdır. Ayrıca, Yazılım Geliştirme Yaşam Döngüsü (SDLC) boyunca güvenlik uygulamalarını entegre etmek, güvenli kodlama, düzenli güvenlik testleri ve güvenlik incelemeleri gibi adımları içerir. Bu süreçler, geliştirme aşamasında güvenlik açıklarını en aza indirir.

Bulut güvenliği, işletmelerin dijital varlıklarını koruma stratejilerinin kritik bir bileşenidir. Bu dokümanda ele alınan yedi temel ilke, güvenli bir bulut ortamı oluşturmak ve sürdürmek için gerekli adımları özetlemektedir. Cloud Security Alliance (CSA) standartlarından denetim günlüklerinin yönetimine, veri şifrelemesinden kimlik ve erişim yönetimine kadar her bir konu, bulut güvenliğini sağlamada önemli bir rol oynamaktadır. İşletmelerin bu prensipleri benimseyerek ve sürekli olarak güncelleyerek güvenlik tehditlerine karşı dayanıklılıklarını artırmaları mümkündür. Güvenli bir bulut ortamı sadece veri güvenliğini sağlamakla kalmaz, aynı zamanda iş sürekliliği ve uyumluluk açısından da büyük avantajlar sunar.

Çalışmaya Katkıda Bulunan TR Cybersecurity Alliance Üyeleri:

Ahmet Özkan
Ahmet Öztoprak
Ali Tursun
Asım Yıldız
Atakan Çetin
Boubker El Mouttahid
Caner Dağlı
Cengiz Keskin
Deniz Şener
Ekrem Kolday
Gökhan Ilgıt
Hakan Tokay
İlker Çağrı Güven
İshak Çelikkanat
Mehmet Üner
Nedim Kaya
Onur Mutlu İmamoğlu
Ömer Çuhadaroğlu
Özgür Orhan
Serkan Akcan