BULUT ALTYAPINIZ GÜVENDE Mİ?

- [ ] **Bulut Hizmet Sağlayıcı Değerlendirmesi**

  Bulut hizmet sağlayıcınızın güvenlik sertifikalarını, uyumluluk raporlarını ve veri koruma politikalarını gözden geçirin. Fiziksel güvenlik önlemlerini, ağ altyapısını, erişim kontrollerini ve olay müdahale prosedürlerini değerlendirin.

- [ ] **Zafiyet Taraması ve Penetrasyon Testi**

  Bulut ortamınızda bulunan güvenlik açıklarını düzenli olarak tespit edin. Saldırganların kullanabileceği zayıflıkları ve potansiyel giriş noktalarını belirlemek için zafiyet taraması ve sızma testleri gerçekleştirin. Tanımlanan açıkları ele almak ve düzeltmek için bir zafiyet yönetim planı uygulayın.

- [ ] **Kimlik ve Erişim Yönetimi (IAM)**

  Bulut IAM politikalarınızı ve uygulamalarınızı değerlendirin. En az ayrıcalık ilkesine uyulmasını sağlamak için kullanıcı rollerini, ayrıcalıkları ve erişim kontrollerini gözden geçirin. Çok faktörlü kimlik doğrulama (MFA) ve parola ilkelerinin kullanımını değerlendirin. Erişim ayrıcalıklarını düzenli olarak gözden geçirin ve gereksizse iptal edin.

- [ ] **Yapılandırma İncelemeleri**

  Sanal makineler, depolama hesapları, veritabanları ve ağ ayarları gibi bulut kaynaklarınızın yapılandırmalarını kontrol edin. Güvenlik kontrollerinin ve en iyi uygulamaların düzgün bir şekilde uygulandığından emin olun ve gereksiz hizmetlerin veya özelliklerin devre dışı bırakıldığından emin olun. Altyapınızı güvenlik risklerine karşı açıkta bırakabilecek herhangi bir yanlış yapılandırmayı kontrol edin.

- [ ] **Günlük Analizi ve İzleme**

  Bulut altyapınızda gerçekleşen olayları izleyin ve günlükleri analiz edin. Bulut hizmet sağlayıcınız tarafından sağlanan günlükleme özelliklerini etkinleştirin ve güvenlik izleme araçları kullanarak herhangi bir şüpheli veya yetkisiz etkinliği tespit etmek için uygulamanızı izleyin.

- [ ] **Olay Müdahale Hazırlığı**

  Güvenlik olaylarına etkili bir şekilde yanıt vermek için iyi tanımlanmış süreçlere ve prosedürlere sahip olduğunuzdan emin olmak için olay müdahale planınızı değerlendirin. Etkinliğini değerlendirmek ve iyileştirilmesi gereken alanları belirlemek için olay müdahale planınızı simülasyonlar aracılığıyla test edin.

- [ ] **Uyumluluk ve Regülasyon Değerlendirmeleri**

  Sektörünüz belirli düzenlemelere veya uyumluluk gereksinimlerine tabiyse, bulut altyapınızın bu standartları karşıladığından emin olmak için değerlendirmeler yapın. Bu, veri gizliliği, güvenlik ve GDPR, HIPAA veya PCI DSS gibi düzenlemeler tarafından zorunlu kılınan diğer özel gereksinimler için kontrollerin değerlendirilmesini içerebilir.

- [ ] **Üçüncü Taraf Değerlendirmeleri**

  Bulut altyapınızın bağımsız değerlendirmelerini yapmak için üçüncü taraf güvenlik uzmanlarıyla veya denetçilerle bağlantı kurun. Bu uzmanlar, güvenlik kontrollerinizin tarafsız bir değerlendirmesini yapabilir, olası güvenlik açıklarını belirleyebilir ve iyileştirme için önerilerde bulunabilir.

- [ ] **Sürekli İzleme ve İyileştirme**

  Bulut güvenliği devam eden bir süreçtir. Güvenlik tehditlerini gerçek zamanlı olarak tespit etmek ve bunlara yanıt vermek için sürekli izleme mekanizmalarını uygulayın. Güvenlik önlemlerinizi en son tehditlere ve güvenlik açıklarına, sektördeki en iyi uygulamalara ve bulut hizmeti sağlayıcınızın sunduğu tüm yeni özelliklere veya güncellemelere göre düzenli olarak gözden geçirin ve güncelleyin.

Lostar
GÜVENLİ GÜNLER