Denetci.org

REFERANS İLKELERİ

Bulut Güvenliği İlkeleri

Rİ-ALT-5

Sürüm 1.0 · 11.08.2026

www.denetci.org

Bulut Güvenliği İlkeleri

Bulut güvenliği, kuruluşun doğrudan sahip olmadığı altyapı ve hizmetler üzerinde kurduğu sistemlerde güvenin hangi taraflar, kimlikler, yönetim düzlemleri ve bağımlılıklar arasında paylaşıldığını ele alır. Amaç belirli bir bulut mimarisi, sağlayıcı veya güvenlik ürünü öngörmek değil; dışarıya devredilen işletim sorumluluklarının kuruluşun kendi güvenlik sonuçlarını görünmez hale getirmediği bir tasarım anlayışı oluşturmaktır.

İlke 1: Bulut kullanımı güvenlik sorumluluğunun bütünüyle devredildiği anlamına gelmemelidir.

Sağlayıcı altyapının bazı katmanlarını koruyabilir; ancak kuruluşun verisi, kimlikleri, yapılandırması ve kullanım biçiminden doğan güvenlik kararları devam eder. Bir görevin sağlayıcı tarafından yerine getirilmesi kuruluş üzerindeki sonucunu ortadan kaldırmaz.

İlke 2: Sorumluluk sınırı kullanılan gerçek hizmete göre anlaşılmalıdır.

Farklı bulut hizmetleri müşteriye ve sağlayıcıya farklı yönetim yetkileri bırakabilir. Genel bir "bulut sağlayıcısı şundan sorumludur" varsayımı, kullanılan hizmetin fiilî kontrol ve görünürlük sınırlarının yerine geçmemelidir.

İlke 3: Bulut hesabı, aboneliği veya projesi kendiliğinden yeterli bir güven sınırı sayılmamalıdır.

Aynı yönetim kimlikleri, ağlar, politikalar veya hizmetler farklı bulut alanlarını birbirine bağlayabilir. İdari ayrım yalnızca gerçekten ayrı etki ve güven alanları oluşturduğu ölçüde güvenlik anlamı taşır.

İlke 4: Bulut ortamındaki güven öncelikle kimlik ve açık yetkilere dayanmalıdır.

Kaynakların aynı sağlayıcı, hesap veya sanal ağ içinde bulunması tarafların birbirlerine otomatik olarak güvenmesini gerektirmez. Kullanıcıların, hizmetlerin ve iş yüklerinin erişimi gerçek kimlik ve işlev üzerinden sınırlandırılmalıdır.

İlke 5: İnsan, hizmet ve otomasyon kimlikleri farklı güven ilişkileri olarak anlaşılabilmelidir.

Bir kullanıcının, uygulamanın veya otomasyonun hangi amaçla hareket ettiği ve hangi yetkiyi taşıdığı birbirine karışmamalıdır. Teknik kolaylık, farklı sorumluluk türlerini ortak ve belirsiz kimliklerde birleştirmemelidir.

İlke 6: Bulut yönetim düzlemi ayrı ve yüksek etkili bir güven alanıdır.

Yönetim konsolları, API'ler ve otomasyon yetkileri çok sayıda kaynağın erişimini, ağını ve çalışma biçimini değiştirebilir. Bu alanın kaybı tek tek iş yüklerinin kaybından daha geniş sonuç doğurabileceği için ayrıca korunmalıdır.

İlke 7: Bir iş yükünün kaybı yönetim düzleminin kaybına doğal geçiş sağlamamalıdır.

Sanal makinenin, konteynerin veya uygulamanın ele geçirilmesi onu oluşturan, başka kaynaklara yetki veren veya bulut ortamını yöneten daha yüksek yetkilere otomatik erişim oluşturmamalıdır.

İlke 8: Bulut kimliklerinin yetkileri oluşturabilecekleri gerçek etkiyle sınırlı olmalıdır.

Bir rolün veya teknik kimliğin çok sayıda kaynağa ulaşabilmesi işletimi kolaylaştırabilir; ancak ele geçirilmesi halinde ortak kayıp alanı oluşturur. Yetki, hesap düzeyindeki kolaylıktan çok gerçek işlev ve etki üzerinden verilmelidir.

İlke 9: Geçici kimlik bilgisinin değeri gerçek kullanım ömründen doğmalıdır.

Teknik olarak kısa süreli bir belirtecin kesintisiz biçimde yeniden üretilebilmesi veya devralınabilmesi fiilen kalıcı güven oluşturabilir. Geçicilik, yalnızca kimlik bilgisinin adına değil erişimin gerçekten ne kadar süre sürdürülebildiğine göre değerlendirilmelidir.

İlke 10: Bulut kaynaklarının kimlere ve nerelere açık olduğu bilinçli bir tasarım kararı olmalıdır.

İnternet, diğer bulut alanları, kurumsal ağlar ve belirli iş yükleri farklı güven ilişkileri oluşturur. Kolay veya varsayılan yapılandırma nedeniyle kaynağın gereğinden geniş erişilebilir hale gelmesi doğal durum olmamalıdır.

İlke 11: Bulut içindeki iletişim yalnızca sağlayıcı altyapısında gerçekleştiği için güvenilir sayılmamalıdır.

Aynı sağlayıcının veya sanal ağın içindeki sistemler de farklı kimlikleri ve güven alanlarını temsil edebilir. İletişimin "içeride" olması kimlik, yetki, bütünlük ve gizlilik gereksinimlerini ortadan kaldırmamalıdır.

İlke 12: Hizmetler arası güven gerçek işlevle sınırlı olmalıdır.

Bir iş yükünün başka bir bulut hizmetini kullanabilmesi bütün hizmetlere veya kaynaklara erişmesi gerektiği anlamına gelmez. Bir bileşenin ele geçirilmesi ilgisiz hizmetlere geniş yanal hareket sağlamamalıdır.

İlke 13: Bulut hizmetinin dayanıklılığı verinin güvenli veya kurtarılabilir olduğu anlamına gelmemelidir.

Sağlayıcının çoklu kopyalama ve yüksek erişilebilirlik özellikleri altyapı arızalarına karşı koruma sağlayabilir; ancak yanlış silme, yetkisiz erişim veya bozuk durumun çoğaltılması gibi farklı riskleri otomatik olarak çözmez.

İlke 14: Veri konumu verinin bütün yaşam döngüsünün konumuyla aynı şey değildir.

Veri belirli bir bölgede saklanırken yedekleme, destek, yönetim, analiz veya başka hizmetler farklı sınırlar oluşturabilir. Güvenlik değerlendirmesi yalnızca ana depolama konumuna dayanmamalıdır.

İlke 15: Bulut kriptografisinin güveni anahtar üzerindeki gerçek kontrole dayanmalıdır.

Verinin şifrelenmiş olması, anahtara hangi tarafların erişebildiği bilinmeden tek başına yeterli güvence sağlamaz. Veri ile anahtarın aynı kimlik ve yönetim kaybına tamamen bağlı olması şifrelemenin sağlayabileceği ayrımı azaltabilir.

İlke 16: Anahtar yönetim sorumluluğunun kimde olduğu bilinçli bir güven kararı olmalıdır.

Sağlayıcı veya kuruluş tarafından yönetilen anahtar yaklaşımlarının her biri farklı erişim, süreklilik ve işletim sonuçları doğurabilir. Değerlendirme yalnızca "şifreleme etkin" durumuna indirgenmemelidir.

İlke 17: Bulut yapılandırması kod kadar gerçek sistem davranışını belirleyen bir güvenlik girdisidir.

Erişim politikaları, ağ kuralları, depolama izinleri ve hizmet ayarları kod değiştirilmeden güven sınırlarını değiştirebilir. Yapılandırma kararları yardımcı işletim ayrıntıları olarak görülmemelidir.

İlke 18: Amaçlanan bulut durumu ile çalışan bulut durumu ayrıştırılabilmelidir.

Şablonlar ve altyapı tanımları sistemin nasıl olması gerektiğini gösterebilir; manuel değişiklikler veya farklı otomasyonlar ise gerçek ortamı değiştirebilir. Güvence yalnızca tanımlanmış duruma değil fiilî ortama dayanmalıdır.

İlke 19: Alternatif yönetim yolları bulutun gerçek güven modelinin dışında kalmamalıdır.

Konsol, API, komut satırı, otomasyon ve başka yönetim yolları aynı ortam üzerinde farklı biçimlerde değişiklik yapabilir. Ana yönetim yolunun güvenli olması alternatif yolların etkisini ortadan kaldırmaz.

İlke 20: Yönetilen hizmet kullanımı gerekli güvenlik görünürlüğünü ortadan kaldırmamalıdır.

Kuruluş bazı altyapı ayrıntılarını doğrudan göremeyebilir; ancak kendi güvenlik kararları için gerekli kimlik, erişim, değişiklik ve olay bilgisinden bütünüyle yoksun kalmamalıdır. Görünmeyen alanlar sağlayıcının sorumluluğuna bırakıldığı için yok sayılmamalıdır.

İlke 21: Sağlayıcının sunduğu güvenlik özelliğinin varlığı kuruluşta güvence oluştuğunu göstermemelidir.

Bir özellik ancak doğru kullanım ve yapılandırma ile beklenen sonucu üretebilir. Güvenlik, sağlayıcının ürün kataloğunda bulunan imkânlara değil gerçek ortamda ortaya çıkan davranışa dayanmalıdır.

İlke 22: Paylaşılan altyapıda izolasyon temel güven varsayımlarından biridir.

Başka müşterilerin veya iş yüklerinin aynı fiziksel ya da mantıksal altyapıyı paylaşması kendi başına kabul edilemez değildir. Ancak kuruluşun güvenliği diğer kiracıların iyi davranacağı varsayımına değil aradaki izolasyonun güvenilirliğine dayanmalıdır.

İlke 23: Bölge ve sağlayıcı çeşitliliği yalnızca gerçek bağımsızlık oluşturduğu ölçüde güvence sağlar.

Farklı bölgeler veya sağlayıcılar aynı kimlik, DNS, dağıtım hattı, yönetim aracı veya başka ortak bağımlılıklara sahip olabilir. Görünürdeki çeşitlilik ortak kayıp nedenlerini gerçekten azaltmıyorsa süreklilik değeri sınırlıdır.

İlke 24: Bulut hesabının veya yönetim ilişkisinin kaybı altyapı arızası kadar gerçek bir süreklilik riskidir.

Kaynaklar teknik olarak çalışıyor olsa bile yönetim kimlikleri, hesap sahipliği, abonelik veya sağlayıcı ilişkisi üzerindeki sorunlar hizmetin kullanılmasını veya yönetilmesini engelleyebilir. Süreklilik yalnızca fiziksel altyapı arızasına göre tasarlanmamalıdır.

İlke 25: Bulutun hızlı kaynak oluşturma yeteneği görünmeyen varlık birikimine dönüşmemelidir.

Kaynakların kolay ve geçici biçimde oluşturulabilmesi, sahibi ve amacı bilinmeyen sistemlerin, kimliklerin ve veri depolarının zaman içinde birikmesine yol açabilir. Kısa ömürlü veya düşük maliyetli olmak güvenlik etkisini ortadan kaldırmaz.

İlke 26: Kullanılmayan bulut kaynakları güvenlik açısından nötr değildir.

Artık gerekli olmayan kaynaklar veri, kimlik, ağ yolu veya başka saldırı yüzeyleri taşımaya devam edebilir. Maliyet oluşturmamaları veya pasif görünmeleri güven ilişkilerinin devamını haklı çıkarmamalıdır.

İlke 27: Bulut kaynağının sona erdirilmesi ona bağlı güven ilişkilerini de sona erdirmelidir.

Bir kaynağın silinmesi sonrasında kimlikler, sırlar, snapshot'lar, veriler, bağlantılar veya dış entegrasyonlar yaşamaya devam edebilir. Yaşam döngüsünün sonu yalnızca görünür kaynağın kaldırılmasıyla tamamlanmış sayılmamalıdır.

İlke 28: Merkezi bulut güvenliği kendi başına yeni bir güven yoğunlaşmasıdır.

Merkezi politika, görünürlük ve güvenlik hizmetleri tutarlılık sağlayabilir; ancak tek bir yanlış yapılandırma veya ele geçirilme çok sayıda kaynağı etkileyebilir. Merkezi güvenlik katmanının varlığı bağımsız güven sınırlarının gereksiz yere kaldırılmasına yol açmamalıdır.

İlke 29: Sağlayıcıya bağımlılık mimarinin değişmez koşulu olarak kabul edilmemelidir.

Hizmet özellikleri, maliyet, güvenlik durumu veya sağlayıcı ilişkisi zaman içinde değişebilir. Kritik bir hizmetin güvenliği ve sürekliliği, mevcut sağlayıcının koşullarının süresiz aynı kalacağı varsayımına bütünüyle bağlı olmamalıdır.

İlke 30: Buluttan çıkış da buluta giriş kadar bir güvenlik yaşam döngüsü olayıdır.

Bir hizmet veya sağlayıcı terk edilirken veriler, kimlikler, anahtarlar, kopyalar, erişimler ve entegrasyonlar eski ortamda yaşamaya devam edebilir. Geçişin tamamlanması yalnızca yeni ortamın çalışmaya başlamasıyla ölçülmemelidir.

İlke 31: Sağlayıcının güvenlik beyanları destekledikleri iddianın sınırları içinde değerlendirilmelidir.

Denetim raporları, sertifikalar ve diğer güven kanıtları belirsizliği azaltabilir; ancak kuruluşun kendi yapılandırmasını, kullanım biçimini veya bütün hizmet katmanlarını otomatik olarak doğrulamaz. Kanıt, gerçekte neyi kapsadığı bilinerek kullanılmalıdır.

İlke 32: Bulut güvenliği gerçek ortam davranışı üzerinden doğrulanabilmelidir.

Mimari diyagramlar, güvenlik ürünleri, sağlayıcı sertifikaları veya altyapı şablonları tek başına güvence oluşturmaz. Gerçekte hangi kimliklerin hangi kaynakları değiştirebildiği, hangi hizmetlerin birbirine erişebildiği, verinin hangi güven alanlarında yaşadığı ve bir güven kaybının ne kadar yayılabildiği gerektiğinde gösterilebilmelidir.