Denetci.org

REFERANS İLKELERİ

Üçüncü Taraf Erişimi İlkeleri

Rİ-TED-1

Sürüm 1.0 · 11.08.2026

www.denetci.org

Üçüncü Taraf Erişimi İlkeleri

Üçüncü taraf erişimi; tedarikçilerin, danışmanların, yüklenicilerin, iş ortaklarının ve kuruluş personeli dışındaki diğer tarafların sistemlere, verilere veya yönetim yeteneklerine erişmesinden doğan güven ilişkilerini ele alır. Amaç dış erişimi bütünüyle engellemek değil; kuruluşun doğrudan yönetmediği bir tarafın hangi ihtiyaca dayanarak, neye, ne kadar süreyle ve hangi etki sınırı içinde erişebildiğini açık ve doğrulanabilir hale getirmektir.

İlke 1: Ticari veya kurumsal ilişki kendiliğinden teknik güven oluşturmamalıdır.

Bir kuruluşla sözleşme, ortaklık veya hizmet ilişkisi bulunması onun personeline ya da sistemlerine otomatik erişim hakkı doğurmaz. Teknik erişim, ayrıca gerekçelendirilmesi gereken bağımsız bir güven kararı olmalıdır.

İlke 2: Üçüncü taraf erişimi açık bir görev ve sonuç ihtiyacına dayanmalıdır.

Dış tarafın neden erişime ihtiyaç duyduğu ve erişimin hangi işi mümkün kıldığı anlaşılabilir olmalıdır. İlişkinin varlığı veya geçmişte verilmiş erişim tek başına güncel ihtiyaç sayılmamalıdır.

İlke 3: Erişimin kapsamı dış tarafın gerçek görevini aşmamalıdır.

Belirli bir hizmeti desteklemek bütün sistemlere, ağlara veya verilere erişmeyi gerektirmez. Teknik kolaylık, gereksiz geniş güven alanı oluşturmanın gerekçesi olmamalıdır.

İlke 4: Sistem erişimi ile veri erişimi birbirine eşit kabul edilmemelidir.

Bir dış tarafın sistemi işletmesi veya desteklemesi, sistemde işlenen bütün veriyi görmesi gerektiği anlamına gelmeyebilir. Teknik görev ile veriyi kullanma ihtiyacı gerektiğinde ayrıştırılabilmelidir.

İlke 5: Farklı işlemler farklı güven etkileri olarak ele alınmalıdır.

Görüntüleme, değiştirme, silme, dışa aktarma ve yönetim aynı sonucu doğurmaz. Bir görevin gerektirdiği erişim diğer yüksek etkili yetkileri kendiliğinden beraberinde getirmemelidir.

İlke 6: Üçüncü taraf erişimi mümkün olduğu ölçüde gerçek bir kimlik ve sorumlulukla ilişkilendirilmelidir.

Bir şirket adına erişim verilmiş olması erişimi fiilen kullanan kişinin veya teknik kimliğin önemsiz olduğu anlamına gelmez. Önemli işlemler gerektiğinde gerçek sorumluluk zinciriyle ilişkilendirilebilmelidir.

İlke 7: Paylaşılan erişim gerçek kullanıcıyı görünmez hale getirmemelidir.

Ortak hesap veya aracılı erişim bazı sistemlerde kaçınılmaz olabilir. Bununla birlikte hangi gerçek kişinin veya sistemin erişimi kullandığının tamamen kaybolması normal güven modeli olmamalıdır.

İlke 8: Dış kimlik altyapısına güvenmek sınırsız kimlik kabulü anlamına gelmemelidir.

Federasyon veya başka bir dış kimlik sağlayıcı kullanıldığında kuruluş, kimliğin bazı özelliklerinin doğruluğunu başka tarafa bırakır. Hangi kimliklerin ve hangi özelliklerin kabul edildiği açık biçimde sınırlandırılmalıdır.

İlke 9: Üçüncü tarafın kendi personel yaşam döngüsü kuruluş erişimini etkileyebilmelidir.

Bir kişinin dış kuruluştan ayrılması veya görev değiştirmesi halinde daha önce verilmiş erişimin fark edilmeden yaşamaya devam etmesi güven ilişkisini gerçek sorumluluktan koparır. Dış taraftaki değişiklik gerektiğinde kuruluş erişimine de yansıyabilmelidir.

İlke 10: Üçüncü taraf erişimi kuruluş içinde anlamlı bir sahipliğe dayanmalıdır.

Erişimin neden gerekli olduğunu ve hâlâ sürmesi gerekip gerekmediğini değerlendirebilen bir taraf bulunmalıdır. Sahipsiz dış erişimler zamanla görünmez ve kalıcı güven ilişkilerine dönüşmemelidir.

İlke 11: Erişim kararı gerçek etkiyi anlayabilecek sorumlulukla ilişkilendirilmelidir.

Biçimsel onay, onaylayan taraf erişimin hangi sistem veya veriler üzerinde ne yapabileceğini anlayamıyorsa sınırlı güvence sağlar. Karar, erişimin gerçek sonucu hakkında muhakeme yapabilen bir konumdan verilmelidir.

İlke 12: Üçüncü tarafın cihazı, kullanıcının kimliğinden ayrı bir güven unsurudur.

Dış kullanıcının doğru kimliği kullandığının bilinmesi cihazının güvenilir olduğunu göstermez. Özellikle yüksek etkili erişimlerde cihazın oluşturduğu belirsizlik erişim kararının dışında bırakılmamalıdır.

İlke 13: Kuruluş tarafından yönetilmeyen cihazlar yönetilen cihazlarla aynı varsayımlara tabi olmamalıdır.

Kuruluş dış cihazların yapılandırmasını, güncelliğini veya yerel kullanımını tam olarak bilemeyebilir. Bu belirsizlik, erişilebilen sistem ve verinin kapsamına gerektiğinde yansıtılmalıdır.

İlke 14: Üçüncü taraf erişimi verinin gereksiz biçimde dış tarafa taşınmasına dönüşmemelidir.

Bir sistemi kullanabilmek veriyi yerel cihaza, başka hizmetlere veya kalıcı kopyalara aktarma hakkını kendiliğinden doğurmaz. Veri hareketi erişim ihtiyacından ayrı bir güven sonucu olarak değerlendirilmelidir.

İlke 15: Yönetim erişimi olağan hizmet erişiminden farklı bir güven ilişkisi olmalıdır.

Bir uygulamayı kullanmak ile onun altyapısını, güvenlik durumunu veya kimliklerini değiştirebilmek aynı etkiyi oluşturmaz. Üçüncü taraf yönetim yetkileri daha geniş güven sonucu taşıdıkları ölçüde ayrıca sınırlandırılmalıdır.

İlke 16: Üçüncü taraf ayrıcalığı sürekli taşıdığı bir özellik olmak zorunda olmamalıdır.

Bakım veya müdahale için zaman zaman yüksek yetki gerekebilir. Kısa süreli yüksek etki ihtiyacı, dış tarafın sürekli aynı güce sahip olmasının gerekçesi haline gelmemelidir.

İlke 17: Üçüncü taraf kendi erişim sınırını tek başına genişletememelidir.

Mevcut bir erişim yeni hesap, yeni yetki veya daha geniş güven alanı oluşturmak için kullanılıyorsa verilen güven kendi kendini büyütebilir. Yetki genişlemesi ayrı ve açıklanabilir bir güven kararı olmalıdır.

İlke 18: Dış tarafın erişimi ile kuruluşun kanıt ve görünürlük yeteneği birbirinden kopmamalıdır.

Kuruluş kendi sistemlerinde yüksek etkili bir dış faaliyetin kim tarafından ve hangi bağlamda gerçekleştirildiğini gerektiğinde anlayabilmelidir. Dış tarafın kullandığı teknik araçlar bu görünürlüğü ortadan kaldırmamalıdır.

İlke 19: Üçüncü taraf kendi faaliyetinin bütün kanıtını tek başına kontrol etmemelidir.

Özellikle yüksek yetkili dış erişimde, aynı tarafın hem sistemi değiştirebilmesi hem de bu değişikliğe ilişkin bütün izleri yok edebilmesi güvenceyi zayıflatır. Önemli kanıtların güveni yalnızca dış tarafın iyi niyetine bağlı olmamalıdır.

İlke 20: Geçici dış erişim kalıcı güven ilişkisine dönüşmemelidir.

Kurulum, bakım, proje veya olay müdahalesi için açılan erişim onu doğuran ihtiyaçtan daha uzun yaşamamalıdır. Geçmişte gerekli olması gelecekte de gerekli olduğunu göstermez.

İlke 21: İlişkinin sona ermesi gerçek teknik erişimi sona erdirebilmelidir.

Sözleşmenin veya görevin sona ermesi sonrasında hesaplar, sertifikalar, anahtarlar, oturumlar veya alternatif erişim yolları çalışmaya devam ediyorsa güven ilişkisi fiilen sona ermemiştir. Sonlandırma kullanılabilir gerçek erişim üzerinden anlaşılmalıdır.

İlke 22: Üçüncü taraf erişim güvencesi gerçek etki alanı üzerinden doğrulanabilmelidir.

Tedarikçi listeleri, sözleşmeler, onay kayıtları veya erişim portalları tek başına güvence oluşturmaz. Hangi dış tarafların hangi kimliklerle hangi sistem ve verilere fiilen erişebildiği, ne ölçüde yetki taşıdığı ve ihtiyaç sona erdiğinde bu erişimin gerçekten kaldırılabildiği gösterilebilmelidir.