Denetci.org

REFERANS İLKELERİ

Fiziksel Güvenlik İlkeleri

Rİ-ALT-4

Sürüm 1.0 · 11.08.2026

www.denetci.org

Fiziksel Güvenlik İlkeleri

Fiziksel güvenlik, bilgi sistemlerinin, cihazların, veri taşıyan ortamların ve bunları destekleyen altyapının fiziksel erişim, müdahale, kayıp ve çevresel olaylar karşısındaki güvenilirliğini ele alır. Amaç belirli erişim teknolojileri veya tesis kontrolleri tarif etmek değil; fiziksel yakınlığın gereksiz teknik güvene dönüşmediği ve fiziksel bir kaybın oluşturabileceği etkinin sınırlandırıldığı bir tasarım anlayışı ortaya koymaktır.

İlke 1: Fiziksel yakınlık teknik güvenin yerine geçmemelidir.

Bir kişinin bir binaya, çalışma alanına veya teknik ortama girebilmesi o alandaki bütün sistemlere ve verilere erişmeye yetkili olduğu anlamına gelmez. Fiziksel konum, kimlik ve teknik yetkilendirmenin yerine geçen genel bir güven kaynağı olmamalıdır.

İlke 2: Fiziksel güven sınırları korudukları gerçek etkiye göre oluşmalıdır.

Bütün alanların ve varlıkların aynı koruma ihtiyacına sahip olduğu varsayılmamalıdır. Bir alandaki sistem, veri veya altyapının kaybı daha geniş sonuçlar doğuruyorsa fiziksel erişimin önemi de buna göre değerlendirilmelidir.

İlke 3: Bir fiziksel sınırın aşılması sonraki sınırları anlamsız hale getirmemelidir.

Bir tesise girebilmek bütün teknik alanlara, bir teknik alana girebilmek de içindeki bütün varlıklara erişim hakkı oluşturmamalıdır. Fiziksel güven mümkün olduğu ölçüde farklı etki alanlarını birbirinden ayırmalıdır.

İlke 4: Fiziksel erişim gerçek görev ve ihtiyaçla sınırlı olmalıdır.

Bir kişinin belirli bir tesiste çalışması veya belirli bir görevi yerine getirmesi ilgisiz alan ve varlıklara erişmesini gerektirmez. Verilen fiziksel güven, amacı bakımından gerekenden daha geniş olmamalıdır.

İlke 5: Fiziksel erişim onu doğuran ihtiyaçtan daha uzun yaşamamalıdır.

Görev, ilişki veya geçici ihtiyaç sona erdiğinde geçmişte verilmiş erişim kendiliğinden devam etmemelidir. Fiziksel güven de diğer erişim biçimleri gibi değişen bağlama göre sona erebilmelidir.

İlke 6: Önemli fiziksel erişimler açıklanabilir bir sorumlulukla ilişkilendirilebilmelidir.

Bir alan veya varlık üzerinde önemli etki oluşturabilecek fiziksel erişimin kim veya hangi sorumlu taraf adına gerçekleştiği tamamen belirsiz kalmamalıdır. Kullanılan erişim aracının biçimi gerçek sorumluluğu görünmez hale getirmemelidir.

İlke 7: Tek bir fiziksel erişim unsurunun kaybı gereksiz ölçüde geniş erişim sağlamamalıdır.

Bir anahtarın, erişim aracının veya başka fiziksel güven unsurunun ele geçirilmesi ilgisiz bütün alanların açılmasına yol açmamalıdır. Fiziksel erişimin kapsamı da oluşturabileceği etkiyle sınırlı olmalıdır.

İlke 8: Güvenini kaybeden fiziksel erişimin etkisi gerçekten sona erdirilebilmelidir.

Bir erişim unsurunun kaybolması, kopyalanması veya kontrol dışına çıkması halinde yalnızca artık kullanılmamasının beklenmesi yeterli olmayabilir. Bu unsurun sağladığı gerçek erişim gerektiğinde ortadan kaldırılabilmelidir.

İlke 9: Ziyaretçi ve dış taraf erişimi kuruluş içi erişimle aynı güven varsayımına dayanmamalıdır.

Bir ziyaretçinin, bakım görevlisinin veya başka dış tarafın belirli bir alana girmesi gerekebilir. Bu ihtiyaç, kuruluş içindeki sürekli erişimlerin veya ilgisiz varlıklara erişimin doğal olarak devralınmasını gerektirmez.

İlke 10: Fiziksel bakım teknik güven durumunu görünmez biçimde değiştirmemelidir.

Bir cihazın, bileşenin, bağlantının veya altyapının fiziksel olarak değiştirilmesi sistemin bütünlüğünü, erişim yollarını veya güvenlik varsayımlarını da değiştirebilir. Fiziksel müdahale yalnızca tesis faaliyeti olarak değerlendirilmemelidir.

İlke 11: Bir cihazın fiziksel kontrolünü ele geçirmek üzerindeki bütün güveni otomatik olarak vermemelidir.

Fiziksel erişim güçlü bir saldırı imkânıdır; ancak mümkün olduğu ölçüde cihazın ele geçirilmesi üzerindeki verilere, kimliklere ve bağlı sistemlere sınırsız erişim anlamına gelmemelidir.

İlke 12: Güvenlik yalnızca cihazın olağan çalışma biçimine bağlı olmamalıdır.

Alternatif başlatma, donanım sökme, yerel konsol veya başka fiziksel yollar normal çalışma sırasında uygulanan bazı teknik sınırların dışına çıkabilir. Cihaz güvenliği yalnızca olağan kullanıcı akışının izleneceği varsayımına dayanmamalıdır.

İlke 13: Fiziksel olarak erişilebilir teknik bağlantılar gerçek erişim yolları olarak görülmelidir.

Ağ, konsol, çevresel arabirim veya başka bağlantı noktaları fiziksel yakınlığı teknik erişime dönüştürebilir. Bu yollar, yalnızca uzaktan erişim kanallarının korunmuş olması nedeniyle güvenlik modelinin dışında kalmamalıdır.

İlke 14: Yetkisiz fiziksel müdahale yüksek etkili varlıklarda bütünüyle görünmez kalmamalıdır.

Bir cihazın, bağlantının veya başka kritik unsurun değiştirilmesi mümkünse bütünlük yalnızca kimsenin müdahale etmeyeceği varsayımına bırakılmamalıdır. Gerektiğinde amaçlanan fiziksel durum ile fiilî durum arasındaki önemli farklar anlaşılabilir olmalıdır.

İlke 15: Taşınabilir cihazların güvenliği bulundukları tesisin sınırlarına bağlı olmamalıdır.

Dizüstü bilgisayarlar, mobil cihazlar ve başka taşınabilir sistemler kuruluş kontrolündeki alanların dışına çıkabilir. Fiziksel konum değiştiğinde üzerlerindeki veri ve güven ilişkilerinin önemi ortadan kalkmaz.

İlke 16: Fiziksel cihaz kaybı yalnızca donanım kaybı olarak görülmemelidir.

Bir cihaz veri, aktif oturum, sertifika, anahtar veya başka erişim unsurları taşıyabilir. Kayıp halinde değerlendirilmesi gereken etki cihazın maddi değerinden çok taşıdığı güven ilişkileridir.

İlke 17: Veri taşıyan fiziksel ortamlar cihazdan bağımsız güvenlik değeri taşır.

Diskler, taşınabilir ortamlar ve başka depolama bileşenleri sistemden çıkarıldıklarında da bilgi taşımaya devam eder. Kullanımda olmamak veya bir cihazdan sökülmüş olmak üzerlerindeki verinin güvenlik ihtiyacını ortadan kaldırmaz.

İlke 18: Fiziksel veri hareketi yeni bir güven alanına geçiş olarak değerlendirilmelidir.

Bir depolama ortamının başka yere veya başka tarafa taşınması verinin de farklı fiziksel ve organizasyonel koşullara geçmesi anlamına gelir. Fiziksel taşıma, dijital veri aktarımından tamamen ayrı ve güvenlik açısından nötr bir işlem değildir.

İlke 19: Varlığın kullanım ömrünün sona ermesi geçmiş veri ve güven ilişkilerini de sona erdirmelidir.

Bir cihazın veya depolama ortamının yeniden kullanılması, iade edilmesi ya da kuruluş kontrolünden çıkması geçmiş kullanıcının verisini, kimliklerini veya erişim yeteneklerini yeni tarafa taşımamalıdır.

İlke 20: Çevresel ve destek altyapısı bilgi sistemlerinin gerçek güvenlik bağımlılığıdır.

Enerji, soğutma, yangın, su, fiziksel yapı ve benzeri koşullar sistemlerin kullanılabilirliğini ve bütünlüğünü etkileyebilir. Teknik sistemlerin güçlü olması onları destekleyen fiziksel çevrenin kaybını önemsiz hale getirmez.

İlke 21: Yedek fiziksel altyapı aynı başarısızlık nedenine gereksiz biçimde bağımlı olmamalıdır.

Birden fazla enerji, iletişim veya tesis unsurunun bulunması gerçek bağımsızlık sağladığını göstermez. Aynı fiziksel olayın bütün alternatifleri birlikte kaybettirebildiği durumlarda görünürdeki yedeklilik sınırlı güvence sağlar.

İlke 22: Kritik varlıkların fiziksel yoğunlaşması ortak kayıp alanı olarak görülmelidir.

Birden fazla kritik sistemin aynı alan, tesis veya fiziksel bağımlılıkta toplanması tek bir olayın etkisini büyütebilir. Yoğunlaşma operasyonel yararıyla birlikte oluşturduğu ortak kayıp açısından değerlendirilmelidir.

İlke 23: Fiziksel ayrım yalnızca mesafeyle ölçülmemelidir.

Farklı odalar veya tesisler aynı enerji kaynağına, erişim yoluna, bölgesel olaya veya başka ortak fiziksel bağımlılığa sahip olabilir. Gerçek bağımsızlık ortak başarısızlık nedenlerine göre değerlendirilmelidir.

İlke 24: Fiziksel güvenliği sağlayan sistemler de kritik bağımlılıklar olarak görülmelidir.

Erişim, gözetim veya başka fiziksel güvenlik sistemleri arızalanabilir veya ele geçirilebilir. Güvenlik tasarımı bu sistemlerin kusursuz ve sürekli çalışacağı varsayımına bütünüyle bağlı olmamalıdır.

İlke 25: Bilgi sistemlerinin fiziksel korunması insan güvenliğinin önüne geçmemelidir.

Yangın, tahliye veya başka acil durumlarda güvenlik mekanizmaları insanların güvenli hareketini ölçüsüz biçimde engellememelidir. Varlık koruması ile insan güvenliği arasındaki çatışma tasarımın bilinçli bir parçası olmalıdır.

İlke 26: Fiziksel güvenlik güvencesi gerçek erişim ve etki üzerinden doğrulanabilmelidir.

Alan sınıfları, erişim listeleri, güvenlik sistemleri veya tesis prosedürleri tek başına güvence oluşturmaz. Gerçekte kimlerin hangi alan ve varlıklara fiziksel olarak ulaşabildiği, bu erişimin hangi teknik veya veri etkisine dönüşebildiği ve önemli bir fiziksel kaybın ne kadar yayılabildiği gerektiğinde gösterilebilmelidir.