Denetci.org

REFERANS İLKELERİ

İnsan Güvenliği İlkeleri

Rİ-GEN-4

Sürüm 1.0 · 11.08.2026

www.denetci.org

İnsan Güvenliği İlkeleri

İnsan güvenliği, bilgi sistemlerinin ve güvenlik mekanizmalarının insanların hata yapabileceği, baskı altında kalabileceği, dikkatinin sınırlı olduğu ve çalışma koşullarının değişebileceği gerçeğiyle birlikte tasarlanmasını ele alır. Amaç güvenlik sorumluluğunu insanlardan kaldırmak veya herkesi potansiyel tehdit olarak görmek değil; güvenli davranışın uygulanabilir olduğu ve tek bir insan hatası, kandırılması veya kötüye kullanımının gereksiz ölçüde büyük sonuçlara dönüşmediği bir çalışma anlayışı oluşturmaktır.

İlke 1: Güvenlik insanların hiç hata yapmayacağı varsayımına dayanmamalıdır.

İnsanlar yanlış seçim yapabilir, bir ayrıntıyı gözden kaçırabilir veya yanlış bilgiyi doğru kabul edebilir. Makul bir insan hatasının sınırsız güvenlik sonucuna dönüşmemesi sistem tasarımının sorumluluğunun bir parçasıdır.

İlke 2: İnsan hatası ile kötü niyet birbirine eşit kabul edilmemelidir.

Yanlışlıkla yapılan bir işlem ile bilinçli kötüye kullanım farklı neden ve müdahaleler gerektirir. Her hatayı saldırı gibi ele almak gerçek saldırıları ayırt etmeyi zorlaştırabilir ve insanların sorunları gizlemesine neden olabilir.

İlke 3: Sistem tasarımındaki zayıflık kullanıcıya devredilen sorumlulukla gizlenmemelidir.

Bir güvenlik sınırı ancak her kullanıcının sürekli olarak doğru kararı vermesiyle korunabiliyorsa tasarım kırılgandır. Eğitim ve dikkat, teknik olarak daha güvenilir biçimde sınırlandırılabilecek risklerin yerine geçen temel kontrol olmamalıdır.

İlke 4: Güvenli davranış olağan işi gereksiz biçimde zorlaştırmamalıdır.

İnsanlar işlerini yapabilmek için güvenlik mekanizmalarını sürekli aşmak zorunda kalıyorsa zamanla kayıt dışı yollar ortaya çıkabilir. Güvenli yol, gerçek çalışma koşulları içinde kullanılabilir ve sürdürülebilir olmalıdır.

İlke 5: İnsanlardan anlamlı biçimde veremeyecekleri güvenlik kararları beklenmemelidir.

Teknik sertifika ayrıntıları, karmaşık izinler veya belirsiz risk soruları çoğu kullanıcının güvenilir biçimde değerlendirebileceği kararlar olmayabilir. Sistem mümkün olduğu ölçüde gerekli uzmanlığı ve bağlamı tasarımın içine taşımalıdır.

İlke 6: Güvenlik uyarıları dikkat kapasitesini tüketen sürekli gürültüye dönüşmemelidir.

Çok sık, önemsiz veya sürekli benzer uyarılar insanların gerçekten önemli sinyalleri de görmezden gelmesine yol açabilir. Uyarının değeri gösterilmesinden çok doğru zamanda anlamlı bir karar oluşturabilmesindedir.

İlke 7: Güvenlik iletişimi hedeflenen kişinin anlayabileceği açıklıkta olmalıdır.

Teknik olarak doğru ancak anlaşılmaz mesajlar güvenli davranış üretmeyebilir. İnsanların ne olduğunu ve kendilerinden ne beklendiğini makul biçimde anlayabilmesi güvenlik iletişiminin parçasıdır.

İlke 8: Korku ve utandırma sürdürülebilir güvenlik davranışının temel yöntemi olmamalıdır.

İnsanları hata yapmaktan korkutmak kısa süreli uyum üretebilir; ancak olayların, şüphelerin ve hataların gizlenmesine de yol açabilir. Güvenlik yaklaşımı insanların sorunları zamanında görünür hale getirebilmesini korumalıdır.

İlke 9: Eğitim tamamlanması gerçek güvenlik yetkinliğiyle eşit kabul edilmemelidir.

Bir içeriğin izlenmiş veya sınavın geçilmiş olması kişinin gerçek durumda doğru davranabileceğini göstermez. Eğitim, insanların karşılaşacağı görev ve kararlarla ilişkili uygulanabilir bir kapasite oluşturduğu ölçüde değer taşır.

İlke 10: Güvenlik bilgisi gerçek rol ve etkiyle uyumlu olmalıdır.

Her çalışanın aynı teknik ayrıntıyı bilmesi gerekli değildir. Yüksek etkili işlem yapanlar ve özel sorumluluk taşıyanlar kendi görevlerinden kaynaklanan riskleri anlayabilecek ölçüde farklı bilgi ve yetkinliğe ihtiyaç duyabilir.

İlke 11: Sosyal mühendislik yalnızca kullanıcının dikkatsizliği olarak görülmemelidir.

Saldırganlar güven, otorite, aciliyet, korku ve alışılmış iş süreçlerini kötüye kullanabilir. Savunma yalnızca bireyin saldırıyı fark etmesine değil, başarılı kandırmanın oluşturabileceği etkinin de sınırlandırılmasına dayanmalıdır.

İlke 12: Otorite, aciliyet ve baskı güvenlik sınırlarını kendiliğinden aşmamalıdır.

Yönetici talebi, acil müşteri ihtiyacı veya benzeri gerekçeler insanları normalde yapmayacakları yüksek etkili işlemlere yönlendirebilir. Kritik güvenlik sınırları yalnızca talebin güçlü görünmesine bağlı olarak ortadan kalkmamalıdır.

İlke 13: Yüksek etkili işlemler tek bir insanın hatasına veya kandırılmasına gereksiz biçimde bağlı olmamalıdır.

Bir kararın yanlışlığı çok büyük sonuç oluşturabiliyorsa ek bağımsızlık veya sınırlandırma anlamlı hale gelir. Amaç her işleme onay eklemek değil, tek bir insan hatasının oluşturabileceği etkiyi riskle orantılı biçimde sınırlamaktır.

İlke 14: Görev ayrımı organizasyon şemasından çok gerçek işlem yeteneğine dayanmalıdır.

Farklı roller tanımlanmış olsa da tek bir kişi bütün kritik işlemi teknik olarak gerçekleştirebiliyorsa gerçek ayrım sınırlıdır. Bununla birlikte ayrım, işi sürdürülemez hale getirerek insanları ortak hesap ve kayıt dışı yollara da zorlamamalıdır.

İlke 15: İnsanların yetkileri gerçek görevleriyle birlikte değişebilmelidir.

İşe giriş, rol değişikliği, geçici görev ve ayrılık insan ile sistemler arasındaki güven ilişkilerini değiştirir. Geçmiş rolün erişimleri yeni duruma görünmez biçimde taşınmamalı ve ilişki sona erdiğinde yalnızca ana hesabın değil gerçek erişim yollarının da durumu değişmelidir.

İlke 16: Yüksek etkili rol, kişiye sınırsız kişisel güven verilmesi anlamına gelmemelidir.

Deneyimli, kıdemli veya uzun süredir çalışan bir kişinin hata yapmayacağı veya hesabının ele geçirilmeyeceği varsayılamaz. Geniş yetki taşıyan rollerin güvenliği kişinin karakterine değil sınırlandırılmış ve açıklanabilir etkiye dayanmalıdır.

İlke 17: Paylaşılan çalışma insan sorumluluğunu görünmez hale getirmemelidir.

Ortak hesap, parola paylaşımı veya başka ortak kimlik kullanımları görevi kolaylaştırabilir; ancak önemli işlemlerin hangi gerçek insan tarafından yapıldığını tamamen kaybettirmemelidir. İşbirliği ihtiyacı, kimlik ile sorumluluk arasındaki bağı gereksiz biçimde koparmamalıdır.

İlke 18: Güvenlik sistemi insan hafızasının ve dikkatinin gerçek sınırlarını kabul etmelidir.

Çok sayıda sır, sürekli değişen kurallar veya hatırlanması güç süreçler insanları güvenli olmayan telafi davranışlarına yöneltebilir. Güvenlik, insanın bilişsel sınırlarını başarısızlık olarak değil tasarım girdisi olarak ele almalıdır.

İlke 19: Kişisel araçlar ve olağan dışı çalışma koşulları görünmez güven alanları oluşturmamalıdır.

Kişisel cihaz, kişisel hesap, uzaktan çalışma veya seyahat işin gerçek koşulları olabilir; ancak bunların kullanılması kurumsal verinin ve erişimin kontrol dışına çıktığını görünmez hale getirmemelidir. Çalışma ortamı değiştiğinde güven varsayımları da gerektiğinde değişebilmelidir.

İlke 20: İç tehdit yalnızca kötü niyetli çalışan modeliyle açıklanmamalıdır.

İçeriden kaynaklanan güvenlik kaybı hata, ihmal, ele geçirilmiş hesap, baskı, çıkar çatışması veya bilinçli kötüye kullanım sonucu oluşabilir. Güvenlik yaklaşımı bir kişiyi "iç tehdit" olarak etiketlemekten çok oluşabilecek davranış ve etkiyi sınırlandırmalıdır.

İlke 21: İnsan davranışının izlenmesi güvenlik amacıyla sınırsız gözetim yetkisine dönüşmemelidir.

Olağan dışı davranışlar güvenlik açısından önemli sinyaller üretebilir; ancak tek bir anomali kişinin kötü niyetli olduğunu göstermez. İzleme gerekli bağlam ve mahremiyet sınırları içinde yürütülmeli, insan hakkında ağır sonuçlar zayıf sinyale bağlanmamalıdır.

İlke 22: Hata ve şüphelerin erken bildirilmesi insanlar için uygulanabilir olmalıdır.

Bir kullanıcı yanlış işlem yaptığını veya şüpheli bir durum gördüğünü fark ettiğinde hızlı bildirim zararı önemli ölçüde sınırlayabilir. Bildirim yolu gereksiz karmaşıklık, belirsizlik veya otomatik suçlama nedeniyle insanları sessiz kalmaya teşvik etmemelidir.

İlke 23: Güvenlik sorunlarını dile getirmek organizasyonel olarak mümkün olmalıdır.

Çalışanlar riskli bir talebi, hatalı kararı veya güvenlik sorununu hiyerarşi ve performans baskısından bağımsız olarak gerekli taraflara taşıyabilmelidir. Bir kuruluşun güvenliği, kötü haberlerin organizasyon içinde rahatça yukarı hareket edebilmesine de bağlıdır.

İlke 24: Kritik güven ve bilgi tek bir insanın sürekli varlığına bağlı olmamalıdır.

Tek bir kişinin bildiği sırlar, karar yolları veya operasyon bilgisi hem kötüye kullanım hem de süreklilik riski oluşturur. Bilgi ve sorumluluk, gereksiz yetki yaymadan kuruluşun güvenilir biçimde devam edebileceği ölçüde paylaşılabilmelidir.

İlke 25: İnsan güvenliği eğitim veya davranış puanlarına indirgenmemelidir.

Eğitim tamamlama oranı, oltalama simülasyonu sonucu veya olay sayısı belirli sinyaller sağlayabilir; ancak insanların güvenli yolu gerçekten kullanabildiğini veya sistemin insan hatasına dayanıklı olduğunu tek başına göstermez. Ölçüm insanı suçlayacak hedefler üretmemelidir.

İlke 26: İnsan güvenliği gerçek çalışma davranışı ve etki üzerinden doğrulanabilmelidir.

Politikalar, eğitim kayıtları, rol tanımları veya farkındalık kampanyaları tek başına güvence oluşturmaz. İnsanların güvenli yolu gerçekten kullanabildiği, görev değişikliklerinin gerçek erişimlere yansıdığı, tek bir hata veya kandırılmanın oluşturabileceği etkinin sınırlandırıldığı ve güvenlik sorunlarının zamanında görünür hale getirilebildiği gerektiğinde gösterilebilmelidir.