

Log saklama kontrol listesi: KOBİ, otel ve okul için

Her kurum için ortak

- ☐ Güvenlik duvarı giden internet trafiği kayıtlarını bir kayıt sunucusuna gönderiyor ve dün tarihli bir kaydı orada gördüm.
- ☐ DHCP sunucusunun kira kayıtları, giden trafik kayıtlarından ayrı olarak toplanıyor.
- ☐ Güvenlik duvarının, DHCP sunucusunun ve kayıt sunucusunun saatleri aynı zaman kaynağına bağlı.
- ☐ Saklama süresi yazılı, süreyi belirleyen kişi veya birim belli ve hukuk danışmanı ile teyit edildi.
- ☐ Kayıtlar saklama süresi dolmadan silinmiyor ve disk dolduğunda ne olacağı yazılı.
- ☐ Kayıt dosyaları için özet (SHA-256) ve zaman damgası (RFC 3161) üretiliyor, mühürleme aralığı yazılı.
- ☐ Zaman damgası sunucusuna (TSA) ağ erişimi açık ve erişim kesilirse haber alınıyor.
- ☐ Arşivin bir kopyası ayrı bir yerde duruyor ve bu kopyadan geri dönüş denendi.
- ☐ Kayıtlara erişen kişiler listelenmiş ve erişim role göre sınırlı.
- ☐ Bir IP adresi ve saat verildiğinde ilgili kaydı çıkarma provası yapıldı, sonucu tarihli olarak saklanıyor.

Otel / konaklama

- ☐ Misafir ağı personel ve yönetim ağından ayrı.
- ☐ Misafir ağında kullanıcıyı belirleyen bir adım var (örneğin SMS ile doğrulama).
- ☐ Lobi, oda ve toplantı salonu ağlarının hangi güvenlik duvarından çıktığı yazılı.
- ☐ Bütün misafir ağlarının DHCP kira kayıtları eksiksiz toplanıyor.
- ☐ Karşılama sayfasındaki doğrulama kaydı, DHCP kira kaydıyla aynı saat kaynağını kullanıyor.
- ☐ Yeni bir erişim noktası ya da ağ segmenti eklendiğinde, kayıt kapsamına girdiğini kontrol ediyoruz.
- ☐ Kayıt talebi geldiğinde kimin neye bakacağı ve kime yanıt vereceği yazılı.

Okul / eğitim

- ☐ Personel ağı ile öğrenci ağı ayrı ve her birinin DHCP kayıtları ayrı izlenebiliyor.
- ☐ Öğrenci ve misafir cihazlarının adres aldığı DHCP sunucusu kayıt kapsamında.
- ☐ Sınıf, laboratuvar ve yurt gibi ağların hangi güvenlik duvarından çıktığı yazılı.
- ☐ Kayıtlara erişim yalnızca görevlendirilen kişilerle sınırlı ve erişimler izlenebiliyor.
- ☐ Yeni dönem başında eklenen ağ ve cihazların kayıt kapsamına girdiğini kontrol ediyoruz.
- ☐ Kayıt talebi geldiğinde sorguyu yapacak kişi ve yedeği yazılı.

Bu liste genel bilgi amaçlıdır, hukuki değerlendirme içermez.

7 Tepe Bilişim · 7tepebilisim.com