KARADENİZ TEKNİK ÜNİVERSİTESİ FARABİ HASTANESİ

BİLGİ GÜVENLİĞİ RİSK ANALİZ TABLOSU

Hazırlayan: Bilgi İşlem Birimi
Tarih: 2025
Sürüm: 1.0

Varlık	Tehdit	Zafiyet	Olasılık (1-5)	Etki (1-5)	Risk Düzeyi (O x E)	Mevcut Kontroller	İyileştirme Önerisi
HBYS Sunucusu	Siber saldırı / Ransomware	Güncellemelerin gecikmesi, kullanıcı farkındalık eksikliği	3	5	15	Firewall (Fortigate), ESET, Oracle otomatik yedekleme	Kullanıcı eğitimleri, yedeklerin çevrimdışı kopyalanması
PACS Sistemi	Donanım arızası	Sunucu yaşlanması, yedek donanım eksikliği	2	5	10	UPS, yedekleme sistemi	Yedek donanım tedariki, felaket kurtarma testi
Oracle Veritabanı	Yetkisiz erişim	Parola politikası zafiyeti	3	4	12	Parola politikası, erişim logları	MFA (çok faktörlü kimlik doğrulama) entegrasyonu
Kullanıcı Bilgisayarları	Zararlı yazılım	USB cihaz kullanımı, güncellemelerin ertelenmesi	4	3	12	ESET antivirüs, otomatik Windows Update	USB erişim kısıtlaması, farkındalık eğitimleri
Ağ Altyapısı	DDOS / Saldırı	Yetersiz izleme	2	5	10	Fortigate IPS, VLAN yapılandırması	Trafik analizi ve log korelasyon sistemi (SIEM) kurulumu
Sunucu Odaları	Yangın / Isı artışı	HVAC arızası, sensör bakımı eksikliği	2	5	10	Yangın algılama, soğutma	Sensör testleri, bakım planının sıkılaştırılması

						sistemi, UPS	
Kablosuz Ağ (Wi-Fi)	Yetkisiz erişim	Zayıf parola politikası	3	4	12	MAC doğrulama, şifreli ağ (WPA2)	WPA3 geçişi, parola periyodik yenileme
Yedekleme Diskleri	Fiziksel zarar / kayıp	Şifreleme eksikliği	2	4	8	Yetkili personel ile fiziksel yedekleme	Yedeklerin şifrelenmesi ve farklı lokasyonda tutulması
IP Telefon Sistemi	Hizmet kesintisi	Güç kesintisi, network bağımlılığı	2	3	6	UPS, VLAN ayrımı	Yedek hat / 2. santral kurulumu
Personel Hesapları	Kimlik hırsızlığı	Zayıf parola, sosyal mühendislik	3	4	12	Şifre politikası, eğitimler	MFA entegrasyonu, phishing simülasyonları

Risk Düzeyi Sınıflandırması

Risk Puanı	Düzey	Açıklama
1–5	Düşük	Takip edilmesi yeterli
6–10	Orta	İzleme ve önlem alınmalı
11–15	Yüksek	İyileştirme planı zorunlu
16–25	Kritik	Acil müdahale gerektirir

Risk Azaltma Öncelik Planı

1. Kullanıcı farkındalığı ve şifre güvenliği eğitimlerinin artırılması

2. MFA sisteminin Oracle ve kritik uygulamalara entegrasyonu

3. Yedekleme güvenliğinin güçlendirilmesi (şifreleme + farklı lokasyon)

4. SIEM sistemi ile log korelasyon ve tehdit izleme altyapısının kurulması

5. Felaket kurtarma tatbikatlarının yılda en az 1 kez yapılması