Ransomware’e Karşı Yedekleme / Segmentasyon / Eğitim Checklist Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu asset; ransomware (fidye yazılımı) saldırılarına karşı savunmayı üç temel ayakta (offline/immutable backup, ağ segmentasyonu ve rol bazlı kullanıcı eğitimi) kurmak için hazırlanmıştır. "Yedeklerimiz var sanıyorduk" riskini periyodik restore testleri ve izole erişim kontrolleriyle ortadan kaldırır; ağ segmentasyonu ile olası zararlı yazılımın yatayda (*lateral movement*) yayılımını sınırlar. Eğitim ve phishing simülasyonlarıyla ilk bulaşma riskini en aza indirmeyi hedefler.

Kim Kullanır?: IT / BT Ekipleri, Güvenlik / Ops Sorumluları, İK (İnsan Kaynakları - Eğitim) ve Otel / B2B Üst Yönetimi.

Nasıl Kullanılır?

1. Kurumsal varlık envanterini çıkartarak Tier-1 kritik sistemleri (*rezervasyon, PMS, ödeme ve veritabanı*) belirleyin.
2. Offline / immutable (değiştirilemez) yedekleme altyapısını ve VLAN/Ağ segmentasyon kurallarını planlayıp devreye alın.
3. Rol bazlı güvenlik eğitimi takvimini ve oltalama (*phishing*) simülasyonlarını başlatın; olay müdahale (*incident runbook*) süreçlerine bağlayın.

CHECKLIST & SPRINT PLAN — Ransomware Savunma Stratejisi

1) Ölçüm & Önceliklendirme Kontrol Listesi (Checklist)

- [ ] **Tier-1 Kritik Sistem Envanteri Tanımlı:** İş sürekliliği için hayati olan veritabanları, PMS/CRM entegrasyonları ve rezervasyon sistemleri belirlendi, RPO/RTO hedefleri kilitlendi.
- [ ] **Offline / Immutable Backup Altyapısı Mevcut:** Yedeklerin zararlı yazılımlar tarafından silinmesini/şifrelenmesini önleyen WORM (Write Once Read Many) veya hava boşluklu (*air-gapped*) yedekleme mimarisi kuruldu.
- [ ] **İzole Backup Erişim Rolleri:** Yedekleme sistemlerine erişim, genel domain/AD yetkilerinden tamamen ayrıştırılmış bağımsız ve MFA korumalı özel hesaplara bağlandı.
- [ ] **Periyodik Restore (Geri Yükleme) Testleri:** Yedeklerin çalışırlığı ve veri bütünlüğü en az üç ayda bir sanal ortamlarda fiili olarak test ediliyor.
- [ ] **Ağ & Segmentasyon Mimarisi:** Yönetim ağı (Management), sunucu parkı, dosya paylaşım alanları ve kullanıcı VLAN'ları birbirinden firewall/ACL katmanlarıyla tamamen ayrıldı.
- [ ] **Kritik Protokol Kısıtlamaları (SMB/RDP):** Ağlar arası RDP, SMB ve uzak yönetim protokolleri strictly allowlist kurallarına bağlandı ve MFA ile zorunlu kılındı.
- [ ] **Geçici Port Kapanış & İzin Süreci:** Bakım/destek için açılan geçici ağ portları ve erişim izinleri için otomatik zaman ayarlı kapanış prosedürleri uygulandı.
- [ ] **Rol Bazlı Phishing & Güvenlik Eğitimi:** Genel çalışanlar, IT personeli ve yöneticiler için ayrı ayrı yapılandırılmış periyodik ransomware farkındalık eğitimleri planlandı.

- [ ] **Oltalama (Phishing) Simülasyonu & Ölçüm:** Çalışanların sahte e-postalara tıklama oranlarını ve tespiti raporlama davranışlarını ölçen simülasyonlar devreye alındı.
- [ ] **Incident Runbook & İletişim Planı:** Ransomware tespiti anında ağ izolasyonu, sistem kapatma ve kriz iletişimi adımlarını içeren olay müdahale rehberi hazırlandı.

2) Problem → Kök Neden → Çözüm Tablosu

Problem	**Kök Neden**	**Çözüm (Ransomware Savunması)**
Backup da Şifreleniyor	Network erişiminin geniş olması / Aynı AD yetkisi	**Offline / Immutable Backup** $\mathbf{+}$ **Erişim Daraltma**
Hızlı Yayılım (Yatay İlerleme)	Ağ segmentasyonunun ve ACL kısıtlarının olmaması	**Yönetim / Dosya / DB Segmentasyonu** $\mathbf{+}$ **MFA**
İlk Bulaşma (Phishing / Oltalama)	Çalışan farkındalığının ve eğitimlerin yetersizliği	**Rol Bazlı Eğitim** $\mathbf{+}$ **Düzenli Phishing Simülasyonu**
Geç Fark Etme / Yanıt Verememe	Anomali alarmlarının ve müdahale akışının olmaması	**Merkezi İzleme** $\mathbf{+}$ **Olay Müdahale (Incident) Runbook**

3) 14 Günlük Uygulama Sprint Planı (Gün 1–14)

[Gün 1–5: Envanter, Backup & Restore Testi] ⟶ [Gün 6–9: Ağ Segmentasyonu & Port Kontrolü] ⟶ [Gün 10–12: Eğitim, Simülasyon & Runbook] ⟶ [Gün 13–14: Dashboard & Takvim]

- **Gün 1:** Tier-1 kritik sistem envanterinin çıkarılması, RPO (Veri Kaybı Tolere Süresi) ve RTO (Kurtarma Süresi) hedeflerinin belirlenmesi.
- **Gün 2:** Backup altyapısı için domain'den bağımsız, MFA korumalı özel erişim ve rol modelinin kurulması.
- **Gün 3–4:** Değiştirilemez (*immutable*) veya offline yedekleme mimarisinin tasarımı, pilot veritabanı üzerinde uygulanması.
- **Gün 5:** Alınan yedeklerin izolasyon ortamında geri yükleme (*restore*) testinin yapılması ve sürenin (RTO) ölçülmesi.
- **Gün 6–7:** Yönetim ağı, kullanıcı bilgisayarları, dosya sunucuları ve DB katmanları arası VLAN/Firewall segmentasyon kurallarının yazılması.
- **Gün 8:** Servisler arası SMB/RDP erişimlerinin taranması, gereksiz bağlantıların kapatılması ve kalanın allowlist + MFA'ya bağlanması.

- **Gün 9:** Bakım amaçlı açılan "geçici port/erişim" talepleri için süreli izin ve otomatik kapama prosedürünün devreye alınması.
- **Gün 10:** Kullanıcı rollerine göre (IK, Finans, IT, Saha) özelleştirilmiş ransomware ve phishing eğitim içeriklerinin yayınlanması.
- **Gün 11:** Tüm kuruma yönelik oltalama (*phishing*) simülasyonunun yürütülmesi ve tıklama/raporlama oranlarının ölçülmesi.
- **Gün 12:** Olay anı isolasyon adımlarını içeren Incident Runbook'un güncellenmesi ve ana ekiple masabaşı (*tabletop*) tatbikat icrası.
- **Gün 13:** KPI dashboard'unun (Restore Başarısı, Phishing Tıklama %, İzole Segment Sayısı) aktif edilmesi.
- **Gün 14:** Yönetim sunumunun yapılması ve 180 günlük periyodik kalibrasyon/test takviminin kilitlenmesi.

4) Öncesi / Sonrası KPI Tablosu

KPI Metriği	**Önce (Mevcut Durum)**	**Sonra (Sprint Sonrası)**	**Hedef Yönü**
Restore Başarı Oranı (%)	$\%40$ (Test edilmemiş yedekler)	$\%100$ (Doğrulanmış restore)	**Hedef ↑ (Yükselme)**
RTO (Kurtarma Süresi)	$\sim 72\text{ saat}$	$< 4\text{ saat}$	**Hedef ↓ (Düşüş)**
Phishing Tıklama Oranı (%)	$\%25$ (Yüksek risk)	$< \%3$ (Eğitilmiş personel)	**Hedef ↓(Düşüş)**
Segmentler Arası İzin Sayısı	Kontrolsüz / Geniş Erişim	Strictly Allowlist + MFA	**Hedef ↓(Düşüş)**

Deliverables (Teslim Edilecek Çıktılar)

- **Offline / Immutable Backup Mimari Dokümanı:** Değiştirilemez yedekleme standartları ve periyodik restore test protokolü.
- **Ağ Segmentasyonu & Port Kısıtlama Kural Seti:** VLAN ayrım matrisi, RDP/SMB allowlist politikası ve geçici port prosedürü.
- **Rol Bazlı Eğitim & Phishing Simülasyon Takvimi:** Personel farkındalık programı, simülasyon senaryoları ve davranışsal ölçüm kriterleri.

- **Ransomware Incident Runbook & Kriz İletişim Planı:** Saldırı anında ağ karantina adımları ve yönetim/yasal bildirim kılavuzu.
- **Ransomware Savunma KPI Dashboard'u:** İş sürekliliği, yedek doğrulama ve insan faktörü risk metriklerini izleme paneli.

[Checklist Card]

IT yöneticileri, siber güvenlik uzmanları ve sistem yöneticileri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Ransomware Defense Checklist Kartı. Koyu karbon gri ve parlak yeşil/kırmızı/mavi tonlarındaki teknolojik zemin üzerinde; kilitli immutable backup kasası, ağ segmentasyon kalkanları, phishing farkındalık rozetleri ve 14 günlük savunma sprint takvimi yer alıyor. Kartın üzerinde; "Offline & Immutable Backup with Verified Restore Tests", "VLAN Segmentation & SMB/RDP Allowlist Controls", "Role-Based Phishing Simulations & Employee Awareness", ve "Incident Response Runbook & Tabletop Exercises" teslimat kalemi başlıkları, yanlarında parlak yeşil onay işaretleriyle scannable ve kurumsal bir checklist-card formatında sergileniyor.