Zero Trust Erişim Mimarisi & Geçiş Checklist Şablonu — Yazılım / Sunucu ve Güvenlik (v1.0)

Asset Amaç: Bu asset; geleneksel çevre güvenliği (*perimeter security*) anlayışından "Never Trust, Always Verify" (Asla Güvenme, Her Zaman Doğrula) ilkesine dayanan Zero Trust mimarisine geçişi, karmaşık bir dönüşüm yerine 14 günlük bir sprint ve kademeli bir yol haritası olarak planlamak için hazırlanmıştır. Kimlik merkezileştirme, cihaz durumu (*device posture*), dinamik politika motoru ve mikro segmentasyon adımlarını önceliklendirir. Erişim ve kimlik doğrulama kayıtlarını merkezi olarak SIEM üzerine toplayarak KVKK/GDPR teknik tedbirlerine uygun tam denetlenebilirlik (*auditability*) sağlar.

Kim Kullanır?: BT / Siber Güvenlik Liderleri, DevOps Mühendisleri, Otel IT Yöneticileri ve B2B Platform Ekipleri.

Nasıl Kullanılır?

1. Mevcut erişim modelinizi (VPN ağları, VLAN/subnet yapısı, kullanıcı rolleri) listeleyerek hazırlık kontrol listesini doldurun.
2. SSO/MFA entegrasyonu, ajans/vendor erişim kuralları ve uygulama bazlı erişim (*ZTNA*) adımlarını 14 günlük sprint planına uygulayın.
3. Öncesi/Sonrası KPI tablosu ve audit log politikalarını tanımlayarak ilk 90/180 günlük Zero Trust yol haritanızı canlıya alın.

CHECKLIST & SPRINT PLAN — Zero Trust Erişim Mimarisi

1) Ölçüm & Önceliklendirme Kontrol Listesi (Checklist)

- [ ] **SSO Merkezi Kimlik Mevcut:** Tüm kurumsal/otomasyon uygulamaları tek bir Kimlik Sağlayıcıya (IdP: Okta, Azure AD, Keycloak) bağlı.
- [ ] **MFA Prod Erişimde Zorunlu:** Canlı ortamlara, veritabanlarına ve yönetim panellerine erişimde Çok Faktörlü Kimlik Doğrulama (MFA) aktif.
- [ ] **Rol Matrisi (RBAC) Yazılı:** En küçük yetki (*Least Privilege*) prensibine göre rol bazlı erişim matrisi tanımlı.
- [ ] **Ajans / Vendor Erişimleri Süreli:** Dış tedarikçi ve ajanslara verilen erişimler süre kısıtlamalı (*Time-bound TTL*) ve onay mekanizmalı.
- [ ] **Erişim Logları Merkezi ve Saklama Politikası Net:** Kimin, ne zaman, nereden bağlandığı bilgisi silinemez biçimde merkezi SIEM'e aktarılıyor.
- [ ] **Uygulama Bazlı Erişim (ZTNA) Hedefleri Belirlendi:** Ağ seviyesinde VPN bağlantısı yerine doğrudan uygulama seviyesinde tünelleme planlandı.
- [ ] **Segmentasyon (En Az Tier) Mevcut:** Sunucular ve servisler en azından katman (*Tier 1 Web, Tier 2 App, Tier 3 DB*) bazında ayrıldı.
- [ ] **Mikro Segmentasyon Roadmap'i Yazıldı:** Doğu-Batı (*East-West*) trafiğini kısıtlayacak sunucular arası mikro segmentasyon kuralları belirlendi.
- [ ] **Device Posture Sinyalleri Tanımlı:** Bağlanan cihazın disk şifrelemesi, EDR/Antivirüs durumu ve OS yama seviyesi doğrulama kriteri yapıldı.
- [ ] **"Allowed Access" Policy Seti Versiyonlanıyor:** Erişim kuralları Git deposunda kod olarak (*Policy as Code*) saklanıyor ve sürümleniyor.

2) Problem → Kök Neden → Çözüm Tablosu

Problem	Kök Neden	Çözüm (Zero Trust Yaklaşımı)
VPN'e Girince Geniş Erişim	Çevre/Perimetre varsayımı (*İç ağdaysa güvenlidir*)	Uygulama bazlı erişim (**ZTNA**) + En küçük yetki prensibi (**RBAC**)
Ajans / Vendor Erişimi Riskli	Süreli rol ve otomatik erişim sonlandırma olmaması	Süreli geçici rol (*Just-In-Time Access*) + Tam oturum denetimi (*Session Audit*)
İç Ağda Yayılım Hızlı (Lateral Movement)	Düz ağ (*Flat Network*) mimarisi ve yetersiz izolasyon	Katmanlı ağ izolasyonu + Sunucular arası **Mikro Segmentasyon**
"Kim Erişti?" Sorusunun Yanıtsız Kalması	Dağınık, merkezi olmayan ve yerel saklanan loglar	**Merkezi SIEM Audit Logging** + KVKK Uyumlu Değiştirilemez Log Arşivi

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

[Gün 1–4: Kimlik & Politika Altyapısı] ──> [Gün 5–7: Pilot Uygulama] ──> [Gün 8–12: Segmentasyon & Posture] ──> [Gün 13–14: KPI & Roadmap]

- **Gün 1:** Kimlik ve erişim envanterinin çıkarılması; taslak Rol Matrisinin (RBAC) oluşturulması.
- **Gün 2:** Tüm Prod ve kritik yönetim panelleri için IdP üzerinde SSO / MFA zorunluluğu planı ve kurgusu.
- **Gün 3:** Ajans, tedarikçi ve otel B2B entegratörleri için süreli/onaylı erişim (*JIT Access*) politikasının yazılması.
- **Gün 4:** Merkezi Audit Log mimarisinin kurulması ve KVKK/5651 uyumlu log saklama kurallarının tanımlanması.
- **Gün 5–7:** Uygulama bazlı erişim pilotu (Kritik 1–2 uygulama seçilerek klasik VPN bypass edilip ZTNA tüneline alınır).
- **Gün 8–10:** Katmanlı ağ segmentasyonunun (*DMZ, App, DB*) iyileştirilmesi ve temel Doğu-Batı güvenlik duvarı kurallarının çekilmesi.
- **Gün 11–12:** Cihaz güvenlik durumu (*Device Posture*) sinyallerinin (EDR kontrolü, OS yama seviyesi) erişim politikalarına dahil edilmesi.
- **Gün 13–14:** KPI Dashboard'unun aktif edilmesi, sonuçların ölçülmesi ve Gelecek 90 Günlük Zero Trust Roadmap'inin kilitlenmesi.

4) Öncesi / Sonrası KPI Tablosu

KPI Metriği	Önce (Mevcut Durum)	Sonra (Sprint Sonrası)	Hedef Yönü
MFA Kapsaması (%)	$\%30$ (Yalnızca e-posta/VPN)	$\%100$ (Tüm Prod ve Admin panelleri)	**Hedef ↑ (Yükselme)**
Süreli / Onaylı Erişim Oranı (%)	$\%0$ (Kalıcı SSH/VPN yetkileri)	$\%95$ (Tüm dış/ajans erişimleri süreli)	**Hedef ↑ (Yükselme)**
Lateral Movement Riski / Sinyali	Yüksek (Düz ağda serbest geçiş)	Düşük (Mikro segmentasyon ile bloklu)	**Hedef ↓ (Düşüş)**
Audit Log Kapsaması (%)	$\%25$ (Yalnızca yerel loglar)	$\%100$ (Merkezi SIEM & KVKK Uyumlu)	**Hedef ↑ (Yükselme)**

Deliverables (Teslim Edilecek Çıktılar)

- **Rol Matrisi & Policy-as-Code Seti (v1.0):** Yetki seviyelerini ve ZTNA erişim kurallarını belirten politika kütüphanesi.
- **Pilot Uygulama Erişim & ZTNA Entegrasyon Planı:** Seçilen kritik uygulamaların Zero Trust mimarisine taşınma rehberi.
- **Ağ & Mikro Segmentasyon İyileştirme Listesi:** Doğu-Batı trafiğini izole eden firewall ve VPC kural seti.
- **Merkezi Audit Log & KVKK Saklama Politikası Dokümanı:** Erişim kayıtlarının güvenli arşivlenmesi ve denetim kılavuzu.
- **Zero Trust Geçiş KPI Dashboard'u & 90 Günlük Yol Haritası:** Dönüşüm başarısını ve sonraki adımları izleyen yönetim paneli.

[Checklist Card]

BT yöneticileri, siber güvenlik mimarları ve DevOps liderleri için tasarlanmış, 1200x1200px (1:1) kare formatında yüksek çözünürlüklü bir Zero Trust Checklist Kartı. Koyu karbon gri ve parlak neon mavi/siyan tonlarındaki teknolojik zemin üzerinde; Zero Trust mimari halkaları, kimlik doğrulama (MFA/SSO) simgeleri, mikro segmentasyon kalkanları ve 14 günlük sprint zaman çizelgesi yer alıyor. Kartın üzerinde; "Identity-Centric Access & MFA Policy", "ZTNA Application-Level Tunneling", "Micro-Segmentation & Device Posture Checks" ve "KVKK Compliant Central Audit Logging" teslimat kalemi başlıkları, yanlarında parlak siyan onay işaretleriyle scannable ve kurumsal bir checklist-card formatında sergileniyor.