DURKON · WHITEPAPER

Kurumsal BT Güvenlik Kontrol Listesi 2026

CEO, CFO ve BT Direktörleri için kapsamlı bir başvuru kılavuzu. Yönetişimden farkındalık eğitimine kadar 9 ana başlıkta 50+ uygulanabilir kontrol noktası.

Durkon

Kurumsal BT Çözümleri & Siber Güvenlik

Sürüm 1.0 · Haziran 2026

durkon.com

İçindekiler

01 · Giriş — Neden Şimdi?

Türkiye'deki kurumsal şirketlerin %43'ü her yıl en az bir önemli siber güvenlik olayı yaşıyor. KVKK kapsamındaki cezalar 2026 itibarıyla 12 milyon TL'ye ulaştı. Bir veri ihlali ortalama 4.45 milyon USD maliyete sebep oluyor. Ancak hâlâ birçok kurum siber güvenliği "ayrı bir BT projesi" gibi görüyor; halbuki bu, doğrudan iş sürekliliği, marka değeri ve yasal yükümlülük meselesidir.

Bu rehber, BT Direktörleri için olduğu kadar CFO ve CEO seviyesindeki karar vericiler için de hazırlandı. Teknik derinliğe inmeden, kurumun güvenlik olgunluğunu hızlıca değerlendirmenizi, eksikleri tespit etmenizi ve önceliklendirmenizi sağlamak hedeflendi.

4.45M USD

2025 yılında küresel ortalama veri ihlali maliyeti (IBM Cost of a Data Breach Report)

Rehberin sonundaki **50 maddelik kontrol listesini** ekibinizle birlikte gözden geçirin; mevcut durumunuzu net görün ve aksiyon planınızı oluşturun.

> **Bu rehberin amacı**
>
> Kurumunuzun güvenlik olgunluğunu hızlı, somut ve uygulanabilir bir çerçevede değerlendirmek. Her bölüm, "neden önemli?", "ne yapmalı?" ve "kontrol noktası" yapısında hazırlandı.

02 · Yönetişim ve Risk Yönetimi

Neden Önemli?

Siber güvenlik bir teknoloji projesi değil; yönetim sorumluluğudur. Üst yönetimin desteklemediği güvenlik girişimleri yarıda kalır, bütçe alamaz ve organizasyonel direnç yüzünden çöker. ISO 27001 ve KVKK gibi standartların tamamı, yönetişimi (governance) ilk gereksinim olarak listeler.

Ne Yapmalı?

- **Bilgi Güvenliği Politikası:** Yönetim onaylı, en az yılda bir gözden geçirilen yazılı bir politika belgesi olmalı.
- **Sorumlu Atama:** CISO (Bilgi Güvenliği Sorumlusu) veya KVKK Veri Sorumlusu Temsilcisi atanmalı. Bu rol, BT Müdürü ile aynı kişi olabilir ama görev tanımı net olmalı.
- **Risk Değerlendirme:** Yıllık risk değerlendirme yapılmalı. Tüm dijital varlıklar listelenmeli, her birine etki ve olasılık skorları atanmalı.
- **Komite Yapısı:** Üç ayda bir toplanan Bilgi Güvenliği Komitesi; CEO veya CFO katılımcı olmalı.

- **KVKK Uyumluluğu:** VERBİS kaydı, açık rıza süreçleri, veri envanteri, ihlal bildirimi prosedürü yazılı olarak hazır olmalı.

> **Sık yapılan hata**
>
> "Bizim politikamız var ama kimse görmemiş." Kullanılmayan, çalışanların habersiz olduğu bir politika, hukuksal güvence sağlamaz. Yıllık eğitimle dağıtım yapılmalı, çalışan beyanı imzalatılmalı.

03 · Kimlik ve Erişim Yönetimi (IAM)

Neden Önemli?

Veri ihlallerinin %81'i çalıntı veya zayıf parolalar yüzünden gerçekleşir. Kimlik ve erişim yönetimi, modern siber güvenlik mimarisinin temel taşıdır. Zero-trust yaklaşımı: "asla güvenme, her zaman doğrula" prensibi.

Ne Yapmalı?

- **Çok Faktörlü Kimlik Doğrulama (MFA):** Tüm yönetici hesapları ve uzaktan erişim için zorunlu. E-posta, VPN, kritik uygulamalarda MFA kapatılmamalı.
- **Parola Politikası:** Minimum 12 karakter, kompleks, yıllık değişim. Hesap kilitleme: 5 yanlış denemeden sonra 30 dakika.
- **Privileged Access Management (PAM):** Yönetici hesapları için ayrı kimlikler. Just-in-time erişim, oturum kaydı, parola kasası.
- **RBAC (Role Based Access Control):** Erişimler kişiye göre değil, role göre verilmeli. İşten ayrılan kullanıcının hesabı 24 saat içinde devre dışı.
- **Düzenli Erişim İncelemesi:** Üç ayda bir tüm hesap ve yetkilerin gözden geçirilmesi. Atıl hesaplar tespit edilip kapatılmalı.
- **Single Sign-On (SSO):** Mümkün olduğunca SSO ile uygulamalar bağlanmalı. Azure AD, Okta, Auth0 gibi çözümler.

%99.9

MFA aktif hesaplarda saldırı başarı oranı düşüşü (Microsoft Security Intelligence Report)

04 · Ağ Güvenliği

Neden Önemli?

Ağ, dijital varlıklarınıza erişimin ilk katmanıdır. Yanlış konfigüre edilmiş bir güvenlik duvarı veya açık bir port, en sıkı endpoint koruması bile geçilmesini sağlar. Modern ağ güvenliği, "perimeter security" (çevre savunması) yerine "zero-trust networking" (her trafiği doğrula) yaklaşımı izler.

Ne Yapmalı?

- **Yeni Nesil Firewall (NGFW):** Uygulama tabanlı kontrol, kullanıcı tabanlı politika, IPS/IDS dahil. Yıllık lisans yenileme ve imza güncellemeleri.
- **Ağ Segmentasyonu (VLAN):** Üretim, ofis, misafir, IoT ağları ayrı VLAN'larda. Sistem hesapları kullanıcı ağına erişemez.
- **VPN ve Uzaktan Erişim:** Site-to-site VPN için IPsec, kullanıcı için SSL VPN veya ZTNA (Zero Trust Network Access).
- **Wi-Fi Güvenliği:** WPA3 Enterprise, sertifika tabanlı kimlik doğrulama. Misafir Wi-Fi izole, captive portal ile.
- **DNS Filtreleme:** Cloudflare for Teams, Cisco Umbrella, ControlD gibi çözümlerle kötü amaçlı domain'lere erişim engellenmeli.
- **SSL Inspection:** Şifrelenmiş trafiğin firewall tarafından açılarak incelenmesi. Hassas regülasyonları göz önünde bulundurularak yapılandırılmalı.

> **İpucu**
>
> "Trust no one" yaklaşımının pratik yolu mikro-segmentasyondur. Aynı VLAN içindeki cihazların birbirine erişimini bile kontrol etmek, ransomware yayılımını engeller.

05 · Endpoint Güvenliği

Neden Önemli?

Modern saldırıların büyük çoğunluğu kullanıcı bilgisayarlarından başlar. Phishing e-postası ile bir kullanıcının laptop'una giren saldırgan, oradan ağ ve sunuculara yayılır. Geleneksel antivirüs (imza tabanlı) artık yetersiz; davranışsal tespit yapan EDR/XDR çözümleri zorunludur.

Ne Yapmalı?

- **EDR / XDR Çözümü:** CrowdStrike, SentinelOne, Microsoft Defender for Endpoint, ESET. Davranış tabanlı, AI destekli tehdit tespiti.
- **Yama Yönetimi:** İşletim sistemi ve uygulama yamaları otomatik dağıtılmalı. Kritik yamalar 72 saat içinde uygulanmalı.
- **USB Kontrolü:** USB depolama cihazları kısıtlanmalı veya tamamen engellenmeli. DLP (Data Loss Prevention) çözümleri.
- **Disk Şifreleme:** Tüm laptop'larda BitLocker, FileVault gibi tam disk şifreleme zorunlu. Cihaz kaybı durumunda veri açığa çıkmaz.
- **Mobil Cihaz Yönetimi (MDM):** BYOD veya kurum cihazlarında MDM (Microsoft Intune, Jamf). Uzaktan silme, uygulama yönetimi, uyum politikası.
- **Web Browser Sıkılaştırma:** Pop-up engelleyici, eklenti politikası, otomatik güncelleme.

06 · Veri Güvenliği ve Yedekleme

Neden Önemli?

Ransomware, modern siber güvenlik tehditlerinin en yıkıcısıdır. 2025'te Türkiye'de en az 23 büyük şirket ransomware kurbanı oldu ve ortalama operasyon kesintisi 21 gün sürdü. Doğru yedekleme stratejisi, hem ransomware'a hem donanım arızasına karşı en sağlam savunmadır.

Ne Yapmalı?

- **3-2-1 Yedekleme Kuralı:** 3 farklı kopya, 2 farklı medya, 1 tanesi off-site (farklı lokasyon).
- **Immutable Backup:** Yedeklerin değiştirilemez (silenemez, üzerine yazılamaz) olması. Ransomware yedekleri şifrelese bile geri dönüş garantisi.
- **Air-gapped Kopya:** Network'ten izole edilmiş bir kopya. Tape (manyetik bant) veya offline disk.
- **Restore Testi:** Yedekleri çalıştırarak geri yükleme testleri en az ayda bir yapılmalı. "Yedeklenmiş ama geri yüklenemeyen" yedekler her zaman vardır.
- **Veri Sınıflandırma:** Açık, dahili, gizli, çok gizli kategorileri. Her sınıfa farklı erişim kontrolü.
- **Şifreleme:** Hareket halinde (TLS 1.2+) ve durağan (AES-256) veri şifreleme. Veritabanlarında TDE (Transparent Data Encryption).
- **DLP (Data Loss Prevention):** Hassas verinin (kimlik no, kredi kartı no, müşteri verisi) izinsiz dışarı çıkmasını engelleyen sistemler.

> **Kritik uyarı**
>
> Yedek sunucunuz aynı ağda ve aynı kimlik bilgileriyle erişiliyorsa, ransomware yedeklerinizi de şifreleyebilir. Yedekleme sunucusu için ayrı kimlik bilgileri, ayrı VLAN ve immutable storage kullanın.

07 · Sürekli İzleme ve SIEM

Neden Önemli?

Bir saldırının tespit edilmesi ortalama 207 gün sürüyor. Yani saldırgan 7 ay boyunca ağınızda dolaşıyor olabilir. Sürekli izleme (SIEM, EDR, NDR) ile bu süre dakikalara iner. "Görmediğinizi koruyamazsınız."

Ne Yapmalı?

- **SIEM Kurulumu:** Wazuh (açık kaynak), Microsoft Sentinel, Splunk, IBM QRadar gibi çözümlerle merkezi log toplama.
- **Log Toplama:** Tüm sunucu, firewall, switch, AD, uygulama logları en az 90 gün saklanmalı. Yasal saklama süreleri (ELOG gibi) gözetilmeli.
- **Korelasyon Kuralları:** "10 başarısız giriş sonrası başarılı giriş" gibi anormal davranış kuralları yazılmalı.
- **SOC (Security Operations Center):** Kendi ekibinizle veya yönetilen SOC ile 7/24 izleme.

- **NDR (Network Detection & Response):** Ağ trafiğinde anomali tespiti. Darktrace, Vectra, Corelight gibi çözümler.
- **Threat Intelligence:** Bilinen tehdit aktörleri ve IoC (Indicator of Compromise) feed'leri.

08 · Olay Müdahale Planı

Neden Önemli?

Bir saldırı olduğunda paniklemek zaman kaybettirir. Yazılı, çalışılmış ve düzenli olarak test edilen bir olay müdahale planı, kayıp süreyi ve maliyeti dramatik şekilde azaltır. NIST 800-61 standardı: hazırlık → tespit → kontrol altına alma → yok etme → kurtarma → öğrenilen dersler.

Ne Yapmalı?

- **Yazılı IR Planı:** Kim, ne zaman, ne yapacak — net rol ve sorumluluklar.
- **Olay Sınıflandırması:** Düşük / orta / yüksek / kritik seviyeleri. Her seviyeye göre eskalasyon ve iletişim.
- **İletişim Listesi:** Yönetim, hukuk, BTK, KVKK Kurulu, üreticiler, müşteriler. Her birinin iletişim bilgisi güncel.
- **Yıllık Tatbikat:** Tabletop egzersiz (masa başı) veya gerçek senaryo simülasyonu. Eksikler tespit edilir.
- **Forensic İmkanı:** Disk imajı alma yetisi, ya da forensic hizmet veren firmayla anlaşma.
- **Yedek İletişim:** Ana iletişim kanalı (e-posta) saldırı altındayken kullanılacak alternatif (WhatsApp grup, kağıt liste).

> **Pratik öneri**
>
> KVKK kapsamında, bir veri ihlali 72 saat içinde Kurul'a bildirilmek zorundadır. Bu süreç için önceden hazırlanmış şablonlar ve karar matrisleri bulunmalı.

09 · Farkındalık ve Eğitim

Neden Önemli?

En sofistike teknolojiler bile, "üzerinde tıklamayın!" yazısına rağmen tıklayan çalışan karşısında yetersiz kalır. İnsan, hem güvenliğin en zayıf halkası hem de en güçlü savunma katmanı olabilir. Eğitimsiz bir güvenlik bütçesi, kapısı açık banka kasası gibidir.

Ne Yapmalı?

- **İşe Başlangıç Eğitimi:** Her yeni çalışan, ilk haftada güvenlik farkındalık eğitimi almalı.
- **Yıllık Tekrar:** Tüm çalışanlar yıllık zorunlu eğitim. Konular: phishing, parola, sosyal mühendislik, veri sınıflandırma, mobil cihaz, USB.
- **Phishing Simülasyonu:** Üç ayda bir gerçekçi phishing e-postaları ile çalışan duyarlılığı ölçümü. Açan kullanıcılara ek eğitim.

- **Yönetici Eğitimi:** CEO, CFO, yönetim kurulu için özel "C-level" güvenlik eğitimi. CEO fraud (BEC), yatırımcı dolandırıcılığı senaryoları.
- **Sektörel Senaryolar:** Eğitim içerikleri sektöre özelleştirilmeli. Üretim için OT tehditleri, sağlık için PHI ihlali, finans için işlem dolandırıcılığı.
- **Öneri Sistemi:** Çalışanların şüpheli olayları kolayca raporlayabileceği bir kanal (Phish Alert düğmesi, e-posta hattı).

%70

Düzenli farkındalık eğitimi alan kurumların phishing açma oranı düşüşü (Proofpoint State of the Phish 2025)

10 · Düzenli Denetim ve Sızma Testi

Neden Önemli?

Güvenlik bir noktadaki durum değildir; sürekli evrilen bir süreçtir. Bugün güvenli olan bir yapılandırma, yarın yeni bir CVE ile savunmasız hale gelebilir. Bağımsız üçüncü taraf denetim, kör noktalarınızı gösterir.

Ne Yapmalı?

- **Yıllık Penetrasyon Testi:** Black-box, gray-box, white-box kombinasyonu. Web uygulamaları, iç ağ, dış ağ, sosyal mühendislik.
- **Vulnerability Scan:** Aylık otomatik tarama. Nessus, OpenVAS, Qualys. CVSS 7.0+ açıklar 30 gün içinde kapatılmalı.
- **Web Application Pentest:** Müşteriye açık uygulamalar için OWASP Top 10 odaklı pentest.
- **Red Team / Purple Team:** Daha olgun kurumlar için saldırı simülasyonu. SOC ekibinin tespit/müdahale yeteneği ölçülür.
- **İç Denetim:** ISO 27001 kapsamında yıllık iç denetim. Bağımsız bir ekibin (BT dışı) tarafından yürütülmeli.
- **Tedarikçi Güvenlik Değerlendirmesi:** Sizin sisteminize erişen tüm üçüncü taraflar (bulut sağlayıcı, danışman, entegratör) için güvenlik anket / sertifika kontrolü.

11 · 50 Maddelik Hızlı Kontrol Listesi

Aşağıdaki listeyi BT ekibinizle birlikte gözden geçirin. Her satırın yanındaki kutucuğu işaretleyin. ✓ Hayır olanlar; aksiyon planınızın temelidir.

Yönetişim (5 madde)

- ☐ **1.** Yönetim onaylı, yazılı bir Bilgi Güvenliği Politikamız var.
- ☐ **2.** CISO veya Bilgi Güvenliği Sorumlusu atanmış.
- ☐ **3.** Yıllık risk değerlendirmesi yapıyoruz ve raporluyoruz.
- ☐ **4.** KVKK uyumluluğu için VERBİS kaydımız ve veri envanterimiz güncel.
- ☐ **5.** Üç ayda bir toplanan Bilgi Güvenliği Komitemiz var.

Kimlik ve Erişim (5 madde)

- ☐ **6.** Tüm yönetici hesapları için MFA zorunlu.
- ☐ **7.** Uzaktan erişim (VPN, kritik uygulamalar) için MFA aktif.
- ☐ **8.** Parola politikamız min. 12 karakter ve düzenli değişim gerektiriyor.
- ☐ **9.** İşten ayrılan çalışanların hesabı 24 saat içinde devre dışı bırakılır.
- ☐ **10.** Üç ayda bir kullanıcı erişim incelemesi yapıyoruz.

Ağ Güvenliği (5 madde)

- ☐ **11.** Next-gen firewall'umuz var ve lisansları güncel.
- ☐ **12.** Misafir Wi-Fi ana ağdan izole.
- ☐ **13.** VLAN segmentasyonu uygulanmış (üretim, ofis, IoT ayrı).
- ☐ **14.** IPS/IDS aktif ve imzaları güncel.
- ☐ **15.** DNS filtreleme çözümü kullanıyoruz.

Endpoint Güvenliği (5 madde)

- ☐ **16.** Tüm uç noktalarda EDR/XDR kurulu (sadece antivirüs değil).

- ☐ **17.** Otomatik yama yönetimi sistemi var.
- ☐ **18.** Tüm laptop'larda tam disk şifreleme (BitLocker/FileVault) aktif.
- ☐ **19.** USB depolama cihazları kısıtlanmış veya yönetilen.
- ☐ **20.** Mobil cihazlar MDM ile yönetiliyor.

Veri Güvenliği (5 madde)

- ☐ **21.** 3-2-1 yedekleme kuralı uygulanıyor.
- ☐ **22.** Immutable backup veya air-gapped kopya var.
- ☐ **23.** Ayda en az bir restore testi yapıyoruz.
- ☐ **24.** Hassas veriler durağan halde şifreli (AES-256).
- ☐ **25.** Veri sınıflandırma politikamız (açık/dahili/gizli) var.

Sürekli İzleme (5 madde)

- ☐ **26.** Merkezi log toplama (SIEM) sistemimiz var.
- ☐ **27.** Loglar en az 90 gün saklanıyor.
- ☐ **28.** Kritik olaylar için otomatik uyarı kuralları yazılmış.
- ☐ **29.** SOC veya yönetilen SOC hizmetimiz var.
- ☐ **30.** Threat intelligence feed'lerini kullanıyoruz.

Olay Müdahale (5 madde)

- ☐ **31.** Yazılı bir Olay Müdahale Planımız var.
- ☐ **32.** Olay sınıflandırma seviyeleri ve eskalasyon yolları belirlenmiş.
- ☐ **33.** İletişim listesi (yönetim, hukuk, BTK, KVKK) güncel ve erişilebilir.
- ☐ **34.** Yıllık IR tatbikatı yapıyoruz.
- ☐ **35.** Forensic destek sağlayan bir firmayla anlaşmamız var.

Farkındalık (5 madde)

- ☐ **36.** Yeni çalışanlar ilk hafta güvenlik eğitimi alıyor.

- ☐ **37.** Yıllık zorunlu farkındalık eğitimimiz var.
- ☐ **38.** Üç ayda bir phishing simülasyonu yapıyoruz.
- ☐ **39.** Yöneticiler için özel C-level eğitim verildi.
- ☐ **40.** Şüpheli e-postaları raporlama kanalı (Phish Alert) var.

Denetim ve Test (5 madde)

- ☐ **41.** Yıllık penetrasyon testi yaptırıyoruz.
- ☐ **42.** Aylık vulnerability scan'imiz var.
- ☐ **43.** CVSS 7.0+ açıkları 30 gün içinde kapatıyoruz.
- ☐ **44.** Tedarikçi güvenlik değerlendirme süreçimiz var.
- ☐ **45.** Yıllık iç denetim yapılıyor.

Genel Operasyonel (5 madde)

- ☐ **46.** Felaket Kurtarma (DR) planımız var ve test edildi.
- ☐ **47.** İş Sürekliliği Planı (BCP) güncel ve onaylı.
- ☐ **48.** Üretici garanti ve destek paketleri süresinde yenileniyor.
- ☐ **49.** Siber sigorta poliçemiz var ve kapsamı yıllık gözden geçiriliyor.
- ☐ **50.** Bu kontrol listesi en az yılda bir tekrarlanıyor.

> **Skorunuz**
>
> 40-50: Çok iyi durumdasınız. Sürekli iyileştirme. 30-39: İyi temel, eksik alanları önceliklendirin. 20-29: Acil önlem gerekli. 0-19: Acil aksiyon. Profesyonel destek alın.

12 · Sonraki Adımlar ve Durkon Hakkında

Bu kontrol listesini doldurdunuz. Şimdi ne yapmalısınız?

Sıradaki 3 Adım

1. Risk skoru ve uygulama maliyeti matrisinde değerlendirin. Quick win'leri (düşük maliyet, yüksek etki) önce yapın.
2. 90 gün, 6 ay, 12 aylık eylem planı. Bütçe ihtiyaçlarını CFO ile paylaşın.
3. Bağımsız bir gözle değerlendirme, kör noktaları görmenizi sağlar. Durkon olarak ücretsiz keşif görüşmesi sunuyoruz.

Durkon Hakkında

Durkon, 15+ yıldır kurumsal BT çözümleri ve siber güvenlik danışmanlığı veriyor. Sertifikalı uzman ekibimizle başta üretim, lojistik, sağlık ve finans sektörü olmak üzere çeşitli kurumlara hizmet veriyoruz. Kendi sistemlerimiz securityheaders.com'da ve SSL Labs'ta skoru ile sertifikalı.

ISO 27001 Danışmanlığı | KVKK Uyum | SIEM / SOC | Penetrasyon Testi | EDR / XDR | Yedekleme & DR

Ücretsiz Keşif Görüşmesi

Bu kontrol listesi üzerinden mevcut durumunuzu değerlendirelim, kurumunuza özel bir yol haritası önerelim. Görüşme 30-45 dakika sürer ve hiçbir taahhüt içermez.

Web: durkon.com
Telefon: +90 212 993 16 73
E-posta: info@durkon.com
Adres: Yakuplu Mh. Hürriyet Bulvarı No:1/62 Skyport Residence, Beylikdüzü/İstanbul