Şirketler İçin Siber Tehdit

Veri İhlali Rehberi

KVKK Uyumundan Fidye Yazılımına: Şirketler İçin Tam Kapsamlı Siber Risk Analizi

İÇİNDEKİLER

1. **Siber Tehdit Görünümü – Türkiye ve Dünya Trendleri**
2. **Şirketlerde En Kritik 6 Siber Risk Alanı**
3. **Operasyonel ve Finansal Etki Analizi**
4. **Dijitalleşme, Veri Güvenliği ve KVKK Yükümlülükleri**
5. **Siber Risk Olgunluk Testi**
6. **En Ağır 12 Siber Hasar Örneği**
7. **Siber Risk Sigortası Kapsamı**
8. **Siber Olay ve Müdahale Akış Şeması**
9. **Siber Dayanıklılık Stratejisi**
10. **Sonuç: Dijital Çağda Güvenlik Bir Seçenek Değil, Stratejidir**

1. Siber Tehdit Görünümü – Türkiye ve Dünya Trendleri

2026 yılı, şirketler için yalnızca teknolojik dönüşümün değil; aynı zamanda **siber tehditlerin hacim ve karmaşıklık açısından zirve yaptığı** bir dönem olacaktır.
Türk şirketlerinin %70'inden fazlasının bulut tabanlı sistemlere geçtiği, yapay zekâ altyapılarının yaygınlaştığı bu dönemde saldırganların yöntemleri de evrildi:

- **Fidye yazılımları %40 büyüdü**
- **E-posta üzerinden yapılan sosyal mühendislik saldırıları %300 arttı**
- **Türkiye'de KVKK kaynaklı idari yaptırımlar son 2 yılda 2 katına çıktı**
- KOBİ'ler artık **büyük şirketler kadar hedef**
- Saldırılar tamamen **otomasyon + AI** ile yapılıyor

2. Şirketlerde En Kritik 6 Siber Risk Alanı

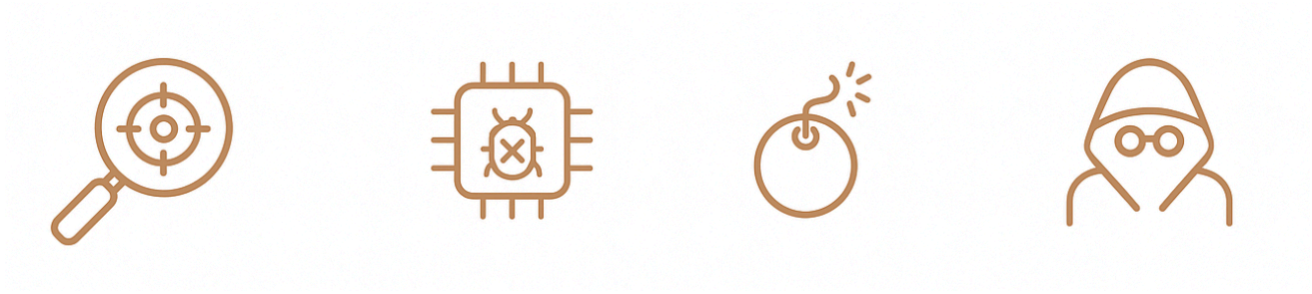
Aşağıdaki tablo, işletmelerinin önümüzdeki 12 ayda karşılaşması beklenen en kritik risk alanlarını özetler:

Siber Risk Alanı	Tehdit Seviyesi	Açıklama
Fidye Yazılımı	Çok Yüksek	Sistemleri kilitleyip veri sızdırma yöntemi çift yönlü hale geldi.
Kimlik Avı / Sosyal Mühendislik	Yüksek	Çalışan hataları en büyük risk.
Veri İhlali / KVKK	Çok Yüksek	Milyonlarca TL ceza + itibar kaybı.
İçeriden Gelen Tehdit	Orta-Yüksek	Hatalı yapılandırma ve ihmal kaynaklı.
Tedarik Zinciri Siber Riski	Orta	Tedarikçinin açıklarından sızma.
Bulut Sistem Açıkları	Yüksek	Yanlış erişim izinleri ciddi risk.

3. Operasyonel ve Finansal Etki Analizi

Bir siber olay sadece IT ekiplerini değil; **finans, üretim, lojistik, satış ve yönetim** dahil tüm departmanları aynı anda etkiler.

Aşağıdaki zincir etkisi ile karşılaşabilirsiniz.



1. Keşif (Reconnaissance)

Saldırgan, şirket hakkında bilgi toplar: çalışan e-postaları, açık portlar, zaafiyetler, sosyal medya verileri.

2. Silahlandırma (Weaponization)

Keşif verilerine göre zararlı yazılım hazırlanır, kötü amaçlı dosya/payload oluşturulur.

3. Teslimat (Delivery)

Zararlı içerik hedefe iletilir. En yaygın yöntemler: phishing, USB, kötü amaçlı link, tedarik zinciri eklentileri.

4. Sömürü (Exploitation)

Sistemdeki zafiyetten yararlanılır, kullanıcı kandırılır veya güvenlik açığı tetiklenir.

5. Kurulum (Installation)

Saldırgan kalıcı erişim için malware'i sisteme kurar, arka kapı oluşturur.

6. Komuta ve Kontrol – C2 (Command & Control)

Zararlı yazılım, saldırganın kontrol sunucusuna bağlanır. Artık saldırgan ağ içinde serbestçe hareket edebilir.

7. Hedefe Ulaşma (Actions on Objectives)

Amaç yerine getirilir: veri çalma, fidye yazılımı şifrelemesi, sistem durdurma, sabotaj, finansal zarar verme.

Örnek Etki Zinciri:

- Sunucu şifrelenir → ERP kapanır
- ERP kapanır → Sevkiyat planı durur
- Sevkiyat durur → Sözleşme cezaları oluşur
- Fatura kesilemez → Nakit akışı bozulur
- Nakit akışı bozulur → Finansal risk artar

Ortalama bir fidye yazılımı saldırısının **Türkiye'de şirket başına maliyeti 2,4 milyon TL**'dir.

4. Dijitalleşme, Veri Güvenliği ve KVKK Yükümlülükleri

Veri ihlali yalnızca teknik bir problem değildir; **hukuki bir sorumluluk** doğurur.

KVKK kapsamında şirketlerin yükümlülükleri:

- Kişisel verilerin güvenliğini sağlamak
- Sızma olması durumunda 72 saat içinde bildirim
- Veri işleyen tüm çalışan ve tedarikçilerin uyum süreçleri
- Aydınlatma metinleri ve açık rıza prosedürleri
- Siber risk değerlendirmesi

Veri ihlallerinin %60'ı yanlış yapılandırılmış sistemlerden kaynaklanıyor.

En Yüksek Ceza Miktarı ve Kapsamı

Bu en yüksek ceza miktarı, 6698 Sayılı Kanun'un 18. maddesinin (b), (c) ve (ç) bentlerinde belirtilen **üç farklı aykırılık** için belirlenen üst sınırdır:

1. **Veri güvenliğine ilişkin yükümlülüklerin yerine getirilmemesi** (Madde 18/b ve 12).
    - *Ceza Aralığı:* **204.285 TL**'den **13.620.402 TL**'ye kadar.
2. **Kurul tarafından verilen kararların yerine getirilmemesi** (Madde 18/c ve 15).
    - *Ceza Aralığı:* **340.476 TL**'den **13.620.402 TL**'ye kadar.
3. **Veri Sorumluları Sicili'ne (VERBİS) kayıt ve bildirim yükümlülüğüne aykırı hareket edilmesi** (Madde 18/ç ve 16).
    - *Ceza Aralığı:* **272.380 TL**'den **13.620.402 TL**'ye kadar.

5. Siber Risk Olgunluk Testi

Siber Risk Olgunluk Testi

Aşağıdaki sorulardan **4 veya daha fazlasına Hayır diyorsanız**, şirketiniz **kırmızı risk bölgesindedir.**

1) Kritik sistemleriniz için çok faktörlü doğrulama (MFA) zorunlu mu?
2) Yedekleriniz şifrelenmiş ve offline ortamda saklanıyor mu?
3) Çalışanlara yılda en az 1 kez siber farkındalık eğitimi veriliyor mu?
4) Tedarikçilerinizin siber güvenlik seviyesi ölçülüyor mu?
5) KVKK uyum süreciniz tam olarak belgelendirildi mi?
6) Siber olay müdahale planınız var mı?
7) Log kayıtlarınız merkezi ve düzenli olarak izleniyor mu?
8) Kritik verileriniz sınıflandırılmış mı?

6. En Ağır 12 Siber Hasar Örneği

1. **Fidye yazılımı ERP'yi kilitledi; 6 gün operasyon durdu.**
2. **E-posta sahteciliği ile yanlış IBAN'a 1,2 milyon TL ödeme yapıldı.**
3. **Tedarikçi üzerinden sisteme sızılıp tüm müşteri verileri çekildi.**
4. **Yanlış yapılandırılmış bulut erişimi nedeniyle sözleşmeler internete sızdı.**
5. **Çalışan hatasıyla KVKK ihlali; 800.000 TL idari ceza.**
6. **Lojistik firmasının sistemine sızılıp gönderiler manipüle edildi.**
7. **CFO'nun e-postası ele geçirilip, ödeme talimatları yönlendirildi.**
8. **Yedekleme bozuk olduğundan veri geri yüklenemedi.**
9. **Raporlama sistemine sızılarak yanlış stok kayıtları oluşturuldu.**
10. **VPN açığı üzerinden iç ağ tamamen ele geçirildi.**
11. **Bir çalışan USB ile zararlı yazılım bulaştırdı.**
12. **Bulut CRM veritabanı şifrelemesi devre dışı unutuldu.**

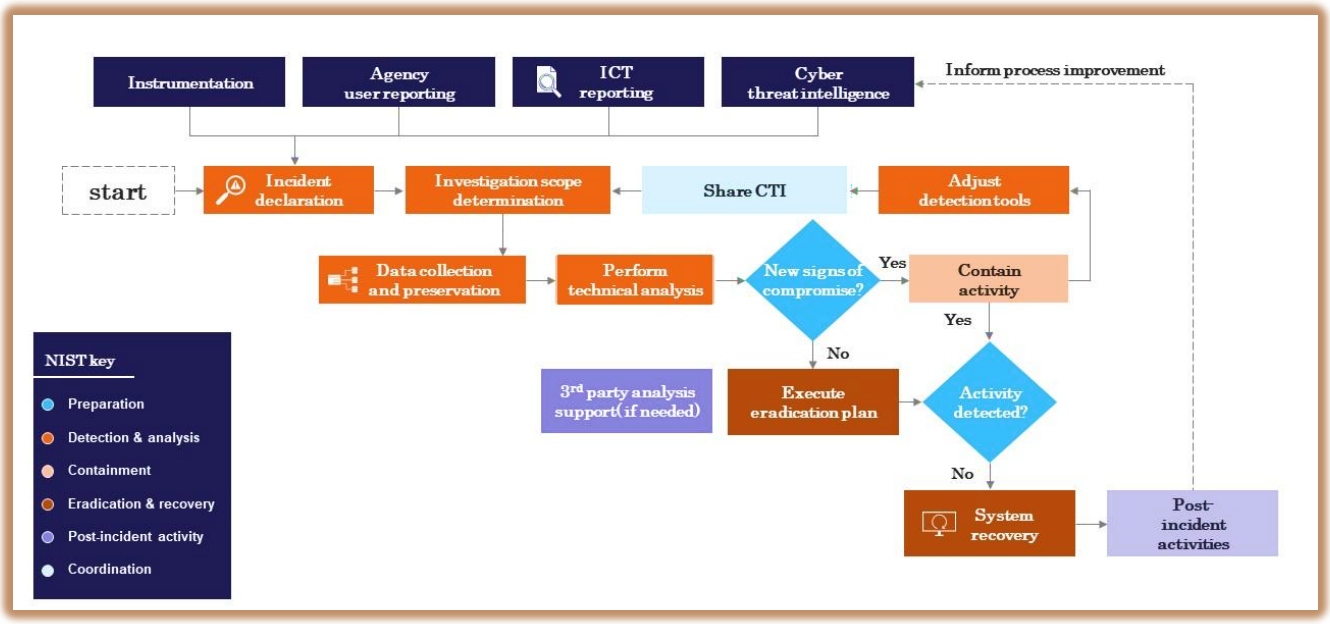
7. Siber Risk Sigortası Kapsamı

Doğru kurgulanmış bir poliçe, sadece saldırı anında değil; **öncesi ve sonrası için finansal koruma sağlar.**

Kapsamda yer alan başlıca teminatlar:

- **Fidye yazılımı saldırıları**
- **Veri ihlali ve KVKK sorumlulukları**
- **Acil müdahale & adli bilişim giderleri**
- **İş durması nedeniyle gelir kaybı**
- **Sözleşmesel yükümlülükler ve müşteri tazminatları**
- **IT sistem kurtarma maliyetleri**
- **Hukuk, danışmanlık ve kriz iletişimi giderleri**

8. Siber Olay ve Müdahale Akış Şeması



Aşamalar:

1. Olay Tespiti
2. İzolasyon
3. Adli Bilişim Analizi
4. Sistem Temizliği
5. Veri Kurtarma
6. İletişim & KVKK Bildirim
7. Operasyonun Yeniden Başlatılması

9. Siber Dayanıklılık Stratejisi

Bir şirketin dijital dayanıklılığı, yalnızca güçlü bir IT ekibine değil; **yönetimsel ve operasyonel disipline** bağlıdır.

2026 için önerilen 5 temel stratejik adım:

1) Sıfır Güven (Zero Trust) Mimarisi

Her erişim isteği doğrulanır.

2) Düzenli Siber Tatbikatlar

Yılda en az 2 kez zorunlu olmalıdır.

3) KVKK + Siber Güvenlik Entegrasyonu

Tek bir çerçevede yönetilmelidir.

4) Tedarikçi Güvenlik Denetimi

Zincirin en zayıf halkası tedarikçilerdir.

5) Siber Risk Sigortası

Finansal koruma ve profesyonel acil müdahale sağlar.

10. Sonuç: Dijital Çağda Güvenlik Bir Seçenek Değil, Stratejidir

Siber tehditler giderek hızlanıyor ve karmaşıklaşıyor.
Bu rehber, şirketinizin yalnızca bugünü değil; **geleceğini korumak için atması gereken adımları** sistematik şekilde ortaya koymaktadır.

Big Sigorta ve Reasürans Brokerliği A.Ş. olarak, işletmelerin siber risklerini analiz etmek, poliçe yapılarını optimize etmek ve doğru teminatlarla finansal dayanıklılık oluşturmak için yanınızdayız.

Bizimle iletişime geçin.

Adres : Maslak Mahallesi, Maslak Meydan Sokak, Beybi Giz Plaza A Blok No:1 Kat:21 İç Kapı No: 79 Sarıyer / İstanbul

Telefon : +90 212 227 07 13 Fax : +90 212 227 07 15

Web : www.bigsrb.com Mail : info@bigsrb.com