

Küçük ve orta ölçekli işletmeler için siber güvenlik

Büyüyen işletmenizi daha güçlü kılan nedir?

%43* KOBİ'leri hedefleyen saldırıların oranı*

≈ 70.000\$*

1 hafta ila 6 ay
Olası hizmet kesintisi



Bir olayın ortalama maliyeti
(veri kaybı, kimlik avı, fidye yazılımı, dolandırıcılık, itibar kaybı)

Neler oluyor ve bunlar işletmeniz için neden önemli?

Bulut platformları, uzaktan çalışma, mobil cihazlar, çevrimiçi araç ve hizmetler ile yapay zeka destekli otomasyon, günlük operasyonların birçok yönünü kolaylaştırırken sistemleri daha da karmaşık hâle getiriyor ve güvende tutmayı zorlaştırıyor.



Daha fazla araç, daha fazla giriş noktası

Her yeni hizmet, işletmenize açılan potansiyel bir kapı daha ekler



Sınırlı zaman ve personel

Küçük BT ekipleri her şeyi her zaman izleyemez



Şirketin kontrolü dışında yürütülen işler

İş için kişisel hesap ve cihazların kullanılması, verileri koruma mekanizmalarının dışında bırakır ve işletmeyi olası para cezalarıyla karşı karşıya bırakır



Yapay zeka destekli saldırıların sayısı artıyor

Yapay zekâ, düşük maliyetli ve otomatik kimlik avı ve parola saldırılarının geniş ölçekte gerçekleştirilmesini sağlıyor

Tüm bu faktörler iş sürekliliğini ve büyümeyi tehdit ederek şunlara yol açar:

- olası mali kayıplar
- veri ihalleri
- ve itibar kaybı.

İşletmenizi içeriden ve dışarıdan riske atan unsurlar

Siber olayların çoğu, başta büyük veya dikkat çekici bir durumla başlamaz. Genellikle günlük hayatta karşılaştığımız sıradan durumlarla ve güncel sorunlarla başlarlar.

Dış ve iç riskler



Fidye yazılımı



Operasyonlar tamamen durur



Kötü amaçlı yazılımlar ve dosyasız saldırılar



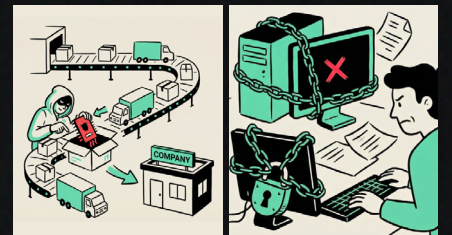
Veri hırsızlığı, kararsız sistemler



Sosyal mühendislik



Çalınan kimlik bilgileri, iş kesintisi



Tedarik zinciri saldırıları



Müşterilere sunulan hizmetlerde kesinti ve bunun sonucunda güven kaybı

Zorluklar



Hızlı BT gelişimi



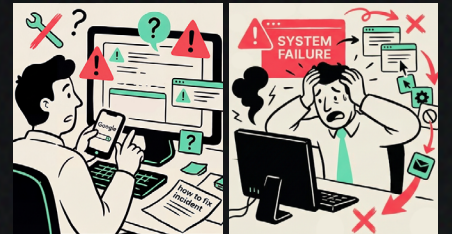
Güvenlik bu hızı ayak uyduramaz



Aşırı yoğun BT



Gözden kaçan tehditler ve geciken müdahale



Olay yönetimi beceri eksikliği



Yanlış kararlar durumu daha da kötüleştirir

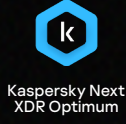


Kısıtlı bütçe



İleride daha yüksek kurtarma maliyetleri

Kaspersky tehditleri ve zorlukları nasıl ele alır?



	Kötü Amaçlı + Yazılım	<i>Yaygın tehditler</i>	•	•	•	•
	Fidye yazılımı		•	•	•	•
	Dosyasız saldırılar		•	•	•	•
	Kimlik avı		•	•	•	•
	Bilinmeyen kötü amaçlı yazılım	<i>Yeni ve hedefli</i>		•	•	•
	İnsan hatası			•	•	•
	Kontrolsüz üçüncü taraflar			•	•	•
	Sosyal mühendislik			•	•	•
	Yanal hareket			•	•	•
	Kaynak eksikliği				•	•
	İş sürekliliği				•	•

Kaspersky uzmanları tarafından sunulan yönetilen hizmet

Güvenilir güvenlik sizin için ne anlama gelir?

Otomatik tehdit koruması

Manuel müdahale ihtiyacını azaltan, kitlesel tehditlere karşı yerleşik koruma

BT departmanı için daha az iş yükü

Kolaylaştırılmış bulut tabanlı dağıtım sayesinde daha az manuel görev ve hata, önemli işlere ayırmak için daha fazla zaman

Erken tehdit tespiti

Atlatma teknikleri kullanan tehditleri olaya dönüşmeden durdurun

Bir sorun çıkması durumunda hızlı çözüm

Daha az hizmet kesintisi = daha fazla işletme istikrarı ve daha az gelir kaybı

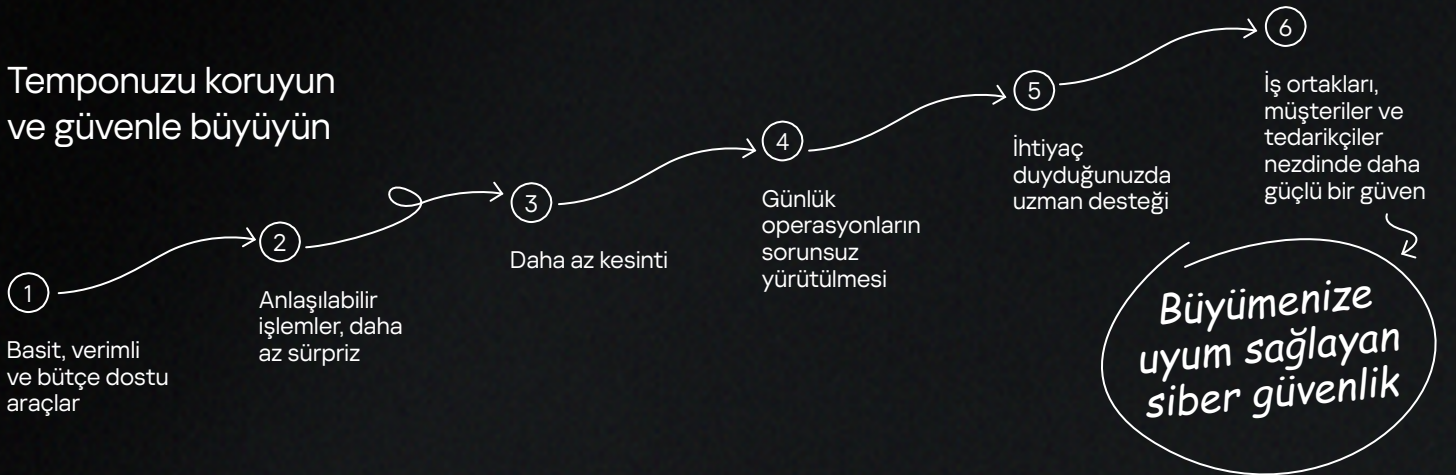
Sosyal mühendislik saldırılarına karşı koruma

Çalışanların; dolandırıcılıkları, kimlik avı ve manipülasyonları fark etmesine yardımcı olan siber güvenlik eğitimi

Ekip kurmanıza gerek kalmadan uzman güvenlik desteği

Uzman işe almanın maliyeti ve zahmeti olmadan güçlü koruma

Temponuzu koruyun ve güvenle büyüyün



Size özel, bulut altyapısına uygun güvenlik çözümüne hazır mısınız?

İlk günden etkili olan koruma edinin

Bize Ulaşın

www.kaspersky.com.tr

© 2026 AO Kaspersky Lab.
Tescilli ticari markalar ve hizmet markaları ilgili sahiplerinin mülkiyetindedir.