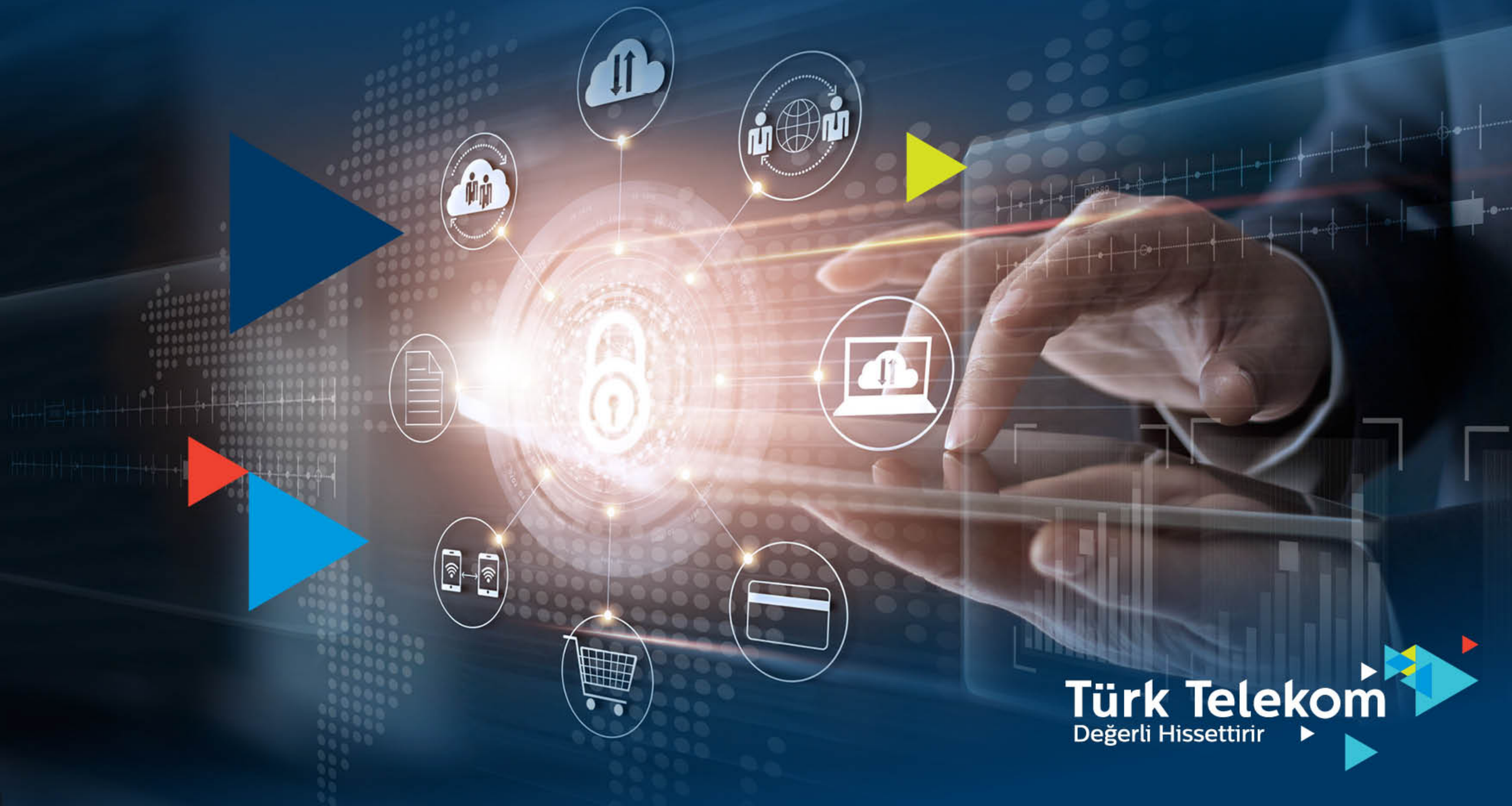
Kobiler İçin
Siber Güvenlik Rehberi



Türk Telekom
Değerli Hissettirir

Kobilere Yönelik Siber Ataklar

Günümüzün giderek dijitalleşen dünyasında, işletmenizin çevrimiçi ortamda karşılaşabileceği risklerin farkında olmanız her zamankinden daha önemlidir. Siber saldırılar sizi çeşitli şekillerde etkileyebilir, büyük finansal ve itibar kayıplara sebep olabilir.

Her işletmede olduğu gibi büyük bir itibar oluşturmak ve müşteri güvenini kazanmak yıllarca süren sıkı bir çalışma gerektirir. Uygun önlemler alınmadan, işletme bir siber saldırıya uğrarsa, yılların emeği dakikalar içinde yok edilebilir ve çok büyük kayıplar yaşanabilir.

KOBİ'lere yönelik siber saldırıların sonucu maliyetli olabilmektedir. Bu tür saldırılar tek bir bağlantının tıklanmasıyla saniyeler içinde gerçekleşir fakat etkileri çok geniş kapsamlıdır. Siber saldırıların ne olduğunu, nasıl önleyeceğinizi ve hangi stratejileri izlemeniz gerektiğini belirleyerek işletmenizi koruma altına alabilirsiniz.

COVID-19 ETKİSİ İLE SİBER ATAKLAR %238 ARTIŞ GÖSTERDİ

(Kaynak:Fintech)

Covid 19 salgınına karşın hükümetlerin yayınladığı tedbirlerle birlikte hem bireylerin hem de kurumların yeni modele uyum sağlamaları gerekti.

Saldırganlar belirsizlikten, benzeri görülmemiş durumlardan ve hızlı değişen BT-organizasyon yapılarından yararlandıkça atak trendleri yeniden şekillendi.

KOBi'lerin %50'si yılda en az 1 kez siber saldırıya uğradığını belirtiyor.

Siber saldırı kurbanı olan küçük işletmelerin %60'ı altı ay içinde iflas ediyor.

Veri sızıntısı için düzenlenen saldırılarda geçen yıla oranla %424 artış yaşanmıştır

KOBİ'lere gönderilen her 323 mailden 1'i zararlı yazılım içeriyor.

Kaynak: Fundera, 2020

Neden Yüksek Risk Altındasınız?

KOBİ'ler, siber saldırganlar için oldukça değerli varlıklar olan müşteri listeleri, müşteri veritabanları veya mali ayrıntılar gibi gizli bilgileri saklama eğilimindedir. Bu sebeple,

- Müşteri Listeleri
- Müşteri Kredi Kartı Bilgileri
- Şirket Banka Bilgileri
- Fiyat Politikaları
- Üretim Tasarımları & Süreçleri

yüksek risk altındadır.

Zararlı yazılımların %94'ü mail yolu ile iletiliyor.

(Kaynak:Verizon)

Her 39 saniyede bir siber saldırı gerçekleşiyor.

(Kaynak:Maryland University)

KOBİ'ler Neden Siber Saldırganların Hedefindedir?

- KOBİ'lerin bilgisayar ve ağ güvenliği genellikle ya yetersizdir ya da hiç yoktur.
- Yedekleme planı genellikle bulunmaz ve bulut hizmetlerinden yararlanılmaz.
- Çalışanlar çeşitli manipülasyonlar ve e-posta saldırıları karşısında yeterli bilgi sahibi değildir.
- Yeterli koruma bulunmadığından hacker'lar müşterilerin finansal verilerine daha kolay erişmek için giriş noktaları bulabilir.
- KOBİ'lerin büyük bir çoğunluğu bilişim teknolojileri personeli bulundurmaz.

KOBİ'ler için 2021 Siber Güvenlik Stratejileri

Gerçekleşen saldırıların **%43**'ü KOBİ'leri hedef alıyor.*

Bulut Güvenliği

Güvenlik açıklarına karşı koruma sağlamak için mevcut en yüksek güvenlik düzeyini sunan ve yerleşik güvenlik önlemlerine sahip bulut platformları ve uygulamaları tercih etmek

Ağ Güvenliği

Ağ yöneticisi tarafından kontrol edilen cihazları ve verileri korumaya yönelik en temel adımlardan biri olan Wi-Fi ağınız için güçlü bir parola kullanmak, güncel ve lisanslı uygulamalar kullanmak

Bilgi Güvenliği Farkındalık Eğitimleri

İstatistiklere göre siber saldırıların %60'ı kurum içi çalışanlar tarafından gerçekleştirilmektedir. Buradaki en iyi strateji olarak çalışanlarınızı eğitmek için daha fazla zaman ayırmak ve ISO uyumluluklarını yerine getirmektir

Firewall & SSL VPN

VPN ile bağlantınızı güvenli hale getirip, güvenlik duvarı sayesinde ağınıza doğru gelen trafiğin ağa giriş çıkışını yönetmek

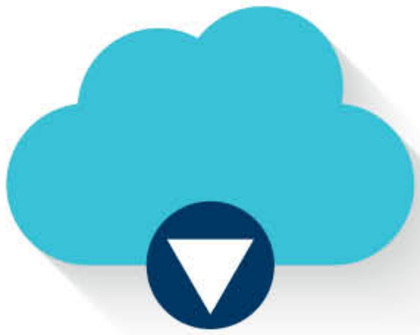
Uç Cihaz Güvenliği

Mobilitenin artması ile mobil cihazlar siber saldırıların merkezinde yer almaktadır. KOBİ'lerin, mobil cihazları kötü amaçlı yazılımlardan koruması, üzerlerindeki erişimleri güvenli bir şekilde takip etmesi ve yetkisiz erişimlere karşı koruması

Oltalama Atakları E-posta Yoluyla Nasıl Gerçekleşiyor?

Sosyal mühendislik yöntemleriyle hazırlanmış e-postalar siber saldırganlar tarafından oltalama amaçlı gönderilir

Hassas verilerin çalınması amacıyla gönderilen, malware yazılım içeren ve gerçek gibi görünen e-postaların konu satırlarında genellikle 'fatura', 'belge' veya 'sipariş' gibi keyword'ler bulunur.



Kullanıcı bağlantıya tıklar / ekteki dosyayı çalıştırır

Kullanıcı, gerçek bir kaynaktan gelmiş olduğunu düşünerek, iletilen e-postadaki zararlı bağlantıya tıkladığı zaman veya ek olarak gönderilen virüslü dosyaların çalıştırılması ile oltalama saldırısının kurbanı olmuş olur.

Kötü Amaçlı Yazılım Cihazı Ele Geçirir

E-postadaki eki indirdikten sonra yerleşen malware sayesinde cihazınız ve cihazınızın bağlı olduğu ağ siber saldırgan tarafından ele geçirilebilir. Maddi olarak zarara ve itibar kaybına uğrayabilirsiniz.

Siber Saldırılardan Korunmak İçin Neler Yapabilirsiniz?

Çalışanlarınıza siber güvenlik eğitimi verin.

KOBİ'lerin gerekli teknik altyapıyı edinmesinin yanı sıra çalışanlarını sosyal mühendislik ve ağ güvenlik protokolleri konusunda eğitmesi gerekiyor.

Güvenli şifreler ve çok faktörlü kimlik doğrulama kullanın.

Yaşanan veri ihlallerinde zayıf şifrelemenin etkileri düşünüldüğünde, KOBİ'lerin bu konuda daha dikkatli olmaları ve çift faktörlü kimlik doğrulaması kullanmaları gerekmektedir.

Tüm verileri düzenli olarak yedekleyin.

Düzenli olarak yedeklemelerinizin durumunu kontrol etmeniz işletmenizde yaşanabilecek aksaklıklara karşı verilerinizin güvende olmasını sağlar.

Siber Saldırılardan Korunmak İçin Neler Yapabilirsiniz?

Güvenlik duvarı kullanın.

Siber saldırılardaki ilk savunma hatlarından biri güvenlik duvarıdır. KOBİ'lerin evden çalışan çalışanları ve siber saldırganlar arasına güvenlik duvarı örmesi ciddi önem taşıyor.

Siber güvenlik politikalarınızı gözden geçirin.

Çalışanların yetkilerinden şirketin siber saldırı esnasında izleyeceği kriz planına kadar belirli bir siber güvenlik politikasının bulunması size önemli fayda sağlar.

Mobil cihazlara dikkat edin.

KOBİ'ler güvenlik açığı yaratabilme ihtimaline karşı şirketin şifre politikasının ağa erişen tüm mobil cihazlar için geçerli olmasını ve düzenli güncellemeler yapılmasını sağlamalı.

Türk Telekom Teknoloji Danışmanları Öneriyor

Penetrasyon testi yaptırın

Zafiyetleri, güvenlik açıklıklarını tespit edin ve sistemleri daha güvenli hale getirin. Konusunda uzman test danışmanlık ekiplerimizle Sızma Testi ve DDOS Atak Simülasyonu hizmetimiz yanınızda.

Güncel bir antivirüs kullanın

Zararlı yazılımlardan korunmak için antivirüs programınızın son sürümünü kullanın. Omurga seviyesinden temel siber güvenlik hizmeti ve uç cihaz güvenliği çözümlerimizi inceleyin.

Verilerinizi yedekleyin

Fidye yazılımlarına karşı önemli dosyalarınızı yedekleyin.
Lokal yedekleme çözümlerinden yararlanın.

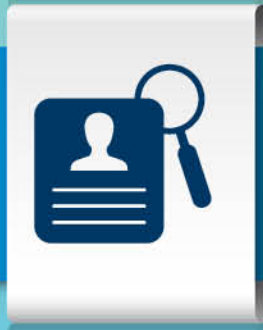
Bağlantınızı güvenli hale getirin

Bilgisayar ve cep telefonlarınızdan ofis ağına ulaşın.
Türk Telekom Paylaşımlı SSL VPN ürününü deneyimleyin.

Türk Telekom Teknoloji Danışmanları Öneriyor

Sınır güvenliğini DDOS saldırılarına karşı güçlendirin

Sahte yoğunluk yaratılması sonucu oluşan veri trafiğinden ötürü hizmet verememesi gibi durumlara karşı önlem alın.
Türkiye'nin en büyük DDOS kapasitesine sahip Türk Telekom ile network katmanından uygulama katmanı DDOS ataklarına karşı katmanlı koruma sağlayın.

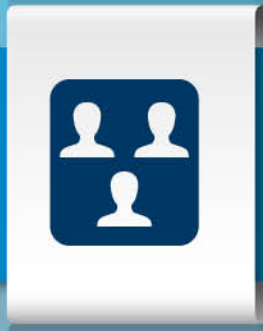


Son kullanıcı hareketlerini kayıt altına alın

Gerçekleştirilen tüm aktiviteleri görsel ve/veya log olarak kayıt altına alın.
Türk Telekom Paylaşımlı 5651 loglama ürünü ile güvenli bir başlangıç yapın.

Oltalama saldırılarına karşı hazırlıklı olun

Kişisel veri sızıntılarına karşı gerekli önlemleri belirleyin ve engelleyin.
Türk Telekom tarafından geliştirilen Phishing simülasyonu ile siber tehditlere karşı olgunluk seviyenizi arttırın.



Regülasyona tam uyumluluk için çalışmaları hızlandırın.

KVK kanunu uyum süreçlerinin tamamlanması için danışmanlık desteği alın.
Türk Telekom KVKK Danışmanlığı hizmeti, güvenlik regülasyon uyumluluğu için yanınızda.

Türk Telekom Siber Güvenlik Çözümleri

Paylaşımlı Güvenlik Hizmetleri

- DDOS Atak Önleme
- Güvenlik Duvarı (Firewall)
- Aktif Savunma Sistemi (IPS)
- İçerik Filtreleme
- Antivirus
- Gelişmiş Tehdit Önleme (APT)
- WAF
- DDOS+7

Dedike Güvenlik Hizmetleri

- Atanmış Siber Güvenlik Servisleri
- SiberLOG
- SiberKALE
- SiberTEST
- Danışmanlık Hizmetleri
- KVKK

Siber Güvenlik Merkezi Yönetim Hizmeti

- 7/24 Güvenlik Olay İzleme
- SIEM Danışmanlık
- Güvenlik Test
- Risk&Uyumluluk
- Güvenlik Cihaz Yönetimi
- SOAR ile Otomatik Müdahale
- Siber İstihbarat
- Paylaşımlı SIEM

Detaylı bilgi için bayiniz ya da satış yöneticiniz ile iletişime geçebilirsiniz.

İşyerim
Çağrı Merkezi
444 5 444

Türk Telekom
Değerli Hissettirir