vodafone business

Yükselen Tehdit Dalgası: Yapay Zeka Çağında İşletmeler için Siber Güvenlik Rehberi

Siber Güvenlik Tehdit Raporu

Nisan 2026

İçindekiler

Önsöz

Vodafone Business olarak, siber güvenliğin işletmeler için karmaşık bir alan olduğunun farkındayız. Bu nedenle, küresel ağımızdan elde edilen en güncel tehdit verilerini içeren **Siber Güvenlik Tehdit Raporu**nu hazırladık. **1,5 milyon kullanıcıdan ve uzman iş ortaklarımızdan** gelen bilgilerle oluşturulan bu rapor, işletmenizin riskleri hızla görmesini ve etkili önlemleri zamanında almasını sağlar.

Araştırmalar, **KOBİ'lerin %49'unun siber güvenliği ilk beş öncelikleri arasına aldığını gösteriyor; ancak birçok işletme nereden başlayacağını bilmiyor**.

Siber güvenlik de tıpkı sağlık gibi, **sorun ortaya çıkmadan önce düzenli bakım** gerektirir. Uzman desteği ve doğru araçlarla güçlü bir koruma sağlamak mümkündür.

Bu raporda odaklandığımız konu **Yapay Zeka**. Yapay zeka, işletmelere verimlilik sunarken aynı zamanda siber suçlulara daha hızlı ve akıllı saldırılar gerçekleştirme imkânı tanıyor. Bu nedenle **siber suçların finansal etkisinin önümüzdeki üç yılda %50 oranında artması** öngörülüyor.

Saldırganların başarıya ulaşması için tek bir açık yeterliyken, sizin savunma sistemlerinizin her zaman tam kapasiteyle çalışması gerekir. Hızla değişen tehdit ortamını anlamak ise güçlü bir güvenlik için ilk adımdır.

Bunun işletmeniz için ne anlama geldiğine bir bakalım.

Andrzej Kawalec
Siber Güvenlik Portföy Direktörü,
Vodafone Business

1. Stylus Media

Yapay zeka ikilemi

Yapay zeka, çalışma şeklimizi kökten değiştirerek işletmelerin zamandan tasarruf etmesine, maliyetleri azaltmasına ve daha iyi müşteri deneyimleri sunmasına yardımcı oluyor. Ancak bu dönüşüm, siber suçu da daha ileri bir seviyeye taşıyor. **Siber suçlular artık yapay zekayı kullanarak çok daha hızlı, daha akıllı ve daha ikna edici saldırılar gerçekleştirebiliyor.**

Birleşik Krallık Ulusal Siber Güvenlik Merkezi'ne göre yapay zeka, siber saldırı operasyonlarının bazı unsurlarını neredeyse kesin olarak daha etkili ve verimli hale getirecek; bu da siber tehditlerin hem sıklığını hem de yoğunluğunu artıracaktır.[2] Sadece hacim değil, hız da artıyor: siber saldırganlar artık beş dakikadan daha kısa sürede birden fazla cihazı şifreleyebiliyor.[3] **Bu durum, sadece BT ekiplerinin bir endişesi değil; çalışanların yarısından fazlası, yapay zekânın dolandırıcılıkları tespit etmeyi zorlaştırdığını belirtiyor.**[4]

Türkiye'de de konu ulusal güvenlik perspektifiyle ele alınıyor. **Milli Güvenlik Kurulu,** yapay zekâdaki ilerlemenin önemli fırsatlar sunmakla birlikte "**siber alanda oluşan yeni tehditleri"** de beraberinde getireceğine dikkat çekiyor.[5]

Artık birçok işletme, müşteri hizmetlerini otomatikleştirmek veya verileri analiz etmek gibi operasyonlarında yapay zekayı kullanmaya başlıyor.

Yapay zeka kullanımı, önlem alma gerekliliğini de beraberinde getiriyor. Ancak **Küçük ve orta ölçekli kuruluşların %69'u**, bu teknolojileri güvenli biçimde kullanıma sunmak için **gerekli güvenlik önlemlerine sahip değil.**[6]

Bu durum, hassas verilerin yanlışlıkla ifşa edilebileceği veya saldırganlar için yeni giriş noktalarının oluşabileceği anlamına geliyor. Yapay zeka destekli saldırıların ölçeği ise, artık hiçbir işletmenin göz ardı edilemeyecek kadar küçük ya da uzak olmadığını gösteriyor. **Çevrimiçiyseniz, hedefte olma ihtimaliniz yüksek.** Özellikle küçük ve orta ölçekli işletmeler için risk son derece gerçek: Hedef alınacak kadar büyüksünüz, fakat genellikle büyük şirketlerle aynı güvenlik kaynaklarına sahip değilsiniz.

Dolayısıyla **işletmeler iki temel zorlukla karşı karşıya:** yapay zeka destekli siber saldırılara karşı kendilerini korumak ve kendi yapay zeka kullanımlarını güvenli hale getirmek.

İyi haber şu: karmaşık çözümlere ihtiyacınız yok. Asıl **ihtiyacınız olan,** riskleri anlamanıza ve hızlıca harekete geçmenize yardımcı olan, **daha basit ve daha akıllı bir siber güvenlik yaklaşımı.** Şimdi, başlıca tehditleri ve işletmenizi nasıl koruyabileceğinizi inceleyelim.

> "Saldırganların küçük işletmeleri hedef alması eskiden pek mantıklı değildi; çünkü çalınacak daha az değerli veri, erişilecek daha az dijital sistem vardı ve saldırı maliyetleri yüksekti. Bugün ise ortalama bir KOBİ, her zamankinden daha fazla veriye ve büyük işletmelerle yarışabilecek bir dijital altyapıya sahip. Özellikle yapay zekânın etkisiyle bu işletmelere yönelik saldırılar artık çok daha ucuz ve kolay. Ekonomik dengeler değişti ve küçük ile orta ölçekli işletmelerin bu yeni duruma hızla uyum sağlaması gerekiyor

Andrzej Kawalec

Siber Güvenlik Portföy Direktörü, Vodafone Business

2. NCSC: Yapay zekanın siber tehdit üzerindeki etkisi hakkında detaylı bilgi için, Open Government Licence (nationalarchives.gov.uk) kapsamında sunulan National Cyber Security Centre (NCSC) kaynağına bakınız.
3. Microsoft
4. CybSafe
5. MGK Genel Sekreterliği
6. WEF

3

Bilmeniz gereken güvenlik tehditleri

1. Kimlik hırsızlığı

Nedir?

Kimlik avı saldırıları, çoğunlukla **oltalama (phishing)** veya **sosyal mühendislik** yöntemleriyle gerçekleştirilen ve saldırganların güvenilir bir kişiyi — örneğin bir iş arkadaşı, tedarikçi ya da yönetici — taklit ederek çalışanları **hassas bilgileri paylaşmaya** veya **para transferi yapmaya** yönlendirdiği bir saldırı türüdür. Örneğin bir dolandırıcı, şirketin finans direktöründen geliyormuş gibi görünen ve acil bir ödemeyi yeni bir banka hesabına yapmanızı isteyen son derece ikna edici bir e-posta gönderebilir. Bu talebe inanılması hâlinde, işletme yalnızca birkaç dakika içinde ciddi bir mali kayba uğrayabilir. Saldırının araştırılması sırasında operasyonlar durabilir, hassas müşteri ya da iş verileri ortaya saçılabilir ve oluşan güven kaybı hem müşteri kayıplarına hem de uzun vadeli itibar zedelenmesine yol açabilir. Bu nedenle kimlik avı, **yalnızca bir siber güvenlik tehdidi değil, aynı zamanda ciddi bir iş riski** olarak değerlendirilmelidir.

Saldırganlar, aramaları otomatikleştirerek, kişisel verileri toplayarak ve ses tonunu neredeyse kusursuz şekilde taklit ederek işletmeleri geniş ölçekte hedef alabiliyor.

> “Konuşma yeteneğine sahip büyük dil modelleri uzun süredir hayatımızda olsa da, bugüne kadar “insan” gibi duyulmaları zordu. Artık bir çalışanın telefonun ucunda duyduğu ses, bir iş arkadaşının, yöneticisinin veya bir aile üyesinin sesinden ayırt edilemeyecek kadar gerçekçi hâle gelebiliyor. Bu da, tamamen doğal bir konuşma izlenimi veren gerçek zamanlı dolandırıcılık aramalarını mümkün kılıyor.

- Andy Linham,
Strateji Direktörü, Vodafone Business

Yapay zeka ile nasıl gelişiyor?

Bazı siber saldırılarda, suçlular artık yapay zeka kullanarak sesleri klonluyor ve BT ekibiniz gibi güvenilir kişilerin kimliğine bürünebiliyor. Bu sahte aramalar son derece gerçekçi geliyor ve genellikle oturum açma bilgileri gibi kritik verileri talep ediyor. 2025’in başında **vishing (voice phishing)** olarak bilinen **sesli kimlik avı**, Cisco Talos’un tespit ettiği **kimlik avı saldırılarının %60’ından fazlasını oluşturdu**.[6] Yapay zekâ destekli araçlar sayesinde dolandırıcılar artık hedeflerini çok daha hızlı, kişiselleştirilmiş ve ikna edici bir şekilde aldatabiliyor.

Yoğun iş temposu sebebiyle çalışanlar, her e-posta veya çağrıyı detaylı inceleyemediğinden, yapay zekâ destekli sosyal mühendislik saldırıları kolayca fark edilemeyebiliyor.

İşletmelerin **94%**’ü gelişmiş tehditlere karşı kendisini hazırlıksız hissederken, harekete geçme ihtiyacı hiç olmadığı kadar artmış durumda.[7]

6. Cisco Talos
7. Vodafone

Dikkat: Phishing artık yalnızca e-postalarla sınırlı değil.

Siber suçlular çalışanlara ulaşmak için çok daha yaratıcı ve ikna edici teknikler kullanıyor. **Lookout**'un verilerine göre oltalama saldırıları, gelen kutusunun çok ötesine taşınarak **sesli oltalama (vishing), SMS oltalama (smishing) ve QR kod oltalama** gibi farklı kanallara yayılıyor.[8.]

Örneğin QR kod oltalamada, saldırganlar tren istasyonları, otopark ödeme noktaları gibi günlük yaşamda karşılaşılan yerlere sahte QR kodlar yerleştiriyor. Kullanıcılar bu kodları taradığında kötü amaçlı sitelere yönlendirilerek hassas bilgilerini paylaşmaya ikna ediliyor.

Daha da tehlikeli olan ise bu yöntemlerin bir araya getirilerek **hibrit oltalama** saldırılarına dönüştürülmesi. Birden fazla iletişim kanalını aynı anda kullanan bu taktikler, **güvenlik kontrollerini aşmakta çok daha etkili** oluyor ve çalışanların dikkatini dağıtarak başarılı olma ihtimalini artırıyor.

Kimlik hırsızlığına karşı nasıl korunulur?

Ekibinizi eğitin.
Çalışanların şüpheli mesajları ve kimlik avı girişimlerini fark edebilmesi için düzenli farkındalık eğitimleri şarttır. Bu eğitimler, tıklamadan önce risk işaretlerini hızlı ve güvenle tanımalarını sağlar.

Doğrulama süreçleri oluşturun.
Hassas talepler için kod kelime kullanımı, ikinci bir onay mekanizması ve çok faktörlü kimlik doğrulama (MFA) gibi güvenlik adımları, saldırı riskini önemli ölçüde azaltır.

Yeni taktiklere karşı tetikte kalın.
Ekiplerinizi deepfake'ler, ses klonlama girişimleri ve çok kanallı dolandırıcılık yöntemleri gibi gelişen tehditler konusunda bilgilendirerek savunmayı güçlendirin.

8. Lookout

2. Kötü Amaçlı Yazılım

Nedir?

Kötü amaçlı yazılımlar, veri çalmak veya sistemlerinizi aksatmak için tasarlanır. Operasyonları durma noktasına getirebilir, müşteri ve iş ortağı ilişkilerine zarar verebilir. Genellikle oltalama e-postaları, zararlı uygulamalar, indirmeler veya güvenliği ihlal edilmiş tedarikçiler üzerinden sızar ve ağa girdikten sonra hızla yayılarak diğer sistemleri de etkiler.

Bir saldırı gerçekleştiğinde, saldırganlar sizin sistemlerinizi kullanarak müşterilerinizi veya iş ortaklarınızı hedef alabilir; bu da işletmenizi tedarik zincirinin zayıf halkası haline getirir. Bu durum **sözleşme kayıplarına, itibar zedelenmesine** ve hassas veri açığa çıkarsa ciddi **hukuki risklere yol açabilir**. Bağlantılı iş ortamında kötü amaçlı yazılımlara karşı korunmak, sadece şirketinizi değil tüm tedarik zincirindeki güveni korumak anlamına gelir.

Yapay zeka ile nasıl gelişiyor?

Saldırganlar yapay zekayı kullanarak kötü amaçlı yazılımları daha "akıllı" hale getiriyor. Bu yeni nesil yazılımlar, **tespit edilmemek için öğreniyor**, uyum sağlıyor ve taktik değiştiriyor. **Geleneksel antivirüs çözümlerinin etkinliğini azaltan** bu trendin hızla büyümesi bekleniyor.[9]

Minimum güvenlik araçlarına sahip işletmeler ve tedarik zincirinde düşük görünürlüğe sahip olanlar, bu tür saldırılara daha açık hale geliyor.

"Günümüzde kötü amaçlı yazılımlar çalışanlara ulaşmak için çok daha fazla cihazı hedef alıyor. İnsanlar iş ve özel yaşamlarında çok sayıda uygulama ve bulut hizmeti kullanırken, saldırganlar tüm bu ortamlardaki açıkları değerlendirmeye çalışıyor.

- **Pedro Peixe Riberio,**
  Vodafone Kurumsal Siber Güvenlik Direktörü

9. Siber Evren

Hackerlar yapay zekayı daha gelişmiş saldırılar için kullanıyor.

Siber suçlular, saldırılarını hızlandırmak ve ölçeklendirmek için yapay zeka araçlarından yararlanıyor. Bu araçlara, kötü amaçlı yazılımların nasıl çalıştığını açıklatıyor, zararlı kodları farklı dillere çevirmesini istiyor ve hatta potansiyel kurbanların profilini çıkarmada kullanıyorlar.[10]

Yerleşik güvenlik önlemlerine rağmen, bazı bilgisayar korsanları bu korumaları kaldıran **"jailbreakli" sürümler** satıyor. Böylece kötü amaçlı yazılım üretmek ve yaymak çok daha kolay hale geliyor.

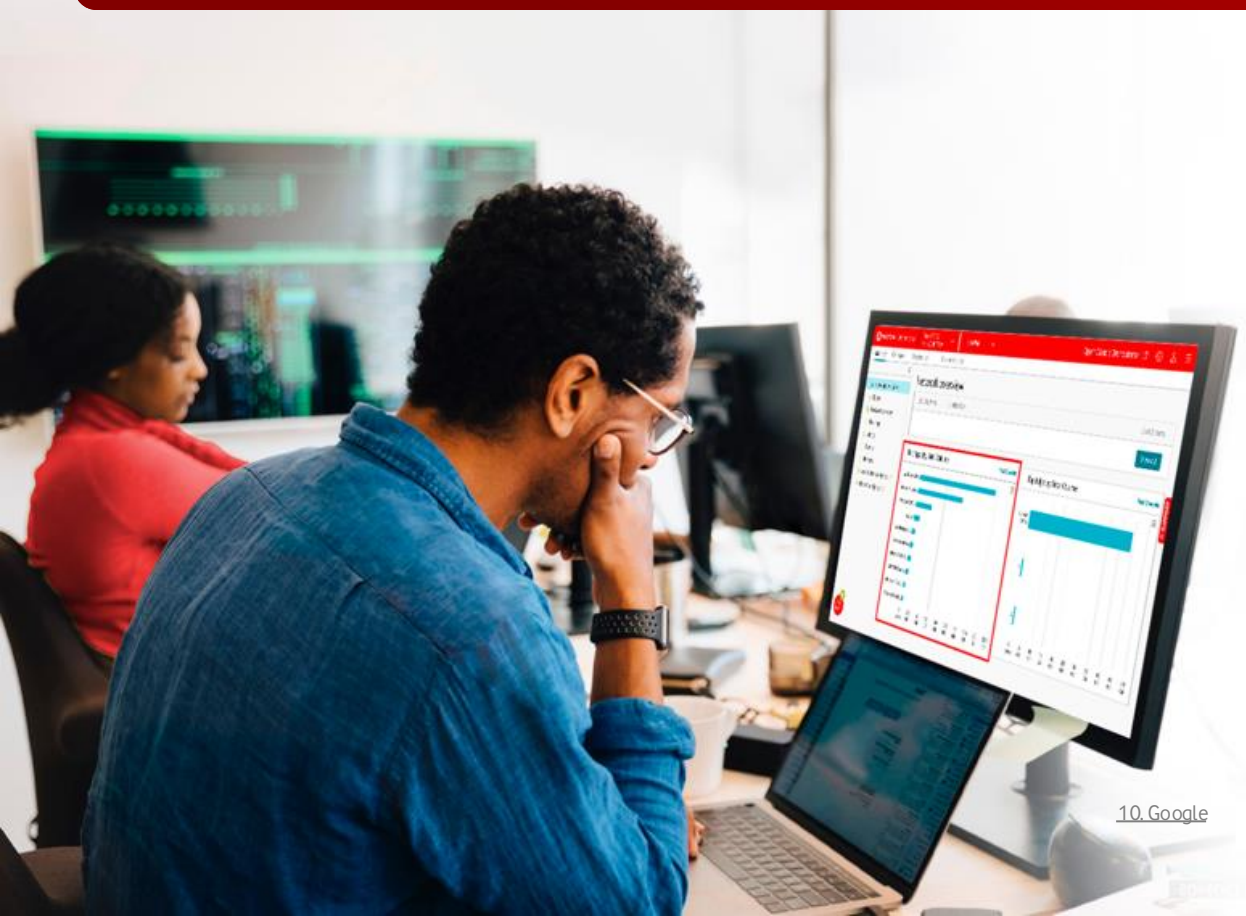
Kötü amaçlı yazılımlar, fatura veya toplantı daveti gibi görünen **eklere gizlenebilir** ve **yapay zeka sayesinde** hedef kitleye uygun şekilde hızlıca **birden fazla dile çevrilebilir**.

Adaptif kötü amaçlı yazılımlara karşı nasıl korunulur?

Modern antivirüs çözümleri kullanın:
Sadece bilinen tehditleri değil, olağan dışı davranışları da tespit edebilen güvenlik araçlarına yönelin. **Vodafone Business** olarak sunduğumuz **Antivirüs ve XDR** çözümlerini incelemek için **tıklayın**.

Temel güvenlik politikaları uygulayın:
Doğrulanmamış sitelerden indirmeleri engelleyin ve yazılım güncellemelerini zorunlu hale getirin. Bu basit adımlar, saldırganların kolay giriş noktalarını kapatır.

İş ortaklarınızı değerlendirin
Siber risk puanlama araçlarıyla tedarik zincirinizdeki güvenlik açıklarını tespit ederek uyarlanabilir kötü amaçlı yazılımların istismar edebileceği noktaları belirleyin.



10. Google

3. Fidye Yazılımı

Nedir?

Fiye yazılımı (ransomware), **ödeme yapılana kadar veri ve sistem erişimini kilitleyen** bir kötü amaçlı yazılım türüdür. Üstelik hedef sadece büyük şirketler değildir. Yakın tarihli bir rapora göre saldırıların yalnızca %2,6'sı çok büyük şirketleri hedef alırken, **en çok etkilenenler 11–1000 çalışanı olan işletmelerdir**; bu segment tek başına **tüm vakaların %65'ini** oluşturuyor.[11] Bir saldırının gerçek maliyeti ise sadece fidye değildir; **iş duruşu, verimlilik kayıpları, veri kurtarma maliyetleri, yasal gereklilikler** ve **itibar kaybı** çok daha yıpratıcı sonuçlar doğurur.

Yapay zeka ile nasıl gelişiyor?

Son araştırmalar, yapay zekanın fidye yazılımlarının oluşturulma, dağıtılma ve ölçeklendirilme şeklini kökten değiştirdiğini gösteriyor. RaaS (Hizmet Olarak Fidye Yazılımı) grupları artık üretken yapay zekadan yararlanarak son derece ikna edici kimlik avı mesajları üretebiliyor, deepfake ses dolandırıcılıklarını otomatikleştirebiliyor ve çok faktörlü kimlik doğrulama gibi güvenlik önlemlerini aşabiliyor.[12]

Bu durum, **teknik bilgisi sınırlı saldırganların bile sosyal medyadan topladıkları kişisel bilgileri kullanarak** karmaşık saldırılar düzenleyebilmesini sağlıyor.

> RaaS modeli ayrıca saldırganların **hedef ağlara erişmek için birden fazla yöntemi aynı anda koordineli biçimde kullanmasını** kolaylaştırıyor. Kişiselleştirilmiş sahte içerikleri telefon, SMS ve e-posta gibi kanallardan gönderebiliyorlar. Bu da iletişimlerin, tehdit farkındalığı yüksek kişiler için bile son derece gerçekçi görünmesine ve duyulmasına yol açıyor.
>
> - **Andy Linham,**
> Strateji Direktörü,
> Vodafone Business

KOBİ'lerin **%28'i** yalnızca tek bir fidye yazılımı saldırısının ardından gelir akışını ve kritik operasyonlarını kaybetme riskiyle karşı karşıya. Dijital güvenliğinizi hemen güçlendirin.

11. Coveware
12. Zscaler
13. Vodafone

Gezinmeden ihlale

Microsoft, Haziran 2025 tarihli bir araştırmasında, son 18 aylık dönemde fidye yazılımı saldırılarında keskin bir artış olduğunu bildiriyor ve saldırganlar sistemlere sızdıklarında dakikalar içinde hasar vermeye başlayabiliyor.[14] Siber suçlular artık yapay zekayı kullanarak detaylı çalışan profilleri oluşturuyor ve son derece hedefli dolandırıcılıklar başlatıyor.[15] Yapay zeka, yazım stilinizi taklit edebiliyor, şirketinizin marka kimliğine benzer içerikler üretebiliyor ve hatta gerçekçi görünen referanslarla sahte web siteleri oluşturabiliyor—tüm bunlar çalışanları tıklamaya, paylaşmaya veya ödeme yapmaya yönlendirmek için tasarlanıyor.

Risk, iş cihazlarının alışveriş yapmak veya internette gezinmek gibi kişisel amaçlarla kullanılmasında daha da artıyor. Bu alışkanlıklar çalışanları kötü amaçlı bağlantılara ve sahte sitelere maruz bırakarak saldırganlara yeni fırsatlar sunuyor.

Ransomware'den nasıl korunulur?

Çok Faktörlü Kimlik Doğrulama (MFA) Kullanın. MFA ön kapınıza ikinci bir kilit eklemek gibidir. Birisi şifrenizi ele geçirse bile ikinci doğrulama olmadan erişim sağlayamaz.

Tüm yazılım ve sistemlerinizin güncel olduğundan emin olun. Güncellemeler, saldırganların sıklıkla istismar ettiği güvenlik açıklarını kapatarak riskleri önemli ölçüde azaltır.

Yedek bir planınız olsun. Kritik sistemlere erişimi kaybettiğinizde hızlıca nasıl toparlanacağınızı bilmeniz iş sürekliliği için önemlidir.

Çalışanları olası bir olay durumunda ne yapmaları gerektiği konusunda eğitin. Bir kesinti ya da fidye mesajı ortaya çıktığında kiminle iletişime geçeceklerini ve hangi adımları izleyeceklerini açıkça bilmeleri gerekir.

14. Microsoft
15. Microsoft

Özet

Siber tehditler gerçek; ancak işletmenizi korumaya başlamak için kapsamlı bir güvenlik dönüşümüne gitmenize gerek yok. Minimum kesintiyle savunmanızı güçlendirmenin yolları:

1 Ekibinizi eğitin

Düzenli güvenlik farkındalığı eğitimleri ve kimlik avı simülasyonları uygulayın. Bu sayede çalışanlar dolandırıcılık girişimlerini erken fark eder ve şüpheli bir durumla karşılaştıklarında nasıl hareket etmeleri gerektiğini bilir.

2 İşlerinizi temiz ve güncel tutun.

Yazılım, uygulama ve antivirüsleri düzenli olarak güncelleyin. Verilerinizi güvenli bulut ve çevrimdışı ortamlara yedekleyin ve bu yedekleri periyodik olarak test edin. Çalışanlara yalnızca ihtiyaç duydukları kaynaklara erişim verin ve ayrılan personelin tüm erişimlerini hızla kaldırın.

3 Uzman desteği alın

Tehditleri erken tespit eden akıllı araçları kurmak için bir güvenlik uzmanıyla iş birliği yapın. Buna sistemlerinizi 7/24 izleyen yönetilen hizmetler de dahildir. Doğru bir iş ortağı, olası bir saldırı durumunda net ve uygulanabilir bir eylem planı oluşturmanıza yardımcı olur.

Birbirini tamamlayan bu adımların ayrıntıları için **siber güvenlik kontrol listemize** göz atabilirsiniz.

vodafone business

Siber güvenlik kontrol listesi: işletmenizi yapay zeka destekli siber tehditlerden koruyun

Yapay zekayla güçlenen siber tehditler hızla artıyor Ancak işletmenizi korumak zor olmak zorunda değil. **İşte bir adım önde kalmak için uygulaması kolay bir kontrol listesi:**

1. Siber güvenlik bilinci yüksek bir ekip oluşturun.

Çalışanlarınızı eğitin

Kimlik avı, fidye yazılımı ve kötü amaçlı yazılım gibi saldırı taktikleri ve oluşturduğu risklere karşı eğitim içerikleri ile çalışanlarınızın farkındalığını artırın.

Sezgilerini test edin

Kimlik avı (phishing) simülasyonlarıyla çalışanların nerede hata yaptığını görün; ve gerçek bir saldırıya karşı dayanıklılık kazandırın.

Destek mi gerekiyor?

Vodafone Business olarak, çalışanlarınızı hedef alan kimlik avı ve sosyal mühendislik saldırılarına karşı farkındalık oluşturan çözümler sunuyoruz. **Bizimle iletişime geçin.**

2. Akıllı siber hijyen ile iş sürekliliğini sağlayın.

Her şeyi güncel tutun.

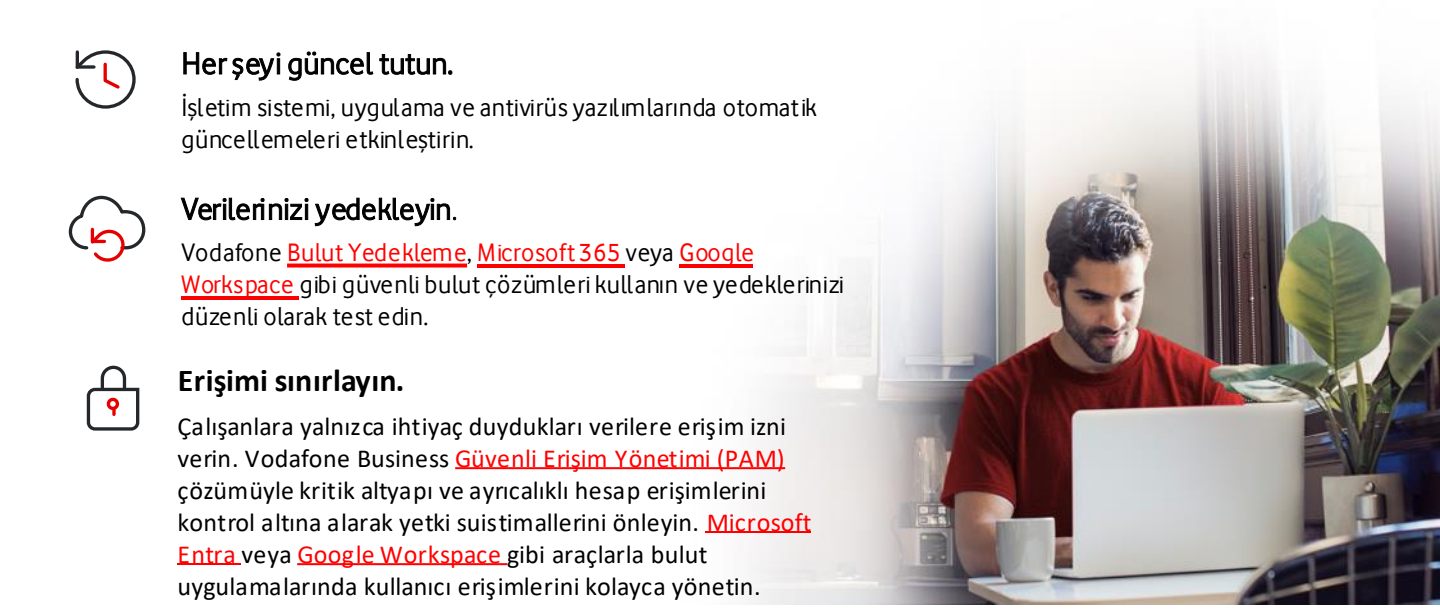
İşletim sistemi, uygulama ve antivirüs yazılımlarında otomatik güncellemeleri etkinleştirin.

Verilerinizi yedekleyin.

Vodafone Bulut Yedekleme, Microsoft 365 veya Google Workspace gibi güvenli bulut çözümleri kullanın ve yedeklerinizi düzenli olarak test edin.

Erişimi sınırlayın.

Çalışanlara yalnızca ihtiyaç duydukları verilere erişim izni verin. Vodafone Business Güvenli Erişim Yönetimi (PAM) çözümüyle kritik altyapı ve ayrıcalıklı hesap erişimlerini kontrol altına alarak yetki suistimallerini önleyin. Microsoft Entra veya Google Workspace gibi araçlarla bulut uygulamalarında kullanıcı erişimlerini kolayca yönetin.



3. Doğru araçları kullanın.

Vodafone Business olarak sunduğumuz çözümlerin bir kısmı:

Antivirüs & XDR

Standart Antivirüs çözümümüz ile bilinen zararlı yazılımları ve şüpheli dosyaları tespit edip engelleyebilirsiniz. Gelişmiş paketlerimiz e-posta ve bulut uygulamaları güvenliği özellikleri ve XDR yeteneklerini de barındırır. **Size en uygun paketi seçin.**

E-Mail Güvenliği

Kimlik avı, zararlı ekler ve sahte bağlantılar gibi e-posta kaynaklı tehditleri filtreleyerek çalışanlarınızı ve verilerinizi korur. E-posta trafiğiniz güvenlik politikalarına göre denetlenir, riskler daha kullanıcıya ulaşmadan durdurulur. **Detaylı bilgi alın.**

Ağ Güvenliği

Firewall, yetkisiz erişimleri ve şüpheli bağlantıları engellerken; **DDoS** koruması, yüksek hacimli saldırıları filtreleyerek sistemlerinize yalnızca temiz trafiğin ulaşmasını sağlar. Böylece hizmet sürekliliğiniz korunur ve ağınız dış tehditlere karşı güvende olur.

4. Kendinizin ve tedarikçileriniz risklerini görün.

Zafiyet Taraması ve Yönetimi

Sistemlerinizdeki güvenlik açıklarını düzenli olarak tespit edip raporlayarak saldırganlardan önce riskleri görmenize ve ihlallerin önüne geçmenize yardımcı olur. **Size ulaşalım.**

Domain Risk Analizi

Üçüncü taraf risklerini değerlendirin ve işletmenize özel detaylı raporlar alın. **Detaylı bilgi alın.**

Neden Vodafone Business?

Dünyanın önde gelen teknoloji sağlayıcılarıyla yaptığımız iş birlikleri sayesinde, işletmelerin yapay zeka destekli tehditler de dahil olmak üzere günümüzün en kritik siber güvenlik riskleriyle güvenle başa çıkmalarına yardımcı oluyoruz.

Küresel tehdit istihbaratımız, gelişmiş güvenlik araçlarımız ve uzman ekibimizle, her ölçekteki işletmenin güçlü ve uygun maliyetli bir korumaya sahip olmasını sağlıyoruz. Çünkü her kuruluşun dayanıklı ve sürdürülebilir bir siber güvenliği hak ettiğine inanıyoruz. **İşletmeniz için en uygun güvenlik çözümünü seçmenize yardımcı olalım.**

Together we can
vodafone business