Türk Telekom Siber Bülten

Mayıs 2021

Türk Telekom Güvenlik

Türk Telekom
Değerli Hissettirir

İçindekiler

Mahmut Küçük

Türk Telekom Siber Güvenlik Direktörü

Dijitalleşen dünyada siber güvenlik, beşinci savaş ortamı olarak kabul edilmenin ötesinde tüm ülkeler için ulusal güvenliğin ayrılmaz ve en önemli bileşeni haline gelmiştir. Öncelikle şunun bilinmesi gerekir: Siber güvenlik konusunda yaşanan olaylar iki devlet arasında çok ciddi krizlere sebep olabilir.

Dolayısıyla kurum ve şirketlerin siber güvenliğe verdikleri önemin artması, önlemlerini önceden almaları çok önemli bir husus haline gelmektedir. Özellikle ülkeler; kritik altyapılarına karşı siber saldırıları önlemek, siber saldırılara karşı ulusal güvenlik açıklarını azaltmak ve siber saldırılardan gelecek zararı ve toparlanma süresini en aza indirmek için şu anda yoğun çaba sarf etmektedir.

Hızlı bir biçimde teknoloji kullanımının artması neticesinde günümüz bireyleri, iş dünyası ve devlet kurumları kritik öneme haiz istihbarat, ekonomik ve kişisel bilgilerini teknoloji araçları vasıtası ile depolamakta ya da transfer etmektedir. Transfer edilen bu verilerin dolaşım sırasında bozulması ya da transferinin gerçekleşememesi gibi durumlarda çok büyük ekonomik veya itibar kaybın olacağı da bilinen bir gerçektir. Bu kapsamda; günümüzde siber suçlular veya teröristler artan bir oranda bilgisayarları, bilgisayar ağlarını, mobil cihazları ve akıllı cihazları (IoT) bu verilere ulaşmak için kullanmaktadır. Siber suçlular tarafından gerçekleştirilen bireysel verilerin elde edilmesi ve kötü amaçlı kullanılması, kritik süreçlerin engellenmesi veya yok edilmesi, ekonomiye büyük maliyetler getirecek saldırıların gerçekleştirilmesi ve milli sırların ele geçirilmesi ya da teşhir edilmesi gibi birçok siber saldırı günden güne artarak devam etmektedir. Bu bağlamda siber güvenliğin önemini de gün geçtikçe artmaktadır. Siber güvenlik konusunun iyi yönetimi, devlet kurumlarının eş güdümünün yanı sıra sivil toplum kuruluşları, üniversiteler ve özel sektörün iş birliğiyle oluşturacağı ekosistem Türkiye'nin teknoloji ihracatı, diplomatik etkinliği, istihbarat gücü, siber alandaki menfaatlerinin korunması gibi birçok önemli konuda ilerlemesinin yolunu açacaktır.

Siber güvenliğin geleceğine baktığımızda, artan otomasyon hayatlarımızı birbirine bağlıyor ve hassas verilerimizin büyük miktarlarını bulutta depoluyor. 5G ve sanayi devriminin dördüncü jenerasyonu olarak bilinen endüstri 4.0 ile ülkelerin siber güvenlik stratejilerinde de değişmeler yaşanmaktadır ve yaşanacaktır. Bu kapsamda bu alanların siber güvenliği ile ilgili her geçen gün yeni siber güvenlik teknolojileri piyasaya sürülmektedir. Güvenlik stratejilerinin de temel olarak bu iki alan üzerinde şekilleneceği öngörülebilir. Bunun yanında bulut güvenliği, kurumlar

arası veri paylaşım güvenliği ve kritik alt yapıların güvenliğinin sağlanması geleceğin siber güvenlik trendleri için örnek verilebilir. Ayrıca veri egemenliği ve dijital özerklik konseptlerinin konuşulduğu günümüz dünyasında ulusal egemenliğin bir parçası olarak yerli güvenlik çözümlerinin desteklenmesi ve kullanım farkındalığının artırılması önem kazanmaktadır.

Bütün bu tespitlerin yanı sıra, hayatımızın en zor yıllarından biri olan 2020 yılının genel bir değerlendirmesini yapacak olursak, pek çok açıdan farklı bir yıl geçirdiğimizi söylemek mümkün. Covid-19 salgınının tüm dünyada etkili olması ile birlikte, yeni iş modellerinin gelişmesi, e-ticaretteki işlem hacimlerinin artışı, şirketlerin evden çalışma modeline geçişi ve uzaktan eğitim gibi günlük hayatımızın işleyişini etkileyen değişiklikler yaşandı.

Yaşanan tüm bu değişimin temelinde ise dijital dönüşümün olduğunu görüyoruz. 2020 yılı hem bireylerin hem de şirketlerin hızla dijital dönüşüme uyum sağlamaya çalıştığı bir yıl oldu. Kullanım alışkanlıkları değişmeye başladı ve her yaştan kullanıcılar gerek bireysel kullanımları için gerekse iş ya da eğitim amaçlı kullanım için dijital platformlar üzerinden günlük aktivitelerinin önemli bir kısmını sürdürmeye başladı. Bu durum siber saldırganların iştahını kabartarak saldırıların daha da artmasına yol açtı. Hızlı dijitalleşmenin sonucunda siber güvenlik alanında yeterli farkındalığı bulunmayan bazı şirketler, kurumlar ve bireyler bu dönemde siber saldırılara maruz kalarak zarar gördü. Bu dönemde yapılan araştırmalar, siber saldırılardan en çok etkilenenlerin başında küçük ve orta ölçekli şirketlerin olduğunu gösteriyor.
KOBİ'ler özelinde yapılan bir araştırmaya göre küreselde düzenlenen siber atakların neredeyse yarısı KOBİ'leri hedef alıyor. KOBİ'ler, bilinirliği ve ekonomik büyüklükleri büyük şirketler gibi olmasa da siber saldırganlar için vazgeçilmez birer hedef durumundalar. Genellikle büyük şirketlere düzenlenen saldırılar daha çok ses getirdiği için daha çok bilinse de KOBİ'lerin siber saldırganların hedef tahtasından hiç inmediği görülüyor.

Unutmayalım ki her şirketin veya kurumun tüm siber güvenlik riskleriyle başa çıkmak için hem altyapı yatırımı yapıp işletmesi hem de uzman kadro oluşturarak saldırılara mukavemet geliştirmesi mümkün değil. Bu ihtiyaç nedeniyle Türk Telekom kurumsal ve bireysel güvenlik çözüm ve hizmetlerini müşterilerine sunmaya devam etmektedir.

Türk Telekom olarak, güvenilir, yenilikçi ve yüksek kaliteli siber güvenlik çözümleri geliştirme konusunda Siber Vatan'ımızın savunmasında üzerimize düşen sorumlulukların bilincinde olarak çalışmalarımıza yoğun bir şekilde devam etmekteyiz. Amacımız ülkemizin siber güvenliğinin sağlanmasında ana unsur olarak yerli ürünleri destekleyerek ulusal ve uluslararası pazarlarda güçlü, güvenilir Siber Güvenlik teknoloji ve hizmet sağlayıcısı olmaktır. Bu amaç doğrultusunda Türkiye'nin en güçlü deneyimli ve güvenilir uzman kadromuz ile daha da güçlenerek ülkemize hizmet sunmaya devam edeceğiz

Yönetici Özeti

Siber güvenlik alanında global ve yerel gelişmelerin anlatıldığı bültenimizin bu sayısında hızla dijitalleşen dünyanın gündeminde olan siber güvenlik konularına ve en çok etkilenen sektörlere değiniyoruz.

Türk Telekom atak istatistiklerini ve güncel siber risklere karşı Türk Telekom uzmanlarının önerilerini bültenimizde bulabilirsiniz.

Her 39 saniyede bir siber saldırı gerçekleşiyor. (Kaynak: Maryland University)

Zararlı yazılımların %94'ü mail yolu ile gerçekleşiyor. (Kaynak: Verizon)

DDOS saldırılarında %151 artış görüldü. (Kaynak: Netscout-2020 H1)

Covid etkisi ile ataklar **%238** artış gösterdi.

Covid-19 içerikli radsomware ataklarında artış yaşandı. (Kaynak: KeepnetLab)

Web uygulamalarına yapılan ataklar %43 arttı. (Kaynak: Verizon)

Veri ihlallerinin küresel toplam maliyeti $3,86 Milyar (Kaynak: IBM)

Gerçekleşen siber atakların %43'ü KOBİ'leri hedef alıyor.

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

KOBİ'lerin %50'si yılda en az bir kez saldırıya uğradığını belirtiyor.

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

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

1. Uzak Masaüstü Protokolü (RDP) Saldırılarında Artış

Geçtiğimiz dönemde uzaktan çalışma modeline geçen şirketler pek çok güvenlik riski ile baş etmek durumunda kaldılar. Bu tarz saldırıların en yaygın olanları arasında uzak masaüstü protokolü saldırılarının olduğunu görmekteyiz. ESET'in 2020 4. Çeyrek Tehdit Raporuna göre, uzak masaüstü protokolü (RDP) saldırıları, geçen yılın ilk çeyreği ile son çeyreği arasında % 768 artış gösterdi. Bununla birlikte, yılın son çeyreğinde daha yavaş bir büyüme hızı gözlemlendi, bu da kuruluşların uzaktan çalışan kullanıcılarının güvenliği konusunda önlemler almaya başladığını gösteriyor.

Uzak Masaüstü Protokolü (RDP) Saldırılarında

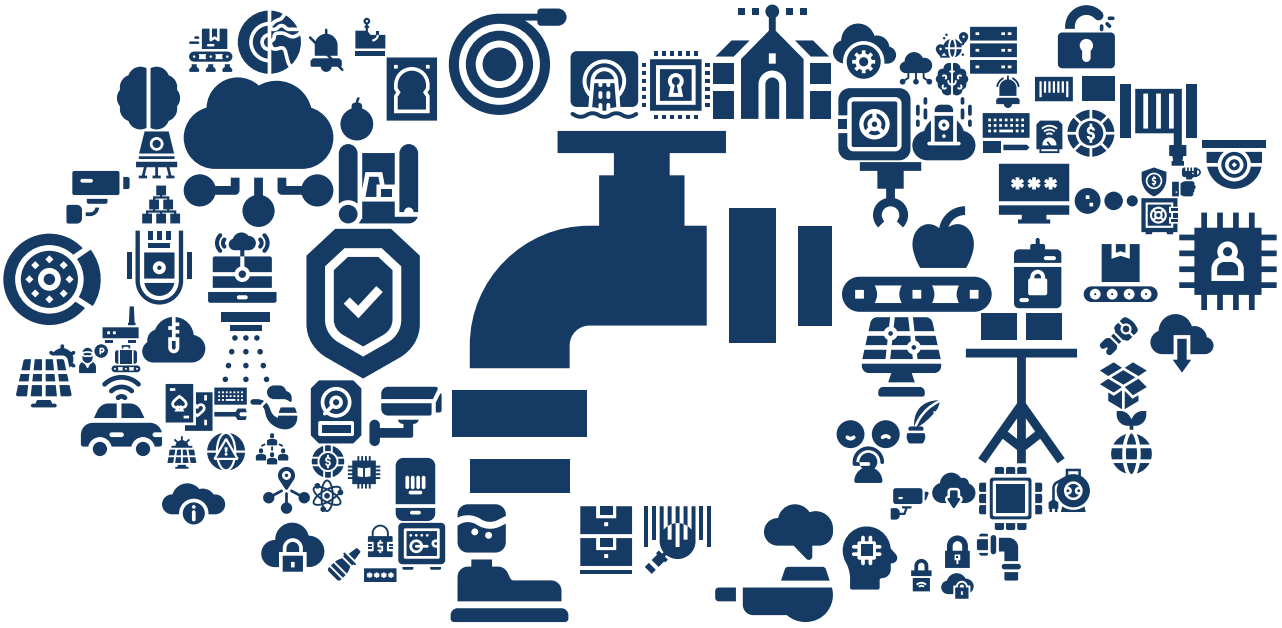
% 768

Artış Meydana Geldi

Rapordan elde edilen bir diğer önemli veri ise dördüncü çeyrekte **COVID-19** temalı e-posta tehditlerinde yaşanan artış. Özellikle aşı kullanımına yönelik maillerin yoğun bir şekilde kullanıldığı görülmüştür. Üçüncü çeyrek ile kıyaslandığında, kötü niyetli e-postalardaki aşı ifadeleri % 50 oranında artmış, bu konunun sunduğu cezbedici güçlü ifadelerin vurgulandığı görülmüştür. Örneğin , aşı geliştirme konusundaki iş önerileri, çok düşük sıcaklıklı dondurucularla ilgili teklifler ve aşıyla ilgili komplo teorileri gibi güncel konular saldırganlar tarafından sıklıkla kullanılmıştır.

Saldırı trendine baktığımızda E-posta yolu ile iletilen saldırıların 2021 yılı içerisinde büyük bir tehdit oluşturacağını söylemek mümkündür. Bu nedenle, RDP güvenliği, özellikle RDP istismarları yoluyla yaygın olarak kullanılan fidye yazılımı nedeniyle küçümsenmemelidir. RDP güvenliği zafiyeti giderek artan saldırgan taktikleri ile hem özel hem de kamu sektörü için büyük bir risk oluşturmaktadır.

2. Florida'nın Oldsmar Kasabasında Su Sistemi Siber Saldırıya Uğradı



Florida'nın Oldsmar kasabası, bir siber saldırganın içme suyu kaynağını zehirlemeye yönelik saldırısı ile gündem olan küçük bir kasaba. Reuters Haber Ajansında yer alan habere göre saldırgan, sistemlere uzaktan erişim bağlantısı sunan yazılım TeamViewer'ı kullanılan su tesisindeki bir bilgisayara erişim sağladı ve suyu içmek için oldukça zehirli hale getirecek olan sodyum hidroksit, diğer adıyla sodalı su seviyelerini yükseltti. Kirli suyun kasaba sakinlerine ulaşmasını önlemek için güvenlik önlemlerinin bulunduğu ve bu sayede saldırının engellenebildiği açıklandı.

Bu saldırı aslında uzak bağlantı yöntemlerinde yeterli güvenlik önlemleri alınmadığı durumda nasıl bir felakete yol açılabileceğini bir kez daha gözler önüne sermiş oldu. Bu nedenle uzaktan erişim sağlanan tüm sistemlerin güvenliği konusunda şirketlerin güçlü bir altyapı üzerinden bu tarz erişimleri yönetmeleri önem arz etmektedir.

3. Aşı Dağıtımı Yeni Siber Güvenlik Risklerini de Beraberinde Getiriyor

Aşı yapmanın ve teslim etmenin arkasındaki karmaşık tedarik zinciri, bilgisayar korsanları için çok sayıda fırsat yaratmış durumda. Pandeminin başlangıcından bu yana Covid-19 siber saldırılarını izleyen IBM Security X-Force'un küresel tehdit istihbaratı lideri Nick Rossman, "Bu saldırı yüzeyinin ne kadar büyük olabileceğini düşünmemiz gerekiyor – büyüyor ve daha da büyüyecek" dedi.

Rossman salgınla birlikte bilgisayar korsanlarının da geliştiğini söyleyerek, aşıları üreticilerden kullanıcılara ulaştıran sürece yönelik saldırıların artmakta olduğunu ve korsanların geçtiğimiz ay aşıları uygun sıcaklıklarda tutmaya çalışan tedarik şirketlerini hedef alan bir kimlik avı saldırısında bulunduğunu belirtti.

Tedarik zincirlerine yönelik düzenlenen siber saldırılar özellikle günümüz koşullarında hayat sürekliliğini de tehdit eden önemli bir faktör. Dolayısıyla tedarik zinciri kapsamında yer alan tüm firmaların üzerlerine düşen sorumluluğu alarak siber risklere karşı önlemlerini sıkılaştırmaları gerekiyor.

4. Veri Sızıntıları

06.04.2021 tarihinde 500 milyon LinkedIn profilinden alındığı iddia edilen verileri içeren bir arşiv Raidforums üzerinde satışa sunulmuş ve 2 milyon kayıt ise kanıt olarak paylaşıma açılmıştır. Kanıt olarak paylaşılan ve tehdit aktörü tarafından LinkedIn üzerinden elde edildiği iddia edilen dört dosya, LinkedIn kullanıcıları hakkında tam adları, e-posta adresleri, telefon numaraları, işyeri bilgileri dahil olmak üzere birçok veri içermektedir. Tehdit aktörünün güncel LinkedIn profillerini satıp satmadığı ya da verilerin LinkedIn veya diğer şirketlerin maruz kaldığı önceki bir sızıntıdan toplanıp toplanmadığı belirgin değildir. LinkedIn tarafından yapılan açıklamada, satılık verilerin bir veri ihlali sonucunda elde edilmediği ve bir dizi web sitesi ve şirketten elde edilen verilerin bir toplamı olduğu belirtilmiştir. Aynı forum sitesi üzerinde 09.04.2021 tarihinde başka bir kullanıcı tarafından 7.000$ değerinde bitcoin karşılığında yeni bir LinkedIn veri tabanı koleksiyonu satışa sunulmuştur. Koleksiyon içerisinde hem orijinal 500 milyon kullanıcı bilgilerinin yer aldığı veri tabanı hem de 327 milyon kazınmış LinkedIn profilini içeren altı ek arşiv dosyasının yer aldığı iddia edilmiştir. Bu paylaşımda 827 milyona ulaşan toplam profil sayısının LinkedIn'in sahip olduğu yaklaşık 740 milyon gerçek kullanıcıdan oluşan veri tabanını veri adeti olarak aştığı görülmüştür. Buradan hareketle satılan yeni verilerin bir kısmının yinelenmiş veya eski veriler olabileceği değerlendirilmektedir.

03.04.2021 tarihinde Raidforums üzerinde 533 milyon Facebook kullanıcısına ilişkin olarak ad-soyad, telefon numarası, e-posta adresi, lokasyon gibi detaylarından oluşan veri paylaşımı yapılmıştır. Paylaşım içeriği ise 8 kredilik (yaklaşık 2 Euro) bir bedel karşılığında görüntülenebilir halde sunulmaktadır. Facebook tarafından yapılan açıklamada, bahsi geçen verilerin 2019 yılında iletişim ithalatçısındaki güvenlik açığından yararlanılması neticesinde gerçekleşen güvenlik ihlâlinin ardından sızdırılmış veriler olduğu beyan edilmiştir. Geçmiş dönemde gerçekleşen bu vaka, kullanıcıların telefon numaraları üzerinden Facebook profillerinin bulunmasına olanak tanıyan bir araçtaki güvenlik açığı neticesinde meydana gelmiştir.

Türkiye'de Siber Atak Trendleri

1. Covid-19 İçerikli Oltalama Saldırılarında Yaşanan Artış

Oltalama saldırıları tüm dünyada olduğu gibi ülkemizde de önemli bir tehdit oluşturuyor. Her ölçekten şirketin kullanıcılarını hedef alan oltalama saldırıları ile sahte içerikler yaratılarak, kullanıcıları zararlı bağlantılara yönlendirilmeye teşvik ediliyor.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi özellikle sağlık konusunda hassas olunan bu dönemde vatandaşları oltalama saldırılarına karşı dikkatli olmaya davet ediyor. Ofis Başkanı Dr. Ali Taha Koç yaptığı açıklamada, COVID-19 pandemisinin tüm dünyayı derinden etkilediğini ve aşılama çalışmalarının tüm dünya ile aynı zamanda ülkemizde de başladığını vurgulayarak, bu süre içerisinde özellikle sosyal medya ve kısa mesaj yoluyla vatandaşlarımızı tuzağa düşürmeye yönelik içeriklerin yer almaya başladığını dile getirdi.

2. Güvenli Mesajlaşma Uygulamaları

Neden güvenli mesajlaşma kullanmak gerekiyor?

Günlük hayatta sıklıkla kullandığımız ve hayatımızın vazgeçilmezi olan bu uygulamalar, hayatımızı kolaylaştırdığı gibi ciddi güvenlik risklerini de beraberinde getirmektedirler.

Kullanılan mesajlaşma uygulamaları ile birçok kişisel bilgi paylaşılmaktadır. Mesajlaşma uygulamalarının güvenliği ile uğraşırken dikkate aldığımız ana özellik, uçtan uca şifreleme iletişiminin uygulanmasıdır. Uçtan uca şifreleme (E2EE) iletişimi, üçüncü tarafların iki muhatap arasında veriler aktarılırken gizlice dinlemesini engeller.

Uçtan Uca Şifreleme Nedir?

Uçtan uca şifreleme, iletişimlerinizin güvenli olmasını sağlayan bir güvenlik yöntemidir. Bundan dolayı, telefonunuz ve gönderdiğiniz telefon arasında gidip gelen mesajları üçüncü taraflar da dahil olmak üzere hiç kimse okuyamaz. Uçtan uca şifrelenmiş mesaj uygulamasını kullandığınızda, veriler cihazlar arasında gidip gelirken metinler ve dosyalar da dahil olmak üzere tüm sohbetler şifrelenir. Şifreleme ile veriler karışık metinlere dönüştürülürler. Okunamaz durumdaki bu metinlerin şifresi yalnızca gizli anahtarla (Mesajı gönderdiğiniz tarafın anahtarı ile) çözülebilir.

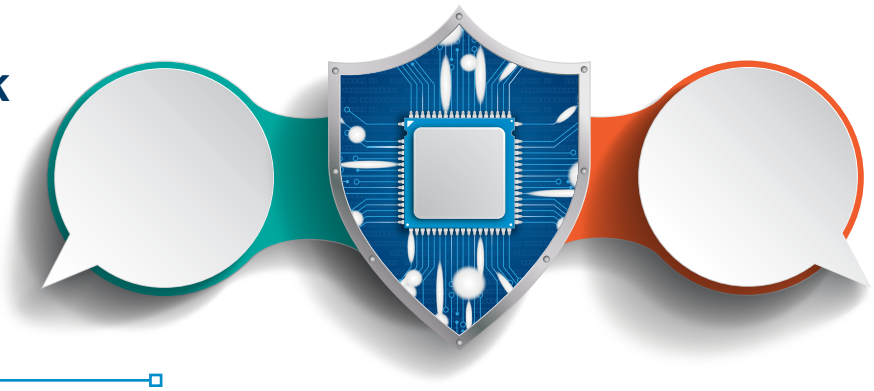
Uçtan uca şifrelenmiş her görüşmenin benzersiz bir doğrulama kodu vardır. Mesajlarınızın uçtan uca şifrelendiğini doğrulamak için sizin ve görüştüğünüz kişinin cihazında bu kodun aynı olması gerekir.

Bir mesaj oluşturduğunuzda, gönder düğmesinde ve mesajın zaman damgasının yanında bir kilit simgesi varsa uçtan uca şifreleme kullanılıyor demektir.

Şifreli bir mesajlaşma uygulamasını güvenli yapan nedir?

Ne yazık ki, bir uygulama uçtan uca şifreleme uygulasa bile bu, varsayılan olarak etkinleştirildiği anlamına gelmez. Bazı mesajlaşma uygulamaları, kullanıcıların bu özelliği açıkça etkinleştirmesini gerektirirken, diğerleri mesajları yalnızca belirli durumlarda şifreler. Şifrelenmiş mesajlaşma uygulamalarını analiz ederken değerlendirilmesi gereken bir diğer önemli faktör, kaynak kodlarının güvenlik denetimleri için kullanılabilirliğidir. Açık kaynaklı uygulamalar, güvenlik açıklarını ve gizli arka kapıları arayan kodun incelenmesine olanak tanır.

Uygulamaların güvenliğini artırabilecek diğer özellikler "Ekran görüntüsü algılama" ve "Ekran yer paylaşımı koruması"dır.



Şifreli mesajlaşma uygulamalarındaki önemli gizlilik ve güvenlik eksiklikleri nelerdir?

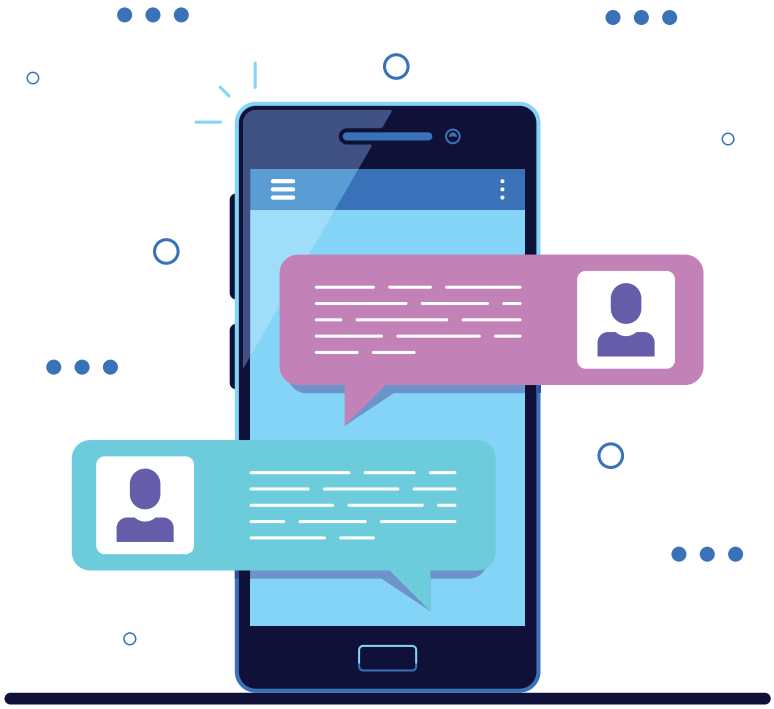
- Şifrelenmemiş bulut yedeklemelerinin kullanımı
- Açık kaynakta bulunmayan uygulamanın koduyla ilgili şeffaflık eksikliği
- Güvenlik zafiyeti tescilli şifreleme algoritmalarının kullanımı
- Uçtan uca şifrelemenin isteğe bağlı ayarı

Türkiye'de Siber Atak Trendleri

Şifreli mesajlaşma uygulamaları saldırılara dayanıklı mı?

Bu soruya cevabımız hayır olacaktır. Bunun nedeni, herhangi bir uygulamanın kodunda bir güvenlik açığını keşfetmenin her zaman mümkün olmasıdır. **Bu nedenle, kodlarını açan ve hata ödül programları çalıştıran uygulamalar daha güvenli kabul edilir.** Saldırıya karşı korumalı uygulamalar genellikle güvenlik açığı ifşa süreciyle ilgilenen kuruluşlar tarafından yönetilen uygulamalardır.

Güvenlik açıkları keşfedildikten hemen sonra yamalanmış olsa bile, bunların varlığı, kullanıcıların gizliliği için ciddi riskler oluşturan kusurlardan etkilenebileceğini göstermektedir.



Kullanacağınız mesajlaşma uygulamasının; Uçtan Uca Şifreleme kısmının varsayılan olarak etkinleştirildiğinden, yedeklemenin şifreli bir şekilde depolanmasına izin verildiğinden ve cihazda herhangi bir meta veri tutmayan bir özelliği etkinleştirdiğinden emin olun.

Siber alandaki zafiyetin farkında olan ülkeler, yerli ve milli yazılımlara yönelmektedir. Dünya'da sanal bir istihbarat çağı yaşanmaktadır. Yabancı menşeili bazı mesajlaşma uygulamalarında yaşanan güvenlik açıkları nedeniyle yerli ve milli ürünlerin kullanılması doğru bir yöntem olacaktır.

3. SSDP (Simple Service Discovery Protocol) DDoS Atakları

Basit bir hizmet keşif protokolü (SSDP) saldırısıdır. Hedefe güçlendirilmiş bir trafik akışı göndermek için UPnP (Universal Plug & Play) ağ protokollerinden yararlanan bir yansıma DDoS saldırı türüdür. UDP 1900 portunu kullanır.

SSDP Saldırısı Nasıl Yapılır?

SSDP, UPnP cihazlarının varlıklarını, ağdaki diğer cihazlara yayınlamasına izin vermek için kullanılır. Örneğin, bir UPnP yazıcı normal bir ağa bağlandığında, multicast adresi adı verilen belirli IP adreslerine bir mesaj göndererek aynı ağdaki diğer bilgisayarlara, sağladığı hizmetlerin türünü duyurur. Ardından, multicast adresi, yeni yazıcının varlığını ağdaki diğer tüm bilgisayarlara duyurur. Her bilgisayar yazıcıyla ilgili bir bildirim alır almaz, yeni aygıtın işlevlerinin tam açıklamasını sağlamasını ister. Yazıcı, hizmetlerinin ayrıntılı bir açıklamasını sağlayarak yanıt verir. SSDP saldırısı, sağlanan hizmet türleri hakkındaki son kullanıcı sorgusundaki güvenlik açığını kullanarak yanıtları kurbanın adresine iletir.

Tipik bir SSDP Yansıtma Saldırısının 6 Adımı:

- Kötü niyetli kişi, amplifikatör görevi görebilecek Plug and Play cihazları aramaya başlar.
- Bilgisayar korsanı, sorgulara yanıt gönderebilen cihazları keşfeder ve bir liste yapar.
- Bilgisayar korsanı, seçilen hedefin sahte IP adresiyle bir UDP paketi oluşturur.
- Saldırgan, her Plug and Play cihazına sahte sorgular içeren paketleri dağıtmak için bir botnet kullanır ve ssdp: rootdevice или ssdp: all gibi özel bayraklar ayarlayarak olabildiğince fazla bilgi ister.
- Sonuç olarak, her cihaz, seçilen hedefe saldırganın sorgusundan yaklaşık 30 kat daha büyük miktarda veriyle bir yanıt gönderir.
- Son olarak, kurban tüm cihazlardan muazzam miktarda trafik alır ve band genişliği dolar, bu da temiz trafiğin işlenememesine neden olur.

Sistem bir SSDP saldırısından nasıl korunur?

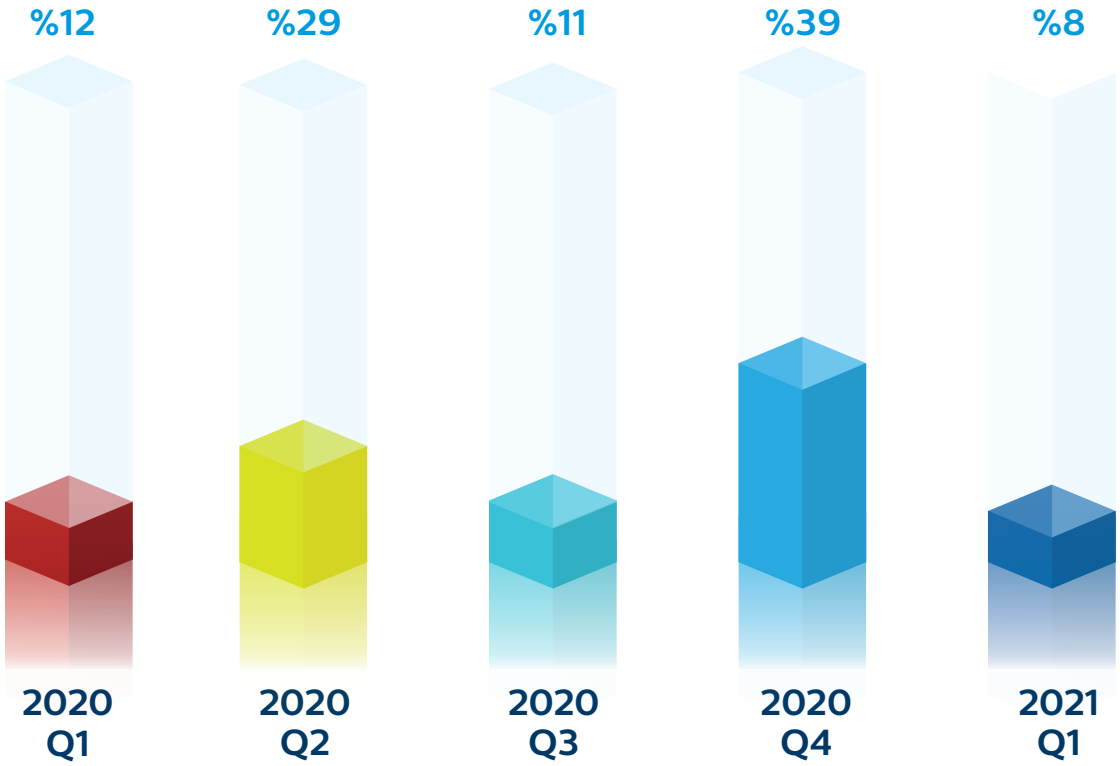
Sistem yöneticilerinin, ağ güvenlik duvarını kullanarak 1900 numaralı bağlantı noktasından gelen tüm UDP trafiğini engellemesi çok önemlidir. Etkilenen trafik hacmi ağ altyapısını tıkamak için yeterli değilse bu tür önlemler makuldür. Bilgisayar korsanları genellikle SSDP'yi diğer saldırı türleriyle birleştirir. Bu nedenle, ağ koruması karmaşık önlemler gerektirir.

**Aralık ayı boyunca 8 adet,
2020 yılında toplam 32 adet
SSDP Amplification saldırısı Türk Telekom
DDoS Atak Önleme sistemlerinde engellenmiştir.**

Türk Telekom Siber Atak İstatistikleri

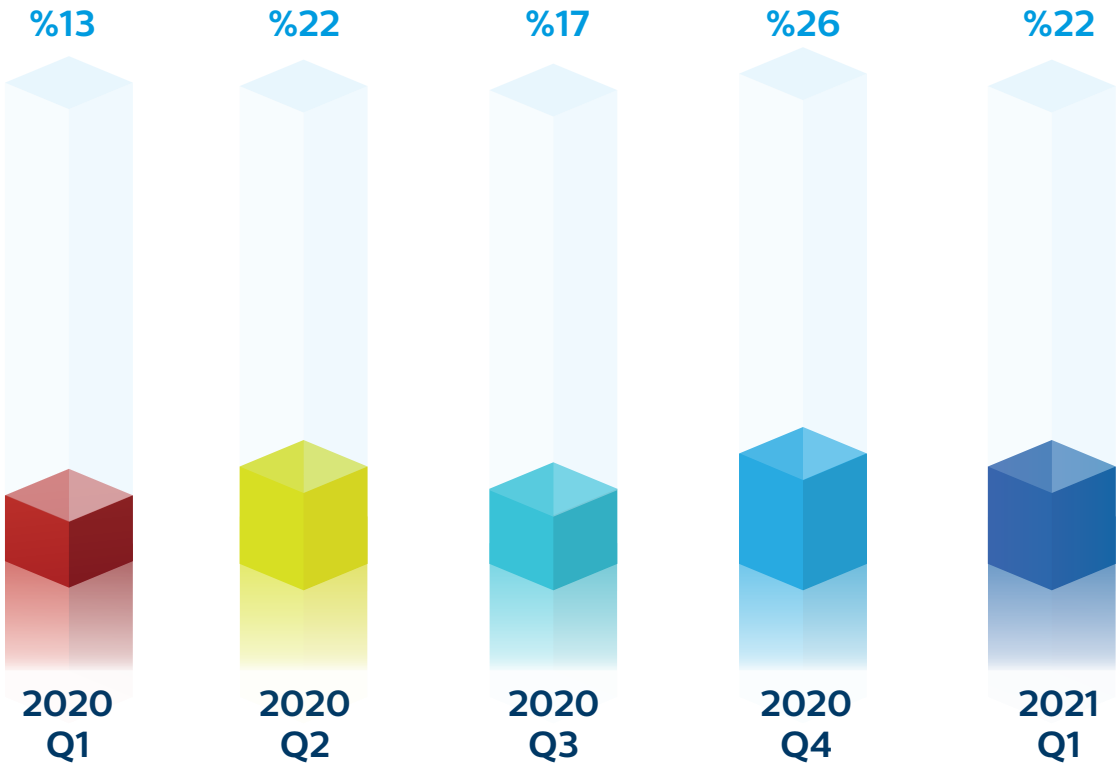
1. Gelişmiş Tehdit Önleme (APT) Atak İstatistikleri

Türk Telekom'un APT sistemlerinde tespit edilen zararlı yazılımların çeyrek bazlı dağılımına baktığımızda 2020'nin son çeyreğinde artış meydana gelmiştir.



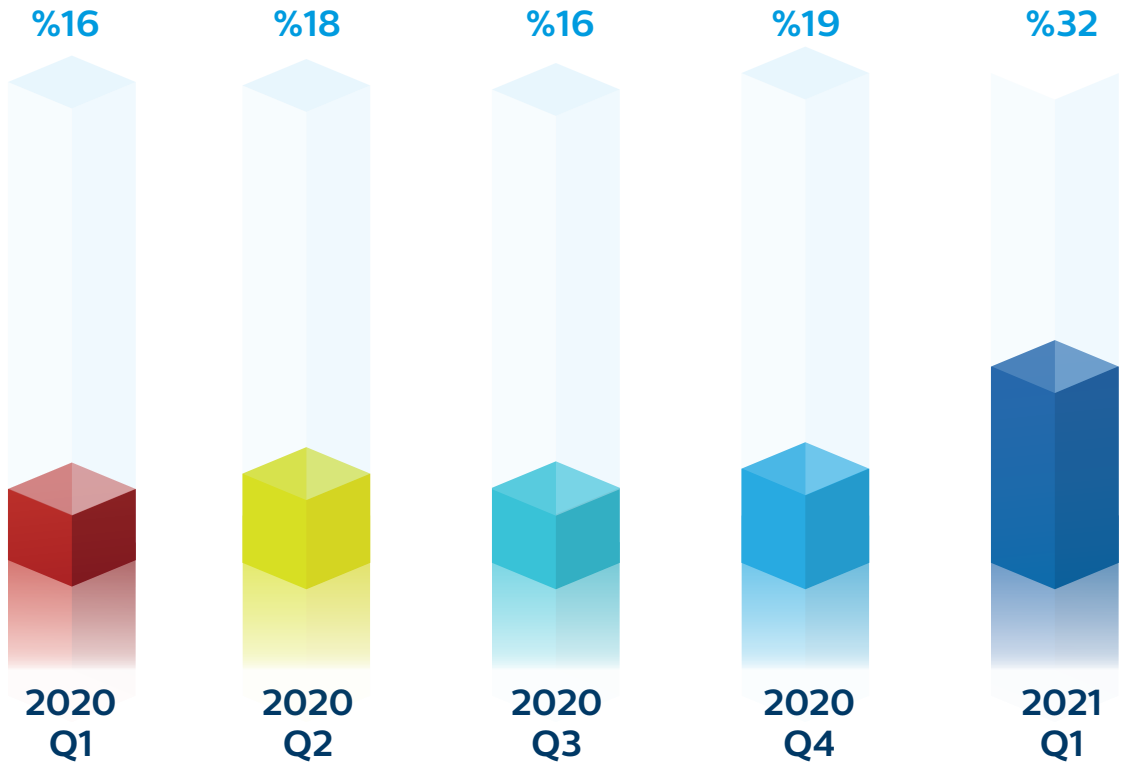
2. Antivirüs Servisinde Tespit Edilen Zararlı İçerikler

Sistemlere gelen trafik tehdit veri tabanında yer alan imzalara göre incelenip filtrelenmektedir. İmza bazlı siber ataklarda 2020'nin son çeyreğinde artış meydana geldiği gözlemlenmiştir.

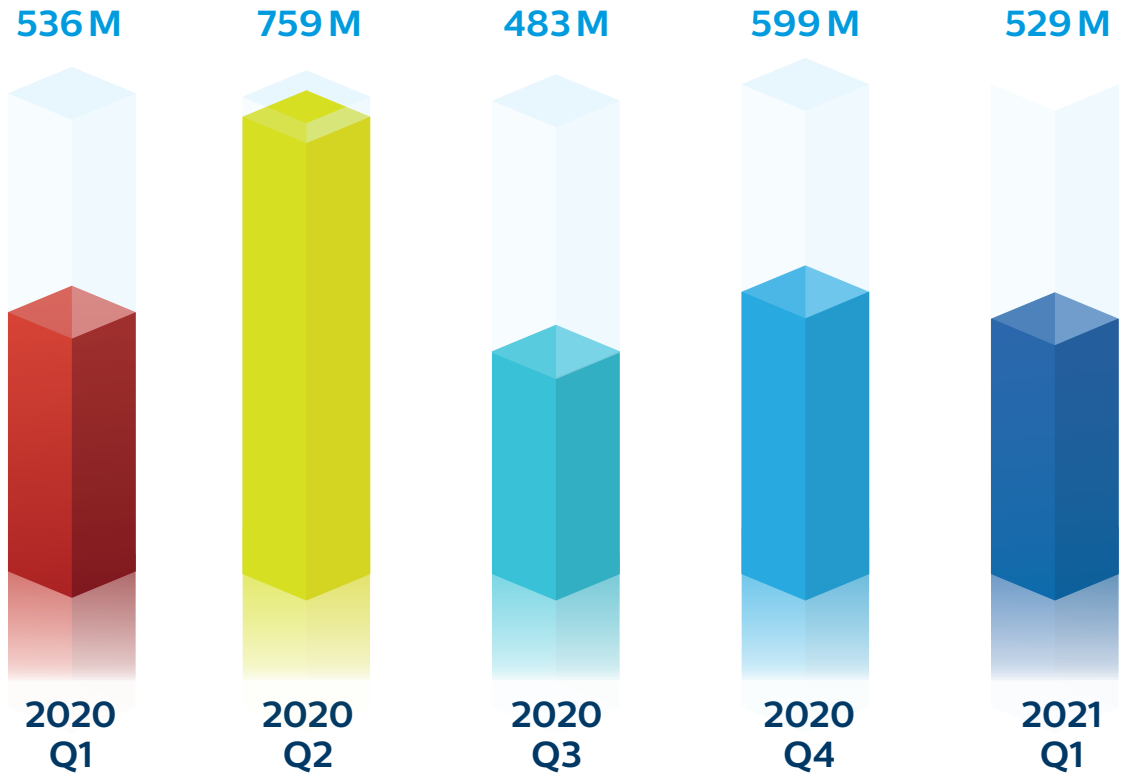


3. İçerik Filtreleme Servisinde Tespit Engellenen Zararlı İçerikler

"Türk Telekom içerik filtreleme servisi; kötü niyetli, oltalama saldırıları içeren veya uygunsuz web sitelerine erişimi engelleyerek kurumunuzu korumanızı amaçladığımız hizmetimizdir. Bunun yanı sıra kullanıcıların, web trafiği için belirlenmiş kurallara göre web erişimlerine izin veren veya engelleyen hizmettir."



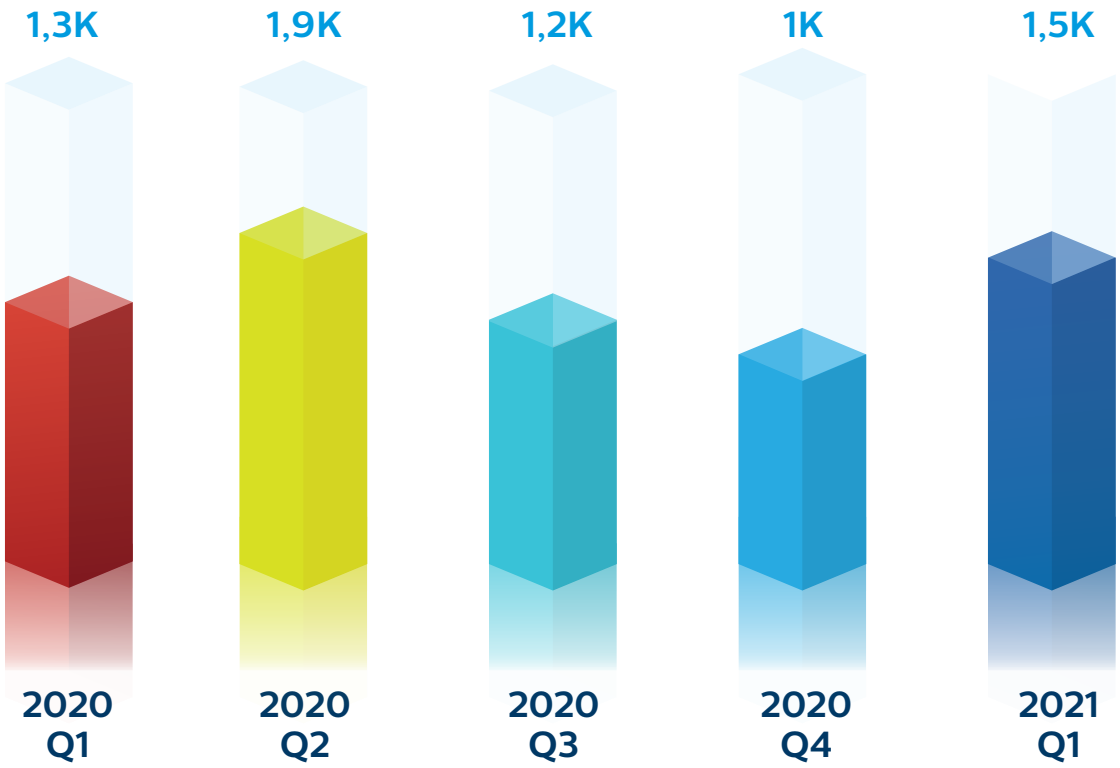
4. Aktif Savunma (IPS) Servisinde Tespit Edilen Zararlı Yazılımlar



5. 1 Gbps ve Üzeri DDOS Atakları

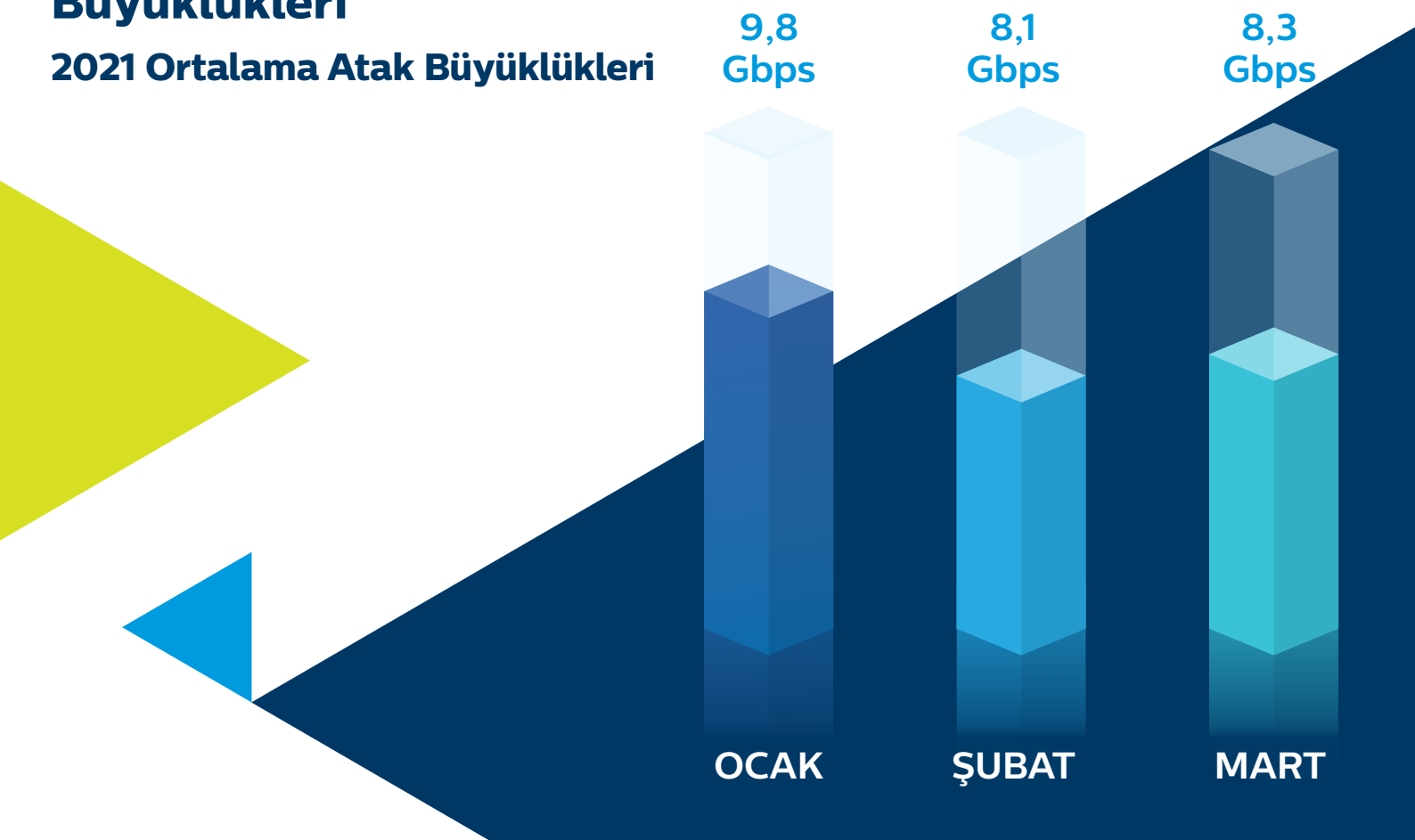
Atak Sayıları

Türk Telekom DDOS koruma servisinde tespit edilen ve engellenen 1 Gbps üzeri atak sayılarının çeyrek bazlı dağılımları



2021 Yılında Gerçekleşen Ortalama DDOS Atak Büyüklükleri

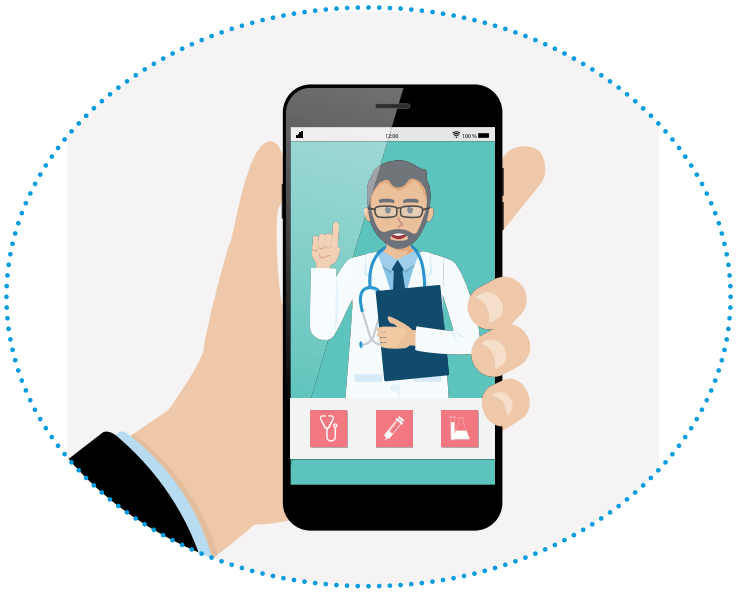
2021 Ortalama Atak Büyüklükleri



Sektörlere Yönelik Siber Güvenlik Önerileri

Finans

Finans kurumlarının, kendilerini büyük ölçekli dağıtılmış hizmet reddi (DDoS) saldırılarından koruyabilmesi çok önemlidir. Ağa gelen yurtdışı kaynaklı atakların, yurtdışı atak temizleme noktalarına yönlendirilip temizlendikten sonra teslim edildiği **Türk Telekom Cloud DDoS hizmetinden yararlanabilirsiniz.**



Sağlık

Teknoloji destekli ve kişiselleştirilmiş sağlık hizmetleri, doktor-hasta ilişkilerini üst düzeye taşıyor. Randevu almak veya test sonuçlarına ulaşmak gibi işlemler online kanallar üzerinden günümüzde kolayca halledilse de dijitalleşme süreci beraberinde çeşitli sorumluluklar da getiriyor.

Güvenli, kaliteli ve verimli bir şekilde süreçleri yürütülürken hasta verilerinin saklanması ve gerekli siber güvenlik önlemlerinin alınması büyük önem taşıyor.

Sağlık hizmetlerinin beklenmeyen saldırılara karşı kesintiye uğramadan devam edebilmesi için Türk Telekom Siber Güvenlik Merkezi kapsamında sunulan **Test Danışmanlık ve 7/24 Güvenlik Olay İzleme** Hizmetlerinden faydalanabilirsiniz.

Sektörlere Yönelik Siber Güvenlik Önerileri

Perakende / E-Ticaret

COVID-19 etkisiyle online alışverişe olan talep artışı beraberinde web sitesi ve web uygulamalarını tehdit eden siber saldırıları da gündeme getirdi. Yaşanabilecek kısa hizmet kesintileri bile perakende ve E-Ticaret sektörünü diğer sektörlerden çok daha fazla etkiler, müşteri ve itibar kayıplarına yol açabilir.

Gelişmiş bir DDOS saldırısı ise savunmasız bir siteyi dakikalar içinde çökertebilir.

Web sitesi üzerinden online ödeme işlemi gerçekleştiğinden müşterilerinizin kredi kartı ve kimlik bilgileri de yüksek risk altındadır.

Türk Telekom'un **DDOS Atak Önleme ve Web Uygulama Güvenlik Duvarı** Hizmetlerinden faydalanarak kesintisiz hizmeti sunmaya devam edebilirsiniz.

Turizm

Müşteriler hakkında son derece hassas kişisel verilerin (pasaport ve kredi kartı bilgileri, uçuş milleri vs.) kişiselleştirilmiş deneyim sunmak amacıyla veri tabanlarında uzun süre bulundurulması turizm sektörünü siber saldırıların hedefi haline getirmektedir.

2020’nin en büyük veri ihlali saldırılarından biri dünyanın en büyük otel zincirlerinden birine yapıldı.

Siber saldırganlar kötü amaçlı yazılım, bilgisayar virüsleri ve sosyal mühendislik yöntemlerini kullanarak sahte web siteleri, e-postalar veya kısa mesaj gibi çeşitli kanallar aracılığıyla otellere yönelik gerçekleştirdikleri veri ihlali saldırıları ile işletmeler ciddi itibar kaybı yaşarlar.

İşletmenizi tehditlerden korumak için Antivirüs, Aktif Savunma Sistemi ve Güvenlik Duvarı, İçerik Filtreleme gibi temel siber güvenlik ihtiyaçlarınızı Türk Telekom’un omurga seviyesinde ya da dedike olarak sunduğu çözümler ile karşılayabilirsiniz.

Altyapınızın 7/24 korunduğundan emin olmak için ayrıca SIEM ve SOAR gibi birinci sınıf siber güvenlik çözümlerini de değerlendirebilirsiniz.

«Başarı Hikayesi»

Savaş ERGEN

BT Altyapı ve Operasyon Direktörü

Tüm dünyayı etkisi altına alan Koronavirüs Covid-19 Pandemisi'nin Mart ayı başında ülkemizde görülmeye başlaması sonrası CK Enerji BT Altyapı ve Operasyon Direktörlüğü olarak öngörülerimiz doğrultusunda koordinasyon çalışmaları yaparak karşılaşabileceğimiz senaryoları belirledik. Bu senaryoları hayata geçirmek gerekliliği ortaya çıktığında optimum başarı ile neyi, ne kadar sürede yapabiliriz sorularının cevaplarını bulabilmek amacıyla gerekli olan testlerimize başladık. En küçük ayrıntısına kadar süreçleri sorguladığımız bu dönemde verdiğimiz hizmetin önemini de düşündüğümüzde, her koşulda çalışanların sağlığını öncelikli olarak ön planda tutatak, hızlı manevra kabiliyetimiz ile birlikte sistem altyapı, iletişim, güvenlik ve operasyonel destek konularındaki test ve canlıya uyarlama planlarımızı başarılı bir şekilde tamamladık.

İçinde bulunduğumuz bu uzaktan çalışma evresinde oluşabilecek her türlü siber tehdit için ilgili birimlerimiz gerekli önlemleri almakta, ulusal ve global kaynakları düzenli bir şekilde takip ederek süreçlerini güncel tutmakta, anlık izlemeler ve müdahaleler ile olası aksaklıkların önüne geçmektedir. Yine süreçte tüm bu aktivitelerin koşturulduğu sistemlerimiz ilgili birimlerimiz tarafından anlık olarak izlenmekte, geneli etkileyebilecek kapasite yoğunlukları ve problemlerde gerekli müdahaleler ile en uygun altyapı kombinasyonları kurgulanarak kullanıcılarımızın bir sorun hissetmemeleri sağlanmaktadır. Aynı zamanda uzaktan çalışmakta olan personelimizin bireysel olarak karşılaşabilecekleri olası sorunlar için yardım masası desteği verilmektedir.

Siber tehditlerin hızla arttığı günümüzde, kurumların siber güvenlik stratejilerini oluşturması, sürekli değişen koşullar ve riskler için proaktif davranışlar sergilemesi kaçınılmaz hale gelmiştir. CK Enerji BT Altyapı ve Operasyon Direktörlüğü olarak siber güvenlik konularındaki farkındalığın tüm kurumlarımızda artırılması için bir dizi çalışmalar gerçekleştik ve sürekli olarak geliştirilmesi içinde çalışmalarımız devam ediyor.
Bu kapsamda; Siber güvenlik durumumuzun sürekli olarak izlenmesi, analiz ve tespitlerin yapılması, güvenlik sorunlarının belirlenmesi ve sonrasında hızlıca ele alınmasının sağlanmasından sorumlu Siber Güvenlik Operasyon Merkezi (SOC) hizmet alımını Turk Telekom bünyesinden sağlıyorduk. Bu dönemde SOC hizmetleri daha da önem kazanmakla birlikte hizmetimizin içeriğini artırarak ,kontrol süreçlerini daha sıkılaştırarak çevikliğimizi artımak bize güç kazandırmıştır. Ağlarımızda, sunucularımızda, veri tabanlarımızda, uygulama-larımızda, web sitelerimizde ve diğer sistemlerimizdeki etkinliklerin izlenmesi ve analiz edilmesi, bir güvenlik olayı veya zafiyetinin göstergesi olabilecek anormal etkinliklerin taranması, güvenlik sorunlarının doğru bir şekilde tanımlanması ve rapor edilmesi gibi kurumlarımızca son derece önemli bu iş birliğini Türk Telekom ile yürütmeye devam etmekteyiz.

Bu hizmetlerin yanında özellike dışarı hizmet veren sistemlere daha fazla güvenlik sıkılaşması uygulanması gerektiğini düşünmekteyiz. Fakat bu konuda bazı handikaplar bulunmaktadır, özellikle DDOS L7 seviyesinde güvenlik koruması ve WAF gibi uygulamaların güvenlğini sağlayacak çözümler hem maliyet hemde kullanım karmaşası açısından sorun teşkil etmektedir. DDOS ve WAF gibi çözümler doğru yönetilmediği ve düzgün konfigurasyon yapılmadığında çok da etkili olmamaktadır. Sadece varmı? Var sorusuna bir yanıt teşkil etmektedir. Bu sıkıntılardan kurtulmak ve dış servislerin güvenlğini artırmak amacı ile Türk Telekom ile yeni bir hizmet çalışmasını gerçekleştirdik ve DDOS saldırılarının önlenmesi konusunda volümetrik ataklar (L3) için Türk Telekom tarafından almakta olduğumuz hizmete, Uygulama Katmanı (L7) ataklarını önleme hizmetini de ekledik. Uygulama katmanındaki saldırılardan korunmak için tüm veri merkezlerimize fiziksel cihazlar konumlandırmamız gerekirken Türk Telekom 'dan aldığımız hizmet sayesinde yatırım gereksimi ve sistemin Türk Telekom bünyesindeki uzman personeller tarafından yönetilmesi nedeniye bakım, güncelleme, izleme ve operasyonel işlemler için kaynak ihtiyacımız ortadan kalktı.

Ek olarak, uygulamalar kodlanırken genelde güvenlik parametreleri gözden kaçırıldığı söylenebilir. Yazılım korsanları da genelde bu atak tiplerini kullanmakta ve sonucunda kurumlar ciddi veri sızıntısı, itibar kayıpları yaşayabilmektedir. Bu noktada yine Türk Telekom Siber Güvenlik Operasyon Merkezi (SOC) ile gerçekleştirdiğimiz işbirliğine Web Uygulama Güvenlik Duvarı (WAF) çözümünüde ekleyerek olası atak senaryolarına karşı önceden koruma önlemleri almaktayız. Bu işbirliği öncesinde yaptığımız güvenlik testerinde aldığımız güvenlik puanları ile WAF hizmetinin devreye alınması sonrası yapılan güvenlik test sonuçlarında ciddi artışlar gözlemledik.

Tüm bu iş birlikteliğimiz güçlenerek devam etmekte olup Türk Telekom'u stratejik çözüm ortağımız olarak değerlendirmekteyiz.

Türk Telekom Siber Güvenlik Servis Kataloğu

Erişim Bağımlı Güvenlik Hizmetleri

- DDOS Atak Önleme
- DDOS7+
- Güvenlik Duvarı (Firewall)
- Aktif Savunma Sistemi (IPS)
- İçerik Filtreleme
- Antivirus

Paylaşımlı Güvenlik Hizmetleri

Erişim Bağımsız Güvenlik Hizmetleri

- Gelişmiş Tehdit Önleme (APT)
- Web Uygulama Güvenlik Duvarı
- Paylaşımlı SSL VPN

Dedike Güvenlik Hizmetleri

- Atanmış Siber Güvenlik Servisleri (NAC, PAM vb.)
- SiberLOG
- SiberKALE
- Penetrasyon Testi
- Danışmanlık Hizmetleri
- KVKK Danışmanlık Hizmeti
- KOBİ Temel Siber Güvenlik

Siber Güvenlik Merkezi

- 7/24 Güvenlik Olay İzleme
- SIEM Danışmanlık
- Güvenlik Test
- Risk & Uyumluluk
- Güvenlik Cihaz Yönetimi
- SOAR
- DDOS Atak Simülasyonu

1. Penetrasyon – Sızma Testi

Pentest hizmetimiz ile ağ, sistem ve uygulama katmanlarındaki teknolojilere ilişkin hataları ve zafiyetleri tespit ederek, söz konusu güvenlik açıklıklarının kötü niyetli kişiler tarafından istismar edilmesini önlüyoruz ve bu şekilde sistemlerin daha güvenli hale getirilmesini sağlıyoruz.

- Web Uygulama Testleri
- Mobil Uygulama Testleri
- İnternetüzerinden Güvenlik Testleri
- Kablosuz Ağ Testleri
- Kaynak Kod Analizi
- Masaüstü Uygulama Testleri
- Yerel Ağ İçinden Güvenlik Testleri
- Sosyal Mühendislik Testleri

TSE · OFFENSIVE SECURITY OSCP · C|EH CERTIFIED ETHICAL HACKER · MASPT

İnternet ve Yerel Ağ Üzerinden Güvenlik Testleri

Hedef sistemin ağ ve sistem altyapısına yönelik gerçekleştirilen sızma testleridir. Testler sırasında aşağıda listelenen denetimler gerçekleştirilecektir.

- Web sunucusu, DNS sunucusu, elektronik posta sunucusu, güvenlik duvarı sunucusu vb. sunucuların kontrol edilmesi,
- Sunucular üzerindeki erişilebilir servislerin belirlenmesi ve güvenlik açıklarının kontrol edilmesi
- Sunucuların kernel, yama ve sürüm bilgilerinin elde edilmesi
- İşletim sistemine ilişkin güvenlik sorunlarının ve ağ zafiyetlerinin kontrol edilmesi,
- Zafiyete yol açabilecek yapılandırma hatalarının belirlenmesi
- Paket filtreleme kurallarına ilişkin problemlerin belirlenmesi
- Sunucu yazılımlarının güncelliğinin kontrolü
- Uygulamalara yönelik güvenlik sorunlarının kontrol edilmesi
- SMTP, FTP, HTTP, HTTPS, TELNET, ICMP, RPC, NETBIOS, SNMP vb. yaygın kullanılan servisler üzerinden gerçekleştirilebilecek sızmalara karşı detaylı kontroller yapılması, sorunların belirlenmesi

WEB Uygulama Testleri

Hedef sistemde kullanılan platform ve geliştirme dillerinden bağımsız olarak gerçekleştirilen sızma testleridir. Testler sırasında aşağıda listelenen denetimler gerçekleştirilecektir.

- Bilgi toplama
- Yapılandırma ve iletişim testleri
- Kimlik yönetimi testleri
- Kimlik doğrulama testleri
- Yetkilendirme testleri
- Oturum yönetimi testleri
- Girdi kontrolü testleri
- Hata durumları ve çıktı testleri
- Kripto testleri
- İş mantığı testleri

Mobil Uygulama Testleri

Akıllı telefon ve tablet bilgisayar gibi sistemler ve bu sistemlerde çalışan uygulamalar üzerine yapılan sızma testleridir. Testler sırasında aşağıda listelenen denetimler gerçekleştirilecektir.

- Veri saklama yöntemlerinin güvenlik testleri
- Kullanıcı gizliliği ihlalinin tespitine yönelik testleri
- Kripto testleri
- Kimlik doğrulama testleri
- Oturum yönetimi testleri
- Ağ haberleşme testleri
- Kullanılan platform fonksiyonlarının kontrolleri
- İstemci tarafı kod kalitesi denetimleri

Sosyal Mühendislik Testleri

Sosyal mühendislik testleri, çeşitli yöntemlerle kullanıcıları aldatmaya yönelik testlerdir. Testler sırasında aşağıda listelenen denetimler gerçekleştirilecektir.

- Kurum jargonu
- Kurumda görevli personel isimleri kurum organizasyonu
- Kurumda uygulanan süreçler ile ilgili olarak

Kurum personele erişerek veya yetkili bir kişiyi taklit ederek personelden bilgi sızdırmaya yönelik testler yapılmaktadır.

2. KOBİ Temel Siber Güvenlik

Temel Siber Güvenlik Kutusu, KOBİ'lerin tek bir cihaz (Bütünleşik Güvenlik Cihazı) üzerinden, Güvenlik Duvarı, Aktif Savunma Sistemi (IPS), İçerik Filtreleme, Antivirüs ve Antispam hizmetlerinden aynı anda faydalanabildiği maliyet avantajı sağlayan güvenlik çözümümüzdür.

Maliyet Avantajı

Birden fazla güvenlik hizmetinin tek cihaz üzerinden karşılanması ile TL bazında tekliflendirme ve taksit imkanı

Altyapı bağımsız

Dedike konumlandırılan cihaz ile tüm altyapılara hizmet sunabilme kolaylığı

Uzman Kadro

81 ilde müşteri ihtiyacını en iyi şekilde karşılayacak hızlı kurulum ve Türk Telekom yetkin insan kaynağı ile cihaz yönetimi

Kurumumuza özel teknolojik çözümlerimiz
ile ilgili detaylı bilgi almak için
Türk Telekom satış yöneticiniz
veya 444 5 444 ile
iletişime geçebilirsiniz.

BU İŞTE BERABERİZ

Türk Telekom
Değerli Hissettirir