KPMG

Bireysel siber farkındalık araştırması

2018

kpmg.com.tr


KPMG

Siber güvenlik ve ötesi...

Teknoloji, inovasyon, dijitalleşme, büyük veri, nesnelerin interneti, siber tehditler, siber güvenlik… Son yıllarda bu kavramları o kadar çok duymamıza rağmen kamuoyunda önemi ne yazık ki halen yeteri kadar anlaşılmış değil. Teknolojinin büyük bir hızla gelişmesi ile siber dünyanın hayatımıza çok daha fazla etki ettiğini görüyoruz. Yaşantımızın en kritik noktalarında yer alarak vazgeçilmez bir hale gelen İnternet; bilgi paylaşımı, para transferleri ve fiziksel dünyanın uzaktan kontrol edilmesi için halen güvenli bir ortam olarak kabul ediliyor. Ocak 2018'de yayımlanan Google Tüketici Barometresi'ne göre yeni teknolojilerin risklerden daha fazla fırsat yarattığına inananların oranı yüzde 70. Oysa internet kullanımının beraberinde getirdiği riskler, dijital dünyamızın yanı sıra doğal yaşamımızı tehdit ederek ciddi kayıplar yaratıyor.

Evet, teknolojik gelişmeler hayatımızı her geçen gün daha da kolaylaştırıyor. Hootsuite Dijital Raporu 2018 verilerine göre Ocak 2018 itibarıyla Türkiye'de internet penetrasyonu yüzde 67 ile dünya ortalaması olan yüzde 53'ün üzerinde. İnternet kullanımı son on yılda inanılmaz bir hızla arttı ve her gün milyonlarca insan akıllı telefonlar, tabletler ve bilgisayarlar aracılığıyla güvenli varsaydığı bu alanı kullanıyor. Ocak 2017 – Ocak 2018 arasında internet kullanıcılarının sayısında yüzde 13 gibi bir artış söz konusu. Bunda elbette bağlantı hızlarındaki artış da etkili oluyor. GSMA Intelligence Q4 2017 ve Ocak 2018 Google Tüketici Barometresi'ne göre ülke nüfusuna oranla Türkiye'de mobil bağlanabilirlik yüzde 90 ve dünya ortalaması da yüzde 112.

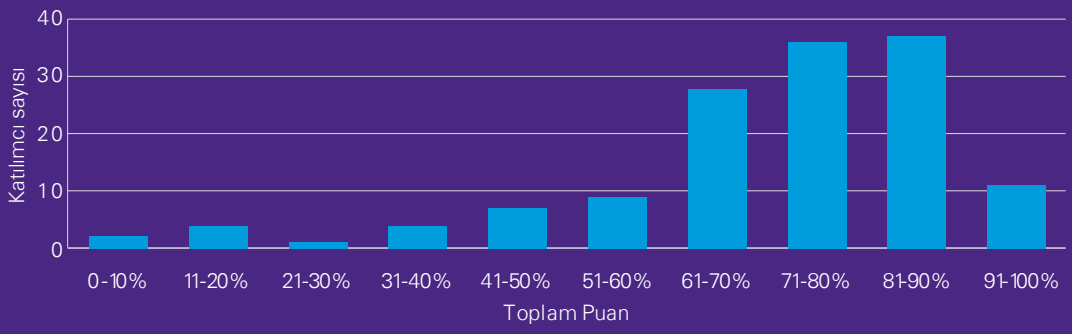
16-64 yaş internet kullanıcıları arasında yapılan bir araştırmaya göre, Türkiye'de ortalama günlük internet kullanım süresi 7 saat 9 dakika. Bunun 3 saat 24 dakikası ise mobil internet kullanımı (Global Web Index, Q2&Q3 2017). Yani günümüzün yaklaşık üçte birini internette geçiriyoruz. Elbette bu yaygın kullanım pek çok konuda farkındalığı artırdı.

Ancak aynı zamanda her gün çok sayıda siber saldırı yaşanıyor ve siber suç oranları da internet kullanımındaki artışa paralel olarak artmaya devam ediyor. Bu da beraberinde şirketlerin siber güvenlik harcamalarında artışa neden oluyor. Siber suçların dünya genelinde verdiği zararın 2021 yılına kadar 6 trilyon dolara ulaşacağı tahmin ediliyor. Siber suçlar hiç şüphesiz günümüz siber dünyasının en karmaşık sorunu…

BTK siber güvenliği şöyle tanımlıyor; siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür. Siber güvenlik, hükümetler için karmaşık sosyo-teknik bir zorluğu ifade eden küresel bir fenomen olmakla birlikte bireylerin de konuya dahil olmasını gerektiriyor.

Bugün kime sorsanız siber güvenlik ile ilgili bir şeyler mutlaka duymuştur ancak siber suçlarla ilgili farkındalık yaşanılan çevre, internet erişim oranı gibi pek çok nedene bağlı olarak kişiden kişiye değişiyor.

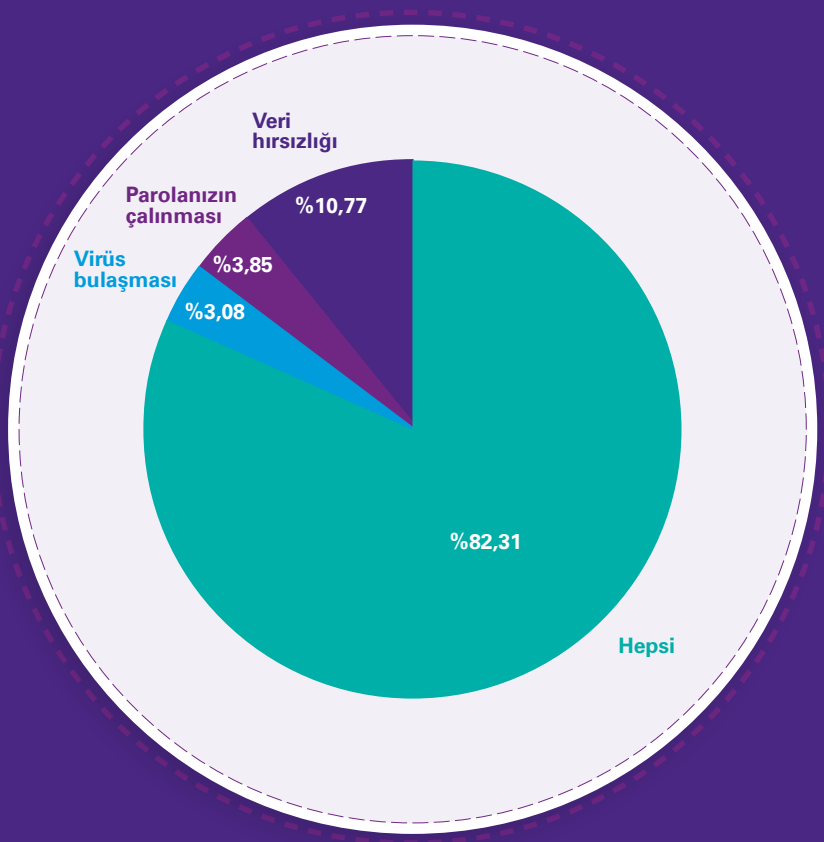
KPMG Bireysel Siber Farkındalık Araştırması'na katılanların ortalama puanı yüzde 75.



Güvenlik araştırmacılarının ortaya çıkardığı istatistiklere göre saldırganlar başarılı bir siber saldırı sonucu hedef sisteme 299 gün erişimi sürdürüyor. Yani kurumlar ele geçirildiklerini ortalama 299 gün sonra fark edebiliyor ya da engelleyebiliyor.

KPMG Bireysel Siber Farkındalık Araştırması'nın sonuçlarına göre kullanıcılar halen nelerin siber saldırı olduğu konusunda net bir bilgiye sahip değil. Siber saldırı, sadece parolalarınızın çalınması veya bilgisayarınıza virüs bulaşması olmadığı gibi kişisel verilerinizin çalınması da tek saldırı türü değil. Araştırma katılımcılarının yüzde 82'si tüm bunların siber saldırı örneği olduğunu ifade ederken, yüzde 18 ise belirttikleri seçenek dışındakilerin siber saldırı olup olmadığının farkında değil.

Aşağıdakilerin hangisi siber saldırılara örnektir?

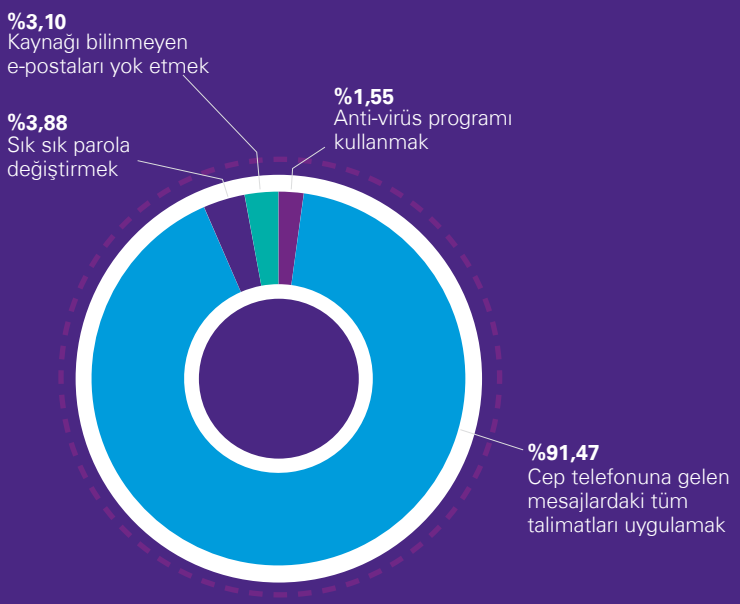


KPMG

Siber saldırıların yaratacağı risklerin en aza indirilmesi için çalışanların siber farkındalığının yüksek olması hiç bu kadar kritik öneme sahip olmamıştı. Hazırlıklı olmanın kilit noktası ise çalışanların siber tehdit ortamı hakkında yeterli bilgiye sahip olmasının yanı sıra, gittikçe karmaşıklaşan siber suçlulara karşı önlem olarak atılması gereken adımlardan haberdar olmasıdır.

Ülkemizde cep telefonu aracılığıyla gerek arayarak gerekse kısa mesaj üzerinden gerçekleşen dolandırıcılıkların gün yüzüne çıkması ve artık neredeyse her gün TV kanallarında veya sosyal medyada örneklerinin paylaşılmasıyla birlikte kullanıcılar arasında bu konuda bir bilinç oluştu. Araştırma sonuçları da bu bilincin geliştiğini ortaya koyuyor, ancak farkındalık çalışmalarına devam edilmesi gerektiği de ortada. Katılımcıların yaklaşık yüzde 92'si cep telefonuna gelen mesajlardaki tüm talimatları uygulamanın siber tehditlere karşı bir önlem olmadığını ifade ediyor. Buna karşılık katılımcılar arasında anti-virüs programı kullanmanın (%1,55), sık sık parola değiştirmenin (%3,88) ve kaynağı bilinmeyen e-postaları yok etmenin (%3,10) önlem olmadığını düşünenler de yer alıyor. Bu da bu konuda atılması gereken adımlar olduğunu gösteriyor.

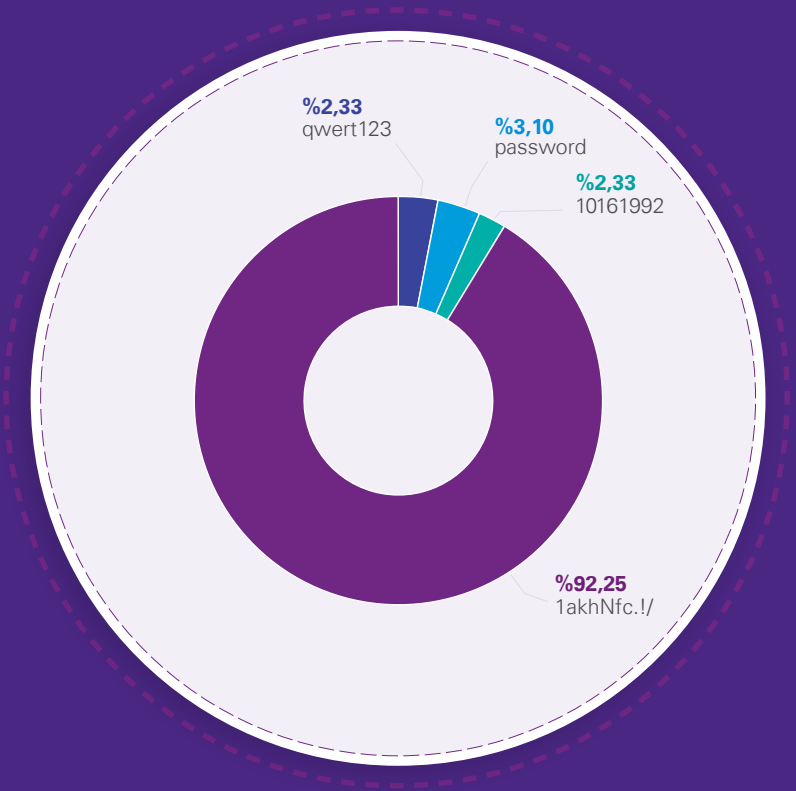
Hangisi siber tehditlere karşı bir önlem değildir?



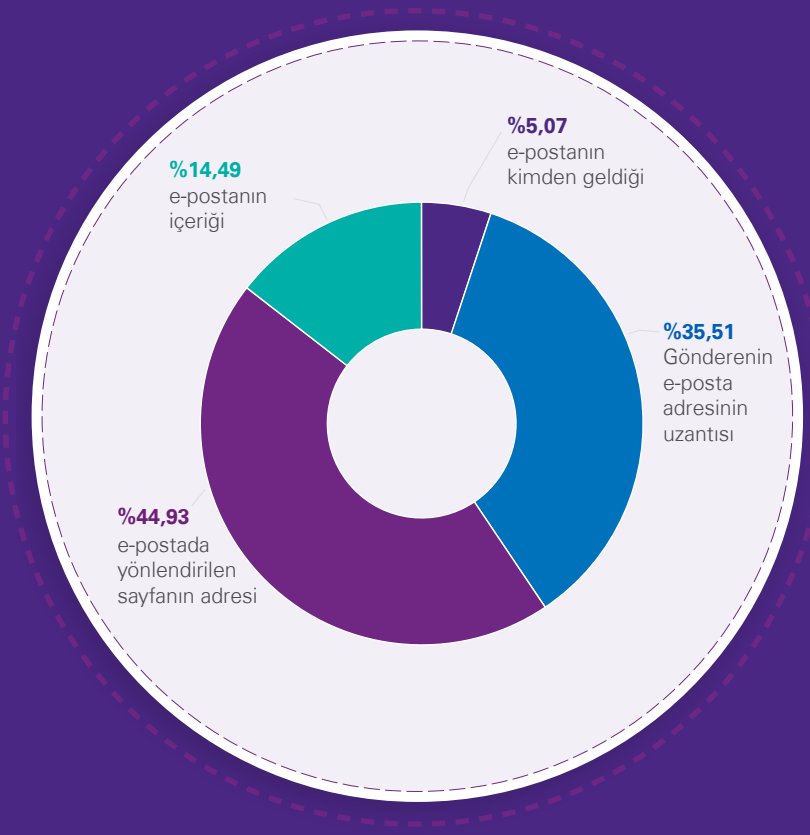
Banka hesapları, e-posta adresleri ve online işlem yapılan her mecrada kullanılan parolalar de siber suçlular açısından birer fırsat halini alıyor. Özellikle son yıllarda kamu kuruluşlarının sunucularının parolalarından, bireysel kullanıcıların mobil bankacılık veya oyun konsolu parolalarına kadar parolaların hackerlar tarafından kırılmasıyla yaşanan küresel krizler gündeme damgasını vurmaya devam ediyor. Her bir küresel krizin ardından da kullanıcıların parolalarını ne derece karmaşık bir formatta kullanması gerektiği tartışılıyor. Peki, kullanıcılar bu konuda gerçekten duyarlı davranıyor mu? Parolalarını seçerken yeteri kadar karmaşık ve zor kırılacak kombinasyonlar kullanıyorlar mı?

Araştırmada en doğru parola kombinasyonunun nasıl olması gerektiğini sorduğumuz katılımcılardan yüzde 92'si en karmaşık kombinasyonu seçerek farkındalığını ortaya koyarken, doğum tarihi veya sadece ikili kombinasyonlardan oluşan parola kullanımının uygun olduğunu ifade edenlerin oranının toplamı yüzde 8 ile hiç de azımsanmayacak bir oranda.

Aşağıdakilerden hangisi kullanılması gereken doğru parola örneğidir?



Aşağıdakilerden hangisi gelen e-postanın oltalama (phishing) mesajı olduğunu gösteren en büyük unsurdur?



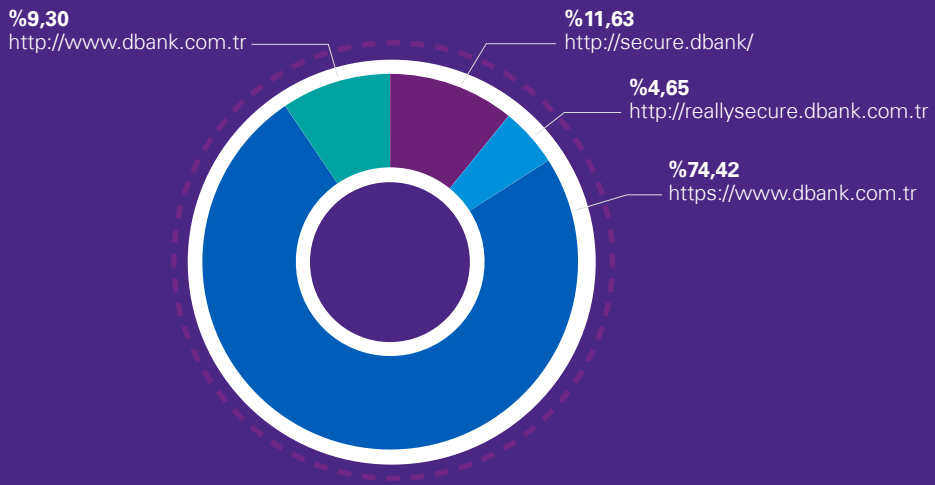
Karmaşık parola kombinasyonları elbette kullanıcıları korumak için yeterli olmuyor. Son yıllarda yayımlanan istatistiklere göre internet kullanıcılarına yönelik saldırıların yüzde 91'i oltalama (phishing) e-postaları üzerinden gerçekleştiriliyor. Kullanıcılar veya şirketler tarafından raporlanan oltalama vakalarının bir güvenlik ihlaline dönüşmesinin temel sebebi, kullanıcıların bilerek veya yanlışlıkla yaptıkları işlemlerden kaynaklanıyor. Temel BT güvenlik ihlallerinin çoğunluğu insan hatasından kaynaklanıyor; dolayısıyla başta şirket çalışanları olmak üzere tüm kullanıcıların eğitilmesi ve farkındalıklarının artırılması siber saldırı ve dolandırıcılıkların zararlarının minimuma indirilmesine yardımcı olacaktır.

Araştırma sonuçlarına göre katılımcıların yarısından azı gelen e-postada yönlendirilen adresin (URL) söz konusu e-postanın oltalama mesajı olduğunu gösterdiğini biliyor. Bu da katılımcıların yarısından fazlasının oltalama e-postalarından dolayı saldırı riski altında olduğunu gösteriyor.

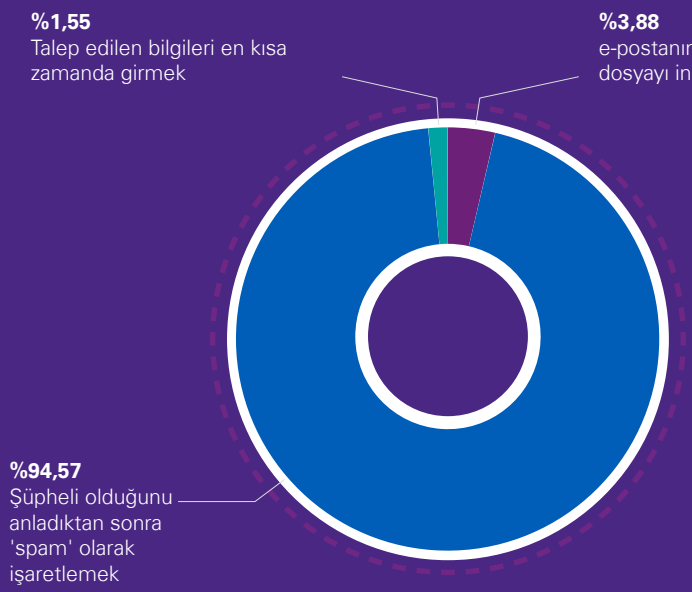
Bilindiği gibi http protokolü yani 'Hypertext Transfer Protocol - Hiper Metin Protokolü' olmadan, herhangi bir internet sitesine bağlanmak mümkün değil. Https de tıpkı http gibi sunucular arasında güvenli bağlantı kurmayı hedefleyen bir protokol. Https de aynen http gibi herhangi bir internet sitesine bağlanmak istendiğinde bu talebini bağlanmak istenen sunucuya ileten bir köprü görevi görüyor. Https protokolünün açılımı 'Secure Hypertext Transfer Protocol - Güvenli Hiper Metin Protokolü'. Https protokolü ile bir siteye bağlanılıyorsa, geliştirilen güvenlik önlemleri daha yoğun olarak aktarılıyordur ve bu bağlantıda kullanıcı bilgileri asla başkaları tarafından okunamaz.

Araştırma katılımcılarının yaklaşık yüzde 75'i güvenli web sitesi örneğinin https protokolü ile başlaması gerektiğini belirtirken, yüzde 25 gibi büyük oranda katılımcı güvenli web sitesi adresi konusunda bilgi sahibi değil.

Aşağıdakilerden hangisi daha güvenli bir web sitesi örneğidir?



Sizden banka bilgilerinizi talep eden ve ekinde “acil_okuyunuz.vbs” adında dosya bulunan bir e-posta gördüğünüzde ne yapmalısınız?



Oltalama saldırılarında alınması gereken önlemler konusunda da araştırma katılımcılarının yüzde 95’i gelen e-postanın şüpheli olduğunu anladıktan sonra ‘spam’ olarak işaretlemek gerektiğinde hemfikir. Bu önlemin tüm kullanıcılar tarafından bilinmesi muhtemel saldırıları önemli ölçüde engelleyecektir.

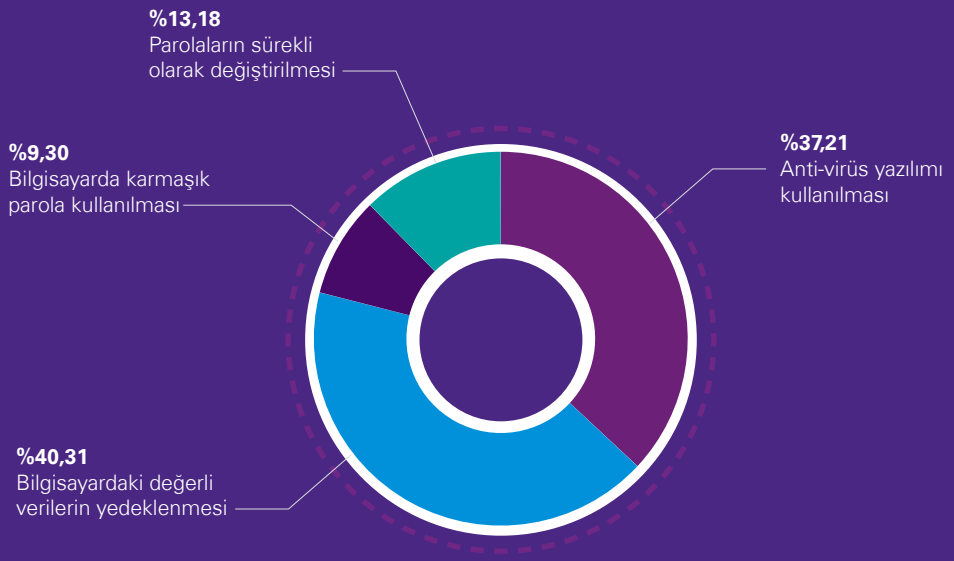
Oltalama e-postalarındaki yönlendirmelerin uygulanması sonucunda kullanıcılar çeşitli risklerle karşı karşıya kalıyor. Bunlardan en çok görülen ve hem bireysel kullanıcılara hem de şirketlere zarar verenlerin başında fidye yazılımları geliyor. Siber suçluların son zamanlarda gözde para kazanma yolu olan fidye yazılımları ile gerçekleştirilen saldırılarda suçlular ağ ve/veya ilgili cihaz üzerinde buldukları hassas dosyaları şifreleyerek para karşılığı parolayı çözmeyi talep ediyor.

Trend Micro’nun 2017 Güvenlik Raporu’na göre, 2016’dan 2017’ye kadar yeni nesil fidye yazılımlarında yüzde 32’lik bir artış oldu. 2016 yılında fidye yazılım saldırısına maruz kalan ülkeler arasında Avrupa’da ilk sırada olan Türkiye, Trend Micro’nun araştırmasına göre 2017’de de bölgesel birinciliği diğer ülkelere bırakmadı. Avrupa ülkelerinin toplam fidye yazılım saldırısına uğrama yüzdesi küresel rakamın yüzde 23,65’ini oluştururken; Türkiye yüzde 15,85’lik oranıyla, Avrupa ülkeleri arasında ilk sıraya yerleşti. Fidye yazılım saldırılarında ise Türkiye, dünyada 6. ülke oldu. Bu tür saldırıların yüzde 94’ü e-posta üzerinden gerçekleşti ve 5 milyar dolara yakın maddi kayba neden oldu.

Fidye yazılımlar ile gerçekleştirilen saldırılara karşı alınabilecek en etkili önlem ise yedekleme. Saldırı gerçekleştikten sonra dosyaları serbest bırakmak için talep edilen ödemeyi gerçekleştirmekten başka alınabilecek iyi bir aksiyon ne yazık ki bulunmuyor. Ne kadar güvenlik önlemi alınırsa alınsın, bir saldırganın ağa sızarak dosyaları şifrelemesini engellemek hiçbir zaman yüzde yüz mümkün değil. Ancak değerli verilerin yedekleri organize ve güvenli bir şekilde tutulması halinde, dosyalar şifrelense dahi en son yedekten kolaylıkla geri dönüş sağlanabilir. Peki, kullanıcılar bu önlemlerden ne kadar haberdar?

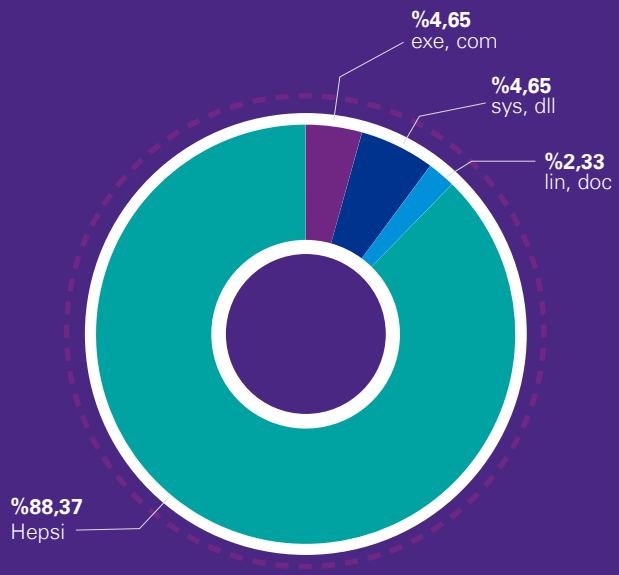
Araştırma katılımcılarının sadece yüzde 40'ı, bilgisayarlarındaki değerli verileri yedeklemenin en etkili önlem olduğunun bilincinde.

Fidye (ransomware) yazılımları için alınması gereken en etkili önlem hangisidir?



Oltalama e-postaları, kullanılan harici diskler veya herhangi bir başka yöntem ile dosyalara virüs bulaşma ihtimali var. Virüsler araştırmaya katılanların yüzde 88'inin de belirttiği gibi her türlü uzantılı dosyaya bulaşabilir.

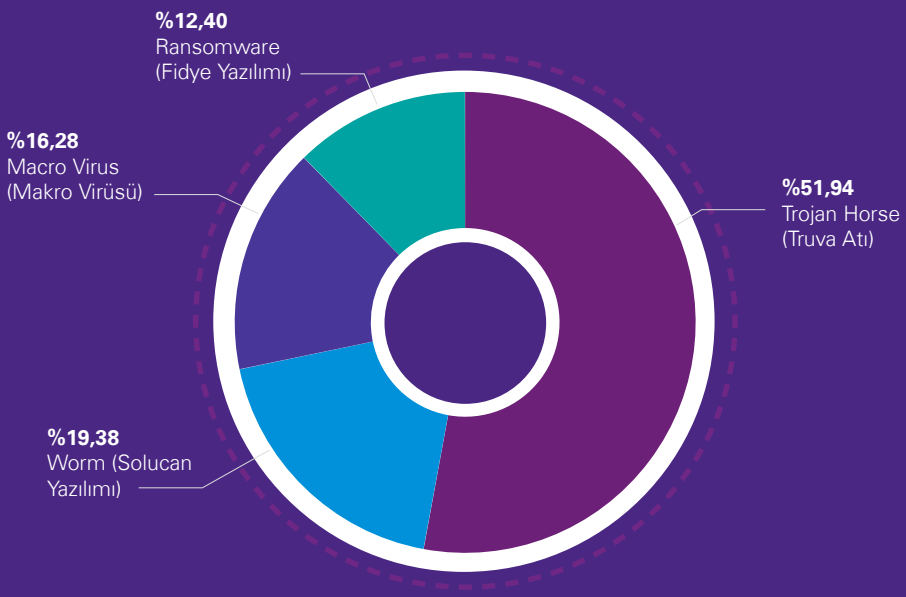
Virüsler hangi uzantılı dosyalara bulaşabilir?



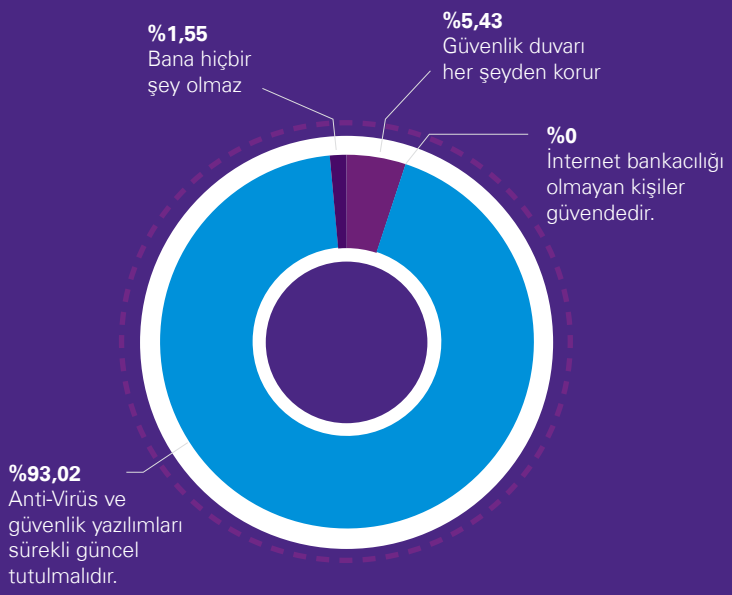
Dosyalara virüs bulaşmasının önüne geçmenin elbette çeşitli yöntemleri var. Yeter ki bu konuda alınması gereken önlemler hakkında kullanıcıların bilgisi olsun, ne yapmaları gerektiğini bilsinler. Bunlardan biri de reklam gibi görünen kimi mesaj ve e-postalar. Global Web Index Q2&Q3 2017 raporuna göre, reklamları engelleme araçlarını kullananların oranı yüzde 40. Bu da kullanıcıların yarısından fazlasının yararlı görünmekle birlikte çalıştırıldığında bilgilere veya programlara zarar veren yazılımlara açık olduğunu gösteriyor.

Araştırma katılımcılarının sadece yarısı bu yararlı gibi görünen ancak aslıdan zararlı olan yazılımların neler olduğunu biliyor.

Kullanıcı için yararlı görünmekle birlikte çalıştırıldığında bilgilerinize veya programlara zarar veren yazılımlara ne ad verilir?



Aşağıdaki ifadelerden hangisi doğrudur?



Sonuç

Siber saldırıların ve hatta siber savaşların sıkça görüldüğü siber dünyaya her gün daha da bağımlı hale geliyoruz. Bu da pek çok riski beraberinde getiriyor. Hackerların kişisel sağlık verilerinden, otonom araçlara ve uçuş kontrollerine kadar her alana ulaşma ihtimali var. Yani Fast & Furious 8'de kriminal deha ve siber terörist Cipher'ın New York'ta tüm otomobillerin elektronik sistemlerini ele geçirip Rusların nükleer silah kumandalarını ele geçirmeye çalışmasının bir film senaryosundan gerçeğe dönüşmeyeceğinin bir garantisi yok…

Bireylerin siber saldırılardan korunmasının temelinde elbette eğitim yer alıyor. Büyüklük, sektör ve coğrafyadan bağımsız olarak siber suçlar sınır tanımıyor. Kullanıcıların eğitilmesi ve farkındalıklarının artırılması siber riskleri fark etmelerini, engellemelerini ve kendilerini siber saldırılara karşı korumalarını sağlayacaktır. Internet kullanımının 9 yaşına kadar indiğini göz önünde bulundurursak, okul müfredatlarına siber güvenlik farkındalığı oluşturulmasını sağlayacak dersler konulması önemli bir katkıda bulunabilir. Elbette bunun yanı sıra sivil toplum kuruluşları, kamu kurumları ve özel sektördeki şirketlerin çeşitli farkındalık ve destek programları uygulamaları da etkili olacaktır.

İletişim:

Sinem Cantürk
Bilgi Sistemleri Risk
Yönetimi Bölüm Başkanı,
Şirket Ortağı
scanturk@kpmg.com

Detaylı bilgi için:
KPMG Türkiye
Kurumsal İletişim ve
Pazarlama Bölümü
tr-fmmarkets@kpmg.com

İstanbul
İş Kuleleri Kule 3 Kat 2-9
34330 Levent İstanbul
T : +90 212 316 6000

Ankara
The Paragon İş Merkezi Kızılırmak Mah.
Ufuk Üniversitesi Cad. 1445 Sok. No:2
Kat:13 Çukurambar 06550 Ankara
T: +90 312 491 7231

İzmir
Heris Tower, Akdeniz Mah. Şehit Fethi Bey
Cad. No:55 Kat:21 Alsancak 35210 İzmir
T: +90 232 464 2045

kpmg.com.tr
kpmgvergi.com