LABRIS SOC RAPORU

/// 2016
SİBER GÜVENLİK RAPORU

/// 2017
SİBER GÜVENLİK ÖNGÖRÜLERİ

Labris NETWORKS

LABRIS
NETWORKS INC.

TELİF HAKKI

FERAGATNAME

Labris Networks bu raporda yer alan bilgilere ilişkin hiçbir bir şekilde beyan veya garanti vermez. Doğrudan veya dolaylı olarak bu raporda yer alan bilgilerin kullanımından kaynaklanan veya kaynaklandığı iddia edilen hiçbir eylem için sorumluluk kabul edilmez

Labris Networks, 2002 yılından bu yana, global olarak kanıtlanmış ürünleriyle Ar-Ge odaklı ve hızla büyüyen bir ağ güvenlik çözümleri sağlayıcısı olmuştur. Labris Networks, LABRIS UTM, Labris LOG ve Harpp DDoS Mitigator cihazlarında Güvenlik Duvarı/VPN, Web Güvenliği, E-posta Güvenliği, Yasal Dinleme ve Erişilebilirlik Koruma çözümlerini içeren geniş ürün yelpazesi aracılığıyla en üst düzey ağ güvenliğini garanti etmektedir. Gelecek nesil çözümler, sızmalar, virüs, spam, zararlı yazılım ve erişilebilirlik saldırılarına karşı bir akıllı kalkan sağlayarak her türlü gerçek zamanlı tehditleri, uygulamaları tespit etmek, tanımlamak üzere geliştirilmiştir.

Labris Networks ürünleri çeşitli topolojiler ve dağıtım senaryolarına sahip tüm boyutlardaki ağları korur. Labris FLEX donanım yazılımı seçenekleri sayesinde kullanıcılar ihtiyaç duydukları güvenlik yazılımının yanı sıra Kablosuz Misafir Kimlik Doğrulaması, Ayrıntılı İnternet Raporlama, Yasal Dinleme ve Günlükleme gibi ekstra modülleri alma ayrıcalıklarına sahiptir. Müşteri odaklı, geleceğe yönelik ve esnek bir yaklaşıma sahip olan Labris Networks, yazılımlarını Bulut içerisinde de sunmaktadır.

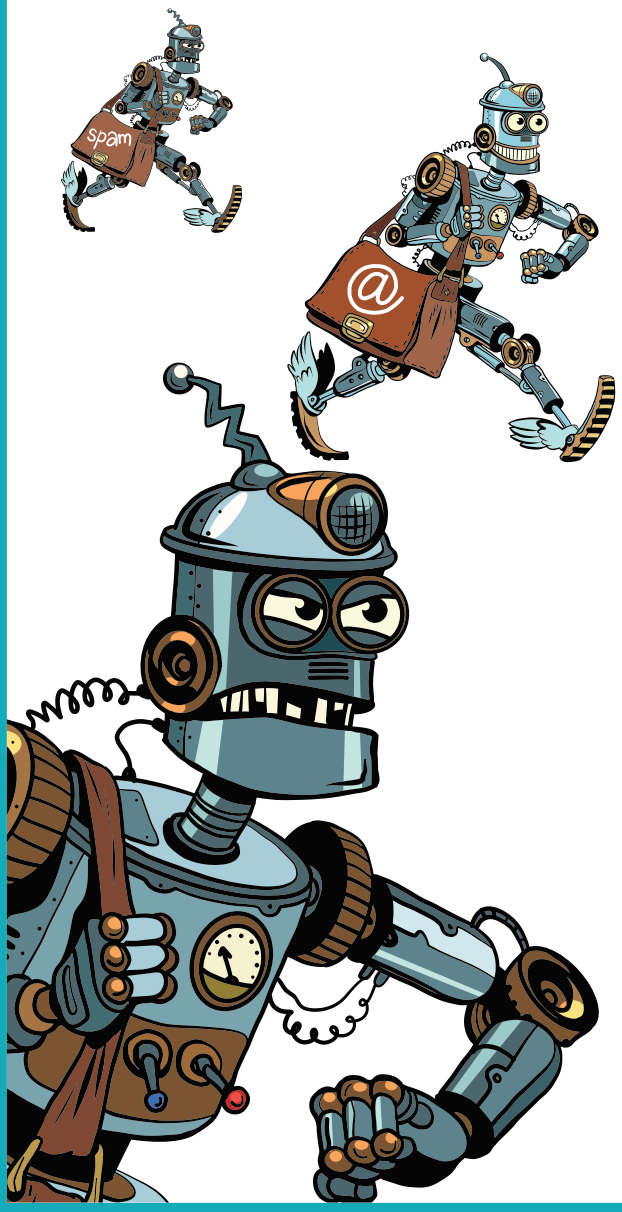
20'den fazla ülkede hızla büyüyen küresel ağlarda işlemleri olan Labris ürünleri, işletmeleri, markaları, devlet kurumlarını, hizmet sağlayıcıları ve kritik altyapıları korumaktadır.

Dünya çapındaki ortakları ile Labris Networks, çok dilli Küresel Destek Merkezi ile en iyi satış sonrası desteği sağlayarak en yüksek düzeyde müşteri memnuniyeti ve sadakatine kendisini adamıştır. Hızla büyüyen küresel bir oyuncu olan Labris müşterilerine en uygun maliyetle en üst düzeyde güvenlik sunmaktadır. Ankara, Türkiye merkezli olan Labris Networks, Avrupa, Orta Doğu, Kuzey Afrika, Kafkaslar, Orta ve Güneydoğu Asya'ya hizmet veren ofislere sahiptir.

2016

SİBER GÜVENLİK TEHDİTLERİ

SANİYEDE 200 GIGABIT



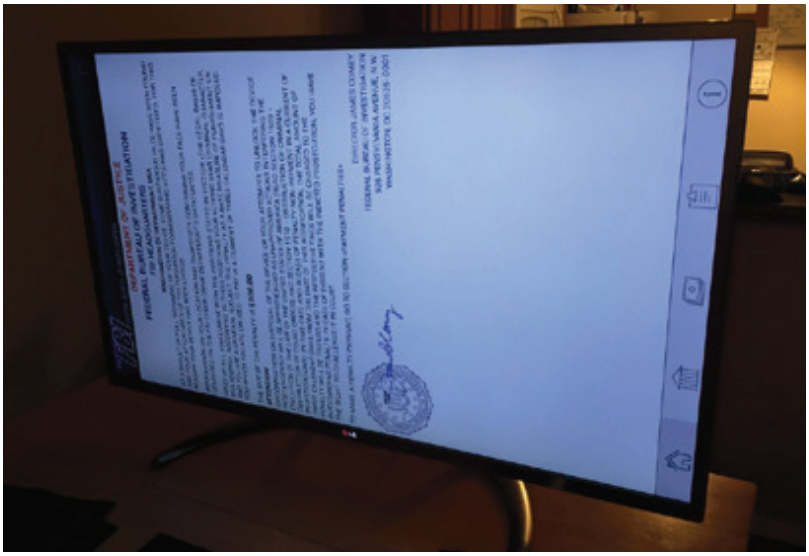
İSS'ler Artık Kritik Altyapılar

2016 yılı Temmuz, Eylül ve Ekim aylarında Hint Internet Servis Sağlayıcıları (İSS) yoğun DDoS saldırılarına maruz kaldı. Saldırının büyüklüğü saniyede yaklaşık 200 gigabitti. Bilişim suçları avukatı Prashant Mali, bütün kamu ve ticari kuruluşların internete İSS'ler üzerinden bağlandığını ve bu nedenle İSS'lere yapılan bir saldırının, aslında ulusa yapılan bir saldırı anlamına geldiğini söyledi.

2016'nın son çeyreğinde, İngiliz TalkTalk, İngiltere postanesi, Kcom ve Alman Deutsche Telekom saldırı aldı ve saldırılar süresince 100.000'lerce müşterinin internete erişimi kesildi. Hatta TalkTalk, gerekli saldırı önleme tedbirlerini almadığı gerekçesi ile İngiliz düzenleme otoritelerince yüklü miktarda ceza aldı.

Mobil, Nesnelerin İnterneti botnetleri ve Daha Fazla DDoS

21 Ekim 2016'da internet altyapı DNS sağlayıcısı DYN, DDoS saldırıları ile hedeflendi. Yaklaşık 1.2 Tbps olarak duyurulan saldırı tarihin en volümetrik DDoS saldırısı olarak kayıtlara geçti. Saldırı DYN'nin yanında onların hizmet verdiği Twitter, Paypal, CNN, Spotify, Reddit, eBay, Airbnb, HBO ve NYTimes gibi birçok siteyi etkiledi. Saldırı birçok IoT cihazından oluşan botnetten geliyordu. Kamera, ev internet cihazları, bebek izleyicileri gibi birçok cihaz Mirai zararlı yazılımı ile enfekte olmuşlardı.

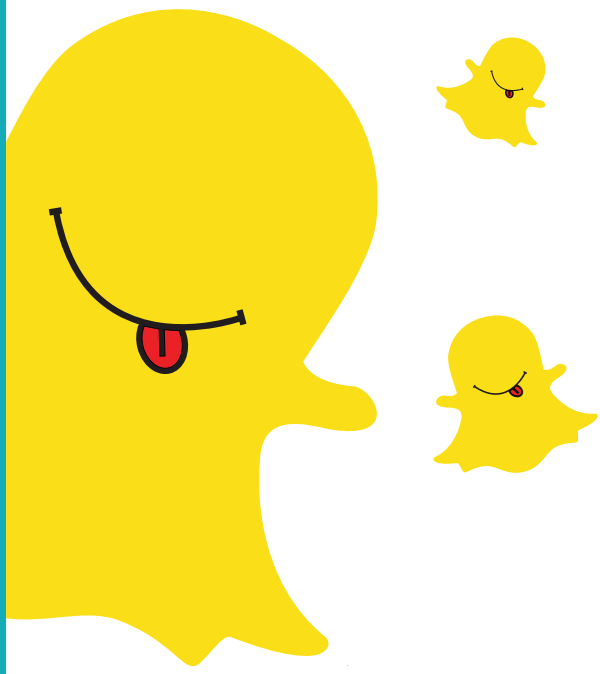


Aralık 2016'da bir akıllı televizyonun Android Locker isimli bir fidye yazılım ile enfekte olduğu gözlendi. Bir twitter kullanıcısı akıllı televizyonunun FBI'dan gelen bir uyarı gibi görünen bir uyarı ile kilitlendiğini yayınladı. Televizyonun resetleme menüleri dahi kilitlenmişti.

Sosyal Mühendislik ve Hedefli Oltalama Saldırıları

WORLD ANTI-DOPING AGENCY

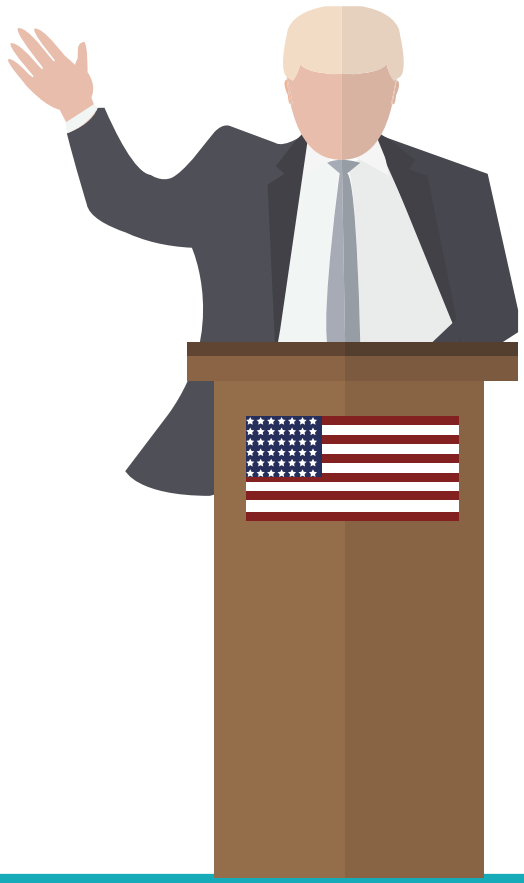
Dünya Anti-Doping Ajansı (WADA), Anti-Doping Yönetim Sistemi (ADAMS) veri tabanına Rus saldırganlar tarafından yasadışı yollarla erişildiğini duyurdu. Saldırganlar, sisteme erişimi, 2016 Rio Olimpiyatları için oluşturulmuş Uluslararası Olimpiyat Komitesi (IOC) hesabına yönelik başarılı bir olta saldırısı sonucu kazandılar. Saldırganlar Olimpiyat oyunlarına olan yoğun ilgiden istifade ederek, kurbanlarını klasik bir sosyal mühendislik saldırısı ile oyuna getirdiler. Çalınan verinin bir kısmını yayınlayan saldırganlar, Amerikalı sporcular, Simone Biles, Elena Delle Donne, Serena ve Venus Williams'ı WADA'nın yasaklamış olduğu ilaçları kullanmakla suçladı.



Bir Seagate çalışanı, Seagate CEO'sundan geliyor gibi görünen ve tüm Seagate çalışanları için 2015 vergi formlarını talep eden bir olta e-postası ile kandırıldı. Bunun sonucunda şirket çalışanlarının sosyal güvenlik numaraları, maaşları ve diğer kişisel bilgilerini içeren verileri çalındı.

SEAGATE

Şubat 2016'da, bir Snapchat çalışanı, Snapchat CEO'su Evan Spiegel'den geliyor gibi görünen ve çalışanların maaş bilgilerini talep edip, ele geçiren bir olta saldırısı tarafından kandırıldı.



Politik Saldırılar

Siber saldırıların hedefi ABD başkanlık seçimleriydi. 22 Temmuz 2016'da, WikiLeaks, Demokratik Ulusal Komite (DNC) personeli tarafından gönderilen veya onlar tarafından alınan 20.000 e-posta yayınladı ve 7 Ekim 2016'da WikiLeaks, Hillary Clinton'ın kampanya yöneticisi John Podesta tarafından gönderilen veya alınan e-postalar serisi yayınlandı. ABD istihbaratına göre, bu saldırılar seçimleri Donald Trump lehine değiştirmişti. Bu saldırılar sonucunda ABD, 35 şüpheli Rus diplomatı sınır dışı etti ve iki Rus tesisini kapattı.

Mobil Uygulamalar ve Mobilde Fidye Yazılım

Bu yıl, Android uygulamaları için resmi pazar olan Google Play'in fidye yazılım uygulamaları barındırdığı tespit edildi. Uygulama Charger olarak, bunu içeren diğer bir uygulama ise EnergyRescue olarak adlandırılmıştı. Uygulama yüklendikten sonra çok fazla izin istiyor, bu izinler verildiğinde ise cihazı kilitleyerek fidye isteyen bir mesaj görüntülüyordu.

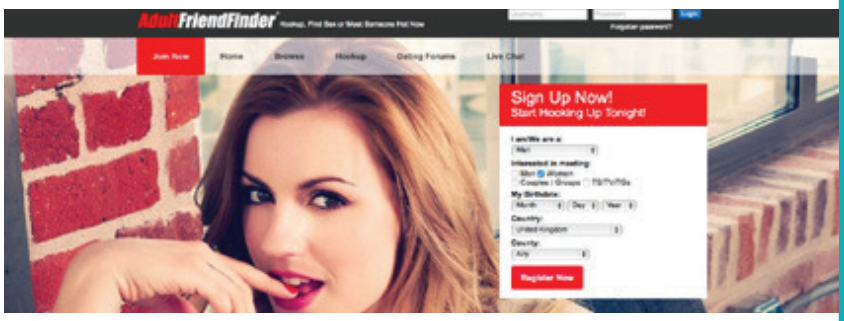
1 MİLYAR YAHOO HESABI ÇALINDI

Mobil platformlar, sadece fidye yazılım ile değil, ana kullanıcı (root) hakkı alan zararlı yazılımlar ve bir takım diğer truva atları ile de karşılaştı.

Google uygulama kabul politikalarında bir değişiklik yapacağını duyurdu. Bu değişiklik ile yetkisiz veri toplama ve işleme yapan uygulamaları engellemeyi planlıyor.

Genel olarak, fidye yazılım türleri, düzenlemeler ve olaylar 2016 yılının başından sonuna kadar olan sürede iki katına yükseldi.

Şirketleri batıran, yöneticileri işinden eden ve intiharlara sürükleyen veri sızıntıları



Adultfriendfinder bu yıl yine saldırıların hedefindeydi. 15 milyondan fazla "silinmiş" hesap da dâhil olmak üzere 412 milyondan fazla hesap bu saldırı sonucu sızdırıldı. Sızdırılan veriler, kullanıcı adlarını, e-posta adreslerini ve son ziyaret tarihi ile şifreleri içeriyordu.

Eylül 2016'da Yahoo, 2014 yılında şirketten en az 500 milyon Yahoo hesabının çalındığını belirten bir veri ihlalini açıkladı. Sadece 3 ay sonra Aralık 2016'da, Eylül ayında açıklanan büyük siber güvenlik olayından ayrı olarak Yahoo; 2013 yılına dayanan bir başka büyük güvenlik ihlali yapıldığını açıkladı. Bu sefer ise isimler, e-posta adresleri ve şifreler de dâhil olmak üzere 1 milyardan fazla hesap bilgisinin çalındığı bildirildi.

Myspace saldırıya uğradı ve Myspace üyelerine ait 427 milyon şifre ve 360 milyon eposta adresi internete düştü.

2016'daki diğer büyük veri ihlalleri ise şu şekilde oldu: Weebly 43 milyon, Berkeley Üniversitesi 80.000, Tumblr 65 milyon, Opera 2 milyon.

Seçmen Bilgileri İfşası

93.4 milyon Meksikalı seçmenin bilgileri açığa çıkarıldı ve bulut sunucular vasıtasıyla indirilebilir hale getirildi.

55 milyon Filipinli seçmene ait pasaport ve parmak izi gibi hassas bilgiler ifşa edildi.

Diğer Önemli Olaylar

SWIFT küresel bankacılık ağı aleyhinde sürekli siber saldırılar gerçekleştirildi. Bu saldırılar sonucunda, 2016 yılı şubat ayında Bangladeş merkez bankasından 81 milyon dolar çalındı. Ayrıca Aralık ayında, Akbank ve farklı 2 Türk bankası da bu ataklara maruz kaldı ve 4 milyon dolar çalındı.

Bir kısım Telegram sohbet servisi hesabı ele geçirildi. Milyonlarca İranlı Telegram kullanıcısı saldırganlar tarafından ifşa edildi. Ataklar, SMS yoluyla iletilen yetkilendirme kodlarını ele geçirilerek başarıya ulaştı. Bu kodlar, saldırganların yeni ve eski mesajları okumalarına olanak sağladı.

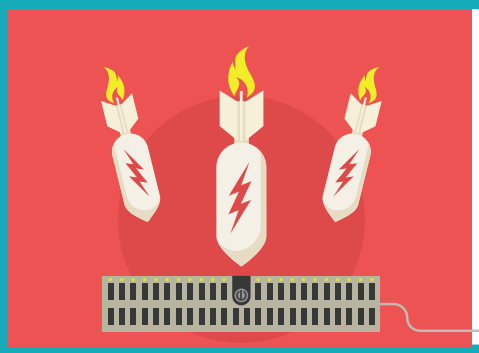
Ağustos 2016'da, Oracle'ın Micros POS sisteminin ele geçirildiği tespit edildi. MICROS, dünyanın en büyük PoS tedarikçilerinden birisidir. Saldırganlar MICROS müşteri destek portalını ele geçirdi ve destek web sitesinde oturum açan müşterilerin kullanıcı adlarını ve şifrelerini ele geçirdi. Sonuç olarak bu durum, saldırganların POS cihazlarına erişerek kredi kartı bilgilerini çalabilmesine ortam oluşturdu.

1.5 milyon Verizon Enterprise müşterisinin iletişim bilgileri, saldırganların güvenlik açıklarından faydalanması sonucunda ele geçirildi.

Şubat 2016'da Hollywood Presbiteryen Tıp Merkezi, EMR'ların ve hastanenin e-posta sisteminin kilidini açmak için 17.000 dolar fidye ödedi.

2017

SİBER GÜVENLİK ÖNGORÜLERİ



DDOS Ataklarında Yeni Rekorlar

2016 yılında, 1 terabit/saniye bant genişliğine ulaşan, dünyanın şimdiye kadar gördüğü en büyük DDOS saldırısına şahit olduk. Bu yıl, özellikle kritik altyapıları hedef alan, hatta bütün bir ülkenin ya da bir bulut altyapı sağlayıcısının internetini çökertebilecek DDOS saldırıları olacağını öngörüyoruz.

Nesnelerin İnterneti DDOS ataklarını büyütmeye devam edecek

Nesnelerin interneti her geçen gün daha güvenli hale gelse de, saldırganlar da daha önce pek bilinmeyen gömülü cihazlar hakkında bilgi edinmeye başladılar. 2016 yılında tahmin ettiğimiz gibi, şimdiye kadar görülmüş en büyük DDOS saldırısı, Mirai adı verilen kötücül yazılım bulaşmış olan internet özellikli cihazlar kullanılarak gerçekleştirildi. Bu yıl da bu cihazların DDOS saldırı tipinde yoğun olarak kullanılacağını düşünüyoruz.

Sosyal mühendislik ve Oltalama (Phishing) Popülerliğini Devam Ettirecek

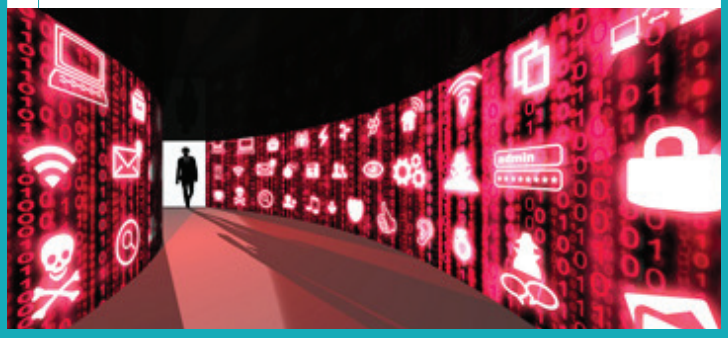
Siber güvenlik alanı sürekli olarak güçleniyor ve gelişiyor. Fakat çalışanlar hala siber güvenliğin en zayıf halkası durumunda. Seagate, Snapchat, World Anti-Doping Agency gibi büyük şirketler/yapılar bile çalışanları yüzünden bu tarz saldırılardan etkilendiler. Ayrıca sosyal mühendislik saldırıları her zaman büyük bir problem olarak karşımıza çıkıyor ve bu sene de problem olmaya devam edecek.

Politik Siber Saldırılar Daha Sık Görülecek

Amerika'daki seçim kampanyalarında görüldüğü üzere siber saldırılar ile özel bilgilerin sızdırılması seçmenlerin kararında önemli bir etken. Tahminimiz bu sene de Wikileaks tarzı yayınlarla politikacılara ait gizli dokümanların sızmasında artma olacağı yönünde.

Yapay Zekâ ve Siber Tehdit Bilgisi

Saldırganlar; zeki ve kendilerini gizlemekte süratli olduklarından siber tehditler her an değişmekteler. Bu sebeple; bir saldırganın daha önceki aktivitelerinden çıkarım yaparak öğrenen yapay zekâ ve makina öğrenmesi yöntemleri; sabit kural tabanlı ölçümlerle karar veren yöntemlerden daha faydalı olacak.



İHA Hırsızlığı

Yakın zamanda Amazon ve UPS, paket taşımacılığında mini İHA'lara (drone) görev verecekleri projelerini açıkladılar. Diğer taraftan hali hazırda birçok amatör ve profesyonel görüntü yönetmeni, pahalı ve gelişmiş mini İHA'ları fotoğraf çekme ve kamera kayıtları için kullanmaktadır. İşte bu araçları havada yakalamak, yakalanmış bu araçları ya da taşıdıkları kargo paketlerini çalıp satmak siber suçlular için cazip gelebilir. İçinde bulunduğumuz yıl ve önümüzdeki yıllarda, İHA sinyallerini hedefleyen uzaktan saldırılar ve araç hırsızlıklarıyla karşılaşacağımızı tahmin ediyoruz.

Siber Sigortada Talep Artacak

Devlet yönetimleri bilgi gizliliği konusuna gün geçtikçe daha çok önem vermektedirler ve işletmeleri gerçekleşen bilgi gizliliği ihlallerinden mesul tutmaya başlamaktadırlar. Siber sigorta pazarı 2012 - 2015 yılları arasında hacmini iki katına çıkararak 2 milyar dolar seviyesine ulaşmıştır. Siber saldırılar ve bu saldırıların maliyetleri artmakta olduğundan, siber sigorta pazarının da genişleyeceğini tahmin ediyoruz.

Fidyeci Yazılımların Gelişimi

2017 yılında da fidyeci yazılımların, yeni ve daha zeki aileler oluşturarak, büyük bir problem olarak kalacağını tahmin ediyoruz. Sık aralıklarla güncel yedekler alan kurumlar, kolaylıkla yedeklerine dönebildiklerinden fidyeci yazılımların ağına düşmemektedir. Bu yüzden fidyeci yazılımları kodlayanlar; meseleye daha zekice yaklaşarak öncelikle yedek alınan ortamı bulup, yedekleri kullanılamaz duruma getirdikten sonra kullanıcı dosyalarını şifrelemeye çalışmaktadırlar. Yerel ortamlarda saklanan yedekleri kullanılamaz duruma getirdikleri gibi bulut ortamında saklanan yedekleri de etkilemeye çalışmaktadırlar. Yakın zamanda fidyeci yazılımların solucan yazılım karakteri göstererek, girdiği bir ağ içindeki tüm cihazlara kendisini kopyalayacağını da tahmin ediyoruz. Talep edilen fidyenin program tarafından otomatik olarak, standart bir ev kullanıcısı için farklı, bir şirket kullanıcı bilgisayarı içinse farklı belirleneceği fidye yazılımlar bekliyoruz.

Servis olarak Güvenlik ve Güvenlik Operasyon Merkezleri

Küçük ve orta ölçekli işletmelerin BT bölümleri ve güvenlik odaklı uzmanları kısıtlı olduğu için sıklıkla siber saldırılara maruz kalmaktalar. Orta ve büyük ölçekli firmalar ise gelişmiş seviyedeki siber saldırılara hedef olmaktalar. Bu tip saldırıları azaltmak ise bir bilgi birikimi ve daha da önemlisi tecrübe istiyor. Bu ise her işletmede, işletme içerisinde sağlanabilecek bir şey değil. Sonuç olarak, ağ güvenliği ile ilgili dışarıdan kaynak tedarik talebinin artacağını bekliyoruz.

Bilinen Zayıflıkların İstismar Edilmesi

Her gün yeni zayıflıkların doğacağı ve bu zayıflıkların istismar edilmeye devam edeceği gerçeği yeni bir durum değil. Bu yüzden, güvenlik güncellemelerini ve tespit edilen zayıf noktaların onarımını yapmak zorlayıcı bir görev olmaya devam edecek.

Avrupa Genel Veri Koruma Yönetmeliği

Önümüzdeki yıl, AB'nin Veri Koruma Yönetmeliği(GDPR) yürürlüğe girecek ve buna hazırlık için çoğu çalışma 2017 yılı içinde tamamlanacak. Özellikle AB vatandaşlarının kişisel verilerinin edinimi, işlenmesi ve depolanması işlemleri ve bunların güvenliği, ilgili kurum ve şirketlerde irdelenecektir.

Siber Güvenlik İnsan Kaynağı

Siber Güvenlik insan kaynağı az, eğitilmesi ve profesyonel bilgi ve deneyim kazanması ise hiç kolay değil. Ancak diğer yandan beklentiler ise yüksek. Disiplinler arası mesleki pozisyon ihtiyaçları, teknik olmayan siber güvenlik uzmanlarını da gerektirecektir.