CISCO™

2014

YARIYIL GÜVENLİK RAPORU

JEOPOLİTİK OLAYLAR VE DOĞAL AFETLER SANAL DÜNYAYI DA ETKİLİYOR

Cisco 2014 Yarıyıl Güvenlik Raporu'na göre, Türkiye ve bölge ülkelerde yaşanan jeopolitik olaylar ve doğal afetler, sanal dünyada yeni trendler yaratıyor. Bu da kurumlar, bireyler ve hükümetler için riskleri artırıyor. Tarım ve madencilik Türkiye'de en riskli dikey endüstriler.

SİBER GÜVENLİKTEKİ EN ZAYIF HALKALAR

Güncelliğini yitirmiş yazılımlar, kötü kodlar, elden çıkarılmış dijital aygıtlar ve kullanıcı hataları gibi siber güvenlik "zayıf halkaları" saldırganların işini kolaylaştırıyor. **DNS sorguları**, **exploit kit'ler, amplifikasyon saldırıları, POS sistemi açıkları, zararlı reklamlar, fidye yazılımlar, şifreleme protokollerine sızmalar, sosyal mühendislik ve "hayati olay" spam'leri gibi yöntemler,** saldırganların başvurdukları kimi yöntemler.

SİNSİ TEHDİTLERE DİKKAT!

Sinsi tehditleri göz ardı edip yalnızca öne çıkan açıklara yoğunlaşan kurumlar kendilerini riske atıyor. **Heartbleed** gibi bilinen tehditlere odaklanınca; saldırganlar, düşük profilli uygulamalara ve zayıf noktaları bilinen altyapılara saldırarak amaçlarına ulaşıyor.

%94 BAĞLANTI İÇİNDE

2014 yılında **müşteri** ağlarının yaklaşık yüzde 94'ünün kötü amaçlı yazılım içeren sitelerle bağlantı içinde olduğu saptandı.

HAPİS CEZASI ÜRKÜTTÜ: EXPLOIT KİT'LER %87 GERİLEDİ

Popüler Blackhole Exploit Kit'in yazarının geçtiğimiz yıl tutuklanması saldırganların gözünü korkuttu. 2014'te exploit kit'leri **yüzde 87 oranında azıldı.** 2014'ün ilk yarısında geliştirilen exploit kit'lerin birçoğu Blackhole'un yerini almaya çalışıyor, fakat henüz hiçbiri bunu başaramadı.

KÖTÜ AMAÇLI YAZILIMLAR EN ÇOK MEDYA, İLAÇ VE HAVACILIK SEKTÖRLERİNİ VURDU

Dikey pazarlarda kötü amaçlı yazılım oranında beklenmeyen artış gözlemlendi. **2014**'ün ilk yarısında, **kötü amaçlı yazılım riskinin en yüksek olduğu üç sektör medya ve yayıncılık,** ilaç ve kimyasal ile havacılık olarak belirlendi.

% 93'LÜK SUİSTİMAL

Java, 2014'te de en çok istismar edilen program oldu; suiistimal oranı yüzde 93'e ulaştı.

DNS SORGULARI

Müşteri ağlarının yaklaşık yüzde 70'i, Dinamik DNS'ler (DDNS) için DNS sorgusu sunuyor. Yüzde 40'ından fazlasıysa, IP Güvenlik (IPsec) VPN, Güvenli Giriş Katmanı (SSL) VPN, Secure Shell (SSH) Protokolü, Basit Dosya Transfer Protokolü (SFTP), FTP ve Güvenli Dosya Taşıma Protokolü (FTPS) gibi hizmetler sunan aygıtlara bağlı site ve domainler için DNS sorgusu sunuyor.

SPAMCİLER ARTIK DAHA ATİK

Spamciler, iletilerini bloke eden teknolojik gelişmelere hızla tepki veriyor, spam filtrelerine takılmamak için metinleri, görselleri ve domain isimlerini değiştiriyorlar. **İletilerinin etkileri azaldığında da değişiklikler yapıyorlar.**

AYDA 200 MİLYAR SPAM MESAJ

Dünya genelinde spam hacmi, 2010'dan bu yana en yüksek seviyesine ulaştı. Haziran 2013'ten **Ocak 2014**'e dek istenmeyen iletilerin sayısı 50 milyar ile 100 milyar arasında değişiyordu. Ancak Mart 2014 itibarıyla bu sayı ikiye katlanarak ayda 200 milyarı aştı. Küresel olarak spamlerde artış söz konusu olsa da, Kasım 2013'ten bu yana **Rusya ve ABD'de düşüş yaşanıyor.**

ZARARLI REKLAMLAR İNTERNET EKONOMİSİNE DARBE VURUYOR

Kötü amaçlı yazılımları yaymak üzere kullanılan zararlı online reklamlar, hem internet kullanıcıları hem de internet ekonomisi için ciddi bir tehdit oluşturuyor. Kullanıcılar, her zaman yaptıkları gibi internette gezinirken zararlı **yazılımlara maruz kaldıklarından, nerede ve nasıl "enfekte" olduklarını bilemiyorlar.** Kaynağına ulaşmak neredeyse imkansız,çünkü kötü amaçlı yazılımı yaydıktan kısa bir süre sonra söz konusu reklamlar kaldırılıyor.

Kart bilgilerinize göz diken saldırganlar, POS sistemlerine odaklanmayı sürdürecek. Bunun nedenleri ise şöyle: İnternete bağlı POS sistemleri, suçluların kurumsal ağlara girebilecekleri bir kapı. **Ayrıca hâlâ pek çok kişi kredi kartı bilgilerinin "kritik veri" olarak değerlendirilmesi gerektiğini anlamadı,** bu da bu bilgilerin iyi korunmadığı anlamına geliyor. Kurumların, POS çözümleri için başvurdukları "üçüncü şahıslar", suçlular için erişim noktası oluşturuyor.

SALDIRGANLAR İÇİN "BALONCUK"

Saldırganlar hangi metodu **(kablolu, kablosuz veya VPN) kullanıyor olursa olsun, BT profesyonelleri, dinamik bir güvenlik domain'i veya sadece saldırganlar için bir "baloncuk" yaratabilir.**
Suçlu, dizüstü bilgisayarıyla bir port on-site'a bağlandığında; ağ bu kişinin önünü kesip kimliğini teşhis ediyor, profilini çıkarıyor, verilerini kaydediyor, takip ediyor ve ardından da kullanıcıyı spesifik ve dinamik yetkilerle donatıyor.
Böylece, içerik politikası üzerinden kullanıcıların ağ erişimleri kısıtlanıyor.

ORTAK SORUN: SİBER GÜVENLİK RİSKLERİ

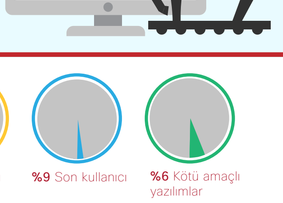
Eskiden kurumlar açıkça siber güvenliği konuşmazdı, ancak bugün durum farklı. Artık pek çok yönetici, **şirketlerin giderek dijitalleşmeleri ve bilginin stratejiye dönüşmesiyle,** siber güvenlik risklerinin tüm kuruluşların karşı karşıya kaldığı ortak bir sorun olduğunu anlamaya başladı.

GERÇEK BİR DEDEKTİF

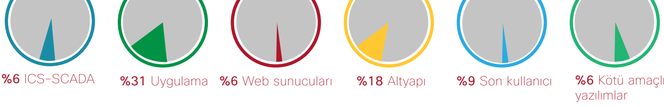
Öngörüsel analiz sayesinde, hem var olan güvenlik teknikleri daha mükemmel hale getiriliyor hem de bilinmeyen veya olağandışı davranışlar daha kolay tespit edilebiliyor.
Bunun içinse, çok sayıda parametreyi analiz eden ve güncel veri trafiğini hesaba katan gelişmiş karar verme algoritmalarını kullanmak gerekiyor. **Otomatik öğrenme, sistemin "gördüklerini" öğrenmesine ve bunlara uyum sağlamasına olanak tanıyor; yani bir nevi dedektif gibiler.** Öngörüsel analiz, içerik bazlı güvenlik çözümleri, perimetre yönetim çözümleri ve politika yönetim çözümleriyle birlikte uygulanmalı.

GÜVENLİK HERKESİN SORUMLULUĞU

Hepimiz, ancak bağlı olduğumuz zincirlerin en zayıf halkası kadar güçlüyüz. **Herkesin ve her şeyin birbirileriyle bağlantı içinde olduğu günümüz dünyasında, hepimiz güvenlikten sorumluyuz.** Açık, güvenli ve esnek sanal alem, tüm topluma ait. Tüm oyuncular, bu varlığı beslemek ve desteklemekle yükümlü.



EN ÇOK SALDIRIYA UĞRAYAN ÜRÜNLER



Ocak 2014'ten bu yana Exploit Kit'ler
Kaynak: Cisco Threat Intelligence Platform (saldırı sayısı) Exploit Kit Adı

CISCO™