SANS SECURITY AWARENESS

OUCH!

Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

Evet, Siz Bir Hedefsiniz

Genel Bakış

Pek çok insan siber saldırganların hedefinde olmadığı yanlış inancına sahiptir: Onlara göre sistemlerinin ve hesaplarının hiçbir değeri yoktur. Bize güvenin, eğer teknolojiyi iş yerinizde ya da evde kullanıyorsanız kötü niyetli kişiler için bir değer ifade ediyorsunuz demektir. Fakat şanslısınız. Siber saldırılara karşı en mükemmel savunma mekanizmasına sahipsiniz, yani kendinize.

Neden bir hedefsiniz?

Günümüzde internet üzerinde birbirinden değişik motivasyonlara sahip birçok farklı siber saldırgan bulunmaktadır. Peki neden onlardan biri size saldırmak istemesin? Çünkü sizin bilgilerinizi ele geçirmek onların hedeflerine ulaşmalarına yardım edecek. İşte, siber saldırganların ve neden size saldırmak isteyebileceklerinin en yaygın iki örneği;

⚠ **Siber Suçlular:** Bu tarz kötü niyetli kişiler mümkün olan en çok parayı kazanmak isterler. İnterneti onlar için değerli hale getiren şey dünya üzerindeki herkesi sadece bir tuş basımı ile hedef alabilmeleridir. Onların sizin üzerinizden para kazanabilmesinin pek çok yolu bulunmaktadır. Örnekler sizin banka ya da emekli maaşı hesabınızdan para çalmak, sizin adınıza kredi kartı çıkartmak ve alışveriş faturalarını size göndertmek, sizin bilgisayarınızı başka insanların bilgilerini ele geçirmek için kullanmak veya sosyal medya ya da oyun hesaplarınızı ele geçirerek onları diğer suçlulara satmak olarak sıralanabilir. Kötü niyetli kişilere sizin üzerinizden para kazanmalarını sağlayacak yöntemler saymakla bitmez. Bu kötü niyetli kişilerden yüzlercesi hatta binlercesi her sabah siz de dahil olmak üzere mümkün olan en çok kişinin bilgilerini ele geçirmek amacıyla uyanıp güne başlarlar.

☆ **Hedefli Saldırganlar:** Bunlar sıklıkla hükümetler, suç organizasyonları veya işyerinizi hedefleyen rakipler için çalışan yüksek eğitimli siber saldırganlardır. İşinizin çok da dikkatleri üzerine çekmediğini düşünüyor olabilirsiniz fakat sürpriz yaşayabilirsiniz.

- İşinizde elde ettiğiniz veriler farklı şirketler veya hükümetler için aşırı önemli değer taşımaktadır.
- Hedefli saldırganlar sizi işyerinde hedefleyebilir, amaçları sizin bilgilerinizi ele geçirmek değildir. İş arkadaşlarınızdan birinin bilgilerini ele geçirmek veya diğer sistemlerden birine sızmak için sizi kullanırlar.
- Bu tip saldırganlar, çalıştığınız veya ortak çalıştığınız diğer şirketlerin bilgilerini ele geçirmek için sizi işyerinizde hedef alabilirler.

Anti-Virüs Programı Kullanıyorum, Güvendeyim

Tamam, ben bir hedefim ama bu benim için sorun değil. Bilgisayarıma hemen bir anti-virüs programı ve firewall kuracağım ve güvende olacağım, doğru mu? Maalesef cevap "hayır". Pek çok insan bilgisayarlarına güvenlik araçlarını kurduklarında güvende olacaklarını düşünürler. Ne yazıkki bu tamamen doğru değildir. Siber saldırganlar her geçen gün kendilerini daha fazla geliştiriyorlar, güvenlik teknolojileri ve çözümleri onların pek çok saldırı yöntemlerine kolayca karşı koyamıyor. Örneğin, sıklıkla anti-virüs programlarının tespit edemeyeceği kötü niyetli programlar geliştiriyorlar. E-posta güvenlik önlemlerinizi, kişiselleştirilmiş oltalama saldırıları ile aşıyorlar ya da telefonla size ulaşıp kandırarak kredi kartı bilgilerinizi, paranızı ya da parolalarınızı ele geçiriyorlar. Teknoloji sizi bu tarz saldırılardan korumada önemli bir rol oynar fakat en mükemmel savunma silahı kendinizsiniz.

Neyse ki, güvende olmak o kadar da zor değildir, sonuçta sağduyu ve bazı temel davranışlar sizin en iyi savunmanızdır. Çok acil, garip veya şüpheli bir e-posta, mesaj veya telefon görüşmesi alırsanız, bu bir saldırı olabilir. Bilgisayarlarınızın ve cihazlarınızın güvenli olduğundan emin olmak için, otomatik güncellemeyi etkinleştirin. Son olarak, her bir hesabınız için güçlü ve benzersiz bir parola kullanın. Siber farkındalık sizin en iyi savunmanızdır. Nereden başlayacağınızdan emin değil misiniz? Aylık yayınlanan OUCH! Bültenlerine sans.org/ouch adresinden abone olmayı düşünün.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup Hawaii Üniversitesinde yazılım mimarileri ve yazılım güvenliği üzerinde doktora sonrası araştırma yapmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, finans, telekomünikasyon, sigortacılık, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, uyum, BT yönetişim/strateji, risk yönetimi, iş sürekliliği, hizmet yönetimi, altyapı hizmetleri, yazılım geliştirme ve program/proje yönetimi alanlarında yönetici ve danışman olarak 19 yılı aşkın süre görev yaptıktan sonra, Truth ISC (www.truth-isc.uk) adıyla kurduğu Türkiye ve İngiltere'de faaliyet gösteren danışmanlık şirketinde hizmet vermeye devam etmektedir.

Konuk Yazar

Matt Bromiley *(@mbromileyDFIR) dünyada yaşanan olaylarda birçok organizasyonla çalışmış, sekiz yılı aşkın tecrübeye sahip, siber olaylara müdahale ve adli bilişim uzmanıdır. Matt ayrıca SANS FOR508 ve FOR572 kurslarının eğitmeni, bir dijital adli bilişim uzmanı ve siber olaylara müdahale eğitmenidir.*

SANS SECURITY AWARENESS

Kaynaklar

Kötü Niyetli Yazılımları Durdurmak:	https://www.sans.org/u/L1J
Sosyal Mühendislik:	https://www.sans.org/u/L1O
Telefon Görüşmesi Dolandırıcılığı:	https://www.sans.org/u/L1T
Parolalar:	https://www.sans.org/u/L1Y
Poster – Siz bir hedefsiniz:	https://www.sans.org/u/L23