Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

Birisi Cihazıma İzinsiz mi Girdi?

Giriş

Ne kadar güvenli olduğunu düşünseniz de arabayı kullanmak gibi eninde sonunda bir kaza yapabilirsiniz. Aşağıda birisinin cihazınıza/cihazlarınıza izinsiz girip girmediğine ait ipuçları verilmiştir. Eğer izinsiz girildiyse ne yapabileceğinizi de aşağıda bulacaksınız. Kotu bir şeyin olduğunu ne kadar erken tespit ederseniz problemi o kadar çözme ihtimaliniz artar.

Birisinin Cihazınıza/Cihazlarınıza Girip Girmediğine Dair İpuçları

- **Anti-virüs programınız sisteminize kötücül yazılım bulaştığına dair size alarm verir. Bu alarmın sizin anti-virüs programınız tarafından oluşturulup oluşturulmadığına dikkat edin, sizin bir numarayı aramanıza ya da bir yazılım yüklemenize sebep olacak şekilde sizi kandırmaya çalışan bir web sitesine ait bir pop-up penceresinden gelmediğinden emin olun. Emin değil misiniz? Anti-virüs programını açın.**
- **Bilgisayarınızdaki dosyaların şifrelendiğini ve dosyalarınızı geri almak için fidye ödemek zorunda olduğunuzu belirten bir pop-up penceresi ile karşılaşırsınız.**
- **Internet tarayıcınız, sizin gitmek istemediğiniz sitelere sizi yönlendirir.**
- **Bilgisayarınız ve uygulamalarınız sürekli çöker ve kapanır. Bilinmeyen uygulamalara ait ikonlar vardır ya da garip pençeler açılıyordur.**
- **Parolanızın doğru olduğunu bilseniz bile parolanız geçerli olmaz.**
- **Arkadaşlarınıza neden onlara sürekli istenmeyen e-postalar gönderdiğinizi sorar ki siz bu e-postaları göndermemişsinizdir.**
- **Sizin bilginiz dahilinde olmadığı halde kredi kartınızla alışveriş yapılmış ya da hesabınızdan para çekilmiştir.**

Ne Yapmalısınız?

Eğer birisinin cihazınıza/cihazlarınıza girdiğinden şüpheleniyorsanız, ne kadar önce harekete geçerseniz o kadar iyi olur. Eğer işyerinde bu durumla karşılaştıysanız, kendi başınıza problem çözmeye çalışmayın, onun yerine hemen durumu rapor edin. Eğer kişisel bir sistem ya da hesaba izinsiz giriş yapıldıysa, alabileceğiniz önlemler şunlardır:

- **Parolalarınızı Değiştirmek:** Bu, bilgisayarınızdaki ya da mobil cihazlarınızdaki parolaların yanında cevrim-içi hesaplarınıza ait parolaların da değiştirilmesini içerir. Daha önceden izinsiz giriş yapılmış bir bilgisayar kullanarak parolalarınızı değiştirmeyin, onun yerine güvenli olduğunu bildiğiniz başka bir cihazı kullanın. Eğer tüm parolalarınızı aklınızda tutamıyorsanız, bir parola yöneticisi kullanın.

Finansal: Kredi kartınızla ya da banka hesabınızla ilgili olan problemler için, hemen bankanızı arayın. Banka kertinizin arkadaşında ya da hesap bildirim cetvelinizde yazan telefon numarası gibi güvenilir bir numarayı kullanın. Ya da güvenilir bir cihazı kullanarak bankanızın web sitesini ziyaret edin. Ayrıca, kredi bilgilerinizin başka kişilerle paylaşılmasını engelleyen kredi dondurma özelliğini etkin hale getirmeyi göz önünde bulundurun.

Anti-virüs: Eğer anti-virüs yazılımınız kötücül bir yazılımın bir dosyanıza bulaşmış olduğunu size haber veriyorsa, yazılımın önerdiği adımları takip edin. Birçok anti-virüs yazılımı, karşılaştığınız bu durumla ilgili detaylı bilgileri içeren bağlantıları sizinle paylaşacaktır.

Tekrar Yükleme: Eğer izinsiz giriş yapılmış bilgisayarınızı düzeltemediyseniz ya da sisteminizin güvenli olduğundan daha emin olmak istiyorsanız, işletim sisteminizi yeniden yükleyin. Yedeklemelerinizi kullanmayın, yedeklemeler sadece kişisel dosyalarınızın kurtarılması için kullanılmalıdır. Eğer bilgisayarı tekrar ayağa kaldırmayla ilgili kendinize güvenmiyorsanız, o zaman bir profesyonel servisten yârdim alin. Ya da cihazınız eski ise belki de yenisini satın almak daha kolay olacaktır. Son olarak, sisteminizi tekrar ayağa kaldırdığınızda ya da yeni bir cihaz aldığınızda, cihazın güncel yazılımlar içerdiğinden ve otomatik olarak güncelleme yaptığından emin olun.

Yedekler: Kendinizi korumak için en önemli adim, herhangi bir durumla karşılaşmadan önce düzenle yedekler almaktır. Bunun için dosyalarınızı günlük hatta saatlik yedekleyen bir çok yazılım çözümü bulunmaktadır. Hangi çözümü kullandığınızdan bağımsız olarak aralıklarla aldığınız bu yedekleri tekrar geri yükleyip yükleyemediğinizi kontrol edin. Çoğunlukla yedeklemeleriniz, birisi cihazınıza izinsiz giriş yaptığınızda dosyalarınızı kurtarmanın tek yoludur.

Güvenlik kuvvetleri: Herhangidir şekilde tehdit edildiğinizi düşünüyorsanız, bu olayı yerel güvenlik kuvvetlerine bildirin.

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

Dr. Johann es Ullrich *(@johullrich), SANS Teknoloji Enstitüsünün dekanı, SANS Internet Kriz Merkezinin yöneticisidir. DShield ortak sensor ağının kurucusudur ve Internet Kriz Merkezinin günlük ağ güvenliği haberlerinin yayınlayıcısıdır.*

Kaynaklar

Yedekler: https://www.sans.org/u/JGP
Parolalar: https://www.sans.org/u/JGU
Parola Yöneticileri: https://www.sans.org/u/JGZ
Kotu Amaçlı Yazılımlar: https://www.sans.org/u/JH4
Kredi Dondurma: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/

OUCH!, SANS Security Awareness Programı tarafından yayınlanır ve Creative Commons BY-NC-ND 4.0 lisansı. altında dağıtılır. Bülteni değiştirmediğiniz sürece, bu bülteni dağıtabilir ya da kendi farkındalık programlarınızda kullanabilirsiniz. Çeviri ya da daha fazla bilgi için, lütfen www.sans.org/security-awareness/ouch-newsletter e-posta adresini kullanarak iletişime geçiniz. Yayın Kurulu : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley