Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Şifreleme

Şifreleme Nedir?

İnsanların "şifreleme" ifadesini kullanarak kendilerini ve bilgilerini korumak için bunu nasıl kullanmaları gerektiğinden bahsettiklerini duymuşsunuzdur. Şifreleme kavramı biraz karmaşık görünebilir. Şifreleme sizi herşeyden korumaz, kendine göre sınırları vardır. Bu sayıda şifrelemenin ne olduğunu, neden kullanmanız gerektiğini ve uygun bir şekilde nasıl uygulayabileceğinizi anlatacağız.

Konuk Yazar

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) Washington, DC'de bir danışman olup SANS Enstitüsünde Mobil Cihaz Güvenliği ile Etik Bilgisayar Korsanlığı (SEC575) derslerinin baş eğitmeni ve Incident Response Team Management (MGT535) dersinin yazarıdır.

Cihazlarınızda finansal dokümanlar, resimler, e-postalar ve tıbbi kayıtlar gibi çok sayıda hassas bilginiz bulunmaktadır. Eğer cihazınızı kaybeder ya da çaldırırsanız hassas verilerinizin tümü cihazınızı ele geçiren kişi tarafından ulaşılabilir olacaktır. Ayrıca, çevrim-içi bankacılık gibi hassas işlemlerinizi çevrim-içi yapıyor olabilirsiniz. Eğer bir siber suçlu sizin çevrim-içi hareketlerinizi izliyorsa sizin hesap ya da kredi kartı numaranız gibi tüm finansal bilgilerinizi çalabilir. Şifreleme, sadece yetkili kişilerin bilgilerinize erişebildiğinden ve bunları değiştirdiğinden emin olmanızı sağlayarak sizi bu gibi durumlardan korur.

Şifrelenmeyen bilgileriniz "açık metin" olarak adlandırılır. Bu da bilgilerinize herkesin kolayca erişip okuyabileceği anlamına gelir. Şifreleme, bilgiyi okunamaz bir formatta olan "şifreli metin" haline getirir. Şifreleme karmaşık matematiksel işlemler ve eşsiz bir anahtar kullanarak sizin bilginizi şifreli bir metne çevirir. Anahtar, kapınızı açma ve kapamada kullandığınız anahtar gibi bilginizin okunmamasını sağlayan ve tersine okunmayan bilgiyi okunabilir hale getiren şeydir. Anahtar için kullanılan çok yaygın bir örnek şifrelerdir, sadece sizin şifrenize sahip olan kişi sizin bilginizi çözebilir ve erişebilir. Şifrelenmiş bilginizi korumak için anahtarınızı korumanız gerekmektedir. Genellikle şifreleme iki biçimde yapılır: dizüstü bilgisayarınızda saklanan bilgileriniz gibi hareketsiz verilerinizi ve çevrim-içi iletilen bilgileriniz gibi hareketli verilerinizin şifrelenmesi.

Hareketsiz Veriyi Şifreleme

Hareketsiz veriyi şifrelemenin öncelikli amacı bilgisayar veya mobil cihazınızı kaybettiğinizde ya da bu cihazlar çalındığında sizin kişisel bilgilerinizi korumaktır. 15 yıl önce çoğu bilgisayar çok büyük boyutlarda olduğunda ve masaüstü bilgisayarlar bir yerden bir yere hareket ettirilemeyecek kadar hantal olduklarından dolayı bu bahse bir konu değildi. Günümüzde artık dizüstü bilgisayarlar bir kaç kilo ve mobil cihazlar bir kaç yüz gram. Bu cihazlar son derece güçlü olup çok fazla da bilgi taşımaktalar aynı zamanda da çok kolay kaybedilebiliyorlar. Bunların yanında USB harici bellekler ya da CD-ROM'lar gibi mobil araçlar da hassas bilgiler taşıyabilir. Bu

Şifreleme

cihazlarda bilgileri şifrelemek için kullanılan yaygın bir yöntem Tüm Disk Şifreleme (TDŞ, Full Disk Encryption)'dir. Bu da sizin neyin şifrelenip neyin şifrelenmeyeceği kararını vermenize gerek duymadan otomatik olarak sistemdeki herşeyin şifrelenmesi anlamına gelir. Günümüzdeki çoğu işletim sistemi TDŞ yöntemi gömülü bir şekilde elinize gelir ve sizin sadece bu özelliği aktif hale getirmeniz gerekir. Örneğin, Mac OS X işletim sistemi FileVault ile, bazı Windows sürümleri de Bitlocker ile gelir. Eğer bilgisayarınız Tüm Disk Şifreleme'yi destekliyorsa bu özelliği aktif hale getirmenizi şiddetle öneriyoruz. Ayrıca, çoğu cep telefonu dahili depolama cihazları için Tüm Disk Şifreleme'yi desteklemektedir. Örneğin, iPhone ve iPad'lar için işletim sistemi, iOS şifre belirlendiğinde otomatik olarak Tüm Disk Şifreleme'yi uygular. İşte kullandığınız bilgisayarınızın ya da mobil cihazlarınızın Tüm Disk Şifreleme'yi destekleyip desteklemediğini öğrenmek isterseniz yardım masasına ya da danışmanlarınıza sorabilirsiniz. Kişisel bilgisayarlarınız için bilgisayar üreticiniz ile iletişime geçebilir ya da çevrim-içi dokümantasyonu gözden geçirebilirsiniz.

Şifreleme bilgilerinizi korumanın en etkili yollarından biridir ancak ve ancak anahtarınız kadar güçlüdür.

Hareketli Veriyi Şifreleme

Bilgileriniz aktarılırken de savunmasız durumdadır. Eğer veri şifrelenmemişse çevrim-içi izlenebilir ve çalınabilir. İşte bu yüzden çevrim-içi bankacılık işlemleri yaparken, e-posta gönderirken ve hatta sosyal medya sitelerine ulaşırken örneğin, hassas bilgilerinizin şifrelendiğinden emin olmak istersiniz. En yaygın kullanılan şifreleme tipi HTTPS'dir. Sizin tarayıcınız ile ağ sitesi arasında tüm trafik şifrelenir. Bağlantısında https:// olan bir ağ sitesini tarayıcınızdan görüntülediğinizde tarayıcınızda bir kilit olduğunu ve bağlantı çubuğunun yeşile döndüğünü görürsünüz. Bunların hepsi tüm trafiğin şifrelendiğine yönelik işaretlerdir. Tarayıcınıza ve ağ sitesine bağlı olarak bu üçünü bir arada görebilirsiniz. Açık bir Wİ-Fİ ağına bağlandığınızda fırsatınız olduğunda şifrelemeyi kullandığınızdan emin olun. Son olarak, e-posta gönderirken ya da alırken e-posta istemncinizin e-postalarınızın şifreli bir bağlantı üzerinden gönderildiğine emin olun. Çoğu e-posta istemcisi şifreleme sağlar, ayrıca internet servis sağlayıcınız da e-posta istemcinizde şifrelemeyi aktif hale getirmekte yardımcı olabilir.

Şifrelemeyi Uygun Bir Şekilde Uygulama

Hangi şifreleme tipini ya da bunu nasıl kullandığınızdan bağımsız olarak hemen hemen tüm şifreleme yöntemleri uygun kullanılmaları için ortak adımlar içerirler:

- Şifrelemeniz ancak anahtarınız kadar güçlüdür. Eğer herhangi biri anahtarınızı tahmin eder ya da ele geçirirse bilgilerinize ulaşacaktır. Anahtarınızı korumalısınız.

Şifreleme

- Eğer anahtarınız için bir şifre kullanıyorsanız uzun ve güvenli bir şifre olduğundan emin olun, kaybetmeyin ya da unutmayın. Eğer unutursanız kendinizin bile kendi bilgilerinize erişmesine engel olmuş olursunuz.
- Şifrelemeniz bilgisayarınızın güvenli olduğu ölçüde güçlüdür. Eğer bilgisayarınız ele geçirilirse ya da bir virüs bulaştırılmışsa siber suçlular şifrelemenizi pas geçerek bilgilerinize ulaşabilirler. Dolayısıyla bilgisayarınızı ve mobil cihazlarınızın güvenli olduğundan emin olun.
- Eğer şifreleme için farklı seçenekler sunulmuşsa her zaman en güçlü olanı seçin.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve http://www.securingthehuman.org adresini ziyaret ederek SANS güvenlik farkındalığı çözümleri hakkında daha fazla bilgi edinin.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup SOSoft Bilişim Teknolojilerinde biyometrik güvenlik sistemleri üzerinde çalışmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, telekomünikasyon, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, iş sürekliliği, risk yönetimi, altyapı hizmetleri, yazılım geliştirme ve proje yönetimi alanlarında yönetici ve danışman olarak 15 yılı aşkın süredir görev yapmaktadır.

Kaynaklar

Mac OS X Filevault:	http://support.apple.com/kb/ht4790
iOS şifreleme:	http://support.apple.com/kb/ht4175
Android şifreleme:	http://www.androidauthority.com/how-to-encrypt-android-device-326700/
Windows şifreleme:	http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
Bilgisayarınızı Güvenli Hale Getirme:	http://www.securingthehuman.org/ouch/2012#december2012
Şifre Yöneticileri:	http://www.securingthehuman.org/ouch/2013#october2013

Yayın Kurulu : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis