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 ve sınırlarını anlamanız gerekir. Bu sayıda şifrelemenin basitçe ne olduğunu, sizi nasıl koruyabileceğini ve uygun bir şekilde nasıl uygulayabileceğinizi anlatacağız.

Konuk Yazar

Francesca Bosco (**@francibosco**) bir araştırmacı ve siber suçlar, siber güvenlik ve teknolojinin yanlış kullanımı konusunda projeler yöneten bir proje koordinatörüdür. Kendisi Birleşmiş Milletler Bölgelerarası Suç ve Adalet Enstitüsünde çalışmakta olup, Teknoloji ve Kanun Merkezinin kurucu ortağıdır.

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, çevrimiçi bankacılık ve alışveriş gibi hassas işlemlerinizi çevrim-içi yapıyor olabilirsiniz. Eğer herhangi biri sizin çevrimiçi hareketlerinizi izliyorsa hesap bilgilerinizi ya da kredi kartı numaranız gibi tüm bilgilerinizi çalabilir. Şifreleme, sadece yetkili kişilerin bilgilerinize erişebildiğinden ve bunları değiştirdiğinden emin olmanızı sağlayarak sizi bu gibi durumlardan korur.

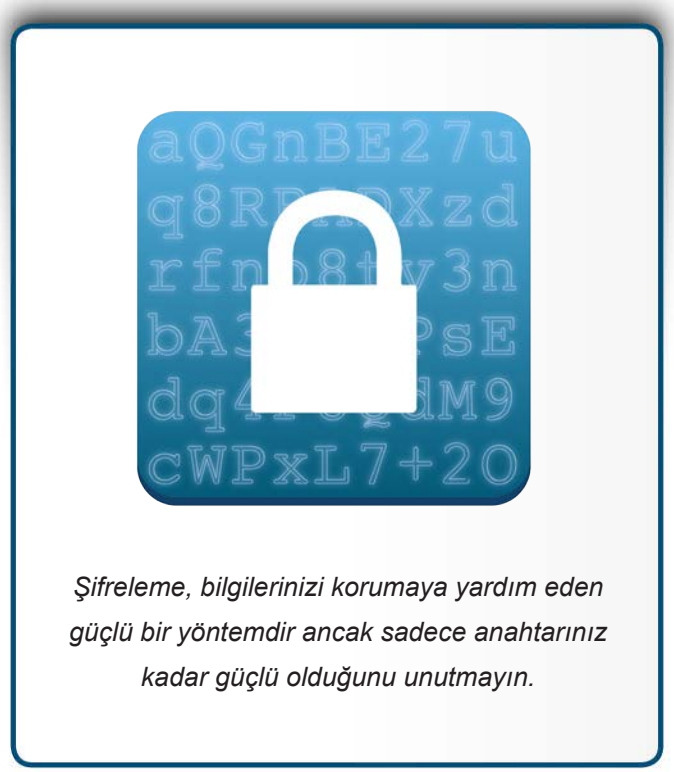
Şifreleme binlerce yıldır kullanılıyor. Bugün, şifreleme çok daha karmaşık olsa da aynı amaca hizmet ediyor : gizli bir mesajı bir yerden diğerine sadece okumaya yetkili olanların erişebildiğinden emin olarak ulaştırmak. Bilgi şifrelenmemişse "düz metin (plain-text)" olarak adlandırılır. Bu herhangi birinin kolaylıkla onu okuyabilmesi ya da erişebilmesi anlamına gelir. Şifreleme bu bilgiyi okunamaz bir formata yani "şifreli metin (cipher text)"e dönüştürür. Bugünün şifreleme yöntemleri, 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 parolalardır.

Neleri Şifreleyebilirsiniz?

Genel olarak şifrelenebilen iki tür veri vardır : hareketsiz veri (örneğin mobil cihazınızda saklanan veri), hareket halindeki veri (örneğin e-posta alma, arkadaşınıza mesajlaşma).

Şifreleme

Hareketsiz veriyi şifrelemenin öncelikli amacı bilgisayar veya mobil cihazınızı kaybettiğinizde ya da bu cihazlar çalındığında sizin kişisel bilgilerinizi korumaktır. Bugünün cihazları oldukça güçlüler ve çok fazla veri barındırabiliyorlar ancak bir o kadar da kolay kaybedilebiliyorlar. Bunların yanında USB harici bellekler ya da harici hard diskler gibi mobil araçlar da hassas bilgiler taşıyabilir. Bu cihazlarda bilgileri şifrelemek için kullanılan yaygın bir yöntem Tüm Disk Şifreleme (FDE - 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 FDE yöntemi gömülü bir şekilde elinize gelir ve sizin sadece bu özelliği aktif hale getirmeniz gerekir. Örneğin, Mac OS X işletim sisteminde FileVault, Windows sürümlerinde de Bitlocker ya da Cihaz Şifreleme'yi kullanabilirsiniz. Ayrıca, çoğu mobil cihaz 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. Android 6.0 (Marshmallow) dan itibaren Google Tüm Disk Şifreleme'nin gömülü olarak aktif hale getirilerek minimum standartların karşılanmasını sağlıyor.



Şifreleme, bilgilerinizi korumaya yardım eden güçlü bir yöntemdir ancak sadece anahtarınız kadar güçlü olduğunu unutmayın.

Bilgileriniz hareket halindeyken de savunmasız durumdadır. Eğer veri şifrelenmemişse çevrimiçi izlenebilir ve çalınabilir. İşte bu yüzden çevrimiçi 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. Başka bir örnek e-posta alma ve gönderme sırasında yaşananlardır. Çoğu e-posta istemcisi sizin aktif hale getiebileceğiniz şifreleme yeteneklerini sunar. Üçüncü bir örnek de iMessage, Wickr, Signal, WhatsApp ya da Telegram gibi uygulamalarla iki kullanıcının yazışması sırasındaki hareketli verinin şifrelenmesi olabilir. Bu uygulamalar gibi olanlar, uçtan uca şifreleme yöntemlerini kullanarak üçüncü partilerin bir sistem ya da cihazdan diğerine iletilen bilgilere erişimini engeller. Bu da, gönderilenleri sadece sizin ve iletişimde bulunduğunuz kişinin okuduğu anlamına gelir.

Doğru Uygulama

Şifreleme ile korunduğunuzdan emin olmanız için, onu doğru uyguladığınızdan emin olmalısınız.

- Şifrelemeniz ancak anahtarınız kadar güçlüdür. Eğer herhangi biri anahtarınızı tahmin eder ya da ele geçirirse bilgilerinize ulaşacaktır. Anahtarınızı korumalısınız. Eğer anahtarınız için bir şifre kullanıyorsanız uzun ve güvenli bir şifre olduğundan

Şifreleme

emin olun, kaybetmeyin ya da unutmayın. Eğer unutursanız kendinizin bile kendi bilgilerinize erişmesine engel olmuş olursunuz. Eğer bütün bu parolalarınızı hatırlayamıyorsanız, parola yönetim uygulamalarını kullanmanızı öneririz.

- Şifrelemeniz cihazlarınız güvenli olduğu ölçüde güçlüdür. Eğer bilgisayarınız ele geçirilirse ya da bir virüs bulaştırılmışsa siber suçlular şifrelemenizi pas geçerek bilgilerinize ulaşabilirler. Bu nedenle cihazlarınızı, anti-virüs, güçlü parolalar ve güncel sürümler kullanma gibi diğer adımlarla korumanız önemlidir.
- Birçok mobil uygulama ve bilgisayar yazılımları verinizi ve iletişiminizi korumak için güçlü şifreleme sunuyor. Eğer kullanmak istediğiniz uygulama, şifrelemeyi desteklemiyorsa, alternatiflerini değerlendirin.

Daha Fazla Bilgi İçin

Aylık OUCH! güvenlik farkındalığı bültenine üye olun, OUCH! arşivlerine erişin ve securingthehuman.sans.org/ouch/archives 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

Şifreleme:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Parolalar:	https://securingthehuman.sans.org/ouch/2015#april2015
Parola Yönetim Uygulamaları:	https://securingthehuman.sans.org/ouch/2015#october2015
Kötü Amaçlı Yazılım Nedir:	https://securingthehuman.sans.org/ouch/2016#march2016
Yeni Tabletinizi Korumak:	https://securingthehuman.sans.org/ouch/2016#january2016

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