Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Mobil Uygulamaları Güvenle Kullanmak

Giriş

Tabletler, akıllı telefonlar ve saatler gibi mobil cihazlar, profesyonel ve özel hayatımızda kullandığımız başlıca teknolojiler haline geldi. Mobil cihazları çok amaçlı yapan şey, seçebileceğimiz milyonlarca uygulamanın olmasıdır. Bu uygulamalar bizi daha üretken yapar, hızlı bir şekilde diğer insanlarla iletişime geçmemizi ve paylaşım yapabilmemize olanak verir, başkalarını eğitim vermemizi ya da daha çok eğlenmemizi sağlar. Ancak, tüm bu uygulamaların kabiliyetleri ile birlikte riskleri de beraberinde getirir. Mobil uygulamalarınızı güvenli bir şekilde kullanabilmek için alacağınız önlemlerden bahsedeceğiz.

Konuk Yazar

Joshua Wright, Counter Hack'de teknik yönetici ve SANS Ensititüsünde kıdemli eğitmendir. SEC575: Mobil Cihaz Güvenliği ve Etik Bilgisayar Korsanlığı ve Bilgisayar Korsanlığına Maruz Kalma:Kablosuz Ağlar derslerinin yazarıdır. Josh'a Twitter'da **@joswr1ght** ile ulaşabilirsiniz.

Mobil Uygulamaların Yüklenmesi

İlk adım, mobil uygulamaları her zaman güvenli ve güvenilir bir kaynaktan indirdiğinizden emin olmanızdır. Siber suçlular, virüslü mobil uygulamaları geliştirip meşru gibi görünecek şekilde dağıtımını yapma konusunda ustalaşmışlardır. Eğer bu virüs bulaşmış uygulamalardan birini yüklerseniz, siber suçlular sizin mobil cihazınızın kontrolünü ellerine alırlar. Sadece iyi bilinen güvenilir kaynaklardan uygulamalar yükleyerek virüslü bir uygulama yükleme olasılığınızı azaltmış olursunuz. Farkına varamayacağınız şey ise uygulama yüklerken, mobil cihazınızın markasının yükleme seçeneklerinize karar vermesidir.

Apple cihazları için, örneğin iPad ya da iPhone, mobil uygulamalarınızı sadece Apple Uygulama Mağazasından yükleyin. Bunun avantajı, mobil uygulamalar mağazada yer almadan önce Apple'ın bu uygulamaları güvenlik taramasından geçirmesidir. Apple tüm virüslü uygulamaları tespit edemese de bu gözetimli ortam virüslü bir uygulama yükleme riskini çarpıcı biçimde azaltmaya yardımcı olur. Bunun yanında eğer Apple, mağazasında virüslü olduğunu düşündüğü bir uygulama bulursa, bu uygulamayı hızlı bir şekilde mağazasından kaldırır. Windows Telefonlar, uygulama yönetimi için buna benzer bir yaklaşım izlerler.

Android mobil cihazlar bu konuda farklıdır. Android internetteki herhangi bir yerde bulduğunuz uygulamayı yükleyebilme özelliği ile size daha fazla esneklik verir. Ancak esneklik, daha fazla sorumluluk getirir. Uygulamaların tümü gözden geçirilmediği için mobil uygulamaları indirip kurma konusunda daha fazla dikkatli olmanız gerekir. Google, Apple'ınkine benzer, Google Play olarak adlandırılan gözetimli bir mobil uygulama mağazası idame etmektedir. Google Play'den

Mobil Uygulamaları Güvenle Kullanmak

indirilebilen uygulamalar temel güvenlik taramasından geçmiş olanlardır. Android cihazlarınıza sadece Google Play'den uygulama yüklemenizi tavsiye ederiz. Siber suçlular da dahil olmak üzere herhangi birinin kötü niyetli mobil uygulamaları geliştirerek dağıtım yapabileceği ve bu uygulamaları, mobil cihazlarınıza virüs bulaştırmak için sizi kolaylıkla kandırmakta kullanabileceğinden dolayı Android cihazlarınıza farklı web sitelerinden uygulama indirmekten kaçının. Ek bir koruma olarak fırsat olduğunda bir antivirüs uygulaması yükleyin.

Mobil uygulamaları güvenle kullanmanın anahtarı, uygulamaları güvenli kaynaklardan yüklemek, mevcut olduğunda güncellemelerini yapmak ve sadece gerekli uygulama izinlerini vermektir.

Hangi cihazı kullanırsanız kullanın, alabileceğiniz ek bir önlem, hiç kullanılmamış, çok az kişinin yüklediği ya da çok az kişinin olumlu yorum yaptığı uygulamaları yüklemekten kaçınmanızdır. Bir uygulama ne kadar uzun süre var olursa o kadar çok kişi tarafından kullanılır ve olumlu yorumlar alır, uygulamaya o kadar çok güvenilir. Ayrıca, sadece ihtiyacınız olan ve kullanacağınız uygulamaları yükleyin. Kendinize sorun, bu uygulamaya gerçekten ihtiyacım var mı? Her uygulama potansiyel olarak sadece yeni açıkları değil aynı zamanda gizlilik sorunlarını da beraberinde getirir. Eğer bir uygulamayı kullanmayı bıraktıysanız, mobil cihazınızdan kaldırın (ihtiyacınız olduğunuzda her zaman geri yükleme şansınız vardır). Son olarak mobil cihazınızı kırdırmayın(jailbreak). Bu, mobil cihazınıza izinsiz girilmesi ve onaylanmayan uygulamaların yüklenmesi ya da var olan ve gömülmüş fonksiyonların değiştirilmesi sürecidir. Bu, sadece mobil cihazınızda yüklü olan birçok güvenlik kontrolünün azaltılmasına ya da pas geçilmesine değil aynı zamanda çoğunlukla da cihazının garanti ve destek kapsamından çıkmasına neden olur.

Erişim İzinleri

Güvenilir bir kaynaktan uygulama yükledikten sonra, güvenli bir şekilde konfigüre edildiğinden ve sizin gizliliğinizi koruduğundan emin olun. Her zaman bir mobil uygulama erişimine izin vermeden önce düşünün: Uygulamanın istediği gibi bir erişim iznini vermek istiyor muyum, uygulama buna gerçekten ihtiyaç duyuyor mu? Örneğin, bazı uygulamalar konumlandırma servislerini kullanırlar. Eğer bir uygulamanın her zaman sizin konumunuzu bilmesine izin verdiğinizde, uygulama geliştiricisinin sizin adımlarınızı takip etmesine ve hatta bu bilgiyi başkalarına satmasına izin veriyor olabilirsiniz. Eğer bu izinleri vermek istemiyorsanız, izin isteklerini reddedin ya da gereksinimlerinize uyan başka bir uygulama bulun. Unutmayın, birçok seçeneğiniz vardır.

Uygulamaların Güncellenmesi

Mobil uygulamalar, bilgisayarlarınız ya da mobil işletim sistemleri gibi güncel olmalıdır. Siber suçlular sürekli olarak

Mobil Uygulamaları Güvenle Kullanmak

uygulamalarda zayıflıklar ararlar. Ve daha sonra bu zayıflıkları kullanarak saldırı yaparlar. Yüklediğiniz uygulamanın geliştiricileri bu zayıflıkları ortadan kaldıran ve cihazlarınızı koruyan güncellemeler yayınlarlar. Güncellemeleri ne kadar sıklıkla kontrol eder ve yüklerseniz o kadar iyidir. Birçok cihaz mobil uygulamaları otomatik olarak güncellemek için sistemi konfigüre etmenize izin verir. Bu ayarı tavsiye ederiz. Eğer bu mümkün değilse, o zaman her iki haftada bir mobil uygulamalarına ait güncellemeleri kontrol etmenizi tavsiye ederiz. Son olarak, uygulamalarınız güncel ise her zaman bu uygulamaların yeni izinler gerektirip gerektirmediğini doğruladığınızdan emin olun.

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 (https://tr.linkedin.com/in/semayuce), 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 yapmış olup, Nisan 2016 itibarıyla Trust ISC (www.trustisc.com) adıyla uzmanlık alanlarında hizmet vermekte olduğu kendi danışmanlık şirketini kurmuştur.

Kaynaklar

Sosyal Mühendsilik:	https://securingthehuman.sans.org/ouch/2017#january2017
Mobil Cihazınızı elden Çıkarma:	https://securingthehuman.sans.org/ouch/2016#december2016
Yeni Tabletinizi Güvenle Kullanma:	https://securingthehuman.sans.org/ouch/2016#january2016
OUCH Arşivleri & Çevirileri:	https://securingthehuman.sans.org/ouch/archives
Mobil Cihazların Güvenliği Kursu:	https://sans.org/sec575

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