Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Mobil Uygulamaları Güvenle Kullanmak

Genel Bakış

Tabletler ve akıllı telefonlar gibi mobil cihazlar hem özel hem de profesyonel hayatımızın en öncelikli teknolojilerinden bir haline geldi. Mobil cihazları bu kadar versatile hale getiren aralarından seçim yapabildiğimiz milyonlarca uygulama. Bu uygulamalar bizim daha üretken olmamızı, anlık iletişim ve başkalarıyla paylaşımı, eğitim ve öğretimi ya da sadece daha fazla eğlenceyi sunuyorlar. Ancak tüm bu güçlü yönlerin yanısıra bu mobil uygulamalar, riskleri de yanında getiriyorlar.

Konuk Yazar

Chris Crowley bağımsız danışman, sertifikalı SANS eğitmeni ve kurs yazarıdır. Twitter'da **@CCrowMontance** ve Google plus'da **+ChrisCrowley** hesapları ile aktiftir.

Mobil Uygulamaları Edinmek

İlk adım her zaman emin olduğunuz, güvenilir bir kaynaktan indirmektir. Herhangi birinin bir mobil uygulama geliştirebileceğini hatırlayın, dolayısıyla onları nereden edindiğiniz konusunda çok dikkatli olmalısınız. Siber suçlular gerçeğinden ayırdedilemeyen ve kötü niyetli yazılımlar içeren uygulamalar yaratma ve dağıtmadaki becerilerini çok geliştirdirler. Eğer bu uygulamalardan birini kurduysanız, bu suçlular e-postalarınızı okumak, konuşmalarınızı dinlemek ya da kontaktlarınızın bilgilerini almak için mobil cihazınızın kontrolünü ele geçirebilirler. Uygulamaları sadece iyi bilinen, güvenilir kaynaklardan indirerek, kötü niyetle değiştirilmiş uygulamaları kurma ihtimalinizi azaltırsınız. Bu konuda farkında olmadığınız şey, seçeneklerinize kullandığınız mobil cihazın markasının karar vermesi olabilir.

iPad ya da iPhone gibi Apple cihazlarında, mobil uygulamaları sadece Apple "app store" adı verilen yönetilen bir ortamdan indirebilirsiniz. Bunun avantajı, Apple'ın hem mobil uygulamalar hem de yazarları ile ilgili güvenlik kontrolü yapmasıdır. Apple tüm kötü niyetli insanları ya da yazılımları yakalayamıyor olsa da, bu yönetilen ortam kötü niyetli bir yazılımı indirme riskini çok büyük bir oranda azaltır. Buna ek olarak, eğer Apple böyle bir yazılımı bulursa, hızlı bir şekilde "app store" dan kaldırmaktadır. Windows Phone da, uygulamaları yönetmek için buna benzer bir yaklaşım kullanır.

Android mobil cihazlar farklıdır. Android size internet üzerinde istediğiniz yerden mobil bir uygulamayı indirme esnekliği verir. Ancak bu esneklik, aynı zamanda daha fazla sorumluluk demektir. İndirip kurduğunuz mobil uygulamaların tamamı gözden geçirilmediğinden çok daha dikkatli olmanız gerekir. Google, adı "Google Play" olan ve Apple'ınkine benzeyen

Mobil Uygulamaları Güvenle Kullanmak

bir yönetilen mobil uygulama dükkanına sahiptir. Google Play'den indirdiğiniz uygulamalar bazı temel kontrollerden geçmektedir. Bu nedenle biz sizlere, Android cihazlarınız için uygulamaları, Google Play'den indirmenizi öneriyoruz. Diğer internet sitelerinden Android mobil uygulamaları indirmekten kaçının zira herhangi bir siber suçlu çok basit bir şekilde bir kötü niyetli uygulama yaratıp dağıtabilir. Ek bir koruma önlemi olarak, mobil cihazınıza anti-virüs yazılımı kurmayı değerlendirin.

Mobil uygulamaları güvenli bir şekilde kullanmanın anahtarı, sadece güvenilir kaynaklardan kurmak, uygulamalarınızın güncel olduğundan ve doğruladığınız izinlere sahip olduğundan emin olmaktır.

Riski daha da azaltmak için, çok yeni olan, sadece birkaç kişinin indirdiği ya da çok az olumlu yorum almış uygulamalardan uzak durun. Bir uygulama ne kadar uzun süredir yayındaysa ya da ne kadar çok olumlu yorum aldıysa, o kadar güvenilir olmaya yakındır. Ek olarak sadece ihtiyacınız olan ve kullanacağınız uygulamaları indirin. Kendinize, bu uygulamaya gerçekten ihtiyacım var mı diye sorun. Her uygulama yeni potansiyel güvenlik açıklıkları getirebileceği gibi, aynı zamanda kişisel bilgi gizliliği konuları da oluşacaktır. Eğer bir uygulamayı kullanmaktan vazgeçtiyseniz, mobil cihazınızdan silin (eğer ihtiyaç duyarsanız her zaman yeniden ekleyebilirsiniz)

Son olarak, mobil cihazınızı jailbreak ya da root yapmış olabilirsiniz. Bu, cihazınızın mevcut özelliklerini değiştirme ve onaylanmamış uygulamaları yükleyebilme sürecidir. Biz bunu sadece birçok güvenlik kontrolünü atlattığınız için değil aynı zamanda garanti ve destek sözleşmelerinizi de geçersiz kıldığı için hiç önermiyoruz.

İzinler

Bir mobil uygulamayı güvenilir bir kaynaktan kurduktan sonraki aşama, güvenli bir şekilde konfigüre edilmesi ve sizin kişisel bilgilerinizin gizliliğinin korunmasıdır.Mobil uygulamaları kurmak ve / veya konfigüre etmek genel olarak belirli izinlerin verilmesini gerektirir. Bir uygulamaya herhangi bir izni vermeden once mutlaka bu uygulamanın işini yapabilmesi için gerçekten bunlara ihtiyacı var mı diye düşünün. Örneğin, bazı uygulamalar konumlandırma servislerini kullanır. Eğer bir uygulamaya bu izni verirseniz, bu uygulamanın yaratıcısına tüm hareketlerinizi izleme hakkı verirsiniz, hatta başkalarına bile satabilirler. Eğer bir uygulamaya, sizden istediği izinleri vermek istemiyorsanız, uygulama dükkanında ihtiyacınızı karşılayan başka uygulama seçenekleri olup olmadını araştırın. Apple cihazları lokasyon bilgisine erişim gibi bazı izinleri "Ayarlar" seçeneğinden değiştirmenize izin verir. Windows ve Android mobil cihazları farklıdır, size ya hep, ya hiç yaklaşımını sunar. Eğer bir uygulamanın istediği tüm izinleri vermezseniz, uygulamayı kuramazsınız.

Mobil Uygulamaları Güvenle Kullanmak

Uygulamaları Güncellemek

Mobil uygulamalar, tıpkı bilgisayarınız ve mobil cihazınızın işletim sistemi gibi güncel kalabilmeleri için güncellenmelidir. Suçlular sürekli bir şekilde uygulamalardaki açıklıkları aramak ve bulmak ile meşgul. Sonrasında da bu açıklıkları kullanan saldırılar geliştiriyorlar. Uygulamalarınızı yazanlar da, bu açıklıkları kapatan ve cihazlarını koruyan güncellemeler yayınlıyorlar. Güncellemeleri ne kadar sık kontrol edip kurarsanız, o kadar iyidir. Birçok platform mobil uygulamalarınızın güncellemelerini otomatik olarak kontrol etmenize izin veriyor. Biz bu seçeneği kullanmanızı öneriyoruz. Bu mümkün değilse, en azından her iki haftada bir uygulamalarınızın güncelliğini kontrol etmenizi öneriyoruz. Bununla birlikte her güncelleme sonrasında uygulamalarınızın yeni izinlere gereksinimi olup olmadığını doğruladığınızdan emin olun.

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

Sosyal Mühendislik:	http://www.securingthehuman.org/ouch/2014#november2014
Mobil Cihazınızı Elden Çıkarmak:	http://www.securingthehuman.org/ouch/2014#june2014
Yeni Tabletinizi Güvenli Hale Getirmek:	http://www.securingthehuman.org/ouch/2013#december2013
Genel Güvenlik Terimleri:	http://www.securingthehuman.org/resources/security-terms
SEC575: Mobil Cihaz Güvenliği Kursu:	http://www.sans.org/sec575

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