Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

- Kişisel Verileriniz
- Cihazınızı Güvenli Bir Şekilde Silmek
- SIM / Harici Depolama Kartları

Mobil Cihazınızı Elden Çıkarmaya Hazırlarken

Genel Açıklama

Akıllı telefonlar ve tabletler gibi mobil cihazlar gelişmeye devam ediyorlar ve bu alanda baş döndürücü bir hızla inovasyon yapılıyor. Sonuç olarak her 18 ayda bir çoğumuz mobil cihazlarımızı yeniliyoruz. Maalesef birçok insan mobil cihazlarını üzerlerinde ne kadar kişisel veri olduğu konusunda çok düşünmeden basitçe elden çıkarıyor. Bu bültende mobil cihazlarınız üzerinde hangi tür kişisel verilerinizin olabileceğini ve elden çıkarmadan ya da iade etmeden önce nasıl güvenli bir şekilde temizleyebileceğinizi ele alacağız. Eğer mobil cihazınız size işvereniniz tarafından verildiyse ya da üzerinde organizasyonel veri bulunuyorsa, aşağıdaki adımları uygulamadan önce, uygun yedekleme ve elden çıkarma prosedürlerini uyguladığınızdan emin olmak için kurumunuzdaki yetkililerle görüşün.

Konuk Yazar

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) Washington, DC bölgesinden bir danışman, SANS Enstitüsü'nde Mobil Cihaz Güvenliği ve Etik Hacking (SEC575) kursunun baş eğitmeni ve Olay Müdahale Ekipleri Yönetimi (MGT535)'in de yazarıdır.

Kişisel Verileriniz

Mobil cihazlarınız farkında olduğunuzdan, hatta bilgisayarınızdan bile daha fazla hassas veri barındırır. Bir mobil cihazda genel olarak aşağıdaki bilgiler tutulabilir:

- Yaşadığınız, çalıştığınız ve sıklıkla ziyaret ettiğiniz yerler
- Adres defterinizde yer alan herkesin (aileniz, kişisel / mesai arkadaşlarınız, vb.) iletişim bilgileri
- Gelen, giden ve cevapsız olan tüm çağrıların tarihçesi
- Metin ve ses mesajları
- Oyunlar ya da sosyal medya sitelerindeki uygulamalar aracılığıyla yaptığınız mesajlaşmalar
- GPS koordinatları ya da hücresel erişim noktası bazında lokasyon tarihçesi
- Internet geçmişiniz, çerezler ve ara belleğe alınan ziyaret ettiğiniz sayfalar
- Kişisel fotoğraflarınız, videolarınız, ses kayıtlarınız ve e-postalarınız
- Çevrimiçi bankacılık uygulamaları ya da kurumsal e-postanız gibi uygulamalar için kullandığınız şifreler ve kişisel hesaplarınıza erişim yetkileri
- Bulut ortamlarında depoladığınız fotoğraflar, dosyalar ya da verilerinize erişim yetkileri
- Sağlığınız ile ilgili nabzınız, tansiyonunuz ya da diyetinize ait bilgiler

Mobil Cihazınızı Elden Çıkarmaya Hazırlarken

Cihazınızı Güvenli Bir Şekilde Silmek

Gördüğünüz üzere mobil cihazınızda azımsanmayacak ölçüde hassas verileriniz olabilir. Bağışlayarak, başka bir aile üyesine vererek, satarak ya da basitçe çöpe atarak bile olsa mobil cihazınızı nasıl elden çıkaracağınızdan bağımsız olarak, ilk önce üzerindeki tüm hassas verileri sildiğinizden emin olmalısınız. Ek olarak, geri veriyorsanız ya da yenisi ile değiştiriyorsanız, üzerindeki tüm bilgileri tamamen silmelisiniz. Eğer bunu yapmazsanız, mobil cihazınızı alan kişi kolaylıkla bilgilerinize erişebilir. Ancak verilerinizi silmeye başlamadan önce, fotoğraflarınız, videolarınız ve diğer bilgilerinizin tamamının yedeğini almalısınız. Bir kez tamamen silme işlemi uyguladığınızda, o cihazdaki hiçbir veriyi geri döndürme şansınız olmayacak.

Mobil cihazınızı elden çıkarmadan önce, fabrika ayarlarına döndürdüğünüzden ve eğer kullanıyorsanız SIM ya da SD kartları içinden çıkardığınızdan emin olun.

Verilerinizin yedeğini aldıktan sonra güvenli bir şekilde silmelisiniz. Basitçe dosyaları, fotoğrafları ya da verilerinizi silmek yeterli değildir. Internette bulunabilecek birçok bedava uygulama aracılığı ile silinen veriler geri döndürülebilir. Bunun yerine cihazdaki tüm veriyi güvenli bir şekilde silmelisiniz. Bunun anlamı bilgilerin üzerine, geri döndürülemeyeceğinden emin olacak şekilde yazmaktır. Bunu yapmanın en kolay yöntemi, cihazının "Fabrika Ayarlarına Dön" seçeneğini kullanmaktır. Bu fonksiyon, cihazınızı ilk alındığı günkü haline döndürür. Deneyimlerimize göre, bu özellik cihazınızı güvenli bir şekilde silmek için, en güvenli ve en basit yöntemdir. Bazı mobil cihazlar arasında farklılıklar gösterse de, en popüler 3 cihaz için izlenmesi gereken adımlar aşağıda listelenmiştir.

- Apple iOS Cihazlar: Ayarlar | Genel | Sıfırla | Tüm İçerik ve Ayarları Sil
- Android Cihazlar: Ayarlar | Güvenlik | Fabrika Ayarlarına Dön
- Windows Telefonlar: Ayarlar| Hakkında | Telefonu Sıfırla

Eğer bu fonksiyonun kullanımı ile ilgili hala sorularınız varsa, kullanım kılavuzunu ya da üreticinin internet sitesini inceleyebilirsiniz. Lütfen unutmayın, basit bir silme işlemi yeterli değildir ve bilgileriniz kolaylıkla açığa çıkarılabilir.

SIM & Harici Depolama Kartları

Cihazında saklanan verilerin yanısıra, SIM (Subscriber Identity Module) kartınızı da değerlendirmelisiniz.
SIM kart mobil cihazınızın telefon görüşmeleri ya da veri bağlantıları için kullandığı karttır. Cihazınızı fabrika ayarlarına döndürseniz bile, SIM kartınızda hesabınız hakkındaki bilgiler duruyor olacaktır. Eğer telefon numaranızı farklı bir cihazda kullanmaya devam edecekseniz, telefon satıcınız ile SIM kartınızın transfer edilmesi için görüşün. Eğer

Mobil Cihazınızı Elden Çıkarmaya Hazırlarken

mümkün değilse, örneğin yeni telefonunuz farklı bir boyutta SIM kart kullanıyorsa, eski SIM kartınızı alın, başka birinin eline geçerek kullanılmasını engellemek için fiziksel olarak kırın ya da imha edin.

Ayrıca, bazı mobil cihazlar ayrı bir SD (Secure Digital) kartı, ek depolama ihtiyaçları için kullanımı destekler. Bu kartlarda genel olarak fotoğraflar, akıllı telefon uygulamaları ve diğer hassas içerik bulunabilir. Cihazınızı elden çıkarmadan önce eğer varsa tüm harici depolama kartlarını da çıkarmayı unutmayın. Bu kartları, yeni mobil cihazınızda yeniden kullanabilir ya da bir USB adaptörü ile bilgisayarınızda genel bir depolama aygıtı olarak değerlendirebilirsiniz. Eğer bu SD kartları yeniden kullanma imkanınız yoksa, tıpkı eski SIM kartlarınız gibi, fiziksel olarak imha etmenizi öneririz.

Eğer bu bültende yer alan adımların herhangi birinden şüpheniz varsa, mobil cihazınızı aldığınız satıcıya giderek, eğitimli bir teknik personelden yardım talep edin. Son olarak, eğer cihazınızı çöpe atacaksanız, ikinci el mobil cihazları kabul eden birçok sosyal yardım kuruluşundan birine bağış yapmanızı öneririz.

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

NIST SP800-88 Revizyon 1: http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf

OUCH! Yedekleme: http://www.securingthehuman.org/ouch/2013#september2013