Bilgisayar Kullanıcıları için Aylık Güvenlik Farkındalığı Bülteni

OUCH!

BU SAYIDA...

Sosyal Medya

Genel Bakış

Facebook, Twitter, Instagram ve Linkedin gibi sosyal medya platformları size dünyanın dört bir yanındaki insanlarla tanışma, etkileşim ve paylaşma imkanı veren harika kaynaklardır. Ancak, böyle bir güç beraberinde sadece sizin için değil aileniz, arkadaşlarınız ve işvereniniz için de riskler getirir. Bu bültende, risklerden doğacak tehlikeleri ve bu platformları güvenli bir şekilde nasıl kullanmanız gerektiği konusunu açıklamaya çalışacağız.

Konuk Yazar

Tanya Baccam, uzun süredir güvenlik danışmanlığı yapmaktadır. Kendisi SANS yazarı olmakta birlikte on yılı aşkın süredir de SEC502, SEC542, SEC401, MGT414, AUD507 ve birçok kursun eğitmenidir. Kendisini Twitter hesabı **@tbaccam** üzerinden takip edebilirsiniz.

Gizlilik

Sosyal medya ile ilgili genel kaygı kişisel bilgilerin korunmasıdır. Potansiyel tehlikeler şunlardır:

- **Geleceğinizin etkilenmesi**: Bazı kuruluşlar özgeçmiş kontrolü için sosyal medya platformlarını kullanmaktadır. Utandırıcı veya suç içeren fotoğraflar veya gönderiler, ne kadar eski olursa olsun, işe alınmanızı veya terfi etmenizi engelleyebilir. Ayrıca, bazı üniversiteler de aynı araştırmaları öğrenci kabul süreçlerinde yapmaktadır. Bu kuruluşlar, sizden sayfalarını "beğenmelerini" veya sayfalarına katılmanızı isteyebileceği veya bazı gönderiler birden fazla sitede arşivlenebileceği için gizlilik ayarları sizi korumayabilir.
- **Size karşı saldırılar**: Siber saldırganlar gönderilerinizi analiz ederek, bu bilgileri size veya sizin kuruluşunuza ait bilgilere erişim sağlamak için kullanabilir. Örneğin, saldırganlar paylaştığınız bilgileri; parolanızı sıfırlamak için kullanılan "gizli soru"larınızın cevaplarını tahmin etmek için, hedef odaklı e-posta oltalama saldırıları yapmak için veya siz gibi davranıp kuruluşunuzdaki birisini telefonla aramak için kullanabilir. Ayrıca, bu ataklar çalıştığınız veya yaşadığınız yerin öğrenilmesi gibi fiziksel dünyayı da etkileyebilir.
- **İşvereninize yanlışlıkla zarar vermek**: Suçlular veya rakipler, kuruluşunuz ile ilgili paylaştığınız her türlü hassas bilgiyi işvereninize karşı kullanabilir. Ayrıca, gönderileriniz kuruluşunuzun saygınlığına zarar verebilir. İşiniz ile ilgili herhangi bir paylaşım yapmadan önce, kuruluşunuzun politikalarını kontrol ettiğinizden ve sosyal medya hesaplarınızın izlenmediğinden emin olun.

En iyi koruma yöntemi, paylaşımlarınızı sınırlamaktır. Gizlilik ayarları bir miktar koruma sağlayabilir, ancak, bu özellikler genelde karışıktır ve sizin bilginiz olmadan çok sık değişir. Gizli olduğunu düşündüğünüz bir şey, çeşitli sebepler nedeniyle bir anda genele açık olabilir. Ayrıca, gönderilerinizin gizliliği insanların onu paylaştığı kadar güvendedir. Bilgiyi ne kadar arkadaşınız veya kişi ile paylaşırsanız, o kadar genele açık olacaktır. Paylaştığınız herhangi bir şeyin genele açık bir hale geleceğinin veya gelebileceğinin ve o paylaşımın internet'in kalıcı bir parçası olacağının veya olabileceğinin farkında olmalısınız.

Sosyal Medya

Son olarak, arkadaşlarınızın sizinle ilgili paylaşımlarına dikkat etmelisiniz. Sizi rahatsız eden bir şey paylaştıklarında, onlardan bu paylaşımı kaldırmasını isteyin. Eğer, bu isteğinizi reddederlerse, sosyal medya platformu ile irtibata geçerek kaldırılmasını istemelisiniz. Aynı zamanda, siz de başkaları ile ilgili yaptığınız paylaşımlarda saygılı olmalı ve dikkat etmelisiniz.

Sosyal medya platformları eğlenceli ve güçlüdür ama ne paylaştığınıza ve kimle paylaştığınıza dikkat edin.

Güvenlik

Gizlilik başlığı altındaki önerilere ek olarak bu başlık altında da sosyal medya hesaplarınız ve çevrimiçi aktivitelerinizi korumak için bazı adımlar bulunmaktadır.

- **Giriş**: Tüm hesaplarınızı güçlü, benzersiz parola ile korumalı ve bu parolayı kimseyle paylaşmamalısınız. Ayrıca, bir çok sosyal medya platformu iki aşamalı doğrulama gibi güçlü kimlik doğrulama yöntemlerini desteklemektedir. Mümkün olan her zaman bu güçlü kimlik doğrulama yöntemleri etkinleştirilmelidir. Son olarak, sosyal medya hesaplarınızı başka internet sitelerine giriş için kullanmayın; eğer hesabınız ele geçirilirse bütün hesaplarınız savunmasız kalacaktır.
- **Gizlilik Ayarları**: Gizlilik ayarlarını kullanıyorsanız, bu ayarları iyi inceleyin ve düzenli olarak test edin. Sosyal medya platformları sık sık gizlilik ayarlarını değiştirdikleri için hata yapmak kolaydır. Ayrıca, bir çok uygulama ve servis konum bilgisi eklemenize imkan tanır (bu özellik geotag olarak adlandırılır). Eğer konum bilginizin gizli kalmasını istiyorsanız, bu ayarları düzenli olarak kontrol edin.
- **Şifreleme**: Sosyal medya platformları çevirimiçi bağlantılarınızı koruyan ve HTTPS olarak adlandırılan şifrelemeyi kullanır. Twitter ve Google+ gibi platformlar bu şifreleme yöntemini varsayılan olarak kullanırken, diğer platformlarda manuel olarak etkinleştirilmesi gerekmektedir. Sosyal medya hesabınızın ayarlarını kontrol edip varsayılan bağlantı olarak HTTPS şifrelemesini etkinleştirin.
- **E-posta**: Sosyal medya platformlarından gelmiş gibi gözüken şüpheli e-postalara dikkat edin, bu e-postalar siber suçlular tarafından gönderilen aldatıcı saldırılar olabilir. Bu tip mesajlara cevap vermenin en güvenli yolu, muhtemelen kaydedilmiş bir yer iminden doğrudan sosyal medya platformuna giriş yapmak ve mesajları okumak veya cevap vermektir.
- **Zararlı bağlantılar/'Scam'**: Sosyal medya platformlarında bulunan şüpheli bağlantılar ve potansiyel 'scam'lar (dolandırıcılık faaliyetlerinde bulunan internet siteleri) konusunda dikkatli olun. Art niyetli kişiler, saldırılarının yayılması için sosyal medya platformlarını kullanır. Arkadaşınız tarafından gönderilen bir ileti, gerçekten ondan geldiği anlamına gelmez; hesabı ele geçirilmiş olabilir. Bir aile üyesi veya arkadaşınız doğrulayamayacağınız garip bir mesaj gönderirse (örneğin, soyulduğunu söylüyor ve sizden para istiyorsa), onlara telefonla veya mesajın ondan geldiğini doğrulayabileceğiniz başka bir yöntemle ulaşın.
- **Mobil Uygulamalar**: Sosyal medya platformlarının çoğu çevirimiçi hesaplarınıza erişmeniz için mobil uygulamalar sağlar. Bu mobil uygulamaları güvenilir kaynaklardan indirdiğinizden ve akıllı telefonunuzun güçlü bir parola ile korunduğundan emin olun. Akıllı telefonunuzu kaybettiğinizde kilitli değilse, herhangi biri sosyal medya hesaplarınıza erişerek sizin yerinize paylaşımlar yapabilir.

Sosyal Medya

Sosyal medya platformları, dünyanın geri kalanıyla iletişim kurmak ve bağlantıda kalmak için harika bir yoldur. Bu bültende özetlenen ipuçlarını takip ederseniz, çok daha güvenli çevrimiçi deneyimi yaşayabilirsiniz. Sosyal medya platformlarını güvenli kullanmak ve yetkisiz faaliyetleri bildirmek ile ilgili daha fazla şey öğrenmek için sosyal medya platformlarının güvenlik sayfalarını inceleyebilirsiniz.

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.

Mustafa Emrah Ünsür, Güvenlik Araştırmacısı olarak araştırmaları, makaleleri ve çevirileri vardır. Beyaz Şapkalı Hacker olarak kendisi tarafından kodlanan ve kodlanmakta olan 'exploit'ler ve 'tool'lar bulunmaktadır. Ayrıca, Sızma Testi Uzmanı olarak özel şirketlere ve devlet kurumlarına Zafiyet ve Sızma Testi yapmış ve yapmaya devam etmektedir.

Kaynaklar

Parolalar:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_tr.pdf
İki aşamalı doğrulama:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201408_tr.pdf
Mobil uygulamaları güvenle kullanmak:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201501_tr.pdf
Çocukları siber güvenlik konusunda eğitmek:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201506_tr.pdf
Facebook Security:	https://www.facebook.com/security

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