SOSYAL AĞLARDA GÜVENLİK VE FARKINDALIK

Prof. Dr. Şeref SAĞIROĞLU

SUNUM PLANI

- Sosyal Ağlar
- Güvenlik Zafiyetleri
- Senaryolar
- Güvenlik Tehditleri
- Önlemler
- Farkındalık Kapsamında Neden Sosyal Mühendislik?
- Sosyal Mühendislik Nedir?
- Saldırı Yöntemleri/Faydalanılan Zayıflıklar
- Kişisel ve Kurumsal Boyutta Nasıl Korunmalıyız?
- Sonuç

SOSYAL AĞLAR

- “bireyleri internet üzerinde toplum yaşamı içinde kendilerini tanımlayarak,
- aynı kültürel seviyesinde rahatlıkla anlaşabilecekleri
- insanlara internet iletişim metotları ile iletişime geçmek için ve aynı zamanda normal sosyal yaşamda yapılan çeşitli jestleri simgeleyen sembolik hareketleri göstererek
- insanların yarattığı sanal ortamdaki sosyal iletişim kurmaya yarayan”

ortamlar olarak tanımlanmaktadır

SOSYAL AĞ KULLANIMI

- Günlük hayatımızda en özel anılarımızı, duygu ve düşüncelerimizi, gelecek planlarımızı ve içinde bulunduğumuz süreçleri paylaşma ihtiyacı duymak
- Belirli bir konuma bağlı arkadaşlıkları yeniden tesis etmek
- Sanal görünümün verdiği rahatlık ve psikolojik tatmin.
  - Kendilerinin toplum tarafından kabul görmediğini düşünen buna bağlı kimlik arayışında olan kişiler
- …

SOSYAL AĞ SİTELERİ

- Facebook
- Twitter
- Myspace
- Yonja
- Friends Reunited
- Linked-in
- Friendster
- Buzz
- Blogger
- Bebo
- Hi5
- Perfspot
- Zorbia
- Netlog
- Badoo
- …

Facebook

- Kullanıcılarının veya üyelerin kişisel bilgilerinin yer aldığı (fotoğraflar, arkadaşlık bilgileri, kişisel yorumlar, ilgi alanları) bir sosyal ağdır.
- 400 milyona üzerinde kullanıcı vardır.
- Günde 10 milyonun üzerinde fotoğraf ve video eklenmektedir.

Twitter

- Kullanıcılarının anlık iletiler yayınlamasına izin veren bir paylaşım sitesidir.
- Anlık mesajların görüntülenebileceği ve kullanıcılar tarafından istenilen bağlantıların paylaşılabileceği bir yapıdadır.
- Twitter sitesinin 2009 yılı itibariyle 100 milyon kullanıcıya ulaştığı tahmin edilmektedir.

Blogger

- Bu sosyal paylaşım sitesi, yorucu bir günün ardından kişilerin günlüklerini yazmak için tercih ettikleri sosyal paylaşım sitesidir.
- Yazılan her günlük içinde o güne ait zaman damgası bulunmaktadır.
- Kullanıcılar sınırsız günlük oluşturabilir ve her günlük 2000 konu başlığı içerebilir.
- Ayrıca Google firmasının fotoğraf yükleme hizmeti Picasa ile bağlanarak günlük içinde albümlerin yayınlanmasına olanak tanımaktadır.

SOSYAL AĞLAR VE ÖZELLİKLERİ

	Facebook	MySpace	Bebo	Friendster	hi5	Orkut	PerfSpot	Yahoo! 360	Zorpia	Netlog
Yaş Sınırı	13	14	13	16	13	18	13	18	16	13
Reşit Olmayan Kullanıcı Yüzdesi	36	33	54	3	24	4	32	16	15	31
Profil Editörü (WYSIWYG)	Var	Var		Var	Var		Var	Var	Var	Var
Kullanıcı Bağıl Kod (HTML or CSS)		Var		Var						
Kişisel Bağlantı Kısayolu		Var	Var	Var	Var			Var	Var	Var
Fotoğraf Yükleme	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Yorum Yazma	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Arkadaşlıklar	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Günlük Hazırlama		Var	Var	Var	Var		Var	Var	Var	Var
3. Parti Uygulamalar	Var	Var	Var	Var	Var	Var	Var			
Gizlilik Ayarları	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Kullanıcı Engelleme	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Spam Bildirme	Var	Var	Var	Var	Var	Var				Var
Kötüye Kullanım Bildirme	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Güvenlik Önerileri	Var	Var	Var		Var	Var	Var	Var		
Kişileri Etiketleme	Var	Var	Var	Var	Var				Var	Var
Gruplar	Var	Var	Var	Var	Var	Var	Var	Var	Var	Var
Grup Oluşturma	Var	Var	Var		Var	Var	Var	Var	Var	Var
Tartışma Forumu	Var	Var		Var					Var	
E-Posta Gönderme	Var	Var	Var		Var	Var	Var	Var	Var	Var
Fotoğraf Paylaşma	Var	Var	Var		Var		Var		Var	
Kişisel Video Yükleme	Var	Var	Var	Var		Var			Var	Var
İsme Göre	Var	Var	Var				Var		Var	Var
E-Posta Adresine Göre	Var	Var	Var	Var	Var				Var	
Okul Adına Göre	Var	Var		Var					Var	
Şehir Adına Göre		Var		Var	Var		Var		Var	Var
İlgili Alanlarına Göre	Var	Var		Var					Var	
İstenilen Kelimelere göre		Var		Var	Var	Var		Var	Var	Var
Üye Olmadan Arama yapma		Var					Var		Var	

GİZLİLİK POLİTİKALARI GENEL BAKIŞ

- Sosyal paylaşım siteleri arayüz desteği verdikleri dillerde gizlilik politikası dil desteği vermemektedir.
- Bu sebeple sadece arayüz anadilinde olan kullanıcılar servise ait ve genellikle İngilizce olan gizlilik bildirimi (Privacy Policy) ve kullanım şartlarını (Terms of Service) görüntüleyebilmekte, kendi anadillerinde okuyamadıkları için bütün hükümleri peşinen kabul etmiş sayılmaktadır. Bu hükümler gereğince sosyal paylaşım sitelerine verdiğiniz tüm bilgiler bu servisi işleten kurumun malı olmaktadır.

GÜVENLİK POLİTİKALARI

	Facebook	Twitter	Myspace	Yonja	Friends Reunited	Linked-in	Friendster	Buzz	Blogger	Bebo	Hi5	Perfspot	Zorbia	Netlog	Badoo
Özel Bilgilerin 3. Kişilerle Paylaşılması	K	K	K	K	K	K	K	K	K	K	K	K	H	K	H
Kişisel Bilgilerden Özel Reklam Profili Oluşturma	E	-	E	E	E	E	E	E	-	E	E	E	E	E	E
Arama Motorlarına Tarama Hakkı	K	E	-	-	-	E	E	-	-	-	-	-	-	-	-
Kanunen Mahkemelere Destek Ulusal/Uluslararası	ABD	-	ABD	ABD	ABD	ABD	ABD	ABD	ABD	ABD	ABD	ABD	-	EU	EU
Profil Öğeleri Gizleme Desteği	E	-	E	E	E	E	E	E	E	E	E	E	-	E	E
Hesap Pasifleştirme	E	-	-	H	-	-	-	-	-	-	-	-	-	-	-
Hesap Silme	E	-	-	E	E	E	-	-	E	E	-	-	-	E	E
Silinen Hesap Bilgi Tutma Süresi	90 gün	-	-	-	1 Yıl	-	-	-	-	-	-	-	-	6 Ay	-
Bilgilerin Tutulduğu Ülke	ABD	ABD	ABD	ABD	UK	ABD	ABD	ABD	ABD	ABD	ABD	ABD	Çin	EU	Kıbrıs
Güvenli Sunucu Desteği	E	-	-	E	E	E	E	E	E	E	E	E	E	-	E
IP Tabanlı Loglama	E	E	E	-	-	E	E	-	-	-	E	E	E	-	E
Çerez Tabanlı Denetim	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Anonim İstatistik Toplama	-	-	E	-	-	E	-	-	-	E	E	E	-	E	-
Anadilde Kural Yayınlama	H	H	E	H	H	H	H	E	E	H	H	H	H	E	E
Kısıtlı: K, Evet: E, Hayır:H, Amerika Birleşik Devletleri: ABD, Birleşik Krallık: UK, Avrupa Birliği Üyesi Ülke: EU															

Güvenlik Zafiyetleri Oluşturabilecek Hususlar - 1

Sosyal ağlarda;

- anlık mesajlaşma
- bağlantı paylaşımı
- siyasi ve ideolojik paylaşımlar
- ailevi ve kişisel paylaşımlar
- fotoğraf paylaşımları
- uygulama paylaşımları

Güvenlik Zafiyetleri Oluşturabilecek Hususlar - 2

- Sanal hayatlarımızla gerçek hayatlarımızı karıştırmamızdan kaynaklanan güvenlik açıkları

- Kötü niyetli kişiler ihtiyacı olan ama bulamadıkları bilgilerin bireylerin kendileri tarafından ifşa edilmesi sayesinde kolaylıkla elde edilebilmektedir.

- Kötü niyetli kişiler sosyal ağlardan elde ettikleri bilgiler doğrultusunda yaptıkları saldırıların başında kimlik hırsızlığı ve sosyal mühendislik saldırıları gelmektedir.

Güvenlik Zafiyetleri Oluşturabilecek Hususlar - 3

- Sosyal ağ siteleri, istatistiksel ve bireysel bilgi toplayarak kullanıcıları izlemektedirler.
- Gizlilik politikalarında kişiye özel reklam hizmetleri altında yapmaktadırlar.
- Bilgi toplama, çerezler vasıtasıyla yapılmaktadır.
- Çerezler ile bireysel alışkanlıklarımıza ve internet kullanma kültürümüze erişilmektedir.

Güvenlik Zafiyetleri Oluşturabilecek Hususlar - 4

Sosyal ağ sitesinde hesabınız silinse bile, arama motorları tarafından taranan bilgilere erişimin kısıtlanması maksadıyla sadece kalıcı olduğunu düşündüğünüz önemsiz bilgiler sosyal ağ sitesinde paylaşılmalı veya yayımlanmalıdır.

TEHDİTLERİN SINIFLANDIRMASI

- Kimlikleri Taklit Etme
- İstenmeyen Epostalar (Spam) ve Bot Saldırıları
- Kötü Amaçlı Sosyal Ağ Uygulamaları
- Siteler Arası Kod Çalıştırma (XSS) ve Siteler Arası İstek Sahteciliği (CSRF) Saldırıları
- Kimlik Hırsızlığı
- Casusluk
- Sahte Linkler/Bağlantılar
- Bilgi Toplama Saldırıları

Senaryo-1

Kişisel Bilgi Elde etme

- Ad Soyad
  - Profil Kimlik Bilgisi (Herkese Açık)
- Doğum Tarihi
  - Profil Kimlik Bilgisi (Herkese Açık)
- Cep Telefonu Numarası
  - Profil Kimlik Bilgisi (Arkadaşlara Açık)
- Listesi
  - Ağ grubu ve arkadaş listesi

Senaryo-2

- Annenizin kızlık soyadı
  - Aile üyelerinden ekli ve etiketlenmiş arkadaşlar
- İnternet Şifresi Sıfırlamak için Gereken Bilgiler
  - Ad Soyad
  - Doğum Tarihi
  - Anne Kızlık Soyadı
  - Meslek, Adres, Eş adı vb.
  - Cep Telefonu

Senaryo - 3

Kişiler tatile çıktıklarını yada yaşadıkları bölgede bulunmadıklarını çeşitli profil mesajlarıyla ifşa etmektedir.

- Ev
- Ofis

Senaryo - 4

- Kendisini çocuk gibi tanıtan yetişkinler kız ve erkek çocuklar ile arkadaşlık kurmaktadır.
  - Video ve Resim paylaşımı
  - Rahatsız edebilirler
  - İstismar

Senaryo - 5

- 3. Parti Yazılımlar
  - Profilime Kim Bakmış
  - Tarla, Bağ, Bahçe
  - Eğlence
  - Müzik
  - …
- Active-X denetimleri
  - Truva Atları

Senaryo-6

İtibar ve değer kayıpları

- Küçük düşürücü fotoğraf ve videolar
  - Kişilerin kendi yüklediği
  - Başkalarının yükleyip etiketlediği
- Prestij ve itibar kaybı
- Fotomontaj teknikler

GELİŞTİRİLEN YAZILIM

- Facebook ID
- Kimlik
- Profil Fotoğrafı
- Doğum Tarihi
- Konum
- Politik Görüşü
- Dini Görüşü
- E-Posta
- Cinsiyet
- İlişki Durumu
- Ağlar
- Yıldönümü

- Yüksek Lisans
- Üniversite
- Lise
- Güncel Adres
- İşveren
- Pozisyon
- Ebeveynler
- Kardeşler
- Çocuklar
- İnternet Sitesi
- Cep Telefonu Numarası

NEDEN SOSYAL MÜHENDİSLİK?

- Bilgi güvenliğinde en zayıf halka
- İnsan
- Katmanlı güvenlik mimarisi ve insan faktörü

SOSYAL MÜHENDİSLİK NEDİR?

- **İkna ederek normalde vermeyecekleri bilgiyi insanlardan alma sanatı**

- **Amaç:** değerli bilgiye ulaşmak
- **Araç:** insan
- **Yöntem:** ikna

- **Etkili**dir, teknik bütün önlemleri bypass geçer
- **Kolay**dır, teknik bilgi gerektirmez
- **Hızlı** sonuç verir

Saldırı Yöntemleri/Faydalanılan Zayıflıklar

Sosyal Mühendislik saldırılarında kullanılan insani özelliklerimiz:

- Başkalarına yardımcı olma isteği
- İnsanlara güvenme eğilimi
- Soruna/çatışmaya girme korkusu

Saldırı Türleri/Yöntemler/Faydalanılan Zayıflıklar

- Taklit etmek (impersonation)
- Önemli biri gibi davranmak
- 3. bir şahsın yetkilerini kullanmak
- Teknik destek personeli gibi davranmak
- Bizzat lokasyona gitmek
- Çöpleri karıştırmak (dumpster diving)
- Omuzdan okuma (shoulder surfing)
- Yan masadan dinleme
- E-maillerle kandırmaya çalışmak
- Web sitesi aracılığıyla kandırmaya çalışmak

Kişisel ve Kurumsal Boyutta Nasıl Korunmalıyız?

- ✓ Kişisel ve kurumsal bilgi güvenliği farkındalığı
- ✓ Eğitim, bilinçlendirme

Kişisel ve Kurumsal Boyutta Nasıl Korunmalıyız?

Kurumsal boyutta:

- ✓ Kurumsal bilgi güvenliği yönetim sisteminin gerekliliği
- ✓ Kurumsal risk analizinin önemi

SONUÇ VE ÖNERİLER

SONUÇ VE ÖNERİLER - 2 Genel

- Gizlilik Politikaları okunmalı ve bu politikalarda yazan kurallara göre profil gizlilik ayarları yapılmalıdır.
- Kullanım Şartları okunmalı ve bu politikalarda yazan kurallara göre profil gizlilik ayarları yapılmalıdır.
- Hukuki Terimler
- Sadece İngilizce Kaynaklar

ŞİFRE KRİTERLERİ

- Şifre en 12 karakter olmalıdır.
- Şifre sayı ve karakter kombinasyonundan oluşmalı ve içinde “+”,”-“,”*” gibi özel karakterler olmalıdır.
- Şifre 3-4 ay arası periyotlar ile değiştirilmelidir.
- Şifre içinde birbirini takip eden rakam ya da harf bulunmamalıdır.
- Herhangi bir dil için sözlüklerde bulunan kelimeler şifre olarak kullanılmamalıdır.
- Şifre dijital ortamlarda saklanacaksa elektronik cüzdan gibi başka şifrelerle korunan, dijital olmayan ortamlarda saklanacaksa sadece evde saklanması tavsiye olunur. USB bellek gibi kaybolabilecek cihazlarda şifre saklanmamalıdır.
- Şifre yakınlık derecesine bakılmaksızın kimseyle paylaşılmamalıdır.
- Tüm hesaplar için farklı ve birbirine benzemeyen şifreler tercih edilmelidir.

FOTOĞRAF KRİTERLERİ

- Sadece profesyonel temalara sahip fotoğraflarınızı yükleyiniz.
- Komik durduğunuz veya aile üyelerinin olduğu fotoğrafları yüklemekten ve yüklediğiniz fotoğraflarda etiket kullanmaktan kaçınınız.
- Sosyal ağın izin verdiği ölçüde başka kişilerin albümlerinden kendi fotoğraflarınızı siliniz ve albüm sahibine fotoğrafınızı yüklememesi veya etiketlememesi gerektiği yönünde uyarıda bulunuz.
- Fotoğraflarınıza yapılan ve kişisel bilgi içeren yorumları siliniz.

ÇOCUKLAR

- sosyal ağ web siteleri kullanımı konusunda bilgilendirme
- yüz yüze konuşarak elde edilen deneyimler paylaşılmalı/ öğrenilmeli
- Gerçek adlarını kullanmamaları
- Adres, telefon, okunulan sınıf ve kimlik gibi ona ulaşılabilecek bilgilerin verilmemesi
- Verilmiş ise de kişisel bilgileri bu ortamlardan çıkartılması
- Yayınlanmak istenilen fotoğraflarda detay verilmemesine dikkat edilmeli
- Mümkünse çocuklar resimlerini paylaşmamalı
- Tanınmayan veya kendisinden emin olunmayan kişilerle haberleşmemeleri konusunda dikkatli olmalarını

UYARI!

Sosyal ağlarda farkında olunması gereken en önemli nokta görüştüğünüz şirket sahibinin 13 yaşında bir çocuk veya şirketin çaycısı olabileceği gerçeğini göz ardı etmemektir.

SONUÇ VE ÖNERİLER - 2

- Kimlik bilgileriniz hiçbir şekilde paylaşılmamalıdır.
- Doğum tarihi ve yeri gibi bilgiler yanlış verilmelidir.
- Ad Soyad yerine arkadaşlarınızın sizi tanımlamada kullandıkları bir takma-ad kullanılabilir.

SONUÇ VE ÖNERİLER - 3

- Sosyal mühendislik ataklarına karşı koyabilmek için mümkün olduğunca yeni ve bilinmeyen gruplar içinde yer alınılmamalıdır.
- Bilişim korsanları kendilerini, alıcı kişinin arkadaşı gibi göstererek tuzak e-postalar gönderebilmektedir.
  - Özellikle, ekinde dosya ya da bağlantı bulunan epostaları gönderen kullanıcıdan **başka bir haberleşme aracı kullanılarak teyit alınması ve daha sonra açılması tavsiye olunur.**

ÖNLEMLER - 3

- Yeni sosyal ağlara katılma davetleri mümkün olduğunca araştırma yapıldıktan sonra çok gerekli ise kabul edilmelidir.
- Arkadaşların e-posta adreslerini vermekten kaçınmak için, sosyal ağ sitelerinin, arkadaş e-posta adreslerine ulaşmak için e-posta adres defterini taramasına izin verilmemelidir.

ÖNLEMLER - 4

- Yeni bir sosyal ağa üye olunduğunda; bu ağdaki diğer kişileri bulmak üzere e-posta hesap ve parola bilgilerini girmeniz istenebilir. Bu sayede elde edilebilecek olan e-posta adresleri, gerçek kişileri beyan eden reklam firmalarına satılabilir. Üye olunan sosyal ağ sitesinin tüm e-posta haberleşmenizi tarayabileceği de unutulmamalıdır.

- Sahte sitelere karşı sadece bir e-posta mesajında veya bir web sitesinde yer alan bağlantılar üzerinden tıklanarak ağlara erişmeye çalışılmamalıdır. Mümkünse adres satırına erişmek istediğiniz web sitenin adresi ilgili yere yazılarak veya kopyalanarak web sitesine erişmeye çalışılmalıdır. Bu sayede, sosyal paylaşım sitesi gibi gösterilen tuzak sitelerin ağlarına düşülmeyecektir.

ÖNLEMLER - 5

- Erişilen veya üyesi olunan sitelerde, 3. parti uygulamalar kişisel bilgilerinize erişmek için bilgisayarınıza yazılım yüklemeye çalışabilirler. Bu durumlarda sadece güvenilir yayımcılar tarafından listelenmiş eklentiler bilgisayarlara kurulmalıdır. Ayrıca; temel güvenlik önlemlerini almak için bilgisayar yazılımları güncel tutulmalı, antivirüs ve Güvenlik duvarı yazılımları mutlaka kullanılmalı ve kötücül yazılım ile spam engelleyici filtreler tercih edilmelidir.
- Sosyal ağ sitelerini kullanırken, kayıt olmak için şirket alan adı uzantılı e-posta adresi kullanılmamalıdır. Çalışılan kurumun üye olmak istenilen sosyal paylaşım sitesi için kuralları varsa bunlara uyulmalıdır.
- Profil sayfalarında kurumsal bilgiler paylaşılmamalıdır.
- Kimlik hırsızlıklarına karşı korunmak için, sadece doğruluğundan emin olunan kişiler arkadaş listesin eklenmelidir.

ÖNLEMLER - 6

- Anlık e-postalarda yazışırken, bulunduğunuz durumu en genel hatlarıyla anlatacak mesajlaşma yaklaşımları seçilmelidir.

- Tatile çıktığınızı belirten veya iş yerinde yaşadığınız sıkıntılı bir olayı belirtir anlık e-postalar gönderilmemelidir. Bu tarz bilgilerin üçüncü taraflar tarafından görüntülenebileceği, sonrasında bu açıklamalar veya bilgilerin kullanılarak, farklı bilgilerin sızdırılabileceği unutulmamalıdır.

ÖNLEMLER-7

- Profilinizde yada arkadaşınızın sayfasında özel bir konuyu, olayı veya kişiyi hedef alan yorum yazmaktan kaçınınız.

- Eriştiğiniz bilgisayarın kötücül yazılım tehdidine karşı işletim sistemi güncellemelerinin tam olduğundan ve sistemi koruyan güvenlik yazılımları(antivirüs, güvenlik duvarı, vb.) bulunduğundan emin olunuz.

SONUÇ VE ÖNERİLER - 3

- Sosyal paylaşım ağları doğru kullanılmadıkları takdirde, kişisel bilgilerin çalınması açısından ve kötücül yazılım saldırıları için büyük bir risk altındadır.

- Kişisel bilgi güvenliğinin sağlanması için kurumların alması gereken tedbirler ise öncelikli olarak kullanım şartları ve gizlilik politikalarının kesin ve anlaşılır kurallar etrafında belirlenmesi olacaktır.

- İnternet ortamında gerçekleştirdiğimiz her türlü işlemi bilgi güvenliği farkındalığına dikkat ederek gerçekleştirmeliyiz.

TEŞEKKÜR EDERİM!