Sosyal Ağlarda Güvenlik

Görkem Erdoğan[1], Şerif Bahtiyar[2]

[1] İstanbul Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü, Ayazağa, İstanbul

[2] Progress Ar-Ge Merkezi, Provus Bilişim Hizmetleri A.Ş., Şişli, İstanbul

erdogangor@itu.edu.tr, serif.bahtiyar@provus.com.tr

Özet: Sosyal ağlar son yılların en önemli teknolojilerden biri haline geldi. Bu ağlar çok sayıda kullanıcının kişisel bilgilerini içerdiği için saldırganlar için çok çekici bir hedef halini aldı. Bu durumun temel sebebi, sosyal ağ kullanıcılarının, bilgi güvenliği ile ilgili yeterince bilinçli olmamasıdır. Bu bildiride, sosyal ağ kullanıcılarını bilgi güvenliği alanında bilinçlendirmek amacı ile bu ağlardaki güvenlik açıklarını araştırdık ve güvenlik ile ilgili dikkat edilmesi gereken noktaları vurguladık.

Anahtar Sözcükler: Sosyal Ağ, Mahremiyet, Güvenlik, Tehdit, Risk

Security Issues in Social Networks

Abstract: Social networking has become one of the significant technologies in recent years. Since lots of people interact over social networks and put their private information on them, the networks have become an attractive target for malicious users. Protecting privacy of users in such networks is an important research challenge. In this paper, we have examined security threads and solutions in social networks to increase security awareness of the users.

Keywords: Social Network, Privacy, Security, Threat, Risk.

1. Giriş

Sosyal ağ iletişimi, insanların elektronik ortamda bir kimlik alarak, birbirleriyle iletişim kurdukları, bilgi alışverişi yaptıkları ve yeni arkadaşlar buldukları bir web tabanlı servistir. Dünyanın her yerinden, özellikle de genç kullanıcılar tarafından her gün bu ağlar ziyaret edilmektedir [1].

Internet aracılığıyla yapılan sosyal haberleşmelerinde genellikle web siteleri kullanılmaktadır. Bu siteler sosyal ağ siteleri olarak adlandırılmaktadır. Sosyal ağ sitelerinin neredeyse bir milyara yakın kullanıcısı bulunmaktadır. Popüler sosyal ağ sitelerinden bazıları Facebook, Twitter, Myspace'tir. Günümüzde, Facebook'un 400 milyondan fazla aktif kullanıcısı ve 2 milyardan fazla medya bileşeniyle (video, resim) en büyük sosyal ağ konumunda [2].

Bu ağlara katılan bireyler bir çok fayda sağladığı gibi, bir çok olumsuzlukla da karşı karşıya kalmaktadırlar.

Bu bildiride, sosyal ağların olumsuz yönlerini ve kişisel hesapların güvenliğini sağlama yöntemlerini ele aldık.

Kısacası, bildirinin ikinci bölümünde sosyal ağlarda güvenlik gereksinimlerini ortaya koyduk. Sosyal ağlarda güvenlik tehditleri ve gizlilik gereksinimlerini üçüncü bölümde açıkladık. Ondan sonraki bölümde, sosyal ağlardaki kötü yazılımları açıkladık. Beşinci bölümde, sosyal ağlardaki mevcut sorunları gösterdik ve olası çözüm önerilerini sunduk. Son bölümü, bildiriyi tamamlayıp gelecekte yapılabilecek çalışmaları anlatmaya ayırdık.

2. Sosyal Ağlarda Güvenlik Gereksinimleri

Bilgi sistemleri kullanıcıları çeşitli güvenlik gereksinimleri vardır. Sosyal haberleşmede temel olan güvenlik gereksinimleri aşağıdaki gibidir:

Mahremiyet: Bilginin kimliği belirsiz şahıslardan gizlenmesini demektir. Mahremiyet hassas bilgilere doğru kişilerce erişimi sağlarken, yanlış erişimleri engeller.

Bütünlük: Bilginin kimliği belirsiz şahıslarca değiştirilmemesi anlamına gelir. Veriler iletişim esnasında değiştirilmemeli ve üçünü kişilerce verilerin bütünlüğü bozulmamalıdır [3].

Uygunluk: Bilgiye erişmesinde sakıncası olmayan kişilere bilgi erişiminin sağlanmasının garanti edilmesidir.

İletişim Gizliliği: Kullanıcılar arası ilişkilerin üçüncü şahıslarca erişilememesi anlamına gelir.

Kullanıcı Haberleşmesi Gizliliği: Sosyal ağlarda güvenlik aynı zamanda kullanıcı bilgilerine, ağ operatörlerince erişimini engellemiyor olabilir. Ancak kullanıcının gizlilik gereksinimlerine göre, kullanıcının IP adresi, mesajları gibi bilgilerine ağ operatörleri erişmemelidir ki kullanıcı haberleşme gizliliği sağlansın.

3. Sosyal Ağlarda Güvenlik Tehditleri ve Gizlilik Meseleleri

Cisco'nun 2013 yılı için Yıllık Güvenlik Raporuna göre online siteler arasında en çok güvenlik tehdidi sosyal ağlarda, özellikle de yüksek sayıda kullanıcısı olan sosyal ağlarda meydana gelmiştir [4]. Sosyal ağların kullanımındaki artış, ilgili risklerin artışını da tetiklemiştir. Bu bölümde tipik sosyal ağ sahtekârlıklarını ve tehditlerini ele aldık.

3.1 Kimlik Hırsızlığı

Kimlik hırsızlığı, bir kişinin kimlik bilgilerine erişmek ve bu bilgileri sosyal ağda kendi menfaati için kullanmak demektir [5]. Kullanıcıların sosyal ağlardaki paylaşımları bazen kimlik hırsızlarının yeterli bilgileri ele geçirmesi için yeterli olmaktadır. Bazı saldırganlar da kullanıcı bilgisine erişim için kullanıcıdan izin isteyen uygulamalarla saldırmaktadır. Kullanıcı bilgilerine erişebilir izni verdiğinde ise saldırgan bu bilgilere erişir ve kötüye kullanabilir. Kimlik hırsızlığı genelde kullanıcı şifresi, banka hesap bilgilerini çalmayı hedefler.

3.2 Dolandırıcılık

Bir başka kullanıcının şifresi kullanılarak ve banka hesap bilgilerini çalma gibi yöntemler e-dolandırıcılık yöntemleri kapsamına girer. Burada saldırganlar yasal bir siteden posta gönderiyormuş gibi yaparak kullanıcı bilgilerini elde etmeye çalışır. Yasal bir siteden posta geldiğini sanan kullanıcı ilgili linki tıklar ve aslında bilgilerinin çalınacağı sayfaya yönlendirilmiş olur. Bilgileri çalınan kişi çalan tarafından bu bilgiler kullanılarak dolandırılır.

3.3 Profil Klonlama

Bu saldırı yöntemi sosyal sitelerde çok sık rastlanılan bir sahtekârlık türüdür. Çünkü profil klonlamayla ilgili neredeyse hiç güvenlik önlemi yoktur [6]. Saldırgan ilgili kişinin profilinin aynısını oluşturur ve genelde ilgili kişinin itibarını Internet ortamında zedeleme hedeflenmektedir.

3.4 Üçüncü-Kişi Uygulama Tehlikeleri

Saldırgan taraf kullanıcı şifresi ve kullanıcı bilgilerini elde etmek için oyunlar gibi sosyal ağ uygulamalarını kullanır. Sahte uygulamayı çalıştırmak için kullanıcı bilgilerini veren kullanıcının bilgileri saldırgan tarafından temin edilmiş olur.

3.5 Sahte Ürün Satışı

Saldırgan, çok satan bir üründe müthiş indirimlerle süslediği reklamlarını sosyal ağ sitelerine koyar. Satıyormuş gibi yaptığı ürün için kullanıcı bilgileri, banka şifreleri gibi kişisel bilgileri ister. Eğer kullanıcı bu gerçek gibi görünen satış için bilgilerini verirse saldırgan da bu bilgileri temin etmiş olur ve amacı doğrultusunda bu bilgileri kullanır.

3.6 Kötü Bağlantı İstekleri
Sahtekârlar hedef kullanıcıların onlarla iletişime geçmesini sağlamak için sahte profiller oluştururlar ve arkadaşlık isteği gönderirler. Eğer ilgili kullanıcı bu arkadaşlık isteğini kabul etmiş olursa, normal arkadaşlarıyla paylaştığı bilgilerini sahtekârlara da vermiş olur. Böylece sahtekârlar bu bilgileri kötü amaçlı kullanabilirler.

3.7 Spamler
Spam, bir liste veya grup e-posta adresine gönderilen genelde reklam içerikli, istenmeyen e-posta anlamına gelir. Aynı şekilde bir saldırgan bu e-postaları bir sosyal ağ aracılığıyla kullanıcılara gönderip, gönderdiği kişinin kullanıcı bilgilerini elde etmeye çalışabilir [7].

3.8. Düzenbaz Site Kodlamaları
Düzenbaz Site Kodlamaları (Cross site scripting - XSS), kullanıcı web sunucusunu kullanıcı kontrolü dışında işlem yaptırma eylemidir. Saldırı türüne göre değişik özellikleri olmasının yanında genelde kullanıcının haberi olmadan zararlı bir yazılım çalıştırılır ve bu sayede kurbanın bilgilerini elde etmeyi hedefler [8].

4. Kötü Yazılımlar

Kötü yazılım, bir sistemi zedelemek veya kullanışsız hale getirmek için özel tasarlanmış yazılım demektir [6]. Sosyal ağların ünü, maalesef bu ağlara bu tür yazılımlarla saldırmak için çekici bir hale getirmiştir. Bir zararlı yazılım sosyal ağlarda hızlı bir şekilde yayılabilir ve kullanıcıların diğer kontakları vasıtasıyla bir ağın neredeyse tamamına bulaşabilir.

Zararlı yazılımlar genelde güvenli kişilerce gönderiliyormuş gibi görünür. Örneğin, bu tür bir yazılım kullanıcının bir arkadaşı tarafından gönderiliyormuş gibi görünebilir. Genelde bir linke tıklanılmasını ister, kullanıcı bu linke tıkladığında zararlı yazılım tetiklenmiş olur ve zararlı yazılım ilgili kullanıcının sitemine zarar vermeye başlar. Bazı yaygın zararlı yazılım örnekleri aşağıda açıklanmıştır:

Gizli Link ve Sahte URL: Genelde güncel konular veya haber kaynağı şeklinde görünür. Bu da kullanıcıları farkında olmadan virüsü indirmek veya kullanıcının sistemine zarar verecek olan yazılımı içeren siteyi ziyaret etmek konusunda cesaretlendirir.

Sahte Mesajlar: Kullanıcının irtibatında olan biri tarafından gönderiliyormuş gibi olan ve bir linke tıklanmasını isteyen mesajlar.

Sahte Ağ Mesajları: Sosyal ağın kendisinden geliyor gibi görünüp kullanıcıdan ilgili linki tıklamasını isteyen e-postalar.

Üçüncü Şahıs Yazılımları: Bu yazılımlar kullanıcıya bulaştıktan sonra kontaklarına da yayılmaya başlar. Bu yüzden kullanıcının arkadaş listesindekiler de kolayca bu zararlı yazılımın saldırısına maruz kalabilir.

Bilgisayar Güvenlik Açığı: HTML kodlarının arasına istemci tabanlı kod gömülmesi yoluyla kullanıcının tarayıcısında istenen istemci tabanlı kodun çalıştırılması sonucu kullanıcı çerezlerinin (web tarayıcısında saklanan bilgiler) saldırgana gönderilmesini sağlayan yöntemdir.

Zararlı Tıklama: Zararlı tıklama (Clickjacking), kullanıcıyı bir butona veya nesneye tıklamasını sağlayarak zararlı yazılımın çalışmasına sebebiyet vermektir [10]. Bazı kötü niyetli Internet siteleri kullanıcı tarayıcısının kullanıcı bilgisi veya izni dışında işlem yapmasını sağlayan kodlar içerir. Örneğin, bu tür Internet sitelerinden birindeki bir bağlantıya tıklamak Internet sitesinin sosyal ağlarda paylaşılmasına sebep olur.

Sahte Güvenlik Alarmları: Bu uygulama türü, bir tür virüsten korunma yazılımı gibi görünür ve kullanıcıyı sanki kullandığı anti virüsün güncellenmeye ihtiyacı varmış veya bir tehdit bulmuş gibi ikaz ederek zararlı kodu farkında olmadan çalıştırmasına sebebiyet verir. Kullanıcı ilgili butona tıkladığı an, zararlı siteye yönlendirilir.

Truva Atı (Trojan): Kurbanının tahmin etmediği bir şekilde ve isteği olmaksızın, gizli ve genellikle kötü amaçlı bir faaliyette bulunan bir programdır. Truva atı kendisini zararsız bir program gibi (örneğin bir oyun ya da yardımcı program) gösterir. Görünümü ve ilk çalıştırıldığındaki aktivitesi zararsız bir program gibidir. Çalıştırıldığında verileri silebilir veya bozabilir. Truva atı yararlı gibi görünen ancak aslında zarara yol açan bir bilgisayar programıdır. Truva atları, insanların, meşru bir kaynaktan geldiğini düşündükleri bir programı açmaya yöneltilmeleri yoluyla yayılır [11].

Sosyal ağların ünü Truva atlarının da dikkatini çekti ve bu ağlar önemli bir hedef haline geldi. Zeus gibi Truva atları sosyal ağlarda sıkça kullanılan tiplerindendir. Genelde 'tıkla beni' gibi bir uyarıyla kullanıcının karşısına çıkar ve kullanıcı zararsız gibi gördüğü bu programı çalıştırmış olur.

Botnet: Bot terimi robotun kısaltmasıdır. Suçlular, bilgisayarınızı bir bot'a (zombi olarak da bilinir) çevirebilen kötü amaçlı yazılımları (kötü amaçlı program olarak da bilinir) dağıtırlar. Böyle bir durumda bilgisayarınız, sizin haberiniz olmadan Internet üzerinden otomatik görevleri gerçekleştirebilir. Suçlular genelde çok sayıda bilgisayarı etkilemek için bot kullanırlar. Bu bilgisayarlar da bir ağ veya botnet oluştururlar. Suçlular botnetleri, istenmeyen e-posta mesajları göndermek, virüsleri yaymak, bilgisayar ve sunuculara saldırmak ve diğer türlerdeki suçları işlemek ve sahtekârlıklarda bulunmak amacıyla kullanır. Bir botnetin parçası olması durumunda bilgisayarınız yavaşlayabilir ve istemeden suçlulara yardımcı olabilirsiniz [9]. Son yıllarda özellikle Twitter, Facebook gibi büyük sosyal ağlarda bazı hesaplar botnet olarak kullanılmaktadır.

Koobface ve Twitter Botları:

- **Koobface:** Sosyal ağlardaki en meşhur kötü yazılım türüdür [10]. Özellikle Facebook kullanıcılarının sayfalarında sahte Youtube linkleriyle diğer kullanıcıların bu linki tıklamasına sebebiyet vererek zararlı yazılımı kurbanlarına yüklemiş olur.
- **Twitter Botları**: Spam ve zararlı yazılımların yanında siber suçlular Twitterı botnet zombilerini kontrol etmek için de kullanabilmektedir. Bu programlar Twitterda otomatik Twitter postları oluşturur ve bunlar genelde spam formunda olur [12].

5. Sorunlar ve Önlemler

Sosyal ağlarda güvenliği ve gizliliği sağlamak zordur. Sosyal ağlardaki sorunlardan biri kullanıcıların bilgilerini ilgili ağlarca paylaşılmaya zorlanmasıdır. Örneğin, bir kullanıcı bir sosyal ağa üye olmak istiyorsa, kullanıcı bilgilerini vermek zorunda kalmaktadır.

Bir diğer sorun ise kullanıcıların bu sitelere olan bağımlılıklarıdır. Bu sitelerde birçok bağlantıları, organizasyon haberleri, hesapları olduğu için asla bu ağlardan kopamazlar. Bazı sosyal ağ siteleri de basit veya çözülebilir şifreleme yöntemi kullanmaktadırlar, bu da kullanıcı bilgilerine üçüncü kötü niyetli şahıslar tarafından erişilmesini kolaylaştırır.

Sosyal ağlarda çözümler, ailede, okulda ve sosyal ağlarda alınacak tedbirlerle sağlanabilir. Kişisel verilerin korunmasında yazılımsal çözümlerin altyapıya eklenmesiyle teknolojik olarak, yasal çözümlerde kullanıcıların hem izlenmesi hem de teknolojik çözümlerin kullanılmasıyla ve bunların yasalarla desteklenmesiyle, sağlanmaktadır. Bunun için ailelerin, eğitim kurumlarının, sosyal ağ hizmet sağlayıcılarının, hükümet birimlerinin beraber çalışması gerekmektedir [11]. Sosyal ağlardaki saldırılardan korunmak için yapılması gerekenler aşağıdaki gibidir:

- Sosyal ağınızı dikkatlice seçin. Kullanmayı planladığınız siteyi değerlendirin ve gizlilik politikasını anladığınızdan da emin olun.
- Sosyal ağın insanların yayınladıkları içerikleri izleyip izlemediğini öğrenin. Bu

web sitesine kişisel bilgiler vereceksiniz, bu nedenle kredi kartı bilgilerinizi gireceğiniz bir siteyi seçerken kullandığınız koşulların aynılarını kullanın.

- Çocukların gizlilik politikalarında belirtilen yaş sınırlarına uygun olarak bu ortamları kullanmaları aileleri tarafından sağlanmalıdır.
- 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 [13].
- Üye olurken güçlü bir şifre seçin. Eğer güvenliği sağlamak için bilgi verilmesi isteniyorsa, diğer insanların bilmedikleri bilgiler seçilmelidir. Şifre seçiminde ise büyük-küçük harf ve rakamların birleşiminden oluşan şifreler seçilmelidir.
- Kişisel bilgi paylaşımı kısıtlı olmalıdır [6].
- Gizlilik ayarlarının son güncel hali kullanıldığından emin olunmalıdır.
- Bir anti-virüs programı kullanılmalıdır. Bu program zararlı yazılımlardan korunmada yararlı olacaktır.
- Özellikle resim paylaşımında iki kere düşünülmelidir. Ailenin veya yakınların görmesini istenmediği resimler sosyal ağlara yüklenmemelidir.
- Bir sosyal ağ ziyaret edildikten sonra tarayıcıların tuttuğu çerezler silinmelidir
- Tatil planları, özellikle tarihleri sosyal ağ üzerinden paylaşılmamalıdır.
- Bilgisayar yazılımları özellikle de web sunucuları güncel tutulmalıdır.
- Bir yabancıdan bağlantı isteği alındığında en güvenli yöntem bu bağlantı isteğini reddetmektir.
- Sosyal ağ sitesinden ayrıldığında çıkış yapıldığından emin olunmalıdır.
- Hangi sebeple olursa olsun spam maillere cevap verilmemeli, linklerine tıklanmamalıdır.
- Link tarayıcı kullanın. Link tarayıcı o linkin ait olduğu ilgili sitenin zararlı bir site olup olmadığını sınayan web uygulamasıdır. 'Urlvoid', 'Mywot' bu bağlamda örnek sitelerdir.
- Kısaltılmış linkleri mutlaka kontrol edin. Bazı zararlı linkler kullanıcıya kısa bir link olarak gösterilir ve bu sayede zararlı link bir nevi gizlenmiş olur. Kullanıcı şüphelendiği kısa linkin yönlendirdiği gerçek linki mutlaka kontrol etmelidir. Gerçek linkleri kontrol eden siteler vardır. 'Sucuri' bu örneklerden bir tanesidir.

6. Sonuç

Sosyal ağ siteleri günümüz Internet dünyasında önemli bir yer tutmaktadırlar ve aynı durumun gelecekte devam etmesi öngörülmektedir. Bu sitelerin kullanıcılara birçok fayda sağladığı açıktır. Ancak bu ağların ciddi güvenlik problemleri de ortadadır.

Sosyal paylaşım ağları bilgi ve bilgisayar güvenliği açısından değerlendirildiğinde, kullanılırken sorumluluk isteyen, konuyla ilgili bilgi birikimi gerektiren, belirli bir kullanıcı bilincine ve disiplinine sahip kişiler tarafından kullanılması gereken, iletişim ve paylaşım ortamlarıdır. Doğru kullanılmadıkları takdirde, kişisel bilgilerin çalınması, istenmeyen durumlarla karşılaşılması, beklenmeyen tehdit ve tehlikelere maruz kalınması ve en önemlisi kişisel bilgilerin mahremiyetine zarar verebilecek pek çok olumsuzlukları içinde barındıran ortamlar olabileceği unutulmamalıdır.

Bu bildiride, sosyal ağ güvenliği, bunların gizlilik meseleleri ve sosyal ağlarda kötü yazılımlar ele alınmıştır. Ayrıca, sosyal ağlardaki güvenlik problemlerine karşı alınması gereken önlemler irdelenmiştir.

Teşekkürler:

Bu çalışma EUREKA ITEA2 projesi ADAX (proje no. 10030) ve TEYDEB projesi AKFİS (proje no. 1130018) tarafından desteklenmiştir.

7. Kaynaklar

[1] Palfrey, J., and Gasser, U., "Understanding the first generation of digital natives", **Harvard Press**, (2008).

[2] Facebook statistics. http://www.facebook.com/press/info.php?statistics (Aralık 2013)

[3] Timm,C., and Perez, R., "Seven Deadliest Social Network Attacks (Seven Deadliest Attacks)", **Syngress Press**, (2010)

[4] "Cisco Annual Security Report", (2013)

[5] Kumar, D. V., Varma, P. S. S., Pabboju, S. S., "Security Issues in Social Networking", **IJCSNS International Journal of Computer Science and Network Security**, 13:120-124 (2013)

[6] Kumar, A., Gupta, S. K., Rai, A. K., Sinha, S., "Social Networking Sites and Their Security Issues", **International Journal of Scientific and Research Publications**, 3: 1-5(2013)

[7] Strighini, G., Kruegel, C., Vigna, G, "Detecting Spammers on Social Networks", **ACSAC'10**, Austin, Texas, ABD, 6-10, (2010)

[8] Grossman,J., "Cross-Site Scripting Worms & Viruses", **WhiteHat Security**, (2007)

[9] Huang, L. S., Moshchuk, A., Wang, H. J., Schechter, S., Jackson, C.,"Clickjacking: Attacks and Defenses", **Security'12 Proceedings of the 21st USENIX Conference on Security Symposium**, Berkeley, CA, ABD, 1-16, (2012)

[10] Virüs güvenlik: http://www.virusguvenlik.com/trojan-truva-ati-nedir/ (Aralık 2013)

[11] Baltazar, J., Costoya, J., Flores, R., "The Heart of KOOBFACE C&C and Social Network Propagation", **Trend Micro Threat Research**, (2009)

[12] Chu, Z., Gianvecchio, S., Wang, H., Jajodia, S., "Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?", IEEE Transactions on Dependable and Secure Computing, 9:811-824, (2012)

[13] Sancho, D., "Security Guide to Social Networks", **White- Paper Trend Micro Inc.**, (2009)