Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler

Uraz YAVANOĞLU [1], Şeref SAĞIROĞLU [2] ve İlhami ÇOLAK[3]

[1, 2] Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Maltepe, Ankara,

[3]Gazi Üniversitesi, Teknoloji Fakültesi, Elektrik Elektronik Mühendisliği Bölümü, Beşevler, Ankara,

ÖZET

Bilişim teknolojilerinin hayatımızı sanallaştırmaya başladığı bir dönemde, bireysel ve toplumsal ilişkiler, paylaşımlar, aktarımlar, görüşmeler, buluşmalar, sohbetler, oyun oynama, vb olaylar sosyal paylaşım siteleri üzerinde yaşanmaya başlanmıştır. Bu makalede, sık kullanılan sosyal paylaşım ağları incelenmiş, bu ağlarda karşılaşılan güvenlik ihlalleri örneklendirilmiş, meydana gelebilecek güvenlik açıkları ve tehlikeleri sınıflandırılmış, sosyal ağlarda alınması gereken güvenlik önlemleri sunulmuş ve çalışmada elde edilen bulgular sonuç bölümünde irdelenmiştir.

Anahtar Kelimeler : Sosyal Ağ, Bilgi Güvenliği, İnternet, Sosyal Mühendislik, Tehditler, Açıklıklar

Information Security Threats and Taking Privacy Precausions in Social Networks

ABSTRACT

Times for information technologies to make our life virtualized, the events like personal and public relations, sharings, transformation, meetings, encounters, chats, games, and so on are being lived on social networks. In this paper, social networks mostly preferred were reviewed. Vulnerabilities and threats encountered were examined and classified. Solutions to those security threats were presented. Finally, the outcomes achieved from this study were evaluated and discussed.

Key Words : Social Network, Information Security, Internet, Social Engineering, Threats, Vulnerabilities

I. GİRİŞ (INTRODUCTION)

Bilişim teknolojilerindeki gelişmeler, bilişim teknolojilerinin kullanımı ile hizmetlerin daha hızlı sunulması, yaygınlaştırılması, doğru ve yeterli bilgiye hızla ulaşma, şeffaflaşma, iş ve zaman verimliliği gibi pek çok kazanımı bizlere sunarken sanal ortamlara güven sorununu da beraberinde getirmiştir. Son zamanlarda yaşanan olumsuzluklar, bu ortamları kullanmanın sosyalleşmeyi kolaylaştırdığı kadar da yeni tehdit ve tehlikeleri de beraberinde getirdiğini göstermektedir. Bunun en güncel örnekleri ise günlük hayatımızda kullanmaktan büyük keyif aldığımız, eski dostlarımızı bulduğumuz onlarla haberleştiğimiz, yeni dostluklar kurduğumuz, ruh ikizlerimizi bulduğumuz, haberleşme grupları oluşturduğumuz, hızlı bilgi paylaşımı yaptığımız, davranış analizimizin tespit edilmesine imkan sunduğumuz, yeni düşmanlar ve/veya tehditler edindiğimiz, kişisel bilgilerimizi paylaşarak güvenliğimizi tehlikeye attığımız, belki de gelecekte hiçte beklemediğimiz veya öngöremediğimiz pek çok olumlu ya da olumsuz durumlarla karşılaşabileceğimiz pek çok tuzakların bulunduğu ücretsiz olarak hizmet veren sosyal paylaşım ağlarıdır.

Sosyal ağlar; "bireyleri internet üzerinde toplum yaşamı içinde kendilerini tanımlayarak, aynı kültürel seviyede 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 ortamlarda sosyal iletişim kurmaya yarayan" araçlar olarak tanımlanmaktadır [1].

Bu tanım, sosyal ortamların insanlara kazandırdıkları veya kazandırabileceklerini anlatmak için yeterli olsa da sosyal ağ ortamlarının olumsuz veya tehdit içerebilecek yönünü içine almamaktadır. Yukarıda ki tanıma "beraberinde bilinmeyen, fark edilemeyecek veya algılanması zor olan pek çok tehdit ve tehlikeyi de beraberinde getiren, faydalı olduğu kadar olumsuz yönlerinin de kullanılırken düşünülmesi gereken sanal ortamlar" ifadesini eklemekte fayda vardır.

Bu makale çalışması, sanal sosyal ağların elektronik ortamlarda sosyalleşme ve iletişimi arttırma için kazandırdıklarından ziyade bu ortamlarda oluşabilecek tehdit ve tehlikeleri öne çıkarmak, bunları vurgulamak ve en önemlisi bilgi ve bilgisayar güvenliği özel hayatın mahremiyeti ilkelerine göre alınması gereken önlemler veya dikkat edilmesi gereken hususları sunmak için hazırlanmıştır.

Etzioni yayımladığı "Kişisel Verilerin Korunmasında Sınırlar" kitabında, kişisel verilerin güvenliğinin sağlanmasında en önemli göstergenin bir problemle karşılaşıp karşılaşılmaması ile ölçülmesi gerektiğini bildirmektedir [2].

Sorumlu Yazar (Corresponding Author) : Şeref SAĞIROĞLU
e-posta: ss@gazi.edu.tr
Digital Object Identifier (DOI) : 10.2339/2012.15.1, 15-27

Chen ve Shi tarafından yapılan çalışmada sosyal ağlarda kişisel bilgilerin güvenliği hususu farklı yönleriyle incelenmiş, bu bilgiler kullanılarak gelişen atak teknikleri irdelenmiş ve kişisel bilgilerin korunmasına yönelik çözüm önerileri sunulmuştur. Bireylerin sahip olduğu bilginin güvenliğinin tamamen korumasız olmadığı; piyasa şartları, bireysel alınan önlemler ve hükümet kurallarıyla bunun sağlanmaya çalışıldığı, yapılan saldırıların direk ve kötücül yazılım olarak ikiye ayrıldığı ve en çok kullanılan yöntemlerin sırasıyla Dağıtık Hizmet Aksattırma (DDoS) ve sazan avlama (phishing) olduğu belirtilmektedir. Sosyal ağlarda kişisel bilgilerin korunması için korumaya dayalı sosyal ağ modelleri geliştirilmesi bu çalışmada vurgulanmıştır [3].

Cutillo ve arkadaşları tarafından yapılan çalışmada sosyal ağların kullanıcı güvenliği endişesini beraberinde getirdiği, internet ortamında var olan tehditlerin sosyal ağlar için daha büyük sıkıntılara yol açtığı vurgulanmıştır. Sosyal ağlar merkeziyetçi çözümler üzerine kurulu yapılar olduğundan tehditlerden tüm ağın etkilenmemesi için merkeziyetçi çözüme karşı noktadan noktaya çalışacak bir çözüm önerilmiştir [4].

Web günlükleri özellikle büyük grupların ideolojilerini açıklamaları ve kitlelere ulaşmaları için gerekli olan platformlardır. Yang ve Ng tarafından yapılan çalışmada web günlüklerinin özellikle terörizm ağırlıklı suç amaçlı kullanımları incelenmiştir. Yazarlar web günlükleri için kullanılabilecek yazılım arabirimi ile sosyal paylaşım ağlarında vb. mesajlar arasındaki içerik analizi ile semantik bağlantıları ortaya çıkarılabilmekte, bu sayede bağlantı analizi yaparak günlük yazarları arasında ilişkileri haberleşme güvenliğini sağlamak amacıyla kullanabilmektedir [5].

Buchegger ve Datta tarafından özelikle Facebook ve Myspace gibi merkezcil yönetimli soysal paylaşım sitelerinin web tabanlı olması, site sahibinin tüm kişisel bilgilere erişim hakkı bulunması ve bu sebeple ortaya çıkan kişisel bilgi güvenliği sorunları gibi bazı özellikleri kullanarak farklı çözüm önerileri sunmuşlardır. Bu sorunları aşmak için mevcut durumda bulunan kullanıcı çifti yerine noktadan noktaya kontrol kabiliyeti olan bir sosyal paylaşım ağı oluşturulmasının gerekliliğini belirtmişlerdir [6].

Lang ve arkadaşları tarafından yapılan diğer bir çalışmada, büyük oranda kimlik hırsızlığı atakları hedef alınarak sosyal paylaşım sitelerinde kişisel bilgi güvenliği farkındalığını ölçmek için İrlanda üniversitesinde öğrenim gören 18-24 yaş arası 120 öğrenci üzerinde araştırma yapılmıştır. Elde edilen sonuçlar durumun iç açıcı olmadığını göstermekle birlikte kişilerin özellikle taşınabilir cihazlar ile yayılan virüs tehditlerine karşı farkındalıktan yoksun olduğu, bilgi güvenliği standartlarında şifre kullanımı ve veri yedekleme konularında ise çoğunluğun bilgisiz olduğu gösterilmiştir [7].

Beach ve arkadaşlarının yaptığı bir çalışmada, taşınabilir cihazların sosyal ağlara açılmasıyla ortaya çıkan güvenlik zafiyetleri araştırılmıştır. Bu cihazların sosyal ağlar üzerinde aktif hale gelen yazılımlar ile kişiye ait konum ve özellik bilgisini ağ üzerinden erişilebilir kılmasından dolayı mevcut kullanılan bilgi transferi modeli ile kişilerin gizliliği ihlal ettikleri savunulmaktadır. Bu tehdidin ortadan kaldırılması için sosyal ağ uygulamalarının taşınabilir cihazda yer alan bilgiler ile haberleşmesini sağlayan güvenli bir katman geliştirilmesi önerilmiştir [8].

Nagy ve Pecho tarafından yapılan çalışmada, sosyal ağ kullanıcılarının profillerini yanlış yönetmelerinden dolayı ortaya çıkan güvenlik açıkları tartışılmıştır. Bu çalışma kapsamında yapılan anketler incelendiğinde sosyal ağlarda bilgi güvenliği farkındalığına sahip kullanıcıların davranışlarını sosyal mühendislerin erişmek istedikleri hassas bilgilere ulaşmalarını kolaylaştıracak şekilde paylaştıklarını ortaya çıkmıştır [9].

Luo ve arkadaşları tarafından yapılan çalışmada, sosyal ağlarda kullanıcılar fark etmeden yayılan kötücül yazılımlar ve bağlı olan tehditler tartışılmıştır. Sosyal mühendislerin özel hazırlanmış sayfalara kişileri yönlendirerek atak yaptıkları, diğerlerine göre daha fazla kişiyle tanışmak amacında olan kullanıcıların bu ataklara daha açık olduğu ve çoğu durumda kullanıcının hassas bilgisini elde eden sosyal mühendisin amacının şantaj olduğu gösterilmiştir. Bu tehditlerin kullanıcıları ve sosyal paylaşım sitelerini nasıl etkiledikleri ayrı ayrı gösterilmiş, sonuç olarak bu tehditlere karşı alınabilecek önlemler ile sosyal ağlar için özel bir güvenlik arabirimi önerilmiştir. Kullanıcıların farkındalığının yüksek olması önerisinin yapıldığı çalışmada sosyal paylaşım sitelerinin de uygulama katmanı güvenliğinin standartların ötesinde yeniden ele alınarak gerekli düzenlemelerin yapılması gerektiği vurgulanmıştır [10].

Yapılan diğer araştırmalarda, sosyal ağ kullanıcılarının (örneğin Facebook'un kişisel verileri korumaya özen gösterdiğini düşünen genç kullanıcılar tarafından) kendi kişisel verilerinin halka açık olabileceğinin farkında olmadığı rapor edilmiştir [11].

Bu çalışmanın; II. Bölümünde kullanılan sosyal ağlar özetlenmiştir. Bölüm III'de, sosyal ağların bilgi güvenliği açısından değerlendirmesi ve sosyal ağların gizlilik politikaları ve kapsamları karşılaştırmalı olarak değerlendirilmiştir. Bölüm IV'de sosyal ağlarda karşılaşılabilecek güvenlik tehditleri tartışılmıştır. V. Bölümde bu tehditlere karşı alınabilecek çözüm önerilerine değinilmiştir. Son bölümde ise genel sonuç ve değerlendirmeler sunulmuştur.

II. SOSYAL AĞLAR (SOCIAL NETWORKS)

İnternette sıkça karşılaştığımız sosyal ağlar aşağıda kısaca tanıtılmıştır.

Facebook

Kullanıcılarının veya üyelerin kişisel bilgilerinin yer aldığı (fotoğraflar, arkadaşlık bilgileri, kişisel yorumlar, ilgi alanları) bir sosyal ağdır [12]. Bu sosyal ağı kullananların sayısının günümüzde 750 milyona yaklaştığı bilinmektedir. Ayda 2 milyara yakın aramanın yapıldığı, günde 15 milyonun üzerinde fotoğraf ve video eklenen, üzerinde bugün için 4 milyarın üzerinde fotoğ-

raf ve video barındıran, yüz binlerce grubun oluşturulduğu, dünyanın en çok kullanılan ve ziyaret edilen ilk 10 sitesi arasında bulunan, en büyük kişisel haberleşme portalıdır.

Twitter

Kullanıcılarının anlık iletiler yayınlamasına izin veren bir paylaşım sitesidir [13]. Günlük olarak yayınlanan paylaşım arşivlerinin aksine twitter anlık mesajların görüntülenebileceği ve kullanıcılar tarafından istenilen bağlantıların paylaşılabileceği bir yapı sağlamaktadır. Kullanıcıların takip ettikleri diğer kullanıcı sayfalarını ve kişilerin kendi sayfasını takip edilmesi için açmasına olanak tanıyan bir kayıt mekanizması vardır. Twitter sitesinin 2011 yılı itibariyle 100 milyon kullanıcıya ulaştığı tahmin edilmektedir.

Live Messenger

Kullanıcılarının anlık ileti almasını ve göndermesini sağlayan Microsoft firması tarafından geliştirilen bir hizmettir [14]. LIVE paketi içinde yer alan sosyal paylaşım yazılımları arasında en popüler olanıdır. Kullandığı özel yönlendirme protokolü sayesinde güvenlik duvarlarına takılmadan özel amaçlar doğrultusunda yapılandırılmış bir web sunucu ile haberleşerek internet bağlantısı olan her ortamda kullanılabilmektedir. Kişilerin animasyonlar ve ikonlar ile duygu hallerini paylaşabilmelerine ayrıca internete bağlı olmadığınızda telesekreter gibi çalışarak size iletilen mesajları kendi sunucuları üzerinden iletilmesini sağlayan bir mimariye sahiptir. Kişilerin Messenger yazılımını yeni kişiler ile tanışmak için değil tanıdıkları kişiler ile iletişim kurmak için kullandıkları görülmektedir. Bu hizmetten yararlanmak için Microsoft e-posta hesaplarından birine sahip olmanın yeterli olması sebebiyle potansiyel kullanıcı sayısının 500 milyonun üzerinde olduğu tahmin edilmektedir.

Myspace

Kullanıcılarının fotoğraflarını, video ve müziklerini kendi sayfalarında yayınlamalarına altyapı desteği veren bir sosyal paylaşım sitesidir [15]. Bu sosyal ağ, özellikle amatör sanatçıların çalışmalarını paylaşabilecekleri ve kendi tanıtımlarını yapabilecekleri bir yapı sunmaktadır. Sayfanızı ziyaret eden kişi sayısı ve sayfanıza yapılan yorumları görüntüleyebileceğimiz bir altyapı üzerine kuruludur. Myspace sosyal paylaşım siteleri arasında aylık sıralamada en fazla vakit geçirilen site olarak değerlendirilmektedir [15].

Yonja

Yonja Türk girişimciler tarafından kurulmuş, ücretli ve ücretsiz hizmet veren arkadaşlık sitesidir [16]. Kişiler Yonja üyesi olduktan sonra yeni arkadaşlıklar kurmak için kişisel detaylarını sisteme kayıt etmektedir. Site içerisinde gönderilen mesaj, eklenebilecek video ve paylaşım sayıları limite tabidir. Ücretli kullanıcılar bu limitlerden muaftır. Yonja diğer paylaşım sitelerinin aksine daha önceden tanınan kişileri bulmaya değil yeni tanışacağınız kişileri bulmaya yönelik bir hizmet sunmaktadır.

Friends Reunited

Bu sosyal paylaşım sitesi, eski arkadaşlarınızda dahil olmak üzere soy ağacınızın izlerini sürmek gibi sizi geçmişe bağlayan kişileri bulmanızı hedefleyen bir sosyal paylaşım ağıdır [17]. Friends Reunited İngiltere merkezli bir yönetim anlayışı ile özellikle bu bölgenin halkı için randevu ve arkadaşlık servisi hizmetleri vermektedir. Bu sayede hem başka kişiler ile soy yakınlığı ilişkisi kurulabileceği gibi bu bilgilerin yanında yeni insanlarla da tanışılabilecek bir ortam sunulmaktadır.

Linked-in

Bu site geçmiş iş arkadaşlarınızı bulmanızın yanında, sınıf arkadaşlarınızla bağlarınızı kopartmamanızı hedefleyen ama aynı anda sisteme kayıt ettiğiniz bilgiler ile iş arama, işçi bulma gibi özellikleri bünyesinde barındıran bir sosyal paylaşım ağıdır [18]. Bu ortam sayesinde uzmanı olduğunuz alanda kendinizi tanıtma fırsatınız olmaktadır. Aynı zamanda alanında uzman kişilere istediğiniz alanda soru sorarak deneyimlerinden faydalanabileceğiniz bir paylaşım servisi sunmaktadır.

YouTube

Bu sosyal paylaşım sitesi görüntü paylaşım sistemi ile internet kullanıcılarına ulaşmaktadır. Slâyt şovlar, animasyonlar, fragmanlar, amatör çekimler ve her çeşit video formatında dosyanın yüklenmesine ve bunları diğer kullanıcılar veya sisteme anlık erişenlerle paylaşmanıza imkân tanıyan bir sisteme sahiptir [19]. Youtube üzerinde, isteyen herkes videolarını ve görüntülerini paylaşabilmektedir. Bu paylaşımlar sayesinde kendinizi ve çevrenizi dünyaya tanıtabileceğiniz gibi yapılan paylaşımlara yorumlar yazarak videolar hakkında fikirlerinizi paylaşabileceğiniz bir altyapı sunulmaktadır. Youtube yükselen trendi sebebiyle 1.6 milyar dolara Google tarafından satın alınmıştır.

Flickr

Sosyal bir fotoğraf paylaşım sitesidir [20]. Kendi albümlerinizi oluşturarak, fotoğraflarınızı paylaşmanıza imkan tanıyan bir servis sunmaktadır. Bu siteyi kullanabilmek için Yahoo hesabınızın olması gerekmektedir. Flickr kullanıcılarına her ay, yükleme yapabilecekleri kotası bulunan bir alan sunulmaktadır. Bu limitin dışına çıkmak ise ücretlidir. Fotoğrafların kim tarafından çekildiği, hangi makine ile çekildiği, konum ve yer bilgisi gibi çeşitli istatistiki veriler sitede yer almaktadır.

Friendster

Friendster Asya kökenli devletlerde yayılmaya başlayan arkadaşlık sitesidir [21]. Benzer siteler gibi hizmet veren ama Avrupa ve Amerika yerine Uzakdoğu ülkelerini hedef bölge olarak belirleyen bir hizmet anlayışı bulunmasına rağmen sağladığı değişik özellikler (Örn: Seçime bağlı profil sayfaları) nedeniyle diğer ülkeler tarafından da kabul görmektedir.

Buzz

Google tarafından geliştirilen Gmail hesabı olan kullanıcıların erişimine açık, anlık iletilerin, video ve bağlantıların paylaşılabileceği bir sosyal paylaşım ağıdır

[22]. Buzz ile fotoğraflarınızı paylaşabilir ya da Twitter gibi diğer sosyal ağlar ile hesabınız arasında paylaşım ilişkisi kurabilirsiniz.

Blogger

Bu sosyal paylaşım sitesi, yorucu bir günün ardından kişilerin günlüklerini yazmak için tercih ettikleri sosyal paylaşım sitesidir [23]. Yazılan her günlük içinde o güne ait zaman damgası bulunmaktadır. Bu servis Google tarafından işletilmektedir. Kullanıcılar sınırsız günlük oluşturabilir ve her günlük 2000 konu başlığı içerebilir. Ayrıca Google firmasının fotoğraf yükleme hizmeti Picasa ile bağlantılı günlük içinde albümlerinizi de yayınlamanıza olanak tanınmaktadır.

Bebo

Bebo ABD merkezli bir sosyal paylaşım ağıdır [24]. Bununla beraber İngiltere ve İrlanda kullanıcılarının da tercihleri arasında olan bir sitedir. Bebo güvenliği ciddiye alan ve her yeni üyesini otomatik olarak yüksek seviyede güvenlik ayarına geçiren bir sosyal paylaşım sitesidir. Ayrıca, bir güvenlik önlemi olarak 21 yaşın altındaki kullanıcıların soyadlarının sadece ilk harfini vermesi gerektiğini vurgulanmaktadır.

Hi5

Hi5 sadece mevcut arkadaşlarınızla değil 70 milyon kadar kişinin birbirleriyle tanışmalarına imkân tanıyan bir yapıya sahiptir [25]. Hi5 sitesini diğer paylaşım sitelerinden ayıran başka bir özellik ise reklamların sayfayla uyum içinde verilerek kullanıcıları rahatsız etmekten kaçınılmasıdır. Hi5 üzerinde oyun oynamak için özelleşmiş sayfalar bulunmaktadır.

Perfspot

Perfspot özellikle gençler arasında yayılmaya başlayan bir sosyal ağ sitesidir [26]. Kişilere profilleri üzerinde satış yapabilecekleri küçük çaplı bir e-ticaret sistemi sunmaktadır. Bazı bölümlerine yaş sınırlamasıyla arama yapılabilmektedir. Bu sayede reşit olmayan kişilerin erişimleri engellenmektedir.

Badoo

Badoo sayfasından kayıtlı kullanıcı sayılarını anlık olarak gösteren bir sosyal paylaşım sitesidir [27]. Şu an itibariyle 60 milyon kullanıcı bulunmaktadır. Badoo'nun merkezi Kıbrıs Rum kesiminde bulunmaktadır. Kullanıcı kitlesi Avrupa Birliği üyesi ülkeler ve özellikle Yunanistan'dır.

Zorbia

Zorbia, üyelerini aynı isimden türetilen Zorbian olarak anma geleneği oluşturmuş olan resim paylaşım sitesidir [28]. Bu site standartların ötesinde gelişmeye açık yapıya sahip olmasına karşın site üzerinde yayınlanan birçok reklam görünümü etkilemektedir. Zorbia Hong Kong merkezli olması sebebiyle ABD merkezli sosyal paylaşım siteleri için rakip teşkil etmektedir.

Netlog

Netlog, Belçika merkezli sosyal paylaşım sitesidir [29]. Bu sebeple Avrupa Birliği üyesi ülke gençliği arasında yükselen bir trende sahiptir. Kullanıcılar kendi günlüklerini oluşturabilir, resim ve video paylaşabilir. Netlog sitesi birçok dil desteği vermesi sebebiyle tercih edilmektedir.

Orkut

Orkut bir Türk tarafından geliştirilen sosyal paylaşım sitesidir [30]. Stanford doktoralı Orkut Büyükkökten, tarafından Google için geliştirilmiştir. Buna karşın Türkiye içinde Orkut sistemine kayıtlı kişi sayısı yaygın değildir. Orkut, Google tarafından geliştirilen diğer sosyal paylaşım sitelerinin yanında kendisine aradığı payı bulamamıştır.

III.SOSYAL AĞLARDA BİLGİ GÜVENLİĞİ İHLALLERİ (PRIVACY VIOLATIONS IN SOCIAL NETWORKS)

Literatürde yayınlanan çalışmalarda; sosyal ağlarda karşılaşabilecek tehdit ve tehlikelerden bazıları aşağıda özetlenmiştir.

K12 düzeyinde eğitim gören çocukların ve gençlerin sosyal ağlarda kendileri ile ilgili pek çok bilgiyi paylaşıma açtıkları [31, 32-34],

Küçük çocukların Pedofili (çocuk istismarı) saldırılarına maruz kaldıkları [35] daha ileri vakalarda sosyal ağlarda tanıştıkları kişiler tarafından zorla alıkonuldukları ve fuhuşa zorlandıkları [36-37],

Şirketlerin market bilgileri topladıkları ve bunu reklam ve satışlarda kullandıkları [38,39],

14 yaş altı çocukların bu ortamları kullanmaması gerekirken sıklıkla kullandıkları [40],

Ad-soyad, doğum tarihi, iletişim adresleri, e-posta adresleri, msn kullanıcı isimleri, kişisel web sayfası bağlantılarının ve cep telefonu bilgilerinin sosyal paylaşım sitelerinde halka açık halde olduğu [41],

Kişilerin sosyal ağ üzerinde yayınladıkları sayfalar nedeniyle öldürülebileceği [42],

Kişilerin kandırılarak sosyal ağ üzerinden para göndermelerinin sağlanabileceği [43],

Sosyal ağ uygulamaları sayesinde bilgisayarların bilişim korsanları tarafından ele geçirilebileceği [43] bu alanda yapılan çalışmalarda vurgulanmıştır.

Bugüne kadar sanal ortamlar; aslında var olmayan sanal kişilikleri yansıtan, günlük yaşantısında tanınmayan, kendilerinin toplum tarafından kabul görmediğini düşünen bireylerin sohbet odalarından veya tartışma sitelerinde en hararetli konuşmaları yaptıkları ve en doğru kararları savundukları kimlikleriyle herkesin beğenisini kazanan popüler kişilere dönüştükleri ortamlar olarak bilinirken son yıllarda bu ortamlarda köklü değişimler yaşanmaktadır.

Elektronik ortamları kullandıkça, aslında rahat, özgür ve korkusuzca istenilen kimlikler ile bilgilerin paylaşıldığı bir ortam algısı da artık değişime uğramaktadır. Sınırsız bir özgürlüğün içinde kaosun kaçınılmaz olacağı olgusu ile sanal ortamlara duyulan güven azalmaktadır. Pek çok kişi kandırılarak bilişim korsanlarının

hedefi olmaya başlamıştır. Birçok organize suç faili kurbanlarını arkadaşlık sitelerinden seçer duruma gelmiştir. Sosyal ağlarda yapabildiklerimiz anlık mesajlaşma, bağlantı paylaşımı, siyasi ve ideolojik paylaşımlar, ailevi ve kişisel paylaşımlar, fotoğraf paylaşımları ve son günlerde uygulama paylaşımları olmak üzere birçok farklı kategoriye yayılmıştır. Bu özelliklerin her biri eski ve yeni saldırı metotlarına davet çıkartmaktadır. Sanal hayatlarımızla gerçek hayatlarımızı karıştırmamızdan kaynaklanan güvenlik açıklarından toplumun her kesimi etkilenmektedir. Bu sitelere verdiğimiz kişisel bilgiler kullanılarak banka hesaplarının boşaltılmasından, bilgisayar sistemlerine virüs bulaştırılmasına, hatta toplum neslinde bireylerin küçük düşürülmesi gibi tehditlerle karşılaşılmaktadır.

IV. BİLGİ GÜVENLİĞİ İHLAL ÖRNEKLERİ (EXAMPLES FOR PRIVACY VIOLATIONS)

Bu ağları da kişisel çıkarları uğruna istismar etmek isteyen bireyler ağa giriş yapan kişi sayısına paralel olarak artmaktadır. Bunun nedeni bilişim korsanlarının ihtiyacı olan ama bulamadıkları bilgilerin, bireylerin kendileri tarafından ifşa edilmesi sayesinde kolaylıkla elde edilebilmesidir. Bilişim korsanların sosyal ağlardan elde ettikleri bilgiler doğrultusunda yaptıkları saldırıların başında kimlik hırsızlığı ve sosyal mühendislik saldırıları gelmektedir. Bilgisayar güvenliğinde sosyal mühendislik "bir bilişim korsanının ilgilendiği bilgisayar sistemini kullanan veya yöneten meşru kullanıcılar üzerinde psikolojik ve sosyal numaralar kullanarak, sisteme erişmek için gerekli bilgiyi elde etme tekniklerine verilen genel ad" olarak tanımlanmaktadır [44].

Bu çalışma kapsamında öngördüğümüz tehdit ve tehlikeler örneklendirilerek sunulmuştur.

ÖRNEK 1:

Sosyal paylaşım ağı üzerinde yapılabileceğini düşündüğümüz ilk yöntem erişim bilgilerini ele geçirmek isteyen bir bilişim korsanının sosyal paylaşım sitesinden hedef kişiye ait profil bilgilerini aşağıdaki gibi elde edebileceğidir.

(1) Ad Soyad

(2) Doğum Tarihi

(3) Annenizin kızlık soyadı

(4) Cep Telefonu Numarası

(1), (2) ve (4) numaralı bilgiler standart profilinizde gözükmesini istediğiniz iletişim ve kişisel bilgilerinizdir. O Halde bilişim korsanının alması için kalan tek bilgi (3) numara annenizin kızlık soyadıdır. Bu bilgiyi vermeyeceğinizi düşünüyorsanız yanılıyorsunuz çünkü arkadaş profilinizde dedeniz, anneanneniz ama daha da önemlisi dayınız kayıtlıysa bu gizli bilgiye ulaşmak hiçte zor değildir. Günümüzde en çok tehdit altında olan bireysel tehlike internet bankacılığı hesaplarıdır.

Bilişim alanında organize suçların önüne geçebilmek için tüm bankacılık işlemlerinde kullanılmak üzere tek kullanımlık SMS şifre kullanılmaya başlanmıştır. Banka hesaplarınızı boşaltmak isteyen bir çete sosyal ağlardan elde ettikleri bilgileri kullanarak internet erişim şifrenize erişmiş olsa dahi tek kullanımlık şifreler nedeniyle telefonunuz çalınsa dahi SIM kartınızın PIN kodunun ancak operatörler vasıtasıyla elde edilebilecek bir bilgi olduğu düşünerek güvende olduğunuz düşünülmektedir. Sanılanın aksine 3 kez hatalı PIN neticesinde kilitlenen telefonun açılması için gerekli olan PUK kodu, operatörlerin otomatik cevaplama sistemine sahip müşteri hatları kullanılarak SIM kartın arkasında yazılı olan seri numarası ile telefon numarasının eşleşmesine bakılarak telefon üzerinden başka hiçbir resmi işlem yapılmaksızın arayan şahıslara bildirilmektedir. Bu sayede sosyal paylaşım ağı üzerinden ifşa edilen bilgiler ile organize suç teknikleri birleştirildiğinde suçlular için yeni yöntemlerin ortaya çıkması kaçınılmazdır.

ÖRNEK 2:

Sosyal ağlarda sık karşılaşılan bir aldatmaca yöntemi ise sahte hesaplar üzerinden sosyal mühendislik ataklarıdır. Bilişim korsanları kimlik hırsızlığı ile elde ettikleri kişisel bilgileri, açtıkları sahte hesaplar üzerinden size ve arkadaş listenizde olan kişilere karşı kullanmaktadır.

Önerdiğimiz senaryoda özgeçmişinizde yer alan okul bilgilerinden yola çıkan saldırgan kendisini de aynı okuldan mezun gibi göstererek güveninizi kazanmaktadır. Sosyal siteler gerçek bilgilerin paylaşıldığı ortamlar olduğu için güveninizi kazanan bir saldırgan çalıştığınızın kurumun gizli bilgilerine kadar birçok hassas bilgiyi çalmak için kimliğinizi kullanabilecektir. Bu senaryoda başınıza açılabilecek sorunların kullanıcı tarafından öngörülebileceği değerlendirilmiştir.

ÖRNEK 3:

Dikkatli olunması gerektiğine inandığımız bir başka konu ise sosyal ağlarda kullanılan ve hızlı bir şekilde yayılmaya devam eden, sayısız güvenlik tehlikesi ve açığı içeren 3. Parti yazılımlardır. Bu yazılımlar sosyal ağın üzerinde yer alan paylaşım ortamı üzerinde geçirilen zamanı artırmaya ve bazılarında uygulamayı yazan kişiye maddi gelir kazandırmaya yönelik eğlence servisleridir. Bu eğlence servisleri ağ kurallarına uyan ama ağ tarafından resmen desteklenmeyen ve her ağ üyesinin kendi yazılımını yazarak dağıtımını ağ üzerinden yapabileceği halde dağıtılmaktadır. Sosyal Ağlar üzerinde en çok bilinen 3. Parti yazılımlar oyun türleridir. Bu yazılımlar kendi bünyesinde yer alan oynama kriterlerine göre kullanıcıların hesaplarına ulaşarak çeşitli iletiler yayınlamakta, oyunun içinde ödüllendirme sistemi geliştirerek oyuna katılma potansiyeline sahip arkadaş listenize sizin sayenizde ulaşabilmektedir. Bu tip bir yazılımı ağ sayfanıza dahil etmek için yapmanız gereken tek şey size gelen davet bağlantısına onay vermektir.

Ağ sayfanıza istediği gibi erişmesine onay verdiğiniz bir yazılım kişisel bilgilerinizi toplayarak kimlik hırsızlığına ya da arkadaş listenize zararlı içerikli bağlantılar göndererek spam veya virüs gibi tehlikeli olu-

şumların yayılmasına neden olacaktır. Bu uygulamalardan bazıları Active-X denetimleri yükleyerek bilgisayarınızda bulunan kişisel dosyalarınızı ele geçirecek Truva atları yükleyebilmektedir.

ÖRNEK 4:

Sosyal ağlar üzerinde karşılaşılabilecek güvenlik zafiyetlerinden bir taneside kullanıcı hesaplarının silinme süreçleridir. Bu çalışma kapsamında elde edilen bilgi birikimi ve deneyim hesapların hiç bir şekilde silinmediğine işaret etmektedir. Bir sosyal ağa dahil kullanıcı hesabını kullanılamaz duruma getirebilmesine rağmen tek yapılabilen hesap ve bağlı işlemlerin dondurulmasıdır. Bu ağlar üzerinde kullanıcılara ait hesapların silinemez olmasının sebebi hesaba ait bilgilerin ileriki bir tarihte hesabın tekrar aktif hale getirilmesi ihtimaline karşın saklanmasıdır. Hesap pasifleştirme sırasında tüm bilgilerinizi sıfırlamanız IP tabanlı konum, aktif durumda kaydolunan ağ grubu ve posta adresi gibi bilgilerin silinmesi anlamı taşımamaktadır. Bu bilgiler sayesinde hesabınız aktif veya pasif iken ilgi alanlarınıza ve konum bilginize göre reklam mesajları almaya devam edebilirsiniz. Ayrıca, gizlilik politikalarında açıkça belirtildiği gibi silinme sürecine alınan hesaplardaki kişisel bilgileriniz silinmeden sosyal ağ şirketi içinde faaliyet gösteren diğer şirket gruplarında kullanılmak üzere saklandığı belirtilmektedir.

ÖRNEK 5:

Sosyal ağları etkin ve verimli kullanmanın en temel şartı olmasına karşın göz ardı edilen hususun gizlilik ilkeleri olduğunu vurguluyoruz. Bir sosyal ağ seçerken bu ağın paylaşım kriterlerine bakılması ve değerlendirilmesi gerekmektedir. Bazı sosyal ağ siteleri en sık kullandığınız e-posta hesabınıza ait erişim bilgilerinizi istemektedir. Bu sayede sosyal ağ sitesinde olduğu halde listenizde ekli olmayan arkadaşlarınızın e-posta adreslerinden bulunarak listenize eklenebileceğinin tarafınıza beyan edilmesidir. Genelde kullanıcılar çeşitli abonelikler ve üyelikler için kullandıkları posta adreslerinin yanında kontrolünü yapmadıkları posta adresleri de kullanmaktadır. Bu sayede hiçbir kişisel bağlantınız olmayan posta adresleri daha az öneme sahip işlemlerde yer almalıdır. Sosyal ağ sitesi tarafından istenilen posta adresi ise tüm arkadaş listenizin olduğu, özel ve gizli yazışmalarınızı yaptığınız ve sürekli kontrolünüzde olan adresinizdir. Bu adrese ait erişim bilgileri ağ üzerinde paylaşıldığında sosyal ağı yöneten kişiler sizin adınıza e-posta göndermekte dahil tüm kişisel işlemlerinize sahip olmaktadır. Bu çok büyük bir güvenlik açığı yaratmasının yanında arkadaş listenizde yer alan e-posta adresleri spam ya da daha kötüsü para karşılığı satılan e-posta listelerine dahil olması gibi istenmeyen durumlar ile karşılaşılmaktadır.

ÖRNEK 6:

Kişisel iletiler deneyimlerimize göre sosyal ağların yükselen tehditlerinden birisidir. Bireysel ağ üzerinde 1 dakika ile n dakika arasında o anki durumlarını bildiren bir anlık mesaj başlığı yayınlamaktadır. Bu başlık, şu an da bu müziği dinliyorum gibi kişisel zevklerinizin açığa çıkmasını sağlayarak size uygun reklamların gönderilmesini sağlayabileceği gibi; "Bu hafta Ankara dışındayım" mesajında olduğu gibi evinize hırsız girmesine de neden olabilecek istenmeyen durumlara neden olmaktadır

ÖRNEK 7:

Araştırmada ortaya çıkan diğer bir kaygı ise ideolojik paylaşımların sanal ortamlarda daha hızlı ve kontrolsüz bir şekilde yayılmasıdır. Sosyal ağlarda ideolojik ve siyasi paylaşımlar aynı ağlar üzerinde kurulan tartışma odalarında veya hayran gruplarında yer almaktadır. Belirli bir görüşü paylaşan kişilerin aksine her ağ üyesinin girebildiği bu grupların üyeleri profilleri vasıtasıyla izlenmekte hatta haklarında çeşitli suçlamalarda bulunulabilmektedir. Bu grupların izlenmesi ve gizlilik ilkelerine aykırı davranışları konusunda ağ sorumluları yetersiz kalmaktadır. Konuşulan tek dilin İngilizce olmadığı konumlarda yaşayan bireyler yasadışı aktivitelerin hızlı bir şekilde yayılmasına neden olmaktadır. Kullanıcılar sadece basit bir daveti kabul etmeleri ile bu tarz oluşumlar içinde istemeden yer almaktadır.

ÖRNEK 8:

Kullanıcıların sosyal ağlar üzerinde tanıştıkları kötü niyetli kişiler tarafından kandırılarak cinsel taciz ve istismar gibi tuzakların kurbanı olabilecekleri aşikardır. Bu kişiler sıklıkla profil içerisinde bulunan mezun olduğu okullar, çalıştığı kurumlar, arkadaşları vb. bilgileri kendilerini ve amaçlarını kamufle etmek maksadıyla kullanmaktadır. Kurbanın güvenini kazandıktan sonra saldırganların kurbanını alı koyma, santaj, taciz ve tecavüz suçlarını işleme olasılığı bulunmaktadır.

ÖRNEK 9:

Kullanıcılar, yükledikleri fotoğraflar sebebiyle taciz ve şantaj gibi tehditlerin hedefinde bulunabilirler. Bazı ağlarda başka kullanıcıların sizin fotoğraflarınızı etiketlemesine izin verilmektedir. Bu sayede, arkadaşlarınız bulunduğunuz tüm fotoğrafları işaretleyerek saldırganlara daha fazla bilgiye erişebilecekleri bir ortam oluşturabilmektedir. Bu fotoğraflara ya da sayfanızda yüklemenize izin verilen kişisel videolarınıza yapılan yorumlar incelendiğinde sizinle ve çevrenizle ilgili çok değerli bilgilere ulaşılabilmektedir. Örneğin, bir aile fotoğrafı ya da videosunda etiketlenen aile bireyleri sayesinde saldırganlar özellikle bankacılıkta sıklıkla kullanılan anne adı, baba adı, çocuk sayısı gibi kişisel bilgilere erişebilmektedir.

Yukarıda 9 farklı örnekte açıklandığımız gibi sanal ortamlar ve özellikle sosyal ağlar, bilinmeyen veya çokta farkında olunmayan pek çok yeni tehlikeleri de üzerinde barındıran paylaşım siteleridir. Gelecekte daha pek çok işlemin sanal ortamlara kayacağı ve bu ortamları kullanmanın kaçınılmaz olacağı düşünülürse, bu ortamlardan alınan hizmetlerin bizi sonu gelmeyen tehlikelere sürükleyebileceği muhtemeldir. Bu konu bizleri meraklandırdığı, heyecanlandırdığı veya korkuttuğu ka-

dar saldırganların veya bilgisayar korsanlarının da iştahını kabartmaktadır.

kişi üzerinde zararlı etkiler oluşturabileceğinin en belirgin göstergesidir.

TABLO 1
SOSYAL PAYLAŞIM SİTELERİNİN GÜVENLİK ÖZELLİKLERİNİN KARŞILAŞTIRILMASI [29]

	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 arama	Var	Var	Var	-	-	-	Var	-	Var	Var
E-Posta Adresine Göre arama	Var	Var	Var	Var	Var	-	-	-	Var	-
Okul Adına Göre arama	Var	Var	-	Var	-	-	-	-	Var	-
Şehir Adına Göre arama	-	Var	-	Var	Var	-	Var	-	Var	Var
İlgili Alanlarına Göre arama	Var	Var	-	Var	-	-	-	-	Var	-
İstenilen Kelimelere göre arama	-	Var	-	Var	Var	Var	-	Var	Var	Var
Üye Olmadan Arama yapma	-	Var	-	-	-	-	Var	-	Var	-

V. SOSYAL AĞ SİTELERİNİN BİLGİ GÜVENLİĞİ AÇISINDAN KARŞILAŞTIRILMASI (COMPARISON FOR SOCIAL NETWORKING SITES FOR PRIVACY)

Tablo 1'de internet ortamından en güncel sosyal paylaşım ağlarının bilgi güvenliği açısından karşılaştırması yapılmıştır [45]. Bu tablodan elde edilen sonuçlar bazı gerçekleri ortaya koymaktadır. Sosyal paylaşım ağları kanunen reşit olmayan kişilerin üye olmasına izin vermektedir. Çocukların ahlaki ve ruhsal yönden tehditlere açık oldukları bir yaşta internet ortamında sanal bir dünya ile bu gelişimi dikkatlice yapmalarına destek verilmemektedir. Bu sorun bazı sosyal ağlar tarafından yaş grubuna uygun olmayan içeriklerin filtrelenmesi ile geçiştirilmeye çalışılmakla birlikte asıl sorun çocukların kendi yaş grupları dışındaki kişilerden gelecek risklere açık olmalarıdır. Bu endişenin farkına varan bazı sosyal ağ tabanlı portal şirketleri ise kayıt yaş sınırını 16 ve 18 olarak belirlemişlerdir. Kayıtlı kullanıcı oranlarına bakıldığında çocukların kayıt olmasına izin veren ağlarda üye sayılarının 1/3 kadarının çocuklardan oluştuğu görülmektedir. Bu ortamlarda kandırılan çocuklar; uyuşturucu, alkol, pedofili, organ mafyası, istismar gibi tehditler ile karşı karşıya kalabilmektedir. Bu tehditler, sosyal paylaşım ağlarının nasıl milyonlarca

Bazı sosyal ağlar, kullanıcılarının kişisel sayfalarında profil editörü ve kullanıcı tanımlı CSS (Cascading Style Sheets) gibi tema betiklerinin kullanılmasına izin vermektedirler. Bu editörler ile uygun filtreleme yapılmayan ortamlarda XSS (Cross Site Scripting) gibi çapraz betik kodu çalıştırma veya SQL Enjeksiyonu gibi daha karmaşık kod çalıştırma saldırıları yapılabilmektedir.

Bazı sosyal ağlar ise kullanıcılarının eğlence servislerine dolayısıyla sosyal ağa bağlılıklarının artması için 3. Parti yazılımlardan destek almaktadır. Bu yazılımlar, sosyal ağ üzerinde genellikle bir Flash ya da Java arayüzünde çalışması için tasarlanan ama sosyal ağ tarafında resmen desteklenmeyen ve gizlilik politikası dışında tutulan servislerdir. Bu yazılımları geliştiren kişiler özel bilgilerinizi ve sağladıkları servisler sebebiyle kredi kartı bilgilerinizi elde ederek tehdit oluşturmaktadır.

Sosyal ağlarda karşılaşılan bir diğer tehdit ise gruplaşmalardır. Siyasetten sanatçılara kadar birçok alanda oluşturulan gruplara üye olunabilmektedir. Bu gruplar sayesinde reklam şirketleri zevklerinizi, fikirlerinizi ve arzularınızı analiz ederek kişiye özel reklamlar üretebileceği gibi sizi takibe alan kişi, kurum ya da kuruluşlara fikir ve görüşleriniz hakkında detaylı bilgilere sağlamaktadır.

Genel olarak irdelendiğinde en büyük güvenlik sorunları arama politikalarından kaynaklanmaktadır. Sosyal ağlar bazı durumlarda üye olmayan kişilerin dahi sistemde arama yapmasına izin vermektedir. Bu aramalar ad-soyad, e-posta adresi, okul adı, şirket veya şehir adı gibi birçok kritere göre yapılabilmektedir. Örneğin; Gazi Üniversitesi grubuna giren ve çıkan kişilerin denetiminin yapılmadığı yerlerde kişiler kendilerini grubunuzun parçası gibi göstererek sosyal mühendislik atakları gerçekleştirebilmektedir.

Kurumlar silinen hesap bilgilerinin içeriklerini bir süreliğine saklayarak kişisel bilgilerinizin kontrolünü kendilerinde kanuni hak olarak görmektedir. Bu amaçla sadece sisteme girdiğiniz bilgiler değil her girişinizde IP bilgisi veya Çerez tabanlı denetimler gibi isteğimiz dışında kayıt altına alınan bilgilerde gizlilik politikalarında bilgi sahibinin her daim sosyal paylaşım ağını yöneten şirket olduğu belirtilmektedir.

Sosyal paylaşım siteleri arayüz desteği verdikleri

TABLO II
SOSYAL PAYLAŞIM SİTELERİNİN GİZLİLİK POLİTİKALARININ KARŞILAŞTIRILMASI [1]

	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	-	AB	AB
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	AB	Güney 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: AB

Bu araştırma kapsamında yaptığımız incelemeler ve elde ettiğimiz bulgular sonucunda Tablo 2 oluşturulmuştur.

Tablo 2'de sosyal paylaşım hizmeti veren ağların gizlilik politikalarına ait karşılaştırmalarının yapıldığı tablo verilmiştir. Tablodan görülebileceği gibi aslında küresel internet kullanıcılarının kişisel bilgileri Amerika Birleşik Devletleri'nde bulunan şirketlerin fiziksel ve yazılımsal güvenlikle koruduklarını teyit ettikleri sunucularda saklanmaktadır. Bu sebeple sosyal paylaşım siteleri ile bilginin 3. Kişilere yasadışı olarak satılması gibi davalık süreçlerden ABD mahkemelerinin yetkili olduğu ifade edilmektedir.

Bazı arama motorları kendi acenteleri ve yüklenici kurumları ile kişisel bilgilerin istatistiksel normlar dâhilinde paylaşıldığını ama 3. Kişilere/Şirketlere bu bilgilerin verilmediğini beyan etmektedir. Bu kurumun bilgiyi uygun gördüğü veya şirketiyle biyolojik bağı bulunan herkesle paylaşabileceğini anlamına gelmektedir. Bu paylaşımlardan kaçınmak için topluma açık profil öğelerini gizleme yeteneğine sahip olan sosyal ağların gerekli ayarlarının yapılarak arama motorları üzerinde veyahut bireysel aramalarda taranabilecek profil nesnelerinin belirlenmesi gerekmektedir.

dillerde gizlilik politikası dil desteği ya hiç vermemekte ya da kısa özetler halinde kural setleri vermektedir. Bu sebeple sadece arayüz anadilinde olan kullanıcılar servise ait ve genellikle İngilizce olan gizlilik bildirimi (Privacy Policy) ve kullanım şartlarını (Terms of Service) görüntüleyebilmekte, tüm kuralları kendi anadillerinde okuyamadıkları için bütün hükümleri peşinen kabul etmiş sayılmaktadır. Bu hükümler gereğince sosyal paylaşım sitelerine verdiğiniz tüm bilgiler bu servisi işleten kurumun malı olmakla birlikte bu bilgiler üzerindeki haklarımız kaybolmaktadır.

Tablo 2'de görülebileceği gibi sosyal ağ siteleri istatistiksel ve bireysel yöntemlerle bilgi toplayarak kullanıcıları izlemektedir. Bu durum gizlilik politikalarında kişiye özel reklam hizmetlerinin verilmesi olarak açıklanmaktadır. Bilgi toplama bilgisayarımıza yerleştirilen çerezler vasıtasıyla yapılmaktadır. Bu çerezler ile bireysel alışkanlıklarımız ve internet kullanma kültürümüze örneğin; reklam üretmek maksadıyla isteğimiz dışında erişilmektedir.

Tablo 2 üzerinde yer alan boş alanlar ise şu an için sosyal ağ sitelerinin gizlilik politikası içinde bahsetmedikleri ve değerlendirmeye açık olmayan özelliklerdir. Bu sebeple kullanıcıların ilgili sitelerde yürüttükleri işlemlerin ve kişisel bilgilerinin güvenliğinin

sosyal ağ servisi sağlayan kurumun esaslarına göre yürütüldüğü ve korunduğu düşünülmektedir.

VI. SOSYAL AĞLARDA OLUŞABİLECEK GÜVENLİK TEHDİT VE TEHLİKELERİN SINIFLANDIRILMASI (CLASSIFICATION OF SECURITY THREATS AND VULNERABILITIES IN SOCIAL NETWORKS)

Sosyal ağlardaki güvenlik açıklıklarının temel nedenleri; bu ağların doğası gereği, mahremiyet ilkelerine uyulmaması, ortamın kontrolünün veya yönetiminin nasıl yapıldığının kullanıcılar tarafından tam olarak bilinmemesi veya kavranamaması belki de en önemlisi kullanıcıların bilgisizliğinden dolayı kişisel bilgilerini bu ortamda paylaşarak kendilerinin açık hedef haline getirmeleridir.

Elektronik ortamların kullanılması ve yaygınlaşması arttıkça, günlük hayatımızdaki iş ve işlemler elektronik ortamlara kaymakta ve günlük hayatımızda yapmış olduğumuz görüşmeler, iletişimler ve sosyalleşme ortamları da sanallaşmaya başlamaktadır. Sanal ortamlar, beklemediğimiz pek çok yeniliği ve farklılıkları kısa sürede ve hızlıca bizlere sunabilmekle birlikte kişisel ve kurumsal bilgi güvenliğini tehdit edecek pek çok tehdit ve tehlikeyi de beraberinde getirmektedir.

Sosyal ağlarda karşılaşılabilecek en tehlikeli sosyal ağ saldırıları 8 ana başlıkta sınıflandırılmış olup aşağıda başlıklar altında değerlendirilmiştir [1, 46, 47, 48, 49, 50].

A. Kimlikleri Taklit Etmek

Sosyal ağlarda bir başkasının yerine geçme, o kişi gibi davranma, bir başkası adına hesap açma veya profil oluşturma kimlikleri taklit etme olarak bilinmektedir. Bu yöntem, sanal ortamlarda karşılaşılan en önemli tehlikelerden birisidir. Bu şekilde, bir başkası kendini ünlü bir şarkıcı, siyasetçi, sanatçı, futbolcu veya öğretim üyesi olarak tanıtabilir, kendisine taraftar toplayabilir, kişilik haklarına zarar verebilir veya başkalarını bu sayede kandırarak haksız kazanç elde edebilir.

B. İstenmeyen E-postalar (Spam) ve Bot Saldırıları:

Saldırganlar, hesaplarını ele geçirdikleri kullanıcılar adına, kişilerin arkadaşlarına, e-posta gruplarına doğrudan e-posta gönderebilir. Gönderilen e-postaların içerisinde, eklerinde veya içeriğinde bulunan genellikle kötü amaçlı uygulamalar ile kullanıcı bilgisayarlarını bir Bot ağının üyesi haline getirebilir. Daha sonra bu bot ağı ile istenilen sistemlere veya ağlara organize saldırılar yapabilir. Sosyal ağlar bot saldırılarına karşın korumasız ortamlardır.

C. Kötü Amaçlı Sosyal Ağ Uygulamaları

Sosyal ağlarda, sohbet, resim ve video paylaşımı, anlık haberleşmenin yanında oyunlar da çokça tercih edilen eğlence araçları veya uygulamalardır. Bu uygulamalar büyük tehditleri beraberinde getirmektedir. Bunlar; iyi, faydalı, eğlenceli veya sevimli bir görünüme bürünmüş olan kötü amaçlı uygulamalar olup herhangi bir oyun, yarışma, bilgi paylaşımı, vb amaçlarla kullanıcılar tarafından yazılan, Facebook gibi bazı paylaşım sitelerinde harici sunucularda çalışan, belirtilen amaçları dışında işlemler de yapabilen uygulamalar olabilmektedir [30]. Orta düzeyde bir web programcılığı bilgisine sahip bir saldırganın, internet ortamlarında bulunan hazır şablonlar kullanarak kısa süre içersinde, uygulamayı yükleyen kullanıcının özel bilgilerini arka planda toplayabileceği ve kullanıcının arkadaş listesindeki tüm kişilere e-posta gönderebilen uygulamalar yazabileceği bilinmektedir [47].

D. Siteler Arası Kod Çalıştırma (XSS) ve Siteler Arası İstek Sahteciliği (CSRF) Saldırıları

CSRF, web tarayıcıların javascript çalıştırma desteğiyle kişilere istenilenin dışında sunuculara komut yollanmasını sağlayan kodlardır 41]. CSRF saldırısı, web uygulamalarının geliştirilmesi aşamasında yapılan basit bir hatadan faydalanılarak yapılır [33]. Kullanıcıların İnternet banka hesabından para transferi, eposta hesabının ayarlarını değiştirme, e-posta gönderme CSRF saldırısı ile yapılabilen saldırılar arasındadır. Sitelerdeki CSRF saldırısına neden olan zafiyetin temelinde, geliştiricilerin uygulamayı geliştirme aşamasında, istemci tarafından gelen her isteğin gerçekten kullanıcıdan geldiğini düşünmeleri yatmaktadır. Web sayfasındaki işlemler, kullanıcının mevcut oturum bilgisi ile yapılmaktadır. Bu oturum bilgisini kesme ya da araya girme yoluyla elde eden saldırganların bu saldırıları yapmaları muhtemeldir.

E. Sazan Avlama (Phishing) Saldırısı

Sosyal ağlardan bilgi toplamayı hedefleyen saldırganlar, sosyal ağların giriş sayfalarını taklit ederek kullanıcıların kullanıcı hesaplarını ve şifrelerini ele geçirebilmekte ve onlar adına işlem yapabilmektedir [49]. Ayrıca, kullanıcıların kendi iradeleriyle sosyal ağlara yükledikleri bilgilerin, kişinin kendi rızasıyla kötü niyetli kişilerin eline geçmesi olasılığı her zaman bulunmaktadır.

F. Casusluk/Casus Yazılımlar

Kritik kurumlarda görev yapan personelin sosyal ağlarda bulunan üyelikleri kurumsal açıdan tehdit oluşturabilmektedir. Üyelik veya profil bilgilerinden, kişilerin arkadaşlıkları, fotoğrafları, yazdıkları veya paylaştıkları bilgiler sayesinde kişisel zafiyetleri ortaya çıkmaktadır. Bu zafiyetler üzerinden farkında olunmadan kurumsal bilgi varlıklarını tehdit eden ve casusluk için iyi bir altyapı oluşturan sorunlar ortaya çıkmaktadır [44]. Bunun yanında, kurumsal bilgisayarlar üzerinden sosyal ağlara yapılan erişimlerde, gerekli önlemler alınmamışsa, kuruma ait sırlarında çalınabileceği değerlendirilmektedir.

G. Sahte Linkler/Bağlantılar

Sosyal ağ sayfalarında veya adres (URL) kısaltması hizmeti veren sitelerde, görünüşte zararlı

olmayan, ancak tıklandıktan sonra kötü niyetli olduğu anlaşılabilen adresler yayınlanmaktadır [49].

H. Bilgi Toplama Saldırıları

Sosyal ağlarda bilgi toplama saldırılarında hedef alınan kişi, grup ya da ağa yönelik bilgilerin elde edilmesi olayıdır. Bilgi toplama aktif ve pasif olmak üzere 2 tipe ayrılır. Sosyal ağlar üzerinde gerçekleşen bilgi toplama girişimleri aktif ataklardır. Tarayıcılar gibi alan adına veya bağlı olduğu alt alan adlarından bilgi çıkartmak amacıyla kullanılabileceği gibi sosyal ağ sayfası üzerinde bulunan dosyalardan, kısayollardan, fotoğraflardan ve özellikle de metadata içeriklerinden kullanıcı bilgileri hasatı(harvesting) ile özel bilgiler toplanabilmektedir [51].

VII. SOSYAL AĞLARDA ALINMASI GEREKEN GÜVENLİK ÖNLEMLERİ (SAFETY PRECAUTIONS IN SOCIAL NETWORKS)

Sosyal ağlarda kişisel güvenlik; sosyal çözümler, teknik çözümler ve yasal çözümler olmak üzere 3 yaklaşım kullanılarak sağlanmaktadır.

- Sosyal çözümler ailede, okulda ve sosyal ağlarda alınacak tedbirlerle,
- 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.

Dünya çapında faaliyet gösteren güvenlik firmaları sosyal ağ sitelerinde karşılaşılabilecek tehditlere karşı çeşitli çözüm önerileri sunmaktadır [46-52]. Bu çalışma kapsamında elde ettiğimiz bilgi birikimleri ve yapmış olduğumuz pratik çalışmalar ile literatürde bulunan mevcut çözümler göz önüne alınarak dikkat edilmesi gereken hususlar sosyal, teknolojik ve yasal çözüm önerileri olarak aşağıda alt başlıklarda özetlenmiştir [31-43].

VII.1. Sosyal Önlemler

Sosyal önlemler, çocuk ve yetişkin olmak üzere iki ana başlıkta değerlendirilmiştir.

Yetişkin olmayan kullanıcılar için çözüm önerilerimiz:

1. Kullanıcıların başına gelebilecek tehdit ve tehlikeleri önlemede aileler birinci derecede sorumludur [35].
2. Aileler, çocuklarını mümkün olduğunca sosyal ağ sitelerini kullanmaktan uzak tutmalı, bu mümkün değilse kullanımda dikkatli olmaları konusunda uyarılmalı, karşılaşılabilecek tehdit ve tehlikeler konusunda bilgilendirmeli, sosyal ağların güvenli kullanımı konusunda eğitmelidir. Konuyla ilgili olarak, çocuklar ile yüz yüze konuşmalı, çocukların elde ettikleri deneyimleri öğrenmeli, bilinmeyen ve algılanmayan hususlar hakkında çocukları mutlaka bilgilendirilmelidir.
3. Sosyal ağ kullanırken gerçek adlarını kullanmadığından, adres, telefon, okul, sınıf, kimlik bilgileri gibi bilgileri sosyal ağlarda paylaşmadığından emin olunmalıdır [52].
4. Ortamlar kontrol edilmeli, verilmiş olan önemli bilgiler var ise bu ortamlardan çıkartılmalı, fotoğraflarda detay verilmemesi, fotoğraf etiketlemelerinden kaçınılması, kişisel resimlerin paylaşılmaması ve tanımadıkları kişilerle haberleşmemeleri konusunda uyarılarda bulunulmalıdır [31, 32, 33, 35, 42].

Yetişkin kullanıcılar için çözüm önerilerimiz:

1. Detay kimlik bilgileri hiçbir zaman paylaşılmamalı, zorunlu ise bu bilgilerde küçük değişiklikler yapılarak verilmelidir. Ad Soyad yerine yakın çevrede kullanılan takma-isimler kullanılmalıdır [49].
2. Sosyal mühendislik ataklarından korunmak için mümkün olduğunca yeni ve bilinmeyen gruplar içinde yer alınmamalı, arkadaş olarak kabul edilecek kişiler konusunda seçici olunmalı, yeni sosyal ağlara katılma davetleri mümkün olduğunca araştırma yapıldıktan sonra kabul edilmelidir. Sosyal ağ üzerinde sahte profiller ile sosyal mühendislik ataklarına maruz kalınabileceğinin farkında olunmalıdır.
3. 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. Bazı sosyal ağ sitelerinde, bölge, çalışma alanı veya şirket adı gibi gruplaşmalar olmaktadır. Grup içerisine sızmaya çalışan bilişim korsanlarına karşı farkında olunmalıdır [11].
4. Anlık e-posta haberleşmesi esnasında, bulunulan durumu, pozisyonu, işi, vb. en genel hatlarıyla anlatacak mesajlaşma yaklaşımları seçilmelidir. Tatile çıktığınızı belirten veya iş yerinde yaşadığınız sıkıntılı bir olayı belirtir anlık e-postalar gönderilmemelidir. Aynı şekilde coğrafi konumunuzu belirten mobil uygulamalardan kaçınılmalıdır. Bu tarz bilgilerin, üçüncü kişiler tarafından görüntülenebileceği, sonrasında bu açıklamaların veya hassas bilgilerin bilişim korsanları ya da organize suç örgütleri tarafından saldırılarda kullanılabileceği unutulmamalıdır [31].
5. Sadece profesyonel temalara sahip fotoğraflar sosyal paylaşım ağlarına yüklenmelidir. Komik duran veya aile üyelerinin olduğu fotoğ-

raflar yüklemekten ve yüklenilen fotoğrafları ise etiketlemekten kaçınılmalıdır. Kendi fotoğraflarınızı izniniz olmadan etiketleyen kullanıcılar ise uyarılmalıdır. Fotoğraflara yorum yaparken kişisel bilgi içermemesine dikkat edilmelidir.

6. Profillerde ya da arkadaş sayfalarında; özel bir konuyu, olayı, finans durumunu veya kişiyi hedef alan yorum yazmaktan kaçınılmalıdır.

VII.2. Önerdiğimiz yasal önlemler

1. Sosyal ağ sitelerine üye olunmadan önce gizlilik politikası, kullanım şartları ve özel şartlar okunarak, karşılaşılabilecek tehdit ve tehlikenin farkında olunarak bu ortamlar kullanılmalı, kişisel bilgilerin hangi şartlarla 3. şahıslarla paylaşılacağı bilincine sahip olunmalı ve ona göre karar verilerek üyelik işlemlerine başlanmalıdır [43].
2. Kullanılan sosyal ağ sitesinin gizlilik politikalarına ve kullanım şartlarına, uyup uymadığı hem hizmet sunan hem de hizmet alan taraflarca kontrol edilmelidir.
3. Sosyal ağ hesapları silinse veya pasif duruma getirilse bile, arama motorları tarafından taranan bilgilere erişimin kısıtlanması maksadıyla sadece genel olduğunu düşündüğünüz önemsiz bilgiler paylaşılmalı veya yayımlanmalıdır.
4. Sosyal ağ kullanıcılarının kanuni haklarını bilmesi, kişisel verilerin korunması kanununa riayet edecek şekilde bilgi ve belge paylaşımını bu ortamlarda yapması önerilmektedir.
5. Çocukların gizlilik politikalarında belirtilen yaş sınırlarına uygun olarak bu ortamları kullanmaları aileleri tarafından sağlanmalıdır [36, 37, 38, 39].

VII.3. Önerdiğimiz Teknolojik Önlemler

1. Sosyal ağ giriş şifresi; bazı kriterler dikkate alınarak, belirli bir politika çerçevesinde ve her hizmet için farklı olacak şekilde belirlenmelidir. Örnek olarak; 12 karakter kombinasyonundan oluşması, içinde büyük küçük harf, rakam, "+", "-", "*", "?" gibi özel karakterleri barındırması, belirli periyotlarda değiştirilmesi, kimseyle paylaşılmaması, vb. kurallara uyulmalıdır.
2. Bilişim korsanları kendilerini, alıcı kişinin arkadaşı gibi göstererek tuzak e-postalar gönderebilmektedir. Alınan e-postaların gerçekten e-posta da belirtilen kişi tarafından gönderilmiş olduğuna güvenmek yanlıştır. Özellikle eklentisinde dosya ya da bağlantı bulunan e-postaları gönderen kullanıcıdan diğer bir haberleşme aracı kullanılarak teyit alınması, verilen linkin tarayıcıya kopyalanarak taşındıktan sonra açılmasına azami dikkat edilmesi gerekmektedir [44].
3. Sosyal ağın arkadaşlarınızın e-posta adreslerine ulaşması için e-posta adres defterini taramasına izin verilmemelidir.
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 [49].
5. 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 farkında olunmalıdır [44].
6. Erişilen veya üyesi olunan sitelerde, 3. parti uygulamaların kişisel bilgilerinize erişmek için bilgisayarınıza yazılım yüklemeye çalışabileceği her zaman hatırlanılmalıdır. Benzer bir tehdidin ilginizi çeken bir resim ya da video paylaşımıyla profilinize erişim denetimi açma istekleri iptal edilmelidir. Öncesinde bu tarz bir uygulamaya izin verilmiş ise uygulama ayarları menüsünden sahte uygulamalar silinerek kaldırılmalıdır. Bu alanda görülen en büyük tehdit sizin adınıza arkadaşlarınızın profiline gönderilen reklam mesajlarıdır.
7. Kullanılan uygulama yazılımları, işletim sistemi vb. yazılımların zamanında güncellenememesinden dolayı güvenlik zafiyeti oluşmaktadır. Temel güvenlik önlemlerini almak için kullanılan tüm bilgisayar yazılımları güncel tutulmalı, anti-viral ve güvenlik duvarı yazılımları mutlaka kullanılmalı ve kötücül yazılım ile spam engelleyici filtreler tercih edilmelidir [44].

VIII. SONUÇLAR ve ÖNERİLER (CONCLUSIONS and RECOMMENDATIONS)

Bu çalışmada sosyal paylaşım ağları; detaylı olarak incelenmiş, güvenlik ihlalleri araştırılmış, karşılaşılabilecek ihlallerinin daha iyi anlaşılabilmesi için örnekler verilmiş, bilgi güvenliği bakış açısıyla sosyal ağlar değerlendirilmiş, paylaşım sitelerinde karşılaşılabilecek tehditler sınıflandırılmış ve alınması gereken önlemler sıralanmıştır.

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, istenilmeyen durumlarla karşılaşılması, beklenilmeyen tehdit ve tehlikelere maruz ka-

lınması ve en önemlisi kişisel bilgilerin mahremiyetine zarar verebilecek pek çok olumsuzlukları içinde barındıran ortamlar olabileceği unutulmamalıdır. Bu nedenle, sosyal ağları kullanırken gerekli güvenlik önlemlerine ve bu makalede sunulan önerilere mutlaka riayet edilmelidir. Bu çalışmada önerilen hususların farkında olunması karışılabilecek tehdit ve tehlikeleri azaltacaktır.

Bu çalışma kapsamında elde edilen hususlar değerlendirildiğinde;

- Saldırıların ve karşılaşılan tehditlerin artmasındaki temel nedenlerin sosyal ağların gizlilik politikalarında yer alan "güvenlik ihlalleri", "güvenlik politikaları" ve "kullanım kuralları" için açıklayıcı bilgilerin anlaşılır şekilde sunulmamasıyla kavramların genelin anlayabileceği şekilde açıklanmaması olduğu görülmüştür.
- Kullanıcıların eş zamanlı pek çok işi yapmalarından kaynaklanan dikkat kayıpları, detaylı okuma, anlama ve uygulama sınırlamalarından dolayı yenilikleri ve değişiklikleri takip edememeleri, tehdit ve tehlikeleri kolaylıkla algılayamamaları ve bilinçsiz kullanımın varlığı karşılaşılan zafiyetlerdir.
- Teknoloji, insan ve eğitim üçgeninin yeni yaklaşımları kullanırken her zaman dikkatli olması gerektiği, bu hususların dikkate alınmaması sonucunda pek çok ciddi tehdit ve tehlikelerle karşılaşılabileceği bilinmelidir.
- Çocukların, bu ortamlarda tehdit ve tehlikelere en fazla maruz kalabilecek kullanıcılar olduğu (Facebook çocuk kullanıcı oranı %36) bilinmeli ve gerekli önlemler, aileler, öğretmenler, yöneticiler, sorumlular tarafından alınmalıdır.

Elbette bu önlemler tek başına yeterli değildir. Sosyal ağ ortamları bizlere pek çok hizmeti sunması yanında beklemediğimiz tehdit ve tehlikeleri de beraberinde getireceğinin farkındalığı için de gereğinden fazla bilginin bu ortamlara aktarılmaması, paylaşılmaması, erişimin denetlenmesi ve korunması, bilincinin halkın her kesiminden bireyler tarafından kullanılması amaçlanmalıdır. Bu tür hizmetleri veren kurumların kişisel verilerin mahremiyetinin sağlanması için kullanım politikalarını geliştirmeleri, tehdit ve tehlikeleri önleyici tedbirleri almaları, kullanıcıları bilgilendirici dokümanlara daha fazla yer vermeleri ve bu konuda daha hassas davranmaları gerektiği düşünülmektedir.

Son olarak, sosyal ağlarda karşılaşılabilecek tehdit ve tehlikelerin azaltılmasına ve kişisel verilerin güvenli olarak paylaşılması için hukuksal olarak korunmaya destek sağlayacak kanun ve yönetmeliklerin oluşturulmasının faydalı olacağı önerilmektedir.

Tehdit ve tehlikelerin daha iyi farkına varılması ve gerekli önlemlerin alınması için bu çalışmada sunulan örneklerden faydalanılmalı ve bu örnekler kullanılarak bilinçlendirme ve bilgilendirme çalışmaları yapılmalıdır.

IX. KAYNAKLAR (REFERENCES)

1) Yavanoğlu U., Sağıroğlu Ş., "Sosyal Ağlar ve Bilgi Güvenliği", **4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı**, Ankara, Türkiye, 6-8 Mayıs 2010.
2) Etzioni A., The Limits of Privacy, Amazon Digital Services, New York, 1999.
3) Chen X., Shi S., "A Literature Review of Privacy Research on Social Network Sites", **IEEE International Conference on Multimedia Information Networking and Security**, 2009.
4) Cutillo L. A., Molva R., Strufe T., "Privacy Preserving Social Networking Through Decentralization", **IEEE**, 2009.
5) Yang C. C., Ng T. D., "Terrorism and Crime Related Weblog Social Network: Link, Content Analysis and Information Visualization", **IEEE**, 2007.
6) Buchegger S., Datta A., "A Case for P2P Infrastructure for Social Networks-Opportunities & Challenges", **IEEE**, 2009.
7) Lang M., Devitt J., Kelly S., Kinneen A., O'Malley J., Prunty D., "Social Networking and Personal Data Security: A Study of Attitudes and Public Awareness in Ireland", **IEEE, ICMeCG**, 2009.
8) Beach A., Gartrell M., Han R., "Solutions to Security and Privacy Issues in Mobile Social Networking", **International Conference on Computational Science and Engineering**, IEEE, 2009.
9) Nagy J., Pecho P., "Social Network Security", **Third International Conference on Engineering Security Information, Systems and Technologies**, IEEE, 2009.
10) Luo W., Liu J., Liu J., Fan C., "An Analysis of Security in social Networks", **Eigth IEEE International Conference on Dependable, Autonomic and Secure Computing**, IEEE, 2009.
11) İnternet: "A Privacy Paradox: Social Networking in the United States", http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312, 2010.
12) İnternet, "Facebook Gizlilik Politikası", http://www.facebook.com/policy.php, 2011.
13) İnternet, "Twitter Gizlilik Politikası" http://twitter.com/privacy, 2011.
14) İnternet, "MSN Gizlilik Politikası" http://privacy.microsoft.com/tr-tr/default.mspx, 2011.
15) İnternet, "Myspace Gizlilik Politikası" http://www.myspace.com/index.cfm?fuseaction=misc.privacy, 2010.
16) İnternet, "Yonja Gizlilik Politikası" http://www.yonja.com/TermsOfService_tr.jsp, 2010.
17) İnternet, "Friends Reunited Gizlilik Politikası" http://www.friendsreunited.co.uk/static/Privacy.aspx, 2010.
18) İnternet, "Linked-in Gizlilik Politikası" http://www.linkedin.com/static?key=privacy_policy&trk=hb_ft_priv, 2010.
19) İnternet, "Youtube Gizlilik Politikası", http://www.youtube.com/t/privacy, 2011.

20) İnternet, “Flickr Gizlilik Politikası”, http://info.yahoo.com/privacy/us/yahoo/flickr/details.html, 2010.

21) İnternet, “Friendster Gizlilik Politikası”, http://www.friendster.com/info/privacy.php, 2010.

22) İnternet, “Buzz Gizlilik Politikası”, http://www.google.com/buzz/help/intl/tr/privacy.html, 2010.

23) İnternet, “Blogger Gizlilik Politikası”, http://www.blogger.com/privacy, 2010.

24) İnternet, “Bebo Gizlilik Politikası”, http://www.bebo.com/Privacy2.jsp, 2010.

25) İnternet, “Hi5 Gizlilik Politikası”, http://www.hi5.com/friend/displayPrivacy.do, 2011.

26) İnternet, “Perfspot Gizlilik Politikası”, http://www.perfspot.com/privacy.asp, 2010.

27) İnternet, “Badoo Gizlilik Politikası”, http://badoo.com/privacy/?sold2=023u57_zWdAxhbEVAZ2ZB0.IzNno60Z1v, 2010.

28) İnternet, “Zorpia Gizlilik Politikası”, http://me.zorpia.com/info/privacy, 2010.

29) İnternet, “Netlog Gizlilik Politikası”, http://tr.netlog.com/go/about/legal/view=privacy, 2010.

30) İnternet, "Orkut Gizlilik Politikası" http://www.orkut.com/html/en-US/privacy.orkut.html?rev=6, 2010.

31) İnternet: "Teens Bold Blogs Alarm School Area” http://www.washingtonpost.com/wp-dyn/content/article/2006/01/16/AR2006011601489.html, 2010.

32) İnternet: “Teens wear their hearts on their blog,”, http://www.usatoday.com/tech/news/techinnovations/2005-10-30-teen-blogs_x.htm 2010.

33) İnternet: “Kids, blogs and too much information: Children reveal more online than parents know,”, http://www.msnbc.msn.com/id/7668788/, 2010.

34) İnternet: “Website’s power to overexpose teens stirs a warning,”, http://www.boston.com/news/local/massachusetts/articles/2005/12/08/websites_power_to_overexpose_teens_stirs_a_warning/, 2010.

35) İnternet: “Gender, identity, and langugage use in teenage blogs,” Journal of Computer–Mediated Communication, volume 10, number 2, at http://jcmc.indiana.edu/vol10/issue2/huffaker.html, 2010.

36) İnternet: “ Will success spoil MySpace? Vanity Fair”, http://www.vanityfair.com/ontheweb/features/2006/03/myspace200603, 2010.

37) İnternet: “MySpace to address Net safety at press conference”, http://news.cnet.com/8301-13577_3-9849795-36.html, 2010.

38) İnternet: “MySpace.com posts safety ads,” http://www.msnbc.msn.com/id/12256764/, 2011.

39) İnternet: “State wants MySpace to raise minimum age,” http://www.usatoday.com/tech/news/techinnovations/2005-10-30-teen-blogs_x.htm, 2010.

40) İnternet: “As freedom shrinks, teens seek MySpace to hang out,” http://msl1.mit.edu/furdlog/docs/2006-05-11_reuters_myspace_kids.pdf, 2010.

41) İnternet: “Gender, identity, and langugage use in teenage blogs,” Journal of Computer–Mediated Communication, volume 10, number 2), at http://jcmc.indiana.edu/vol10/issue2/huffaker.html, 2010.

42) İnternet: “Colombian teens murdered after Facebook threats posted”, http://www.msnbc.msn.com/id/38837285/ns/technology_and_science-tech_and_gadgets, 2011.

43) İnternet: “Facebook Security”, http://www.facebook.com/security?v=app_4949752878, 2010.

44) Canbek G., Sağıroğlu Ş., “Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri”, ISBN: 975-6355-26-3, Grafiker, Ankara, 2006.

45) İnternet: “Sosyal Siteleri Karşılaştırması”http://social-networking-websites-review.toptenreviews.com/, 2010.

46) İnternet, “The Seven Deadliest Social Networking Hacks”, http://www.darkreading.com/security/app-security/showArticle.jhtml? articleID=211201065, 2011.

47) İnternet, “Identity 'at risk' on Facebook”, http://news.bbc.co.uk/2/hi/programmes/click_online/7375772.stm, 2011.

48) İnternet, CSRF~XSRF Nedir?, http://www.cyber-security.org /Madde/ 209/ CSRF~XSRF-Nedir, 2011.

49) Sancho, D., “Security Guide to Social Networks”, White-Paper Trend Micro Inc., 2009.

50) Davies K., Coming of Age Online: The Developmental Underpinnings of Girls Blogs, Journal of Adolescent Research, Vol.25, No.1, pp.145-171, 2010.

51) Internet: “Bilgi Toplama Saldırıları”, http://www.edge-security.com/docs/OWASP-Christian_Martorella-InformationGathering.pdf 31.03.2010

52) İnternet, “Sosyal Ağ Güvenliği için 10 İpucu”, http://www.microsoft.com/turkiye/protect/yourself/phishing/socialnet.mspx, 2010.

53) İnternet: “Gender, identity, and langugage use in teenage blogs,” Journal of Computer–Mediated Communication, volume 10, number 2), at http://jcmc.indiana.edu/vol10/issue2/huffaker.html, 2010.

54) İnternet: “Pedophiles Find a Home for Social Networking”, http://www.foxnews.com/scitech/2010/09/28/pedophiles-find-home-social-networking-facebook/, 2010.

55) İnternet: “Colombian teens murdered after Facebook threats posted”, http://www.msnbc.msn.com/id/38837285/ns/technology_and_science-tech_and_gadgets, 2011.

56) İnternet: “Facebook Security”, http://www.facebook.com/security?v=app_4949752878 2010.