

InCyT Eğitim Modülleri

Çalışanlar için Bilgi Güvenliği

Ünite No: (4) 8. Hafta

Birim (Modül) adı: (Sosyal Ağ)

Öğrenme Aktiviteleri	☐ Web semineri ☐ Alıştırmalar ☐ Çalıştay ☐ Sunum ☐ Diğer Streaming Webinar, Metin, Öz Değerlendirme Alıştırmaları, Tartışma forumlarında ve eğitmen/mentor ile düzenlenen oturumlarda cevaplarla alıştırmalar, e-portfolyolar
Öğrenme Sorumlusu	- David Sommer - Ileana Hamburg
Öğrenme Hedefleri	Etkinliği - Sosyal ağ rolleri - Sosyal ağ platformlarının işlevselliği - Sosyal ağlarda güvenlik ve gizlilik - Çevrimiçi sosyal ağlara yönelik tehditler ve bunlardan kaçınmak için çözümler - Sosyal ağlarda disiplinlerarasılık
Kazanılacak Beceriler	- TS3 Ağ güvenliği - TS4 Penetrasyon (istismar edilebilir güvenlik açıkları) testi - TS5 İzinsiz giriş algılama - SS3 Bilişsel ve davranış analizi
Öğrenme süresi	aktivitesinin 2 hafta
Öğrenme donatımları	Neye ihtiyaç var? - İnternet erişimi - İnternet Tarayıcısı - MS Office365

Modül hakkında kısa bilgi

Giriş

Sosyal ağ, insanların ve kuruluşların arkadaşlarıyla bağlantı kurmasına, iletişim aracı olmasına, yeni bir iş fikri başlatmasına, ürün veya hizmet satmasına ve kendi markasının erişimini genişletmesine yardımcı olur. Elbette, yüz yüze iletişim becerilerinin azalması gibi sosyal ağın dezavantajları da vardır. Kuruluşlar sosyal medyayı yoğun bir şekilde kullandığından, saldırganlar saldırılar için bu platformların güvenliğini ve kamusal doğasını kullanır. Sosyal ağ güvenliği, iş ve özel başarı için önemlidir, böylece bu modüldeki gibi çalışanların eğitiminin büyük bir katkısı olabilir.

Çalışanlar, ilgili metni okuyarak, akış web seminerlerini izleyerek ve egzersizleri kendi hızlarında çözerek ve öğrendiklerini yansıtarak (e-portföyler) bu yönleri öğrenirler. Tüm modül dokümanları dijital interaktif proje platformundadır.

Öğrenciler cevaplarını Öz değerlendirme alıştırmalarında test edebilirler. Diğer alıştırmalarla ilgili cevaplar ilgili tartışma forumlarına kaydedilmeli ve haftada bir kez ortak organize toplantıda mentorla tartışılmalıdır. Öğrenci, özellikle haftalık toplantılarda başkalarıyla işbirliği içinde çalışabilir ve mentorluk yapabilir.

Öğrenme Materyalinin İçeriği

Giriş

Ayrıca artan teknoloji nedeniyle, (çevrimiçi) sosyal ağlar son birkaç yılda çok popüler hale geldi. Bunun bir nedeni, kullanıcıların aileleri, arkadaşları ve meslektaşlarıyla iletişim kurmaları için bir platform sağlama yetenekleridir.

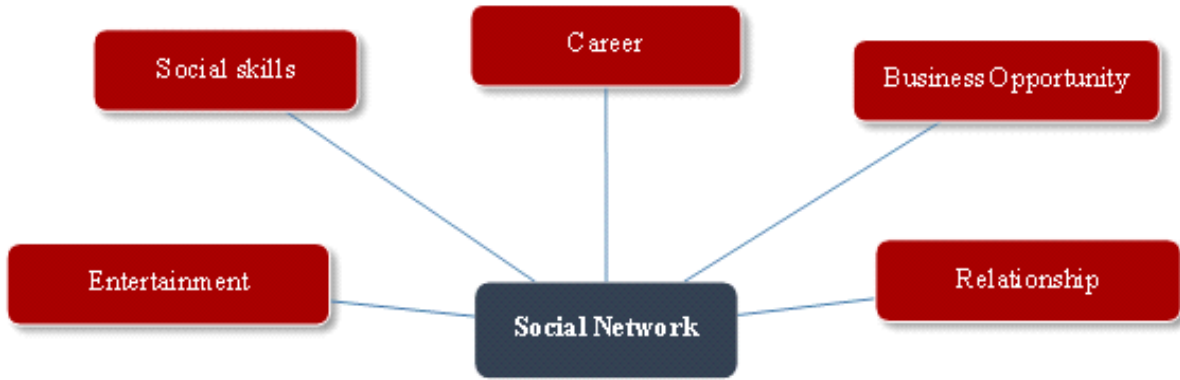
Sosyal ağ, internet tabanlı sosyal medya sitelerinin arkadaşlar, aile, iş arkadaşları, müşteriler veya müşterilerle bağlantı ve iletişim için kullanılmasını ifade eder.

Sosyal medya, insanların aileleri, arkadaşları, müşterileri ile daha iyi ilişkiler kurmalarına yardımcı olur ve sosyal medyayı destekleyen mobil cihazlar, diğer internet erişim yollarına kıyasla giderek daha fazla ilgi görmektedir.

Sosyal ağlar, sunucularını mümkün olduğunda, büyük İnternet servis sağlayıcılarının birbirine bağlandığı ve İnternet'in hızlı bağlantılarına doğrudan erişim sağladıkları büyük İnternet Ağ Erişim Noktaları (NAP'ler) ile birlikte bulunan veri merkezlerinde bulundurulur.

Sosyal ağ rolleri

Sosyal ağlar, Facebook, Twitter, LinkedIn ve Instagram gibi siteleri kullanarak sosyal bir role, bir işletmeye veya her ikisine birden sahip olabilir. Şekil 1, sosyal ağların rol oynadığı bazı alanları göstermektedir (Milsova ve ark.): eğlence, iş fırsatları oluşturma, kariyer yapma, sosyal becerileri geliştirme ve diğer bireylerle ilişkiler geliştirme.

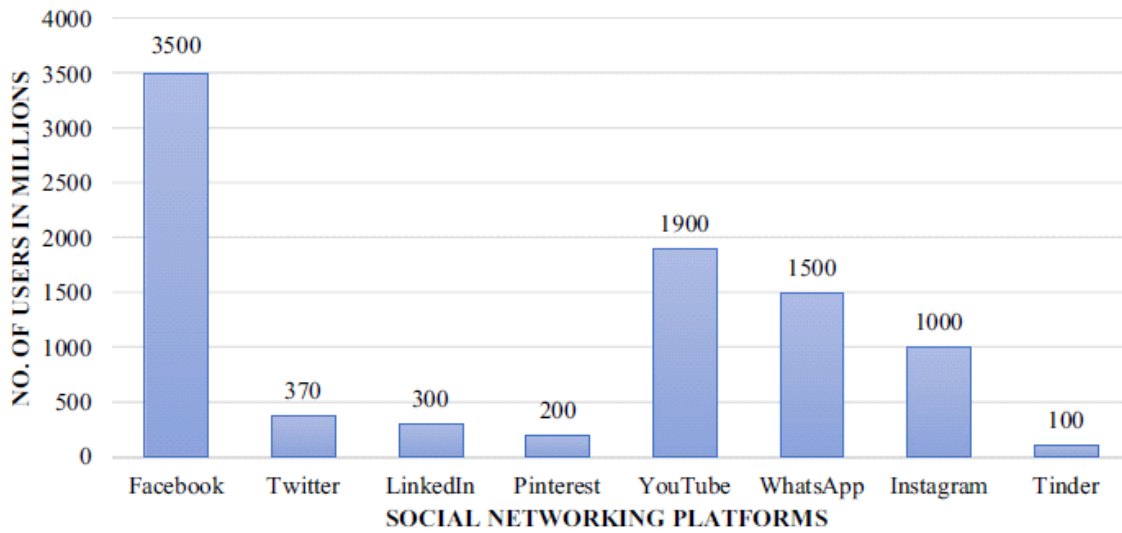


Şekil 1: Sosyal ağlar rolleri

Sosyal ağ, müşteri arayan pazarlamacılar için bir temeldir. Pazarlamacılar, marka bilinirliğini artırmak ve marka sadakatini teşvik etmek için sosyal ağları kullanır. Sosyal medya, insanları ve işletmeleri birbirine bağlamaya yardımcı olabilir ve marka bilinirliğini artırmaya yardımcı olabilir. Örneğin, sık sık Twitter kullanıcısı bir haber kaynağı aracılığıyla ilk kez bir şirket hakkında bilgi edinebilir ve bir ürün veya hizmet satın almaya karar verebilir. Şirketin yeni müşteriler bulma ve elde tutma şansı sosyal ağlar aracılığıyla artmaktadır. Pazarlamacılar, dönüşüm oranlarını artırmak, yeni, yeni ve eski müşterilere erişim ve etkileşim sağlamak için sosyal ağları kullanır. Blog yayınlarını, resimleri, videoları veya yorumları sosyal medyada paylaşılarak daha fazla insan şirketin web sitesini ziyaret edecek ve müşteri olacak. Ancak pazarlama stratejilerine tek bir yaklaşım yoktur; her işletme benzersizdir ve farklı bir hedef demografiye, tarihe ve rekabetçi pazara sahiptir. Sosyal ağ şirketleri, işletmelerin reklamları için ödeme yapmalarını istediğinden, şirketler genellikle ücretsiz yayınlar yoluyla alınan erişim işletmelerinin sayısını kısıtlar. Örneğin, bir şirketin 500 takipçisi varsa, takipçilerin hepsi aynı gönderiyi alamayabilir. Sosyal ağın gelişen doğası,

değişikliklere ayak uydurmayı zorlaştırır ve aynı zamanda bir şirketin pazarlama başarı oranını da etkiler.

Facebook, Instagram, Facebook Messenger ve Twitter, Amerika Birleşik Devletleri ve Avrupa'daki en popüler sosyal paylaşım siteleridir. Diğerleri arasında Pinterest, Tumblr, Snapchat, TikTok ve YouTube, WhatsApp, Messenger by Google ve Tumblr bulunmaktadır. LinkedIn, profesyonelleri iş arkadaşları, iş bağlantıları ve işverenlerle buluşturmaya yardımcı olan başka bir popüler sitedir. Facebook, 31 Aralık 2021 itibariyle platformu aylık olarak kullanan 2,91 milyar kişi ile en büyük ve en popüler sosyal ağ olmaya devam ediyor. Şekil 2, platformlardaki kullanıcı sayısını göstermektedir.



Şekil 2: Platformlardaki kullanıcı sayısı ([https://w ww.dreamg satırı .com/t op](https://www.dreamg satırı .com/t op))

Sosyal Ağların İşlevselliği

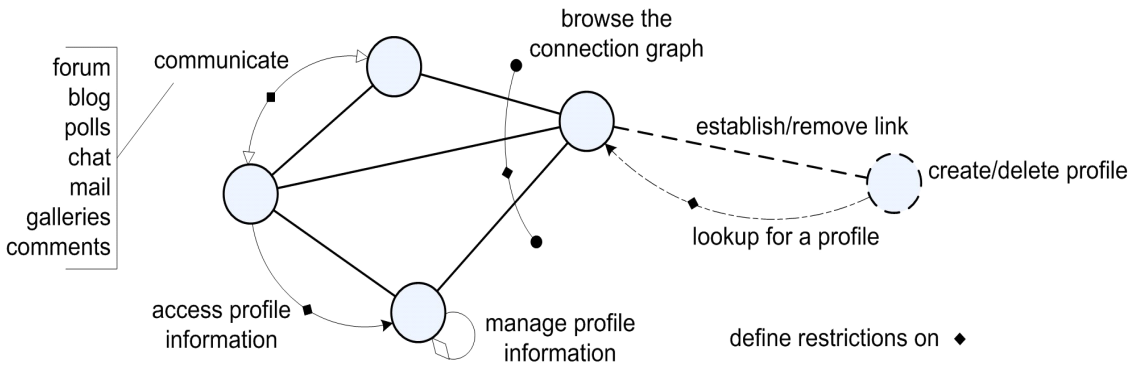
Sosyal ağ, sosyal ağ sitelerinin kullanımı ile teknolojiyi kullanarak kişisel ve iş ilişkilerinin geliştirilmesine ve sürdürülmesine dayanmaktadır. Bu siteler, insanların ve şirketlerin birbirleriyle bağlantı kurmalarına izin verir, böylece ilişkiler geliştirebilir ve bilgi, fikir ve mesaj paylaşabilirler.

Uzakta olan aile üyeleri, Facebook gibi kişisel sosyal ağ siteleri aracılığıyla bağlı kalabilir ve fotoğraf paylaşabilir ve hayatlarından başka mesajlar gönderebilir. İnsanlar aynı ilgi alanlarını paylaşan başkalarıyla (yabancılarla) da bağlantı kurabilirler. Bireyler, gruplarda, listelerde ve hashtag kullanımında üye olarak birbirlerini bulabilirler.

Ancak, yanlış bilgilerin yayılması ve sosyal ağ profillerini kullanmanın ve sürdürmenin yüksek maliyeti de dahil olmak üzere sosyal medya ile ilgili dezavantajlar da vardır.

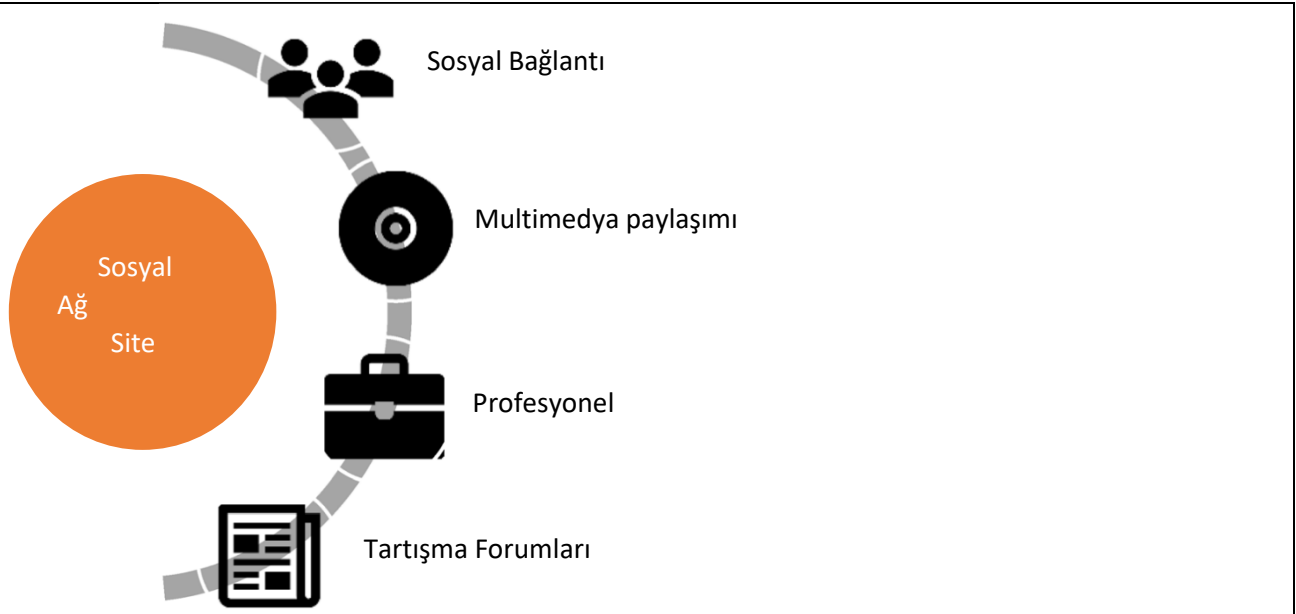
Her sosyal ağ genellikle belirli bir kullanıma hizmet eder, ancak bu platformların işlevselliği benzerdir ve üç ana tipte sınıflandırılabilir:

- Ağ oluşturma işlevleri, sanal platformlardaki kullanıcılar arasındaki sosyal ilişkileri geliştirmeye hizmet eder. Özellikle, sosyal ağ grafiğini oluşturmak ve sürdürmek için işlevsellik sağlarlar.
- Veri işlevleri, kullanıcı tarafından sağlanan içeriğin yönetiminden ve kullanıcılar arasındaki iletişimden sorumludur. Çeşitlilik, kullanıcıların etkileşiminin iyileştirilmesine (genişletilmiş) katkıda bulunur ve platformu daha çekici hale getirir.
- Erişim kontrolü işlevleri, kullanıcı tanımlı gizlilik önlemlerini uygulamayı ve kullanıcı tarafından sağlanan veri ve bilgilere yetkisiz erişimi kısıtlamayı amaçlamaktadır. Şekil 3, tipik bir sanal sosyal ağ platformu tarafından sağlanan işlevselliği gösterir ve daha fazla ayrıntı sağlar (Cuttillo et al. 2010) .



Şekil 3: Tipik bir sosyal ağ platformunun ana işlevselliği (<https://hal.archives-ouvertes.fr/hal-00687145>)

Sosyal ağ siteleri 'sosyal bağlantılar' 'multimedya paylaşımı', 'profesyonel' ve 'tartışma forumları' olarak sınıflandırılabilir (Şekil 4 Jain ve ark., 2021)



Şekil 4: Sosyal ağ siteleri (Jain ve ark., 2021)

Sosyal Ağın Avantajları ve Dezavantajları

Sosyal ağlar hem bireyleri hem de şirketleri hem olumlu hem de olumsuz yönde etkileme yeteneğine sahiptir ve bu nedenle bu tür sosyal medya sitelerini kullanmanın avantajlarını ve dezavantajlarını dikkate almak önemlidir.

Avantaj -ları

Sosyal ağ, bireylerin mesafe veya dokunma kaybı nedeniyle aksi takdirde mümkün olmayacakları aile ve arkadaşlarla iletişim halinde kalmalarını sağlar. İnsanlar aynı ilgi alanlarını paylaşan ve yeni ilişkiler geliştiren diğer bireylerle de bağlantı kurabilirler.

Sosyal ağ, şirketlerin yeni ve mevcut müşterilerle bağlantı kurmasını sağlar. Şirketler ayrıca marka bilinirliğini oluşturmak, tanıtmak ve artırmak için sosyal medyayı kullanabilirler. Ayrıca, müşterileri tarafından marka için önemli olan incelemelere ve yorumlara da güveniyorlar. Satışları artırabilir ve arama motorlarında daha yüksek bir sıralama yapabilir.

Sosyal ağlar yeni bir marka oluşturmaya yardımcı olabilir. Bir şirket, müşterisine yüksek hizmet seviyesini göstermek ve ürünleri ve tüketicilerle ilişkilerini geliştirmek için sosyal ağları kullanabilir. Örneğin, bir müşteri Twitter'da bir ürün veya hizmetten şikayet ederse, şirket özür diler ve durumu iyileştirmek için harekete geçer.

Dezavantaj -ları

Sosyal ağlar yanlış bilginin yayılmasına katkıda bulunabilir Sahoo ve Gupta, 2020, yanlış bilgilerin Twitter'daki doğru bilgilerden %70 daha fazla paylaşılma olasılığının daha yüksek olduğunu tespit etti.

Sosyal medyada ağ kurmanın şirketler üzerinde zararlı etkileri olabilir. Bir markanın eleştirisi sosyal medyada çok hızlı bir şekilde yayıldı. Bunun bir şirketin halkla ilişkiler (PR) departmanı için dezavantajları vardır.

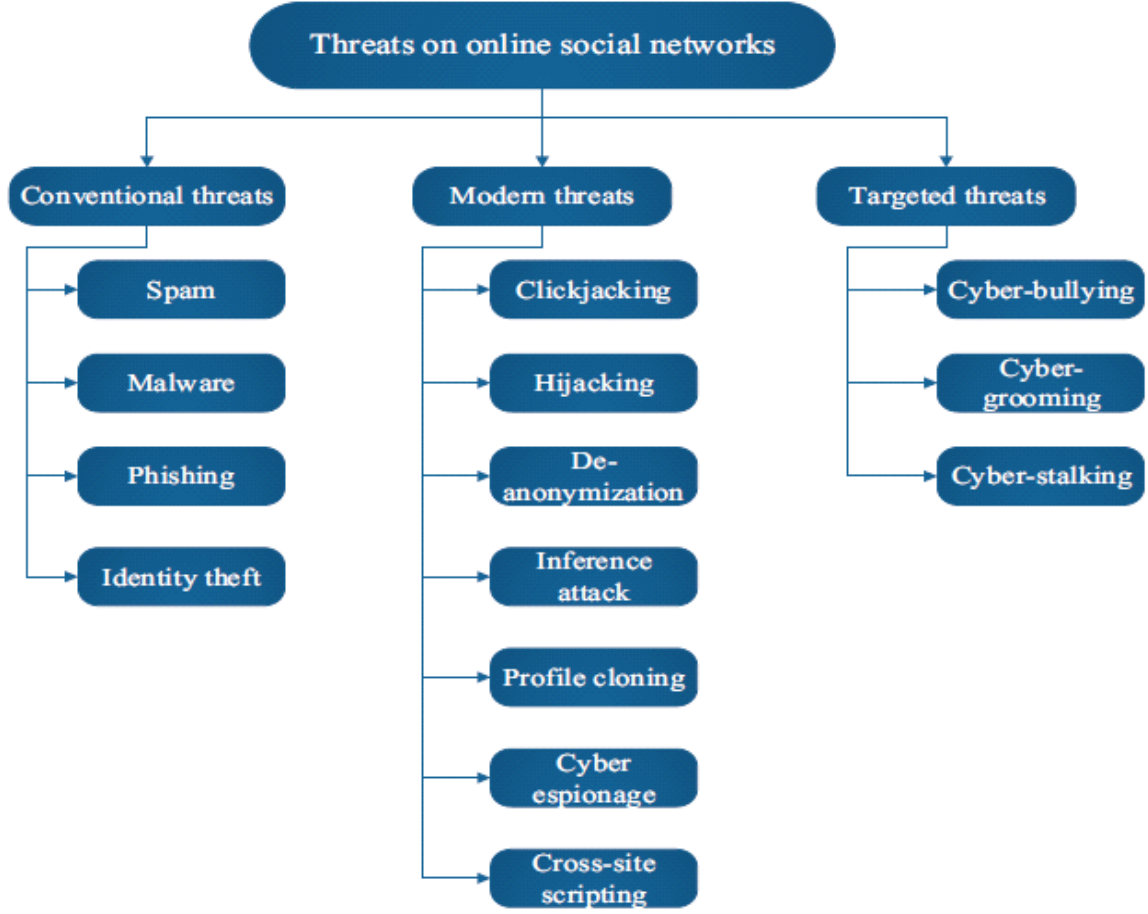
Sosyal ağın kendisi ücretsizdir, ancak bir şirket profili oluşturmak ve sürdürmek her hafta saatlerce çalışmaya ve maliyete ihtiyaç duyar. Bir sosyal medya pazarlama kampanyası olumlu bir yatırım getirisi (ROI) üretmeye başlamadan önce işletmelerin birçok takipçiye ihtiyacı vardır. Örneğin, bir gönderiyi 15 takipçiye göndermek, gönderiyi 15.000 takipçiye göndermekle aynı etkiye sahip değildir.

Sosyal ağlarda güvenlik ve gizlilik

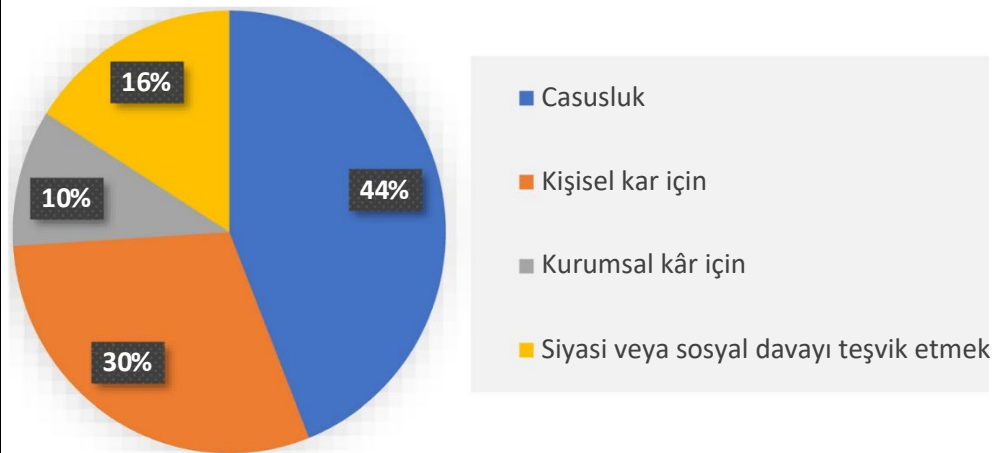
Sosyal ağlarda ve medyada paylaşılan bilgiler çok hızlı yayılıyor ve bu da saldırganların bunu kazanmasını cazip kılıyor. Bir kullanıcı fotoğraf, video ve ses gibi kişisel içerik yüklediğinde kullanıcının paylaşılan bilgileriyle ilgili güvenlik ve gizlilik sorunları vardır. Saldırgan, paylaşılan bilgileri gayri meşru amaçlarla kötü amaçlarla kullanabilir.

Sosyal ağ kullanıcılarına güvenlik sağlayabilecek bazı farklı güvenlik ve gizlilik tehditleri ve mevcut çözümler kısaca sunulmaktadır.

Teknolojinin yoğun kullanımı nedeniyle, etkileşimler internet üzerinden genişletilmiştir. Ne yazık ki, kullanıcılar arasında güvenlik ve gizlilik konusunda farkındalık eksikliği, sosyal medya aracılığıyla çeşitli siber saldırılara yol açma potansiyeline sahiptir Kullanıcıların sosyal ağların başlangıcından itibaren tespit ettikleri tehditler, geleneksel tehditler, modern tehditler ve hedefli tehditler olmak üzere üç kategoriye ayrılabilir (Şekil 5, Jain ve Gupta, 2018). Geleneksel tehditler, kullanıcıların sosyal ağın başlangıcından beri yaşadıkları tehditleri içerir. Modern tehditler, kullanıcıların hesaplarını tehlikeye atmak için gelişmiş teknikler kullanan saldırılardır ve hedefli saldırılar, herhangi bir kullanıcı tarafından çeşitli kişisel kan davaları için işlenebilen belirli bir kullanıcıyı hedef alan saldırılardır.



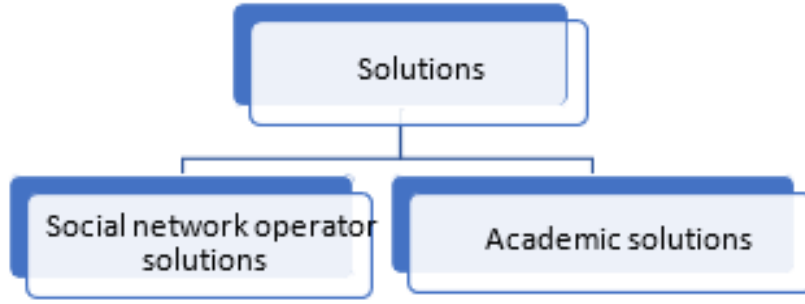
Şekil 5: Tehditlerin sınıflandırılması (Jain ve ark., 2018)



Şekil 6: 2021'de çoğu bilgisayar korsanlığı türü (Jain ve ark., 2021)

Tehditlere yönelik çözümler

Akademi ve endüstrilerdeki araştırmacılar, Şekil 6'da gösterildiği gibi farklı hack türleri için sosyal ağlardaki tehditlere çözüm bulmaya çalışmaktadır. Çözümler ve bazı yaklaşımlar önerilmiştir ve iki gruba ayrılabilir: sosyal ağ operatörü çözümleri ve akademik çözümler (Jain ve ark., 2021). Şekil 7 sınıflandırmayı göstermektedir. Aşağıda kısa bir açıklama sunulmuştur.



Şekil 7: Tehditlere yönelik çözümlerin sınıflandırılması (Jain ve ark., 2021)

Sosyal ağ operatörü çözümleri

Kimlik doğrulama mekanizması

Sosyal bir Bot'a değil, yalnızca meşru bir kullanıcının bir sosyal ağa giriş yaptığından veya kaydolduğundan emin olmak için, CAPTCHA, çok faktörlü kimlik doğrulama ve arkadaş fotoğrafları kimliği gibi kimlik doğrulama prosedürleri önerilmiştir. Örneğin, Twitter ve Facebook gibi sosyal ağlar iki faktörlü kimlik doğrulama ilkelerini kullanır. Bu ilke, bir giriş parolası ve bir mobil cihaz aracılığıyla alınan bir doğrulama kodu kullanır. Bu, bir hesabın güvenliğinin ihlal edilme riskini azaltmaya yardımcı olur ve bir saldırganın meşru bir hesabı ele geçirmesini ve kötü amaçlı içerik yayınlamasını önler.

Güvenlik ve gizlilik ayarı

Birçok sosyal ağ sitesi, istemcinin kişisel bilgilerini yabancılar veya uygulamalar tarafından istenmeyen erişimden uzak tutmasını sağlamak için yapılandırılabilir güvenlik ve gizlilik ayarı sağlar. Örneğin, Facebook istemcisi güvenlik ayarlarını değiştirebilir ve ağdaki ayrıntılarını, resimlerini, gönderilerini ve diğer hassas bilgilerini görebilecek hedef kitleyi (arkadaşlar, arkadaşların arkadaşları ve herkes gibi) seçebilir.

Rapor kullanıcıları

Sosyal ağlar, ağlarındaki herhangi bir kullanıcı tarafından yapılan her türlü kötüye kullanımı veya politika ihlalini bildirme olanağı sağlayarak insanları saldırılardan korur. Örneğin, bir kullanıcı Facebook'ta bireyin duygularına karşılık gelen bir şey görürse, ancak Facebook koşullarını ihlal etmezse, kullanıcı bir rapor (bağlantılar) kullanarak gönderen kişiye bir mesaj gönderebilir ve onu

kaldırmasını veya kaldırmasını isteyebilir. Facebook bir kullanıcı şikayeti aldığı anda, şikayeti Facebook topluluk standartlarına göre incelenir ve kaldırılır.

Akademik araştırmaya dayalı çözümler

Kimlik avı algılama

Kimlik avı, web siteleri, sosyal ağ siteleri, e-postalar ve bloglar gibi birçok geleneksel web uygulamasının gizliliğini ve güvenliğini endişelendiriyordu. Sonuç olarak, kimlik avı saldırılarını tespit etmek için çeşitli kimlik avı önleme teknikleri geliştirilmiştir. Örneğin, Aggarwal ve ark., Twitter'da meydana gelen kimlik avı saldırılarının gerçek zamanlı olarak tanımlanması için PhishAri tekniğini önerdi. Gönderilen tweet'in kimlik avı mı yoksa güvenli mi olduğunu tespit etmek için hesap yaşı ve takipçi sayısı gibi belirli Twitter özelliklerini kullandı.

Siber zorbalık tespiti

Siber zorbalık, bir kişiyi ezmek için e-postalar, sohbetler, telefon görüşmeleri ve çevrimiçi sosyal ağlar gibi elektronik medyanın kullanılmasıdır. Geleneksel zorbalığın aksine, siber zorbalık sosyal medya aracılığıyla sürdürülen sürekli bir süreçtir. Siber zorbalığı tespit etmek, ırkçı dili ve spam'i tespit etmekten daha karmaşık olsa da, bazı araştırmacılar daha karmaşık belge temsili ve mağdurlar ve zorbalılar hakkında ek bilgiler kullanarak tespit etmeye çalışmışlardır. Siber zorbalığı tespit etmek için makine öğrenimi teknikleri uygulanabilir.

Clickjacking (Tıklama Kaçırma)

Otomatik bir sistem, kullanıcıyı tıklama korsanlığı saldırılarına karşı korumak için web sayfalarını analiz edebilir. Çakışan tıklanabilir öğeleri algılayabilen bir koddan oluşur. Ve bu çözüme ek olarak, içinde bir anti-clickjacking özelliğine sahip olan NoScript aracını da benimsediler.

Siber takip

Şifreleme teknikleri, Android ve iOS'un son sürümlerindeki cihazlar için kullanılabilir. Bir cihaz çalınırsa, şifreleme etkinse hırsız içeriği okuyamaz. Ayrıca, bilgileri dahili veya harici bellekten okuma girişimleri, bir cihaz şifresinin varlığı ile engellenir. Akıllı telefon parmak izi kilidi gibi takipçilere karşı kullanılabilecek çeşitli teknolojiler vardır.

Spam algılama

Spam Spotter adlı bir çerçeve, Facebook'taki bir spam saldırısına karşı yardımcı olabilir. Akıllı karar destek sistemine (IDSS) dayanmaktadır. IDSS'deki bir karar sürecinin yardımıyla kullanıcı profilinden

ilgili tüm bilgileri toplar ve daha sonra kullanıcı verilerini bir kullanıcı profilinin spam gönderen veya meşru olarak sınıflandırılmasıyla eşleştirerek analiz eder.

Kötü amaçlı yazılım

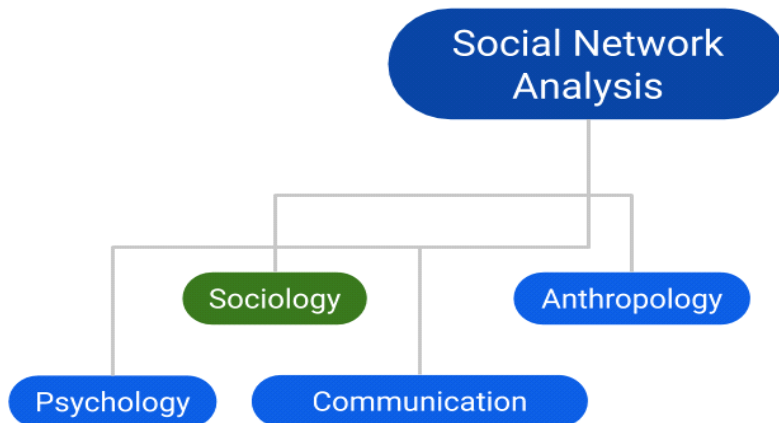
Siteler Arası Komut Dosyası Oluşturma Solucanları (XSS solucanları), diğer ziyaretçilere aşamalı olarak virüs bulaştırmayı amaçlayan bir web sitesinin ziyaretçileri arasında yayılan kötü amaçlı programlardır.

Solucan, üyeler çoğunlukla yabancılardan ziyade arkadaşlarını ziyaret ettiğinde daha yavaş yayılır. Sosyal ağların kümelenmiş doğası nedeniyle de yavaşlatılabilir.

Akademi, sosyal ağ güvenliği ile bağlantılı güvenlik önlemlerini ele almak için bu tür yenilikçi çözümler geliştirmiş olsa da, gerçek dünyadaki uygulama ve fizibiliteden yoksundur. Bu nedenle, teknolojik gelişmeler göz önünde bulundurularak sosyal ağlardaki güvenlik konularının sürekli ve yinelemeli olarak gözden geçirilmesine acilen ihtiyaç duyulmaktadır.

Sosyal ağlarda disiplinlerarasılık

Sosyal ağlara atıfta bulunan disiplinlerarası alan sosyal ağ analizidir (SNA) ve sosyoloji, antropoloji, psikoloji, iletişim ve diğerleri gibi diğer sosyal bilim disiplinlerinden içgörülerini içerir. SNA, fizik, bilgisayar bilimi, veri bilimi, biyoloji, mühendislik, matematik ve diğer alanlardaki çalışmaları içeren ağ bilimi adı verilen her türlü ağı incelemekten sorumlu daha büyük bir disiplinlerarası alanın bir parçasıdır. Bu alanlar arasındaki ilişki Şekil 8'de gösterilmiştir (<https://bookdown.org/omarlizardo/main/1-2-what-is-a-social-network.html>).



Şekil 8: SNA'daki alanlar arasındaki ilişkiler (<https://bookdown.org/omarlizardo/main/1-2-what-is-a-social-network.html>)

Soru:

Sorular Tartışma Forumu kısa bir açıklama ile cevaplandırılacaktır. Mentorluk oturumları sırasında cevaplar mentor ile tartışılacaktır.

1. Sosyal ağlar rolleri
2. Sosyal ağ siteleri
3. Sosyal ağlarla bağlantılı disiplinlerarası alanlar

Ekler:

1. Sunum
2. Video filmler

Başvuru:

Başvuru

Aggarwal A., Rajadesingan A & Kumaraguru P. (2012). PhishAri: Twitter'da otomatik gerçek zamanlı kimlik avı algılama. eCrime Res. Summit, eCrime. 1–12.

Ankit Kumar J., Somya Ranjan S. & Kaubiyal J. · (2021). Veri ihlali dünya çapında neden olur. URL: <https://www.statista.com/statistics/263303/proportion-of-the-most-common-causes-for-possible-identity-theft/> mon- causes- for- possi ble- ident ity- theft/.

Cuttillo, A., Manulis, M. & Strute, T.(2010). Çevrimiçi Sosyal Ağlarda Güvenlik ve Gizlilik. EUROCOM. TU Darmstadt.

Gupta B. & Sahoo, S. (2021). Çevrimiçi sosyal ağ güvenliği: ilkeler, algoritma, uygulamalar ve perspektifler. CRC Yayınları.

Jain A. & Gupta B. (2018). Finansal ve e-bankacılık web sitelerindeki kimlik avı saldırılarının link ve görsel benzerlik ilişkisi kullanılarak tespiti. Int J Inf Comp Secur 10(4):398–417.

Jain, A. , Sahoo, S.R. & Kaubiyal, J. (2021). Çevrimiçi sosyal ağlar güvenliği ve gizliliği: kapsamlı inceleme ve analiz. Karmaşık Intell. Syst. 7, 2157–2177.

Kangur, K. (2022). En Büyük 15 Sosyal Medya Sitesi ve Uygulaması. URL: <https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/>.

Mislove A., Viswanath B., Gummadi K. & Druschel, P. (2010). Sen tanıdığın kişisin. İçinde: Web araması ve veri madenciliği üzerine üçüncü ACM uluslararası konferansının bildirileri—WSDM '10, 251.

Rydstedt, G. (2018). Clickjacking – OWASP. URL: <https://owasp.org/www-community/attacks/Clickjacking>.

Sahoo SR, Gupta BB (2020). Çevrimiçi sosyal ağlardaki multimedya büyük verilerinde sahte profil algılama. Int J Inf Comput Secur 12(2–3), 303–331.