

Moduł treningowy InCyT

Bezpieczeństwo informacji dla pracowników

Część 4, Tydzień 8

Moduł: Sieci społecznościowe

<i>Zajęcia edukacyjne</i>	☒ Webinar ☐ Ćwiczenia ☐ Warsztaty ☐ Prezentacja ☐ Inne
<i>Odpowiedzialni za zajęcia</i>	• David Sommer • Ileana Hamburg
<i>Cele aktywności edukacyjnej</i>	1. Role w serwisach społecznościowych. 2. Funkcjonalność platform społecznościowych. 3. Bezpieczeństwo i prywatność w sieciach społecznościowych 4. Zagrożenia dla internetowych sieci społecznościowych i rozwiązania pozwalające ich uniknąć 5. Interdyscyplinarność w sieciach społecznych
<i>Umiejętności do zdobycia</i>	• TS3 Bezpieczeństwo sieci • TS4 Testy penetracyjne (wykorzystywanie podatności na ataki) • TS5 Wykrywanie włamań • SS3 Analiza poznawcza i analiza zachowania
<i>Czas trwania okresu edukacyjnego</i>	2 tygodnie
<i>Wymagania wstępne</i>	Co jest potrzebne? • Dostęp do Internetu • Przeglądarka Internetowa • MS Office365

Krótką informacją o module



Opis

Sieci społecznościowe pomagają ludziom i organizacjom łączyć się z przyjaciółmi, są środkiem komunikacji, pomagają wprowadzić na rynek nowy pomysł biznesowy, sprzedawać produkty lub usługi oraz zwiększać zasięg własnej marki. Oczywiście, istnieją również wady sieci społecznościowych, takie jak spadek umiejętności komunikacji twarzą w twarz. Ponieważ organizacje intensywnie korzystają z mediów społecznościowych, napastnicy wykorzystują zaufanie i publiczny charakter tych platform do ataków. Bezpieczeństwo sieci społecznościowych jest ważne dla sukcesu biznesowego i prywatnego, więc szkolenie pracowników, jak w tym module, może mieć duży wkład.

Pracownicy uczą się o tych aspektach poprzez czytanie odpowiednich tekstów, oglądanie webinarów, rozwiązywanie ćwiczeń we własnym tempie i refleksje na temat tego, czego się nauczyli (e-portfolio). Wszystkie dokumenty modułu znajdują się na cyfrowej, interaktywnej platformie projektowej.

Uczniowie mogą sprawdzić swoje odpowiedzi na ćwiczeniach samooceny. Odpowiedzi na inne ćwiczenia powinny być zapisywane na odpowiednich forach dyskusyjnych i omawiane z mentorem na wspólnym, zorganizowanym spotkaniu raz w tygodniu. Uczący się mogą współpracować z innymi i mentorem szczególnie podczas cotygodniowych spotkań.

Treść materiałów dydaktycznych

Wprowadzenie

Również ze względu na rozwijającą się technologię, sieci społecznościowe (online) stały się bardzo popularne w ciągu ostatnich kilku lat. Jednym z powodów jest ich zdolność do zapewnienia platformy dla użytkowników do komunikowania się z rodziną, przyjaciółmi i kolegami.

Sieci społecznościowe odnoszą się do korzystania z internetowych stron mediów społecznościowych w celu połączenia i komunikacji z przyjaciółmi, rodziną, kolegami, klientami lub klientami.

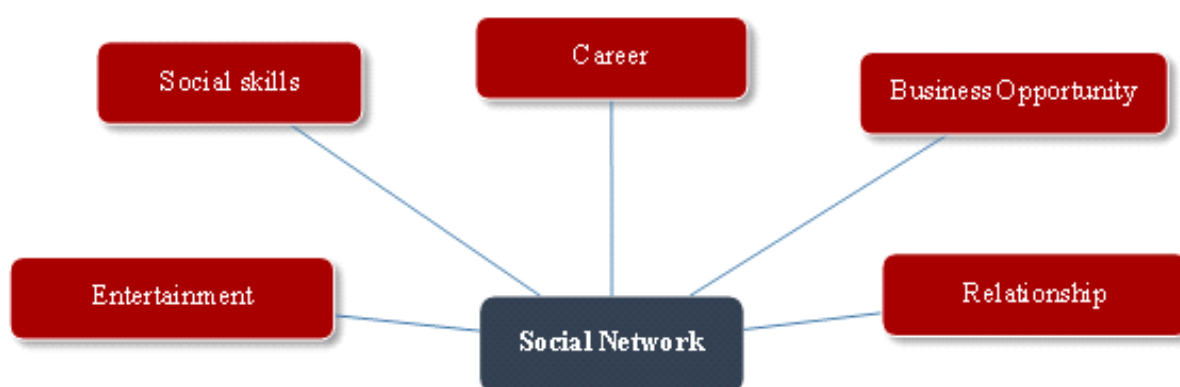
Media społecznościowe pomagają ludziom mieć lepsze relacje z rodziną, przyjaciółmi, klientami, a urządzenia mobilne obsługujące media społecznościowe zyskują coraz większe zainteresowanie w porównaniu z innymi sposobami dostępu do Internetu.

Sieci społecznościowe mają swoje serwery w centrach danych zlokalizowanych, jeśli to możliwe, w głównych punktach dostępu do sieci internetowej (NAP), gdzie łączą się ze sobą wielcy dostawcy usług internetowych i gdzie zapewniają bezpośredni dostęp do szybkich łącz

internetowych.

Role sieci społecznościowych

Sieci społecznościowe mogą pełnić rolę społeczną, biznesową lub obie, dzięki wykorzystaniu takich serwisów jak Facebook, Twitter, LinkedIn i Instagram. Rysunek 1 przedstawia niektóre dziedziny, w których sieci społecznościowe odgrywają rolę (Milsova i in.): rozrywka, budowanie możliwości biznesowych, robienie kariery, doskonalenie umiejętności społecznych i rozwijanie relacji z innymi osobami.

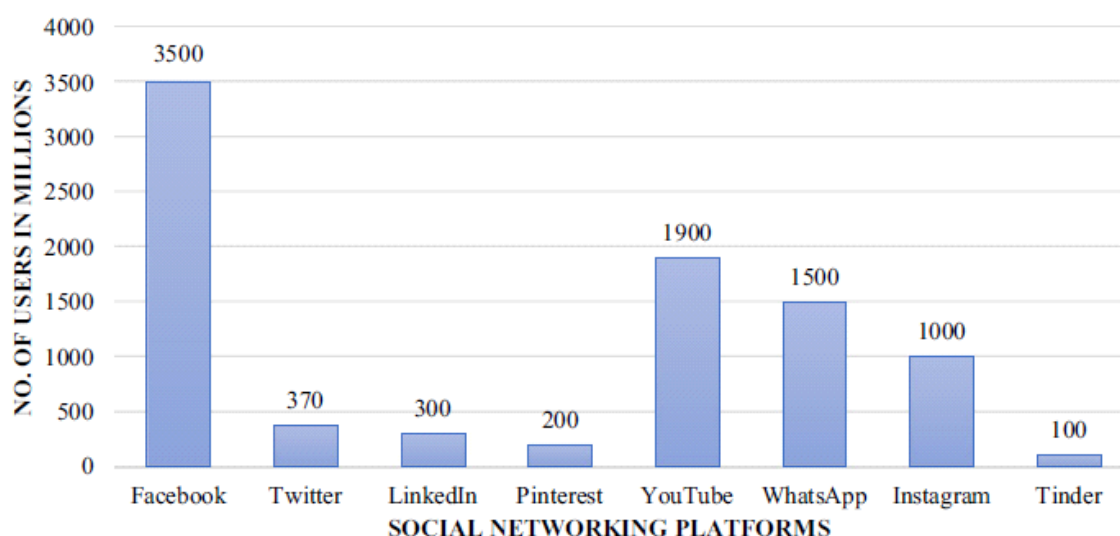


Rysunek 1: Role w sieciach społecznych

Sieci społecznościowe to baza dla marketerów, którzy poszukują klientów. Marketerzy wykorzystują sieci społecznościowe m.in. do zwiększania rozpoznawalności marki i zachęcania do lojalności wobec marki. Media społecznościowe mogą pomóc w łączeniu ludzi i firm oraz mogą pomóc w promowaniu świadomości marki. Na przykład, częsty użytkownik Twittera może dowiedzieć się o firmie po raz pierwszy poprzez kanał informacyjny i zdecydować się na zakup produktu lub usługi. Szanse firmy na znalezienie i utrzymanie nowych klientów rosną dzięki sieciom społecznościowym. Marketerzy wykorzystują sieci społecznościowe do poprawy współczynników konwersji, zapewniają dostęp i interakcję z nowymi, niedawnymi i starymi klientami. Poprzez udostępnianie postów na blogu, zdjęć, filmów lub komentarzy w mediach społecznościowych więcej osób odwiedzi stronę internetową firmy i stanie się klientami. Ale nie ma jednego podejścia do strategii marketingowych: każda firma jest wyjątkowa i ma inną docelową demografię, historię i konkurencyjny rynek. Ponieważ firmy społecznościowe chcą, aby firmy płacić za ich reklamy, firmy często ograniczają liczbę zasięgu firm otrzymanych przez niepłatne posty. Na przykład, jeśli firma ma 500 zwolenników, zwolennicy nie mogą wszyscy otrzymać tego samego postu. Ewoluujący charakter sieci społecznych sprawia, że trudno jest nadążyć za zmianami, a także wpływa na wskaźnik sukcesu marketingowego firmy.

Facebook, Instagram, Facebook Messenger i Twitter to najpopularniejsze serwisy

społecznościowe w Stanach Zjednoczonych, a także w Europie. Inne obejmują Pinterest, Tumblr, Snapchat, TikTok, a także YouTube, WhatsApp, Messenger by Google i Tumblr. LinkedIn to kolejna popularna strona, która pomaga łączyć profesjonalistów ze współ-pracownikami, kontaktami biznesowymi i pracodawcami. Największą i najpopularniejszą siecią społecznościową pozostaje Facebook, z 2,91 mld osób korzystających miesięcznie z platformy, według stanu na 31 grudnia 2021 roku. Wykres 2 przedstawia liczbę użytkowników na platformach.



Rysunek 2: Liczba użytkowników na platformach (<https://www.dreamgrow.com/top>)

Funkcjonalność serwisów społecznościowych

Social networking opiera się na rozwoju i utrzymywaniu relacji osobistych i biznesowych przy użyciu technologii poprzez wykorzystanie serwisów społecznościowych. Strony te pozwalają ludziom i firmom łączyć się ze sobą, dzięki czemu mogą rozwijać relacje i mogą dzielić się informacjami, pomysłami i wiadomościami.

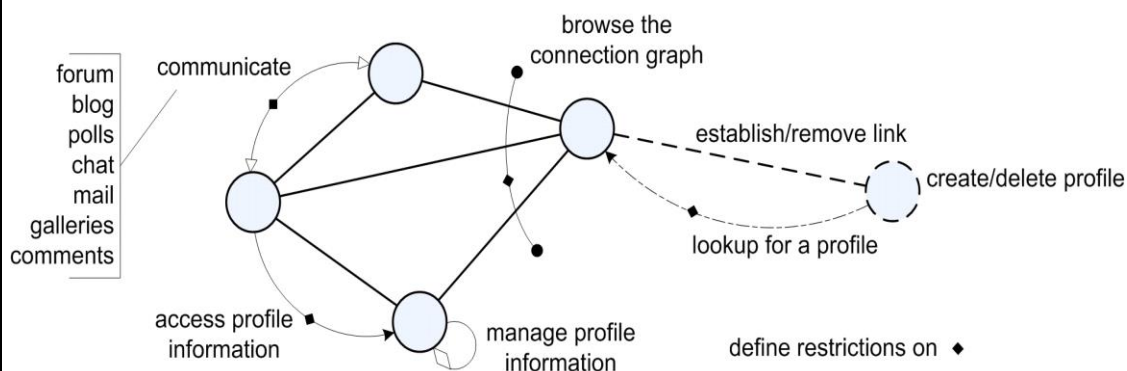
Członkowie rodziny, którzy są daleko mogą pozostać połączeni poprzez osobiste serwisy społecznościowe, takie jak Facebook i dzielić się zdjęciami i wysyłać inne wiadomości ze swojego życia. Ludzie mogą również łączyć się z innymi (nieznajomymi), którzy dzielą te same zainteresowania. Osoby mogą się nawzajem odnajdywać dzięki członkostwu w grupach, na listach i stosowaniu hashtagów.

Istnieją jednak również wady związane z mediami społecznościowymi, w tym rozprzestrzenianie się dezinformacji oraz wysokie koszty korzystania i utrzymywania profili w sieciach społecznościowych.

Każda sieć społecznościowa służy zwykle jakiemuś konkretnemu zastosowaniu, ale

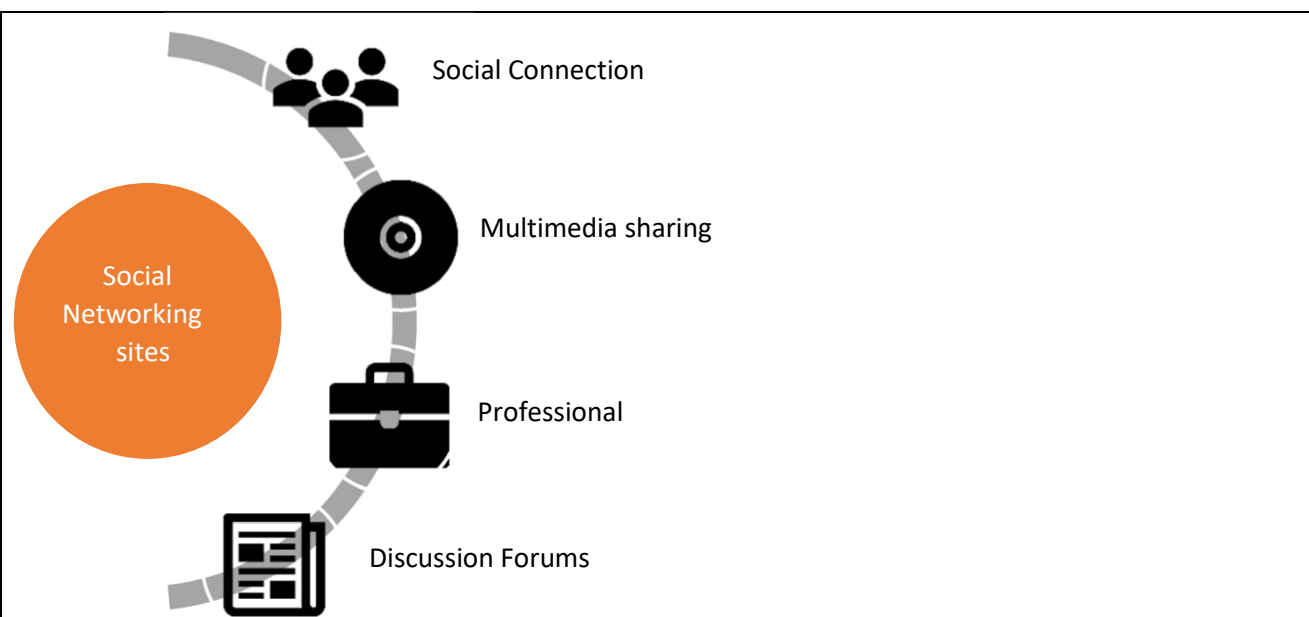
funkcjonalność tych platform jest podobna i można je podzielić na trzy główne typy:

- Funkcje sieciowe służą do wspierania relacji społecznych wśród użytkowników w ramach platform wirtualnych. W szczególności zapewniają one funkcjonalność w zakresie budowania i utrzymywania grafu sieci społecznej.
- Funkcje danych są odpowiedzialne za zarządzanie treściami dostarczonymi przez użytkowników i komunikację między nimi. Różnorodność przyczynia się do poprawy (rozszerzenia) interakcji użytkowników i uatrakcyjnienia platformy.
- Funkcje kontroli dostępu mają na celu wdrożenie zdefiniowanych przez użytkownika środków ochrony prywatności oraz ograniczenie nieautoryzowanego dostępu do dostarczonych przez użytkownika danych i informacji. Rysunek 3 przedstawia funkcjonalność dostarczaną przez typową platformę wirtualnych sieci społecznościowych i zawiera więcej szczegółów (Cutillo et al. 2010).



Rysunek 3: Główna funkcjonalność typowej platformy społecznościowej (<https://hal.archives-ouvertes.fr/hal-00687145>)

Social networking sites can be classified into 'social connections' 'multimedia sharing', 'professional' and 'discussion forums' (Figure 4 Jain et al., 2021)



Rysunek 4: Portale społecznościowe (Jain i in., 2021)

Zalety i wady sieci społecznościowych

Serwisy społecznościowe mogą wpływać zarówno na osoby indywidualne, jak i na firmy - zarówno w sposób pozytywny, jak i negatywny, dlatego ważne jest, aby wziąć pod uwagę zalety i wady korzystania z takich serwisów społecznościowych.

Zalety

Social networking pozwala jednostkom utrzymywać kontakt z rodziną i przyjaciółmi, którzy w przeciwnym razie nie mogliby z powodu odległości lub utraty kontaktu. Ludzie mogą również łączyć się z innymi osobami, które dzielą te same zainteresowania i rozwijać nowe relacje.

Sieci społecznościowe pozwalają firmom łączyć się z nowymi i istniejącymi klientami. Firmy mogą również korzystać z mediów społecznościowych do tworzenia, promowania i zwiększania świadomości marki. Polegają one również na recenzjach i komentarzach swoich klientów ważnych dla marki. Może to zwiększyć sprzedaż i wyższy ranking w wyszukiwarkach.

Sieci społecznościowe mogą pomóc w ustanowieniu nowej marki. Firma może korzystać z sieci społecznościowych, aby wykazać swój wysoki poziom obsługi klienta i poprawić produkty i relacje z konsumentami. Na przykład, jeśli klient skarży się na produkt lub usługę na Twitterze, firma przeprosza i podejmuje działania w celu poprawy sytuacji.

Wady

Sieci społecznościowe mogą przyczynić się do rozprzestrzeniania dezinformacji Sahoo i Gupta, 2020 stwierdzili, że dezinformacja jest o 70% bardziej prawdopodobna do udostępnienia niż właściwa informacja na Twitterze.

Tworzenie sieci w mediach społecznościowych może mieć szkodliwy wpływ na firmy. Krytyka marki rozprzestrzenia się bardzo szybko na mediach społecznościowych. Ma to niekorzystne skutki dla działu public relations (PR) firmy.

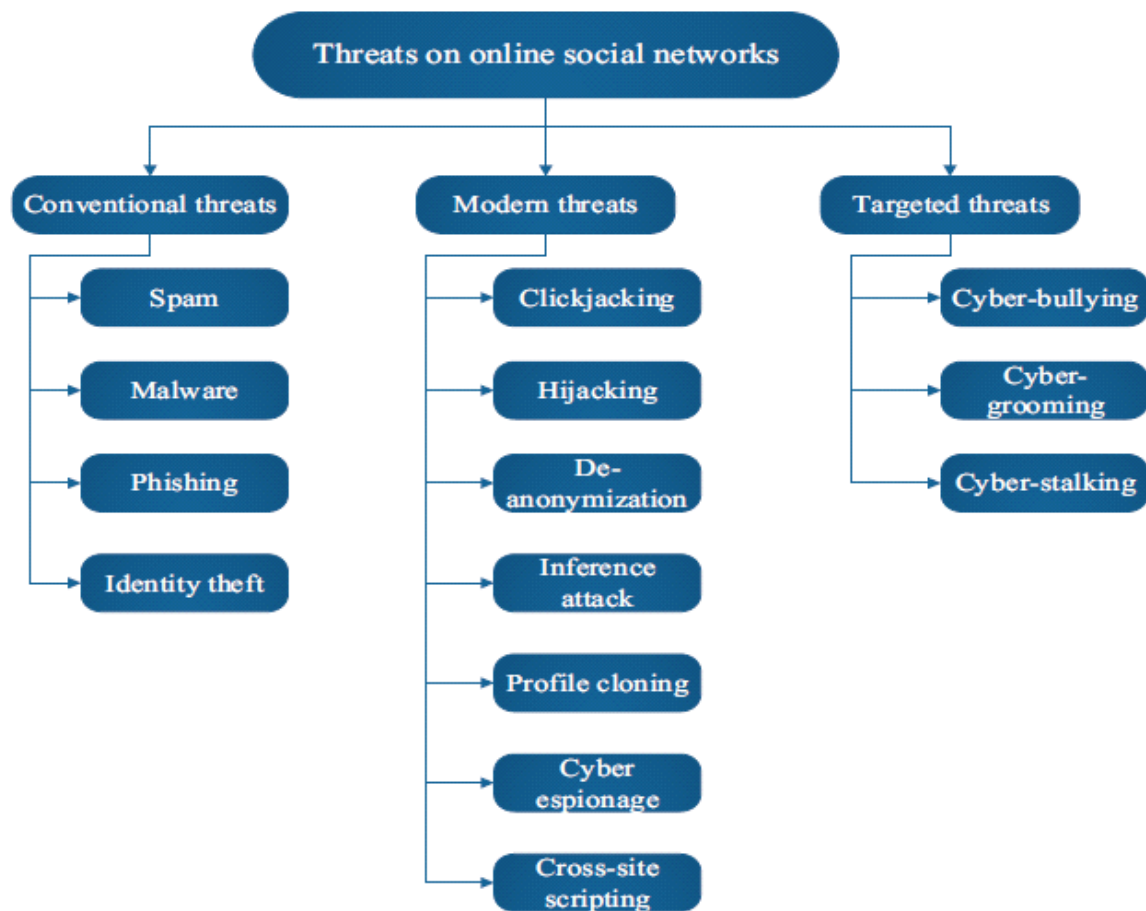
Same portale społecznościowe są darmowe, ale budowanie i utrzymywanie profilu firmy wymaga godzin pracy i kosztów każdego tygodnia. Firmy potrzebują wielu followersów, zanim kampania marketingowa w mediach społecznościowych zacznie generować pozytywny zwrot z inwestycji (ROI). Na przykład, przesłanie postu do 15 followersów nie daje takiego samego efektu jak przesłanie postu do 15 000 followersów.

Bezpieczeństwo i prywatność w sieciach społecznościowych

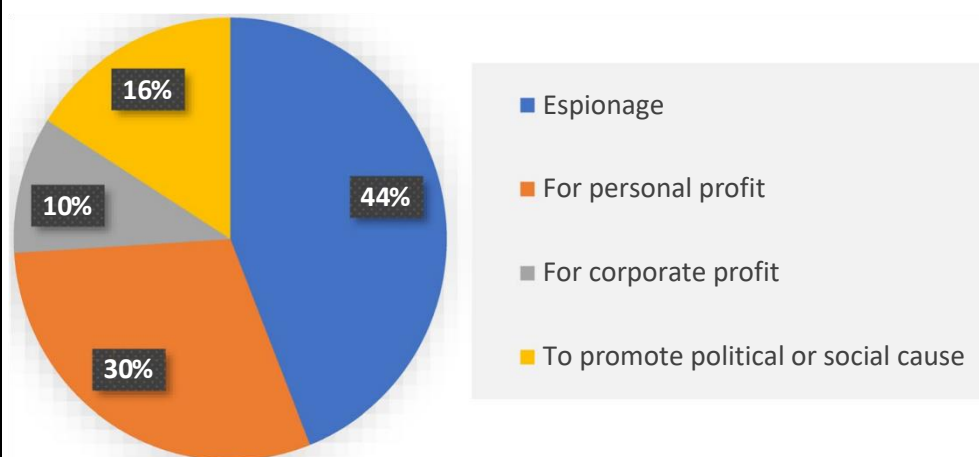
Informacje udostępniane w sieciach społecznościowych i mediach rozprzestrzeniają się bardzo szybko, co czyni je atrakcyjnymi do zdobycia przez napastników. Istnieją kwestie bezpieczeństwa i prywatności związane z udostępnionymi informacjami użytkownika, gdy użytkownik przesyła osobiste treści, takie jak zdjęcia, filmy i nagrania dźwiękowe. Napastnik może złośliwie wykorzystać udostępnione informacje do celów niezgodnych z prawem.

W skrócie przedstawiono niektóre różne zagrożenia dla bezpieczeństwa i prywatności oraz istniejące rozwiązania, które mogą zapewnić bezpieczeństwo użytkownikom sieci społecznościowych.

Ze względu na intensywne wykorzystanie technologii, interakcje zostały rozszerzone poprzez Internet. Niestety, brak świadomości wśród użytkowników w zakresie bezpieczeństwa i prywatności potencjalnie może prowadzić do różnych cyberataków za pośrednictwem mediów społecznościowych. Zagrożenia, które użytkownicy wykryli od początku istnienia sieci społecznościowych, można podzielić na trzy kategorie, tj. konwencjonalne zagrożenia, nowoczesne zagrożenia i ukierunkowane zagrożenia (rys. 5, Jain i Gupta, 2018). Konwencjonalne zagrożenia obejmują zagrożenia, których użytkownicy doświadczają od początku istnienia sieci społecznościowej. Nowoczesne zagrożenia to ataki wykorzystujące zaawansowane techniki w celu kompromitacji kont użytkowników, a ataki ukierunkowane to ataki skierowane na konkretnego użytkownika, które mogą być popełnione przez każdego użytkownika dla zróżnicowanych osobistych wendet.

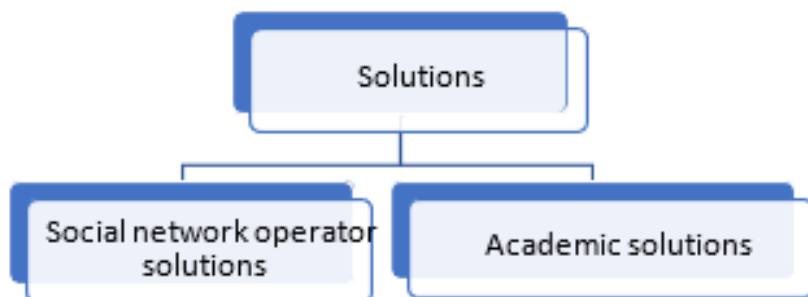


Rysunek 5: Klasyfikacja zagrożeń (Jain et al, 2018)



Rysunek 6: Większość rodzajów włamań w 2021 r. (Jain et al, 2021)

Naukowcy w środowisku akademickim i w przemyśle próbują znaleźć rozwiązania dla zagrożeń w sieciach społecznościowych dla różnych typów włamań, jak pokazano na rysunku 6. Zaproponowano rozwiązania i pewne podejścia, które można podzielić na dwie grupy: rozwiązania operatorów sieci społecznościowych i rozwiązania akademickie (Jain i in., 2021). Rysunek 7 przedstawia tę klasyfikację. Krótki opis został przedstawiony poniżej.



Rysunek 7: Klasyfikacja rozwiązań dla zagrożeń (Jain et al, 2021)

Rozwiązania dla operatorów sieci społecznościowych

Mechanizm uwierzytelniania

Aby upewnić się, że tylko uprawniony użytkownik loguje się lub rejestruje w sieci społecznościowej, a nie bot społecznościowy, zaproponowano procedury uwierzytelniania, takie jak CAPTCHA, uwierzytelnianie wieloczynnikowe i identyfikacja za pomocą zdjęć znajomych. Na przykład, sieci społecznościowe takie jak Twitter i Facebook wykorzystują zasady uwierzytelniania dwuczynnikowego. Zasada ta wykorzystuje hasło logowania oraz kod weryfikacyjny otrzymany za pośrednictwem urządzenia mobilnego. Pomaga to zmniejszyć ryzyko kompromitacji konta i uniemożliwia napastnikowi porwanie legalnego konta i zamieszczenie złośliwej treści.

Ustawienia bezpieczeństwa i prywatności

Wiele serwisów społecznościowych zapewnia konfigurowalne ustawienia bezpieczeństwa i prywatności, aby umożliwić klientowi umieszczenie informacji osobistych przed niepożądanym dostępem osób postronnych lub aplikacji. Na przykład, klient Facebooka może zmodyfikować swoje ustawienia bezpieczeństwa i wybrać publiczność (jak przyjaciele, przyjaciele przyjaciół i wszyscy) w sieci, którzy mogą zobaczyć swoje dane, zdjęcia, posty i inne wrażliwe informacje.

Raportowanie użytkowników

Sieci społecznościowe chronią ludzi przed atakami, zapewniając możliwość zgłaszania wszelkich form nadużyć lub naruszeń zasad przez dowolnego użytkownika w ich sieci. Na przykład,

jeśli użytkownik zobaczy na Facebooku coś, co odpowiada jego indywidualnym odczuciom, ale nie narusza warunków Facebooka, to użytkownik może wykorzystać raport (linki), aby wysłać wiadomość do tego, kto go zamieścił, prosząc go o zdjęcie lub usunięcie.

Kiedy Facebook otrzymuje raport użytkownika, jest on przeglądany i usuwany zgodnie ze standardami społeczności Facebooka.

Rozwiązania oparte na badaniach akademickich

Wykrywanie phishingu

Phishing zagraża prywatności i bezpieczeństwu wielu tradycyjnych aplikacji internetowych, takich jak strony internetowe, serwisy społecznościowe, e-maile i blogi. W związku z tym opracowano kilka technik anty-phishingowych, których celem jest wykrywanie ataków phishingowych. Na przykład, Aggarwal et al. zaproponowali technikę PhishAri do identyfikacji w czasie rzeczywistym ataków phishingowych występujących na Twitterze. Wykorzystuje ona specyficzne cechy Twittera, takie jak wiek konta i liczba followersów, aby wykryć, czy opublikowany tweet jest phishingiem, czy też jest bezpieczny.

Wykrywanie cyberprzemocy

Cyberprzemoc jest wykorzystanie mediów elektronicznych, takich jak e-maile, czaty, rozmowy telefoniczne i sieci społecznościowe online, aby prześladować osobę. W przeciwieństwie do tradycyjnego nękania, cyberprzemoc jest ciągłym procesem utrzymywanym za pośrednictwem mediów społecznościowych. Chociaż wykrywanie cyberprzemocy jest bardziej złożone niż wykrywanie języka rasistowskiego i spamu, niektórzy badacze próbowali wykryć ją przy użyciu bardziej złożonej reprezentacji dokumentów i dodatkowych informacji o ofiarach i dręczycielach. Do wykrywania cyberprzemocy można zastosować techniki uczenia maszynowego.

Clickjacking

Zautomatyzowany system może analizować strony internetowe w celu ochrony użytkownika przed atakami typu clickjacking. Składa się on z kodu, który może wykryć nakładające się elementy klikalne. A oprócz tego rozwiązania przyjęli również narzędzie NoScript, które ma zawartą funkcję antyclickjackingową.

Cyberstalking

Techniki szyfrowania są dostępne dla urządzeń na ostatnich wersjach systemów Android i iOS. Jeśli urządzenie zostanie skradzione, złodziej nie może odczytać jego zawartości, jeśli szyfrowanie jest włączone. Ponadto wszelkie próby odczytania informacji z pamięci wewnętrznej lub zewnętrznej są udaremniane przez istnienie hasła do urządzenia. Istnieją różne technologie, które można wykorzystać przeciwko stalkerom, takie jak blokada odcisków palców smartfonów.

Wykrywanie spamu

Przed atakiem spamowym na Facebooku może pomóc framework o nazwie Spam Spotter. Jest on oparty na inteligentnym systemie wspomagania decyzji (IDSS). Zbiera wszystkie istotne informacje z profilu użytkownika za pomocą procesu decyzyjnego w IDSS, a następnie analizuje je, mapując dane użytkownika do klasyfikacji profilu użytkownika jako spamera lub legalnego.

Złośliwe oprogramowanie

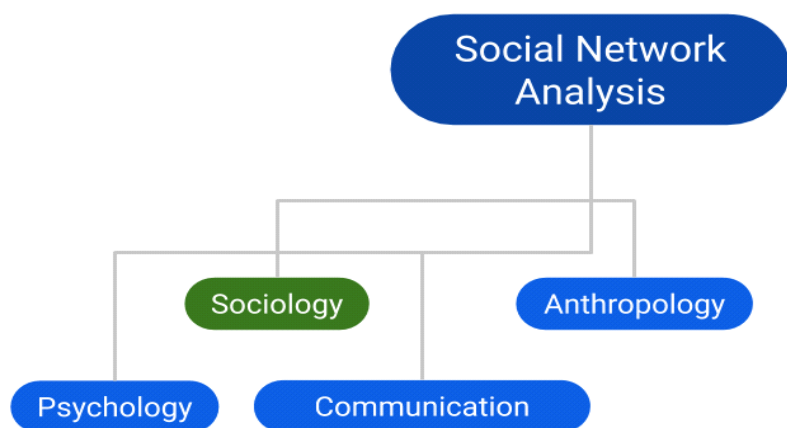
Cross Site Scripting Worms (XSS worms) to złośliwe programy, które rozprzestrzeniają się wśród odwiedzających stronę internetową, stopniowo infekując innych odwiedzających.

Robak rozprzestrzenia się wolniej, gdy użytkownicy odwiedzają głównie swoich znajomych, a nie obcych. Może być również spowolniony przez klastrowaną naturę sieci społecznych.

Chociaż środowiska akademickie opracowały takie innowacyjne rozwiązania w zakresie środków bezpieczeństwa związanych z bezpieczeństwem sieci społecznościowych, brakuje im implementacji w świecie rzeczywistym i wykonalności. Istnieje zatem pilna potrzeba ciągłego i iteracyjnego przeglądu kwestii bezpieczeństwa w sieciach społecznościowych z uwzględnieniem rozwoju technologii.

Interdyscyplinarność w sieciach społecznych

Interdyscyplinarne pole odnoszące się do sieci społecznych to analiza sieci społecznych (SNA) i obejmuje spostrzeżenia z innych dyscyplin nauk społecznych, takich jak socjologia, antropologia, psychologia, komunikacja i inne. SNA jest częścią jeszcze większej interdyscyplinarnej dziedziny zajmującej się badaniem wszystkich rodzajów sieci, zwanej nauką o sieci, która obejmuje prace z zakresu fizyki, informatyki, nauki o danych, biologii, inżynierii, matematyki i innych dziedzin. Związek między tymi dziedzinami pokazano na rysunku 8 (<https://bookdown.org/omarlizardo/main/1-2-what-is-a-social-network.html>).



Rysunek 8: Związki między polami w SNA (<https://bookdown.org/omarlizardo/main/1-2-what-is-a-social-network.html>)

Pytania:

Pytania na forum dyskusyjnym, na które należy odpowiedzieć z krótkim uzasadnieniem. Odpowiedzi zostaną omówione z mentorem podczas sesji mentorskich

1. Role w sieciach społecznych.
2. Serwisy społecznościowe.
3. Dziedziny interdyscyplinarne w powiązaniu z sieciami społecznymi

Załączniki:

1. Prezentacja
2. Materiały wideo

Referencje:

Aggarwal A., Rajadesingan A & Kumaraguru P. (2012). PhishAri: automatic realtime phishing detection on twitter. eCrime Res. Summit, eCrime. 1–12.

Ankit Kumar J., Somya Ranjan S. & Kaubiyal J. (2021). Data breach causes worldwide. URL: <https://www.statista.com/statistics/263303/proportion-of-the-most-common-causes-for-possible-identity-theft/>

Cutillo, A., Manulis, M. & Strute, T.(2010). Security and Privacy in Online Social Networks.
EUROCOM. TU Darmstadt.

Gupta B. & Sahoo, S. (2021). Online social networks security: principles, algorithm, applications, and perspectives. CRC Press.

Jain A. & Gupta B. (2018). Detection of phishing attacks in financial and e-banking websites using link and visual similarity relation. Int J Inf Comp Secur 10(4):398–417.

Jain, A., Sahoo, S.R. & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex Intell. Syst. 7, 2157–2177.

Kangur, K. (2022). The 15 Biggest Social Media Sites and Apps. URL:
<https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/>.

Mislove A., Viswanath B., Gummadi K. & Druschel, P. (2010). You are who you know. In:
Proceedings of the third ACM international conference on Web search and data mining—
WSDM '10, 251.

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

Sahoo SR, Gupta BB (2020). Fake profile detection in multimedia big data on online social networks.
Int J Inf Comput Secur 12(2–3), 303–331.