

InCyT-Trainingsmodule

Informationssicherheit für Mitarbeiter

Einheit Nr.: (4) Woche 8

Name der Einheit (des Moduls): (Soziale Netzwerke)

Lernaktivitäten	☐ Webinar ☐ Übungen ☐ Workshop ☐ Präsentation ☐ Sonstiges Streaming Webinar, Text, Übungen zur Selbsteinschätzung, Übungen mit Antworten in Diskussionsforen und in den organisierten Sitzungen mit dem Trainer/Mentor, E-Portfolios
Lehrverantwortliche	- David Sommer - Ileana Hamburg
Ziele der Lernaktivitäten	1. Rollen in sozialen Netzwerken 2. Funktionsweise von Plattformen zur sozialen Vernetzung 3. Sicherheit und Datenschutz in sozialen Netzwerken 4. Bedrohungen für soziale Online-Netzwerke und Lösungen, um sie zu vermeiden 5. Interdisziplinarität in sozialen Netzwerken
Zu erwerbende Fertigkeiten	• TS3 Netzsicherheit • TS4 Penetrationstests (ausnutzbare Sicherheitslücken) • TS5 Erkennung von Eindringlingen • SS3 Kognitions- und Verhaltensanalyse
Dauer der Lernaktivität	2 Wochen
Lernanforderungen	Was wird benötigt? • Zugang zum Internet • Internet-Browser • MS Office365

Kurze Informationen über das Modul

	Beschreibung
	Soziale Netzwerke helfen Menschen und Organisationen, mit Freunden in Kontakt zu treten, sind Kommunikationsmittel, helfen bei der Einführung einer neuen Geschäftsidee, beim Verkauf von Produkten oder Dienstleistungen und vergrößern die Reichweite der eigenen Marke. Natürlich gibt es auch Nachteile der sozialen Netzwerke, wie z. B. die Abnahme der persönlichen Kommunikationsfähigkeiten. Da Unternehmen soziale Medien intensiv nutzen, nutzen Angreifer das Vertrauen und den öffentlichen Charakter dieser Plattformen für Angriffe. Die Sicherheit in sozialen Netzwerken ist wichtig für den geschäftlichen und privaten Erfolg, so dass die Schulung von Mitarbeitern wie in diesem Modul einen großen Beitrag leisten kann. Die Mitarbeiter lernen über diese Aspekte, indem sie die entsprechenden Texte lesen, Webinare per Streaming ansehen, Übungen im eigenen Tempo lösen und das Gelernte reflektieren (E-Portfolios). Alle Modulunterlagen befinden sich auf der digitalen interaktiven Projektplattform. Die Lernenden können ihre Antworten in den Selbsteinschätzungsübungen testen. Die Antworten auf die anderen Übungen sollten in den entsprechenden Diskussionsforen gespeichert und mit dem Mentor bei dem wöchentlich stattfindenden gemeinsamen Treffen besprochen werden. Die Lernenden können vor allem während der wöchentlichen Treffen mit anderen und dem Mentor kooperativ zusammenarbeiten.

Inhalt des Lernmaterials

Einführung

Auch aufgrund der zunehmenden technologischen Entwicklung sind (Online-)soziale Netzwerke in den letzten Jahren sehr beliebt geworden. Ein Grund dafür ist ihre Fähigkeit, den Nutzern eine Plattform für die Kommunikation mit ihrer Familie, ihren Freunden und Kollegen zu bieten.

Social Networking bezieht sich auf die Nutzung von internetbasierten Social-Media-Sites für die Verbindung und Kommunikation mit Freunden, Familie, Kollegen, Kunden oder Klienten.

Soziale Medien helfen den Menschen, bessere Beziehungen zu Familie, Freunden und Kunden zu pflegen, und mobile Geräte, die soziale Medien unterstützen, gewinnen im Vergleich zu anderen Möglichkeiten des Internetzugangs immer mehr an Interesse.

Die Server der sozialen Netze befinden sich in Datenzentren, die nach Möglichkeit mit den großen Internet-Zugangspunkten (NAP) zusammengelegt sind, über die die großen Internet-Diensteanbieter miteinander verbunden sind und über die sie den direkten Zugang zu den schnellen Internet-Verbindungen herstellen.

Rollen in sozialen Netzwerken

Soziale Netzwerke können eine soziale oder eine geschäftliche Rolle spielen oder beides, wenn man Websites wie Facebook, Twitter, LinkedIn und Instagram nutzt. Abbildung 1 zeigt einige Bereiche, in denen soziale Netzwerke eine Rolle spielen (Milsova et al.): Unterhaltung, Aufbau von Geschäftsmöglichkeiten, Karriere, Verbesserung der sozialen Fähigkeiten und Entwicklung von Beziehungen zu anderen Personen.

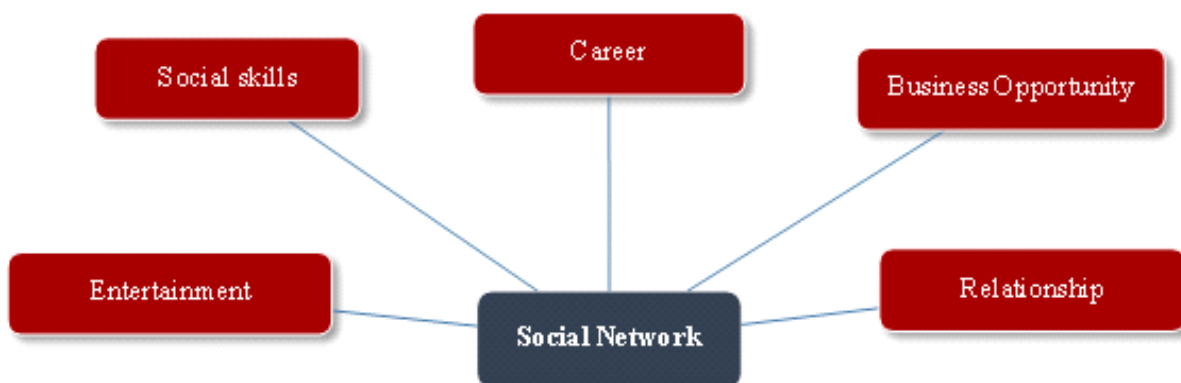


Abbildung 1: Rollen in sozialen Netzwerken

Soziale Netzwerke sind eine Basis für Vermarkter, die Kunden suchen. Vermarkter nutzen soziale Netzwerke, um die Markenbekanntheit zu erhöhen und die Markentreue zu fördern. Soziale Medien können dazu beitragen, Menschen und Unternehmen miteinander zu verbinden und das Markenbewusstsein zu fördern. Ein häufiger Twitter-Nutzer erfährt z. B. zum ersten Mal über einen News-Feed von einem Unternehmen und entscheidet sich für den Kauf eines Produkts oder einer Dienstleistung. Die Chancen des Unternehmens, neue Kunden zu finden und zu binden, steigen durch soziale Netzwerke. Vermarkter nutzen soziale Netzwerke, um die Konversionsraten zu verbessern, und bieten Zugang zu und Interaktion mit neuen, aktuellen und alten Kunden. Durch das Teilen von Blogbeiträgen, Bildern, Videos

oder Kommentaren in sozialen Medien werden mehr Menschen die Website des Unternehmens besuchen und zu Kunden werden. Es gibt jedoch nicht nur einen Ansatz für Marketingstrategien: Jedes Unternehmen ist einzigartig und hat eine andere demografische Zielgruppe, eine andere Geschichte und einen anderen Wettbewerbsmarkt. Da Unternehmen in sozialen Netzwerken für ihre Werbung bezahlen wollen, beschränken sie oft die Anzahl der Reichweite, die Unternehmen durch unbezahlte Beiträge erhalten. Wenn ein Unternehmen beispielsweise 500 Follower hat, können nicht alle Follower denselben Beitrag erhalten. Die sich ständig weiterentwickelnde Natur der sozialen Netzwerke macht es schwierig, mit den Veränderungen Schritt zu halten, und beeinflusst auch den Marketingerfolg eines Unternehmens.

Facebook, Instagram, Facebook Messenger und Twitter sind die beliebtesten sozialen Netzwerke in den Vereinigten Staaten und auch in Europa. Zu den anderen gehören Pinterest, Tumblr, Snapchat, TikTok und YouTube, WhatsApp, Messenger von Google und Tumblr. LinkedIn ist eine weitere beliebte Website, die Fachleute mit Kollegen, Geschäftskontakten und Arbeitgebern zusammenbringt. Facebook ist nach wie vor das größte und beliebteste soziale Netzwerk mit 2,91 Milliarden Menschen, die die Plattform monatlich nutzen (Stand: 31. Dezember 2021). Abbildung 2 zeigt die Anzahl der Nutzer auf den Plattformen.

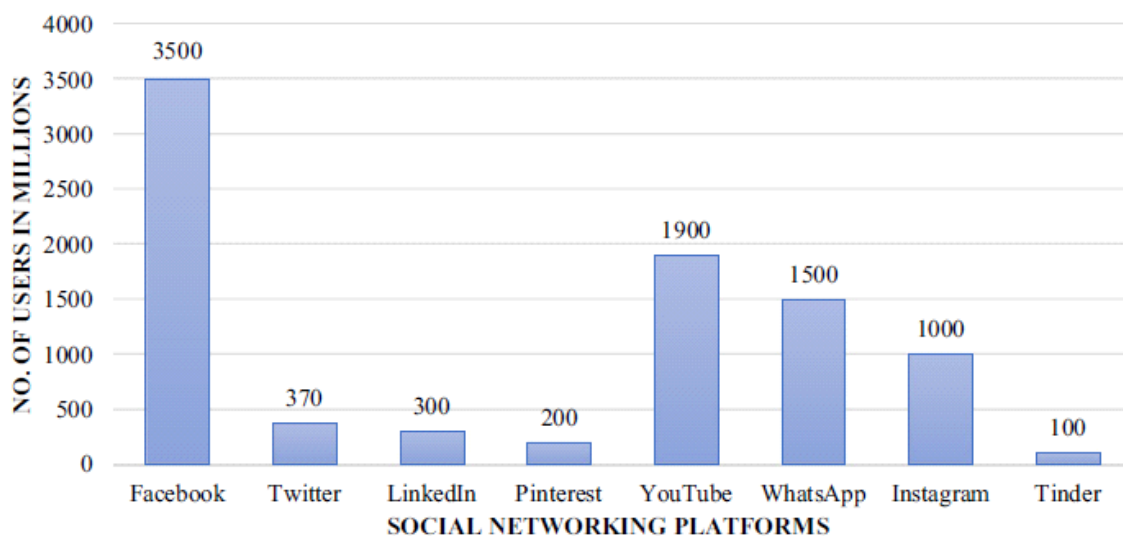


Abbildung 2: Anzahl der Nutzer auf Plattformen (<https://www.dreamgrow.com/top>)

Funktionalität von sozialen Netzwerken

Soziale Netzwerke basieren auf dem Aufbau und der Pflege persönlicher und geschäftlicher Beziehungen unter Einsatz von Technologie durch die Nutzung von Websites für soziale Netzwerke. Diese Websites ermöglichen es Menschen und Unternehmen, miteinander in Verbindung zu treten, um Beziehungen zu entwickeln und Informationen, Ideen und Nachrichten auszutauschen.

Familienmitglieder, die weit weg sind, können über persönliche Social-Networking-Websites wie Facebook in Verbindung bleiben, Fotos austauschen und andere Nachrichten aus ihrem Leben schicken. Menschen können auch mit anderen (Fremden) in Verbindung treten, die dieselben Interessen teilen. Einzelpersonen

können einander durch die Mitgliedschaft in Gruppen, in Listen und durch die Verwendung von Hashtags finden.

Aber es gibt auch Nachteile im Zusammenhang mit sozialen Medien, darunter die Verbreitung von Fehlinformationen und die hohen Kosten für die Nutzung und Pflege von Profilen in sozialen Netzwerken.

Jedes soziale Netzwerk dient in der Regel einem bestimmten Zweck, aber die Funktionalität dieser Plattformen ist ähnlich und kann in drei Haupttypen unterteilt werden:

- Die Vernetzungsfunktionen dienen dazu, die sozialen Beziehungen zwischen den Nutzern innerhalb der virtuellen Plattformen zu fördern. Sie bieten insbesondere Funktionen zum Aufbau und zur Pflege des sozialen Netzwerkgraphen.
- Die Datenfunktionen sind für die Verwaltung der von den Nutzern bereitgestellten Inhalte und die Kommunikation zwischen den Nutzern zuständig. Die Vielfalt trägt zur Verbesserung (Erweiterung) der Interaktion der Nutzer bei und macht die Plattform attraktiver.
- Die Zugriffskontrollfunktionen zielen darauf ab, die vom Benutzer definierten Datenschutzmaßnahmen umzusetzen und den unbefugten Zugriff auf die vom Benutzer bereitgestellten Daten und Informationen zu beschränken. Abbildung 3 zeigt die von einer typischen virtuellen sozialen Netzwerkplattform bereitgestellten Funktionen und enthält weitere Details (Cutillo et al. 2010).

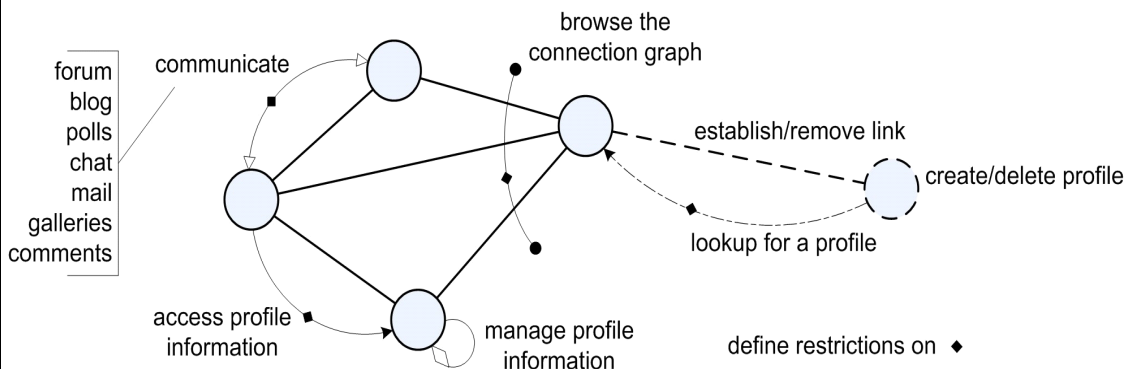


Abbildung 3: Hauptfunktionen einer typischen Social-Networking-Plattform (<https://hal.archives-ouvertes.fr/hal-00687145>)

Social-Networking-Sites lassen sich in "soziale Verbindungen", "Multimedia-Sharing", "professionelle" und "Diskussionsforen" einteilen (Abbildung 4 Jain et al., 2021)

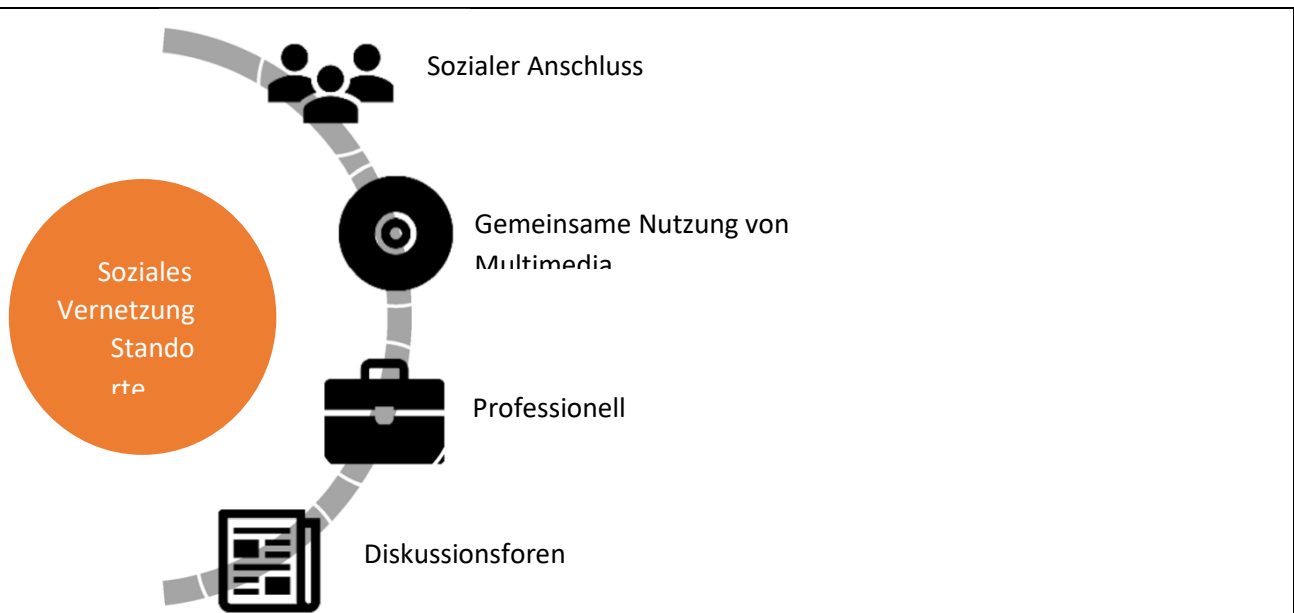


Abbildung 4: Websites zur sozialen Vernetzung (Jain et al., 2021)

Vorteile und Nachteile von Social Networking

Soziale Netzwerke können sich sowohl auf Einzelpersonen als auch auf Unternehmen auswirken - sowohl positiv als auch negativ. Daher ist es wichtig, die Vor- und Nachteile der Nutzung solcher Social-Media-Sites zu berücksichtigen.

Vorteile

Soziale Netzwerke ermöglichen es dem Einzelnen, mit Familie und Freunden in Kontakt zu bleiben, was sonst aufgrund der Entfernung oder des Verlusts des Kontakts nicht möglich wäre. Die Menschen können auch mit anderen Personen in Kontakt treten, die die gleichen Interessen haben, und neue Beziehungen aufbauen.

Soziale Netzwerke ermöglichen es Unternehmen, mit neuen und bestehenden Kunden in Kontakt zu treten. Unternehmen können soziale Medien auch nutzen, um ihre Marke bekannt zu machen, zu fördern und zu stärken. Sie verlassen sich auch auf die Bewertungen und Kommentare ihrer Kunden, die für die Marke wichtig sind. Sie können den Umsatz steigern und eine höhere Platzierung in Suchmaschinen erreichen.

Soziale Netzwerke können dazu beitragen, eine neue Marke zu etablieren. Ein Unternehmen kann soziale Netzwerke nutzen, um sein hohes Serviceniveau zu demonstrieren und Produkte und Beziehungen zu den Verbrauchern zu verbessern. Wenn sich zum Beispiel ein Kunde auf Twitter über ein Produkt oder eine Dienstleistung beschwert, entschuldigt sich das Unternehmen und ergreift Maßnahmen zur Verbesserung der Situation.

Benachteiligungen

Soziale Netzwerke können zur Verbreitung von Fehlinformationen beitragen Sahoo und Gupta (2020) fanden heraus, dass Fehlinformationen auf Twitter mit 70 % höherer Wahrscheinlichkeit geteilt werden als richtige Informationen.

Die Vernetzung in sozialen Medien kann sich nachteilig auf Unternehmen auswirken. Kritik an einer Marke verbreitet sich in den sozialen Medien sehr schnell. Das hat Nachteile für die Öffentlichkeitsarbeit (PR) eines Unternehmens.

Soziale Netzwerke an sich sind kostenlos, aber der Aufbau und die Pflege eines Unternehmensprofils erfordern jede Woche viele Stunden Arbeit und verursachen Kosten. Unternehmen brauchen viele Follower, bevor eine Social-Media-Marketingkampagne eine positive Kapitalrendite (ROI) erzielt. Wenn beispielsweise ein Beitrag an 15 Follower gesendet wird, hat dies nicht dieselbe Wirkung wie ein Beitrag an 15.000 Follower.

Sicherheit und Datenschutz in sozialen Netzwerken

Die in sozialen Netzwerken und Medien geteilten Informationen verbreiten sich sehr schnell, was es für Angreifer attraktiv macht, sie zu erlangen. Wenn ein Benutzer persönliche Inhalte wie Fotos, Videos und Audiodateien hochlädt, gibt es Sicherheits- und Datenschutzprobleme im Zusammenhang mit den freigegebenen Informationen. Der Angreifer kann die freigegebenen Informationen böswillig für unrechtmäßige Zwecke verwenden.

Einige verschiedene Bedrohungen der Sicherheit und des Datenschutzes sowie bestehende Lösungen, die den Nutzern sozialer Netzwerke Sicherheit bieten können, werden kurz vorgestellt.

Durch die intensive Nutzung der Technologie haben sich die Interaktionen über das Internet ausgeweitet. Leider hat das mangelnde Bewusstsein der Nutzer in Bezug auf Sicherheit und Datenschutz das Potenzial, zu verschiedenen Cyberangriffen über soziale Medien zu führen. Die Bedrohungen, die die Nutzer seit den Anfängen sozialer Netzwerke wahrgenommen haben, können in drei Kategorien unterteilt werden: konventionelle Bedrohungen, moderne Bedrohungen und gezielte Bedrohungen (Abb. 5, Jain und Gupta, 2018). Zu den konventionellen Bedrohungen gehören die Bedrohungen, denen die Nutzer seit Beginn des sozialen Netzwerks ausgesetzt sind. Moderne Bedrohungen sind Angriffe, die fortgeschrittene Techniken verwenden, um Konten von Nutzern zu kompromittieren, und gezielte Angriffe sind Angriffe, die auf einen bestimmten Nutzer abzielen und von jedem Nutzer aus verschiedenen persönlichen Gründen begangen werden können.

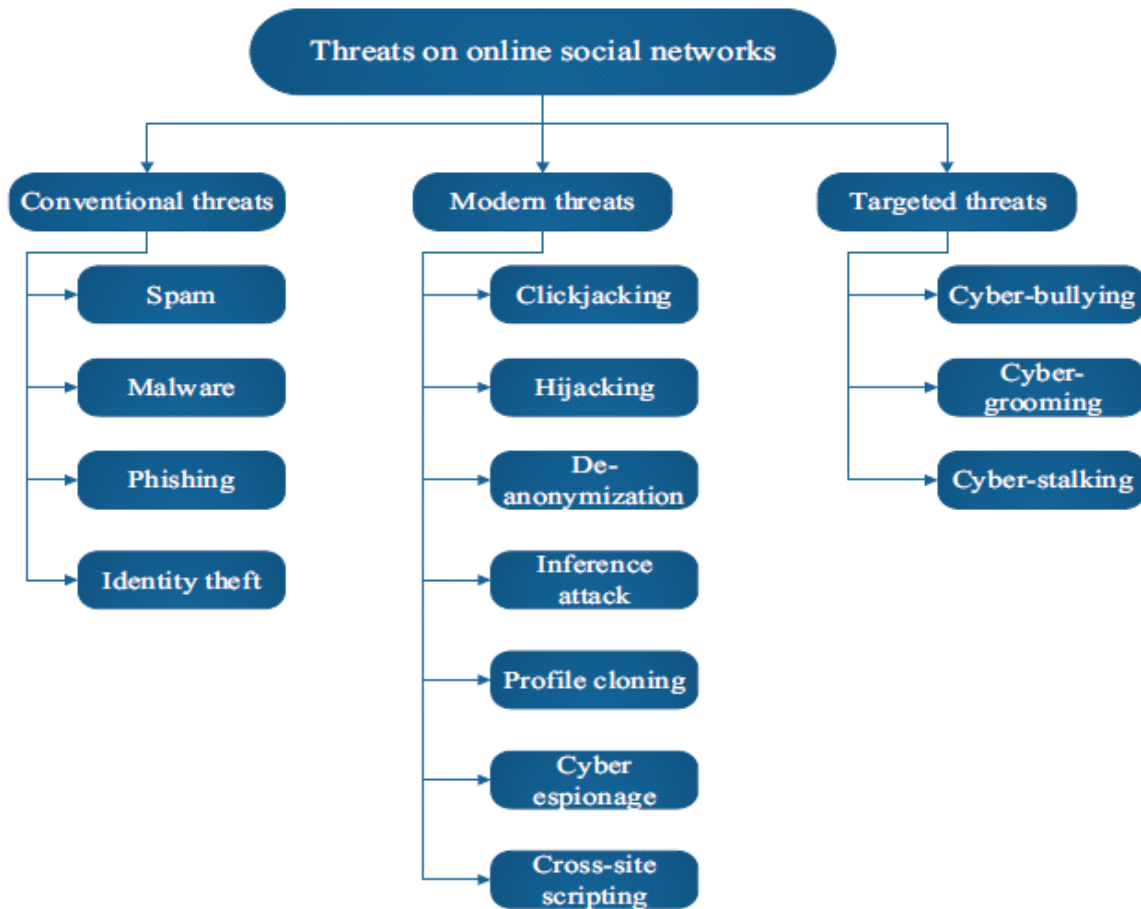


Abbildung 5: Klassifizierung von Bedrohungen (Jain et al, 2018)

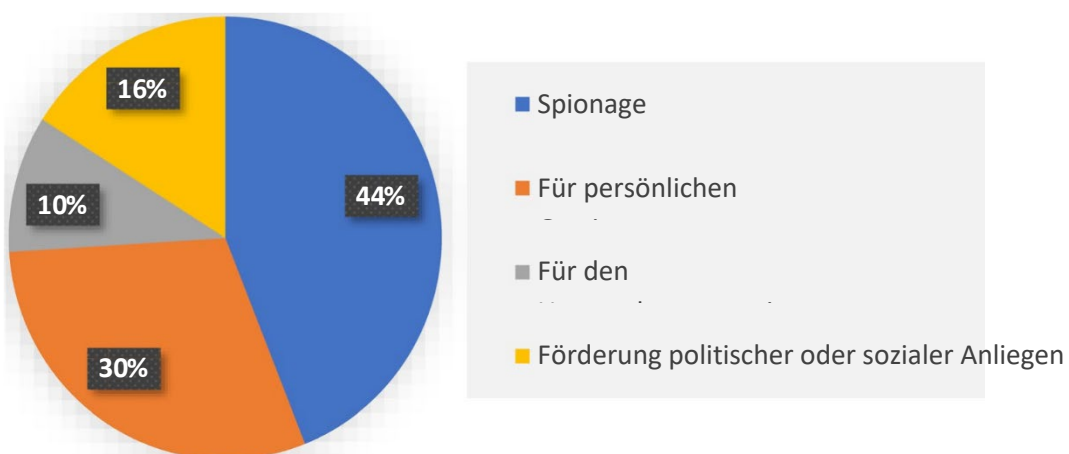


Abbildung 6: Die meisten Arten von Hackerangriffen im Jahr 2021 (Jain et al., 2021)

Lösungen für Bedrohungen

Forscher in Wissenschaft und Industrie versuchen, Lösungen für die Bedrohungen in sozialen Netzwerken für verschiedene Arten von Hacking zu finden, wie in Abbildung 6 dargestellt. Es wurden Lösungen und einige

Ansätze vorgeschlagen, die in zwei Gruppen eingeteilt werden können: Lösungen für Betreiber sozialer Netzwerke und akademische Lösungen (Jain et al., 2021). Abbildung 7 zeigt die Klassifizierung. Im Folgenden wird eine kurze Beschreibung gegeben.

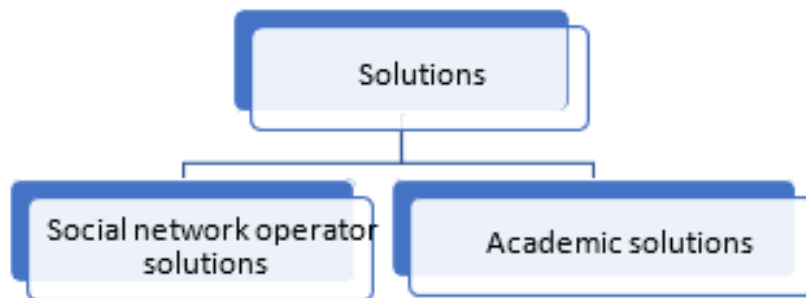


Abbildung 7: Klassifizierung von Lösungen für Bedrohungen (Jain et al, 2021)

Lösungen für Betreiber sozialer Netzwerke

Authentifizierungsmechanismus

Um sicherzustellen, dass sich nur ein legitimer Benutzer in einem sozialen Netzwerk anmeldet oder registriert und nicht ein sozialer Bot, wurden Authentifizierungsverfahren wie CAPTCHA, Multi-Faktor-Authentifizierung und die Identifizierung durch Fotos von Freunden vorgeschlagen. Soziale Netzwerke wie Twitter und Facebook verwenden beispielsweise das Prinzip der Zwei-Faktoren-Authentifizierung. Dieses Prinzip verwendet ein Anmeldepaswort und einen Verifizierungscode, der über ein mobiles Gerät empfangen wird. Dies trägt dazu bei, das Risiko der Kompromittierung eines Kontos zu verringern, und verhindert, dass ein Angreifer ein legitimes Konto entführt und bösartige Inhalte veröffentlicht.

Einstellungen für Sicherheit und Datenschutz

Viele Social-Networking-Websites bieten konfigurierbare Sicherheits- und Datenschutzeinstellungen, die es dem Kunden ermöglichen, persönliche Informationen vor unerwünschtem Zugriff durch Außenstehende oder Anwendungen zu schützen. Der Facebook-Kunde kann zum Beispiel seine Sicherheitseinstellungen ändern und die Zielgruppe (wie Freunde, Freunde von Freunden und alle) im Netzwerk auswählen, die seine Details, Bilder, Beiträge und andere sensible Informationen sehen können.

Benutzer melden

Soziale Netzwerke schützen Menschen vor Angriffen, indem sie die Möglichkeit bieten, jede Form von Missbrauch oder Verstößen gegen die Richtlinien durch einen Nutzer in ihrem Netzwerk zu melden. Wenn ein Nutzer beispielsweise etwas auf Facebook sieht, das seinen Gefühlen entspricht, aber nicht gegen die Facebook-Bedingungen verstößt, kann er demjenigen, der es gepostet hat, über einen Bericht (Links) eine Nachricht schicken und ihn auffordern, es zu löschen oder zu entfernen. Wenn Facebook eine Nutzermeldung erhält, wird sie geprüft und gemäß den Gemeinschaftsstandards von Facebook entfernt.

Akademische, forschungsbasierte Lösungen

Phishing-Erkennung

Phishing beunruhigt die Privatsphäre und die Sicherheit vieler traditioneller Webanwendungen wie Websites, Social-Networking-Sites, E-Mails und Blogs. Daher wurden mehrere Anti-Phishing-Techniken entwickelt, um Phishing-Angriffe zu erkennen. Aggarwal et al. schlugen beispielsweise die PhishAri-Technik zur Echtzeit-Erkennung von Phishing-Angriffen auf Twitter vor. Es nutzt spezifische Twitter-Merkmale wie das Alter des Kontos und die Anzahl der Follower, um zu erkennen, ob es sich bei dem geposteten Tweet um einen Phishing-Angriff handelt oder nicht.

Erkennung von Cybermobbing

Cybermobbing ist die Nutzung elektronischer Medien wie E-Mails, Chats, Telefongespräche und soziale Online-Netzwerke zur Unterdrückung einer Person. Im Gegensatz zum traditionellen Mobbing ist Cybermobbing ein kontinuierlicher Prozess, der über soziale Medien aufrechterhalten wird. Obwohl die Erkennung von Cybermobbing komplexer ist als die Erkennung von rassistischer Sprache und Spam, haben einige Forscher versucht, Cybermobbing mit Hilfe einer komplexeren Dokumentendarstellung und zusätzlichen Informationen über Opfer und Mobber zu erkennen. Techniken des maschinellen Lernens können zur Erkennung von Cybermobbing eingesetzt werden.

Clickjacking

Ein automatisiertes System kann Webseiten analysieren, um den Benutzer vor Clickjacking-Angriffen zu schützen. Es besteht aus einem Code, der überlappende anklickbare Elemente erkennen kann. Zusätzlich zu dieser Lösung haben sie auch das NoScript-Tool übernommen, das eine Anti-Clickjacking-Funktion enthält.

Cyberstalking

Verschlüsselungstechniken sind für Geräte mit neueren Versionen von Android und iOS verfügbar. Wenn ein Gerät gestohlen wird, kann der Dieb den Inhalt nicht lesen, wenn die Verschlüsselung aktiviert ist. Außerdem wird jeder Versuch, die Informationen aus dem internen oder externen Speicher zu lesen, durch das Vorhandensein eines Gerätepassworts vereitelt. Es gibt verschiedene Technologien, die gegen Stalker eingesetzt werden können, z. B. die Fingerabdrucksperrung für Smartphones.

Spam-Erkennung

Ein Rahmenwerk namens Spam Spotter kann gegen einen Spam-Angriff auf Facebook helfen. Es basiert auf dem intelligenten Entscheidungsunterstützungssystem (IDSS). Es sammelt alle relevanten Informationen aus dem Benutzerprofil mit Hilfe eines Entscheidungsprozesses in IDSS und analysiert sie dann, indem es die Benutzerdaten der Klassifizierung eines Benutzerprofils als Spammer oder legitim zuordnet.

Malware

Cross-Site-Scripting-Würmer (XSS-Würmer) sind bösartige Programme, die sich über Besucher einer Website verbreiten und nach und nach andere Besucher infizieren.

Der Wurm verbreitet sich langsamer, wenn die Mitglieder hauptsächlich ihre Freunde besuchen und nicht Fremde. Er kann auch durch die Clusterbildung in sozialen Netzwerken verlangsamt werden.

Obwohl die Wissenschaft solche innovativen Lösungen für die Sicherheitsmaßnahmen im Zusammenhang mit der Sicherheit sozialer Netzwerke entwickelt hat, fehlt es ihnen an der praktischen Umsetzung und Durchführbarkeit. Daher besteht die dringende Notwendigkeit, Sicherheitsfragen in sozialen Netzwerken unter Berücksichtigung der technologischen Entwicklungen kontinuierlich und iterativ zu überprüfen.

Interdisziplinarität in sozialen Netzwerken

Der interdisziplinäre Bereich, der sich mit sozialen Netzwerken befasst, ist die soziale Netzwerkanalyse (SNA) und umfasst Erkenntnisse aus anderen sozialwissenschaftlichen Disziplinen wie Soziologie, Anthropologie, Psychologie, Kommunikation und anderen. Die SNA ist Teil eines noch größeren interdisziplinären Bereichs, der sich mit der Untersuchung aller Arten von Netzwerken befasst, der so genannten Netzwerkwissenschaft, die Arbeiten aus der Physik, der Informatik, der Datenwissenschaft, der Biologie, dem Ingenieurwesen, der Mathematik und anderen Bereichen umfasst. Die Beziehung zwischen diesen Bereichen ist in Abbildung 8 dargestellt (https://bookdown.org/omarlizardo/_main/1-2-what-is-a-social-network.html).

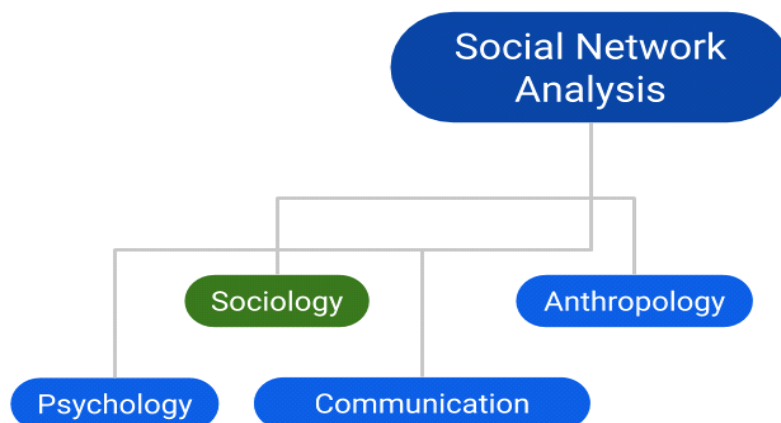


Abbildung 8: Beziehungen zwischen Feldern im SNA (https://bookdown.org/omarlizardo/_main/1-2-what-is-a-social-network.html)

Fragen:

Fragen Diskussionsforum, die mit einer kurzen Erklärung beantwortet werden müssen. Die Antworten werden mit dem Mentor während der Mentoring-Sitzungen besprochen

1. Rolle der sozialen Netzwerke
2. Websites zur sozialen Vernetzung
3. Interdisziplinäre Bereiche in Verbindung mit sozialen Netzwerken

Anhänge:

1. Präsentation
2. Video-Filme

Referenzen:

Referenzen

- 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). Ursachen für Datenschutzverletzungen weltweit. URL: <https://www.statista.com/statistics/263303/proportion-of-the-most-common-causes-for-possible-identity-theft/>.
- Cutillo, A., Manulis, M. & Strute, T. (2010). Sicherheit und Datenschutz in sozialen Online-Netzwerken. EUROCOM. TU Darmstadt.
- Gupta B. & Sahoo, S. (2021). Sicherheit sozialer Online-Netzwerke: Prinzipien, Algorithmen, Anwendungen und Perspektiven. 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). Sicherheit und Datenschutz in sozialen Online-Netzwerken: Umfassender Überblick und Analyse. Complex Intell. Syst. 7, 2157-2177.
- Kangur, K. (2022). Die 15 größten Social Media Sites und Apps. URL: <https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/>.
- Mislove A., Viswanath B., Gummadi K. & Druschel, P. (2010). Du bist, wen du kennst. 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). Erkennung gefälschter Profile in multimedialen Big Data in sozialen Online-Netzwerken. Int J Inf Comput Secur 12(2-3), 303-331.



Co-funded by the
Erasmus+ Programme
of the European Union