Gefahren in sozialen Netzwerken

In diesem Modul werden die Gefahren in sozialen Netzwerken erklärt, welche Konsequenzen diese haben können und wie Sie sich dagegen schützen können.

Aufbau dieses Moduls

Dieses Modul ist in drei aufeinanderfolgende Teile gegliedert. Es wird erklärt, welche Gefahren in sozialen Netzwerken existieren, welche Konsequenzen diese haben können und Empfehlungen gegeben, wie Sie sich schützen können. Im dritten Teil werden außerdem Tools und Methoden vorgestellt, mithilfe derer diese Gefahren weiter reduziert werden können. Die Gefahren sind wie folgt aufgeteilt:

1. Wie soziale Netzwerke Ihre Daten sammeln können

2. Wie soziale Netzwerke Ihre Meinung beeinflussen können

3. Wie soziale Netzwerke Ihnen finanziellen, sozialen oder einen Image-Schaden zufügen können

Erklärungen

In den einzelnen Teilen werden jeweils die Gefahren detailliert vorgestellt und dann erklärt, was Sie gegebenenfalls verändern können, um das Risiko zu minimieren. Zu manchen Gefahren erhalten Sie weitere Hinweise, welche über die einfache Erklärung hinausgehen. Damit Sie immer den Überblick behalten, sind die drei Arten von Information jeweils durch entsprechende Symbole gekennzeichnet:

Beschreibung der Gefahr

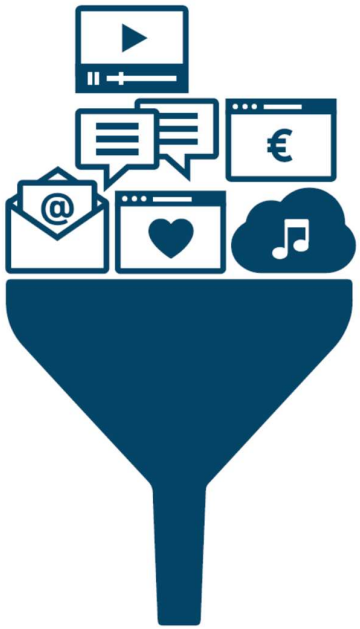
Empfehlungen zur Risikominderung

Weitere Hinweise

Teil 1:
Wie soziale Netzwerke Ihre Daten sammeln können

Wer sammelt Daten und warum?

Daten können von jedem gesammelt werden, der damit direkt, indirekt, zum aktuellen oder zu einem späteren Zeitpunkt profitieren kann:



- Der Betreiber des sozialen Netzwerks sammelt Daten und kann diese nutzen, um daraus Profit zu schlagen. Zum Beispiel könnten Sie Werbung für Reisen erhalten, die auf Ihr Reiseverhalten angepasst ist. Damit werden Reisebuchungen wahrscheinlicher und Provisionen für den Betreiber des sozialen Netzwerks höher.
- Eine neugierige Person, die Ihr Profil aufrufen kann, könnte Daten gezielt sammeln, um Sie auszuspionieren.
- Kriminelle könnten Ihr Profil gezielt beobachten und Ihre Daten in anderen Bereichen (z.B. für Vertragsabschlüsse) nutzen.
- Kontakte in sozialen Netzwerken könnten Daten sammeln und in anderen Kontexten nutzen (z.B. private Informationen an andere Personen weitergeben)

Konsequenzen von Datensammlung

Das Sammeln von Daten hat erst einmal keine direkten Konsequenzen. Jedoch das Nutzen dieser Daten kann verschiedene Konsequenzen haben, die aber zum Zeitpunkt des Sammelns meist noch nicht sichtbar oder absehbar sind. Einige Beispiele sind:

- Es können Vorhersagen bezüglich Ihres Kaufverhaltens getroffen werden und so gezielt Angebote und deren Preise individualisiert werden.
- Daten könnten dazu genutzt werden, um Ihre Versicherungsprämien nach der Risikostufe aus der Vergangenheit zu berechnen.
- Ihre politische Ausrichtung könnte abgeleitet werden, wodurch Ihnen Nachteile entstehen können, z.B. bei der Jobsuche.
- Die gesammelten Daten können Aufschluss über Ihre Verhaltensweisen geben, auf Basis derer Ihre Kreditwürdigkeit bewertet und ein Kredit verweigert werden kann.
- Das Wissen über geplante Abwesenheiten kann genutzt werden, um einen Einbruch zu planen.

Wie werden Daten gesammelt?

Daten können auf verschiedenste Arten in sozialen Netzwerken gesammelt werden. Dabei ist zwischen gewollter und nicht gewollter Datenpreisgabe durch den Benutzer zu unterscheiden.

Gewollte Datenpreisgabe geschieht immer dann, wenn der Benutzer die Daten mit der Intention hochlädt, dass diese Daten geteilt oder gesehen werden können. Zum Beispiel wäre dies der Fall, wenn Sie Bilder in ein soziales Netzwerk hochladen, so dass Ihre Kontakte diese ansehen können.
Mögliche Varianten, die das Sammeln von Daten bei gewollter Datenpreisgabe ermöglichen, sind

- die Angabe von Registrierungsdaten zur Anmeldung im sozialen Netzwerk,
- die freiwillige Datenpreisgabe über die Veröffentlichung von Nachrichten in sozialen Netzwerken,
- die freiwillige Bereitstellung von Bildern und Videos im sozialen Netzwerk.

Wie werden Daten gesammelt? *Fortsetzung*

Ungewollte Datenpreisgabe geschieht immer dann, wenn Daten preisgegeben werden, die nicht mit der eigentlichen Intention (z.B. Bilder für Freunde ins soziale Netzwerk laden) zusammenhängen. Ein Beispiel hierfür ist die Freigabe des Standorts anhand von GPS-Koordination, die in Bildern gespeichert wurden.

Mögliche Varianten, wie ungewollt Daten entstehen und gesammelt werden können, sind

- Preisgabe von Daten ohne Registrierung im sozialen Netzwerk,
- Preisgabe von Kontextinformationen mit dem Hochladen von Bildern und Videos,
- Preisgabe von Daten aufgrund Ihrer Kontakte,
- Preisgabe von Daten mit Bestätigung von vermeintlichen Kontaktanfragen,
- Preisgabe von Daten aufgrund gefährlicher Links in sozialen Netzwerken,
- Preisgabe von Daten aufgrund automatisierter oder gezielter Abfragen.

Bei vielen, aber nicht allen, Fällen von gewollter oder ungewollter Datenpreisgabe ist die Registrierung im sozialen Netzwerk notwendig.

Warum dürfen die Daten gesammelt werden?

Bei den meisten sozialen Netzwerken haben Sie mit der Registrierung im sozialen Netzwerk die Zustimmung gegeben, Ihre Daten, Bilder oder Videos vom Betreiber weiterverarbeiten zu lassen, gemäß Ihren Einstellungen anderen Nutzern zur Verfügung zu stellen und auch an Dritte weiterzugeben und durch diese verarbeiten zu lassen.

Es sind nicht nur die direkt eingegebenen Daten, Bilder oder Videos betroffen, sondern auch sogenannte Sekundär- oder Metadaten, wie zum Beispiel Ihr derzeitiger Aufenthaltsort, Ihre Nutzungsgewohnheiten (zu welcher Zeit Sie das Netzwerk nutzen, was Sie dann tun) und weitere technische Metadaten, wie z.B. Ihre IP-Adresse und das genutzte Gerät.

Alle diese Daten können zum Beispiel für Werbedienstleister wertvoll sein, um Profile zu erstellen, um so personalisierte Werbung ausliefern zu können. Eine weitere (aber derzeit seltene Form) ist, dass man Nutzerdaten verwendet, um Ihnen persönliche Empfehlungen auszusprechen. Beispielsweise könnte ein guter Kontakt Ihnen (automatisiert) ein Produkt vorschlagen, was die Wahrscheinlichkeit, dass Sie das Produkt auch gut finden, erhöht.

Beschreibung
„(Gewollte) freiwillige Preisgabe Ihrer Daten“

Soziale Netzwerke, wie zum Beispiel Facebook, Google+ oder auch XING und LinkedIn, verdienen Geld mit den Daten, Bildern und Videos, die Sie als Benutzer zur Verfügung stellen bzw. eingeben.

Es gibt verschiedene Arten von Daten, die Sie freiwillig und gewollt preisgeben:

- Sie geben dem Betreiber des sozialen Netzwerks bei der Registrierung Ihre E-Mail-Adresse, Ihren Geburtstag und Ihren Namen frei. Wie diese Daten anderen Nutzern zur Verfügung gestellt werden, wird meist über die Einstellungen im sozialen Netzwerk bestimmt.
- Sie posten Nachrichten in sozialen Netzwerken mit verschiedenen Informationen (z.B. dass Sie heute zum Sport gehen wollen), die dem Betreiber immer zugänglich sind und anderen Nutzern gemäß den Einstellungen zur Verfügung gestellt werden.
- Sie laden Bilder oder Videos in soziale Netzwerke, um Ihren Kontakten diese zu präsentieren. Der Betreiber des sozialen Netzwerks hat immer Zugang zu diesen Bildern. Andere Nutzer bekommen diese gemäß Ihren Einstellungen präsentiert.

Beschreibung
„(Gewollte) freiwillige Preisgabe Ihrer Daten“ *Fortsetzung*

In den Einstellungen des sozialen Netzwerks oder auch unmittelbar beim Einstellen der Daten können Sie in der Regel diese Einstellungen zur Verbreitung anpassen.

Die Datensammlung durch den Betreiber ist immer gegeben. Dieser hat Zugriff auf alle Daten und kann diese zur späteren Verarbeitung speichern.

Mit Ihnen verbundene Kontakte können auf Ihre eingegeben Daten gemäß Ihrer Einstellungen zugreifen, diese sammeln und nutzen.

Beschreibung
„(Ungewollte) Preisgabe von Daten ohne Registrierung“

Viele soziale Netzwerke bieten Möglichkeiten für Webseitenbetreiber, Funktionen aus sozialen Netzwerken zu integrieren. Das beste Beispiel ist der Like-Button aus Facebook oder +1 aus Google Plus.

Diese Funktionalität kann Daten über Sie sammeln, ohne dass Sie im jeweiligen Netzwerk angemeldet sind. Diese Daten bestehen in der Regel aus sogenannten Meta-Daten, die Sie zwar nicht als Person identifizieren können. Aber Sie können zum Beispiel als der gleiche Besucher identifiziert werden. Durch eine solche Möglichkeit kann beispielsweise gezählt werden, wie häufig Sie eine bestimmte Seite besucht haben. Dies führt dazu, dass das soziale Netzwerk erfährt, wie häufig Sie andere Webseiten besucht haben.

Durch die Einbindung und die Nutzung dieser Meta-Daten ist es dem sozialen Netzwerk später möglich, diese Daten mit Ihrem Profil zu verbinden.

Wenn Sie in einem sozialen Netzwerk angemeldet sind, werden diese Besuchsdaten direkt Ihrem Profil zugeordnet.

Beschreibung „(Ungewollte) Preisgabe von Kontextinformationen mit dem Hochladen von Bildern und Videos.“

Bilder und Videos, die Sie in soziale Netzwerke hochladen, können nicht nur von Nutzern angesehen, sondern auch von Computern analysiert werden und es können verschiedene Informationen entnommen werden.

Die Verfahren und Algorithmen sind mittlerweile so leistungsfähig, dass sie aufgrund der Umgebung den Standort aus Bildern erkennen können. Manchmal werden Bilder zusätzlich mit Ihren Aufenthaltskoordinaten (GPS) versehen, dann sind die Daten eindeutig im sozialen Netzwerk hinterlegt.

Auch Gesichts- und Objekterkennung sind seit einiger Zeit der Standard. In sozialen Netzwerken sehen Sie das zum Beispiel daran, dass Gesichter direkt einen Namen erhalten. Der Betreiber des sozialen Netzwerks kann so zahlreiche Daten auch über hochgeladene Bilder sammeln, die Sie nicht direkt preisgegeben haben.

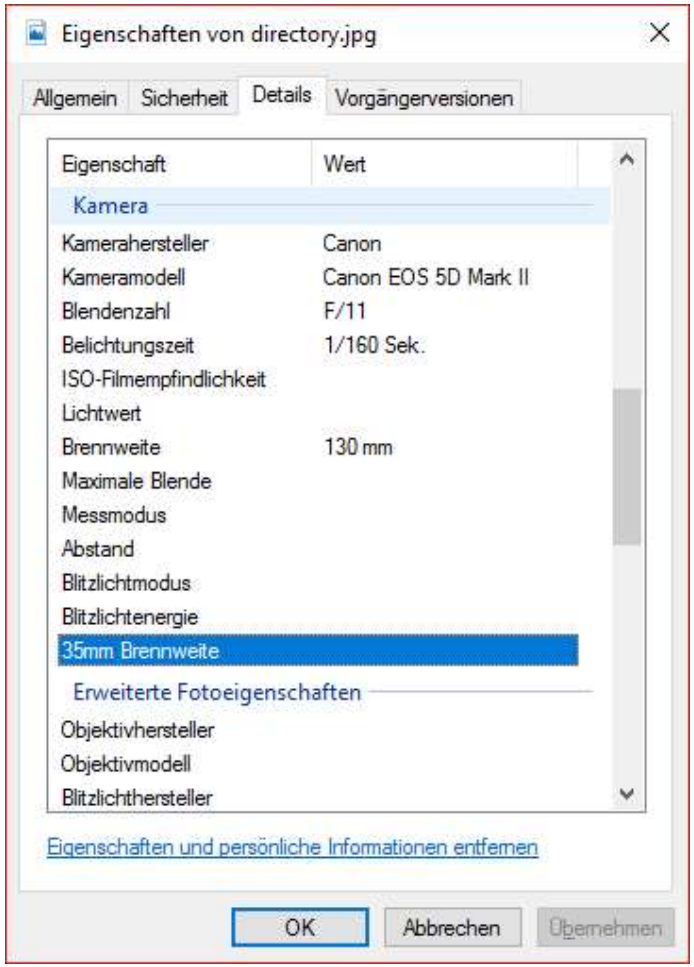
Beschreibung „(Ungewollte) Preisgabe von Kontextinformationen mit dem Hochladen von Bildern und Videos.“ *Fortsetzung*

In vielen Fällen sind auch zusätzliche Meta-Daten in Bildern enthalten. Dies können z. B. Kamerahersteller, Kameramodell, Blendenzahl und viele mehr sein (siehe Anzeige der Eigenschaften eines Bilds directory.jpg)

Videos können ähnlich wie Bilder ausgewertet werden, enthalten nur zusätzlich noch Toninformationen.

Toninformationen können Informationen zu Musikgeschmack und Ort enthalten. Weiterhin kann über die Stimme ein ungefähres Alter festgestellt werden.

Aus Bildern und Videos lassen sich somit umfangreiche Informationen automatisch auslesen, die unter Umständen auch sehr privat sein können.



Beschreibung
„(Ungewollte) Preisgabe von Daten aufgrund Ihrer Kontakte“

Nicht nur durch direktes Einstellen von Daten, wie zum Beispiel Nachrichten, Bildern oder Videos, können Daten preisgegeben werden, sondern auch durch die Verbindung mit anderen Kontakten.

Ihre Kontakte könnten Sie dazu verleiten, Daten preiszugeben, da sie selbst ähnliche Informationen preisgeben. Zum Beispiel stellt einer Ihrer Kontakte ein Urlaubsbild in ein soziales Netzwerk. Sie wollen nun auch zeigen, dass Sie im Urlaub sind und posten ebenfalls ein Urlaubsbild.

Eine weitere Ausprägung der Gefahr ist, dass Sie zwar bestimmte Daten im Profil absichtlich nicht eingegeben haben, dass aber durch den Kontakt mit anderen auf Ihre Eigenschaft geschlossen werden könnte. Sie haben zum Beispiel viele Kontakte mit einer bestimmten politischen Ausrichtung, die diese Kontakte auch offen zugeben. Dadurch ist es mit hoher Wahrscheinlichkeit möglich, dass Sie eine ähnliche politische Ausrichtung haben, auch wen Sie dies niemals öffentlich bekundet haben.

Beschreibung
„(Ungewollte) Preisgabe von Daten mit der Bestätigung von vermeintlichen Kontaktanfragen“

Ein soziales Netzwerk lebt durch die Verbindungen unter Kontakten. Bei einer neuen Kontaktanfrage müssen Sie häufig entscheiden, ob dieser Kontakt für Sie legitim ist oder nicht.

Leider erhalten Sie hin und wieder Kontaktanfragen von Kontakten, die Sie nicht kennen. Wenn Sie diese Kontakte nicht bestätigen, können diese Kontakte je nach Einstellung nur Ihre öffentlich freigegebenen Daten, Bilder und Videos sehen. Bestätigen Sie diese Kontakte, können diese auch Ihre nicht öffentlich freigegebenen Daten, Bilder und Videos sehen. Eine Überprüfung jedes Kontakts ist also essenziell für den Schutz Ihrer Daten.

Gut ist, dass die sozialen Netzwerke Algorithmen und Methoden haben, die vermeintliche Kontaktanfragen erkennen und damit von Zeit zu Zeit automatisch sperren. Aber seien Sie trotzdem vorsichtig bei unbekannten Kontaktanfragen, da diese Methoden leider nicht alle vermeintlichen Kontaktanfragen zeitnah erkennen.

Beschreibung
„(Ungewollte) Preisgabe von Daten aufgrund gefährlicher Links“

In Nachrichten von anderen Nutzern eines sozialen Netzwerks können gefährliche Links versteckt sein. Überprüfen Sie bei jeder Webadresse, die Sie anklicken wollen, ob diese dem erwarteten Ziel entspricht.

Nähere Informationen über die Prüfung von Links und Webadressen sowie zum Thema Phishing und gefährliche Nachrichten allgemein erhalten Sie in der Schulung „Phishing und gefährliche Nachrichten“.

Beschreibung „(Ungewollte) Preisgabe von Daten aufgrund automatisierter oder gezielter Abfragen“

Soziale Netzwerke speichern viele wertvolle Informationen, die noch wertvoller werden, wenn diese Informationen gezielt abgefragt werden können.

Gezielte Abfragen werden zum Beispiel von folgenden Gruppen durchgeführt:

- Angreifer, die Social Engineering-Techniken nutzen, bei denen Ihre Daten dazu genutzt werden können, um an andere vertrauliche Informationen (z.B. Passwörter) zu gelangen.

- Arbeitgeber, die Informationen rund um einen Bewerber für einen Job suchen, um eine Vorabentscheidung zu treffen - ihre Entscheidung wird somit durch die erlangten Informationen beeinflusst.

- Strafverfolgungsbehörden, zwecks Überprüfung von Verbindungen zu anderen Kontakten.

Beschreibung „(Ungewollte) Preisgabe von Daten aufgrund automatisierter oder gezielter Abfragen“ *Fortsetzung*

Harvesting beschreibt das automatisierte Sammeln von Daten durch einen Angreifer mithilfe eines speziellen Programms. Es können auf diese Weise große Mengen an Daten gesammelt werden und aus verschiedenen Quellen zusammengeführt werden. Über Harvesting ist es somit möglich, umfangreiche Daten über einen Benutzer aus verschiedenen sozialen Netzwerken zusammenzufassen und für spätere Zwecke aufzubewahren. Harvesting beschränkt sich dadurch nicht nur auf Ihr Profil, sondern es können viele Profile gleichzeitig abgefragt werden.

Empfehlung „Datensparsamkeit“

Sie können das Sammeln und die Weitergabe sowie die Weiterverarbeitung Ihrer Daten nur so verhindern, indem Sie das sogenannte „Prinzip der Datensparsamkeit“ anwenden. Folgende Hinweise und Denkanstöße helfen Ihnen dabei:

- Überlegen Sie sich genau, bei welchen sozialen Netzwerken Sie sich registrieren. Überdenken Sie, ob Sie eine Mitgliedschaft wirklich benötigen. Nicht benötigte Mitgliedschaften sollten beendet werden.

- Wenn Sie sich registriert haben, überlegen Sie, welche Daten Sie dort hinterlegen wollen und für welchen Zweck. Je weniger Sie soziale Netzwerke nutzen, desto weniger Daten produzieren Sie. Beschränken Sie sich also selbst in der Nutzung.

- Überlegen Sie gründlich, welche Daten Sie eingeben und damit dem Betreiber des sozialen Netzwerks zur Verfügung stellen.

Empfehlung „Datensparsamkeit“ *Fortsetzung*

- Überlegen Sie sich genau, welche Bilder und Videos Sie in ein soziales Netzwerk laden. Nachträglich gelöschte Bilder und Videos sind nicht unbedingt tatsächlich gelöscht. Schauen Sie in den AGB nach. Laden Sie nicht pauschal alle Bilder und Videos die Sie haben in ein soziales Netzwerk. Auch, wenn Bilder und Videos Ihren Kontakten nicht angezeigt werden, kann der Betreiber des sozialen Netzwerks diese auswerten.

- Überprüfen Sie die Datenschutzeinstellungen des sozialen Netzwerks und die Einstellungen bei jedem Veröffentlichen. Beachten Sie auch, dass die Privatsphäreneinstellungen im sozialen Netzwerk häufig keine Auswirkung auf die Weitergabe und Weiterverarbeitung durch den Betreiber haben.

- Bitte beachten Sie, dass auch Informationen, die mit speziellen Rechten versehen wurden von Berechtigten kopiert werden können und auf anderen Wegen (z. B. Messenger) an weitere Personen verteilt werden können. Betroffen sind alle veröffentlichten Informationen (Bilder/Videos, Texte) in einem sozialen Netzwerk.

Empfehlung „Datensparsamkeit“ *Fortsetzung*

- Nutzen Sie Funktionen, über die Sie dem Netzwerk Informationen über sich geben, sparsam. Spezielle Algorithmen und Methoden können Informationen über Sie finden, die sie nicht eingegeben haben. Bekannte Beispiele dafür sind die „Könnten Sie kennen“ oder „Like“-Funktionen. Diese Methoden können durch Ihre Entscheidungen und Informationen lernen.

- In diesem Zusammenhang ist es wichtig zu wissen, dass Sie vom sozialen Netzwerk wiedererkannt werden können, wenn Sie das gleiche Surfverhalten an verschiedenen Standorten zeigen. Z. B. Sie surfen im Büro auf den gleichen Seiten, die Teile eines sozialen Netzwerks einbinden, wie auch Zuhause. Die Wahrscheinlichkeit ist sehr hoch, dass das soziale Netzwerk Sie im Büro mit dem Profil Zuhause verbindet. Dies macht es anhand der Reihenfolge und Häufigkeit der besuchten Seiten. Seien Sie auch hier vorsichtig und versuchen Sie wenn möglich Cookies zu löschen.

Empfehlung „Plausibilitätsprüfung“

Damit Sie keine Daten an Absender von vermeintlichen Kontaktanfragen preisgeben, stellen Sie sich folgende Plausibilitätsfragen:

- Kenne ich diesen Kontakt?
- War ich auf einer Veranstaltung, auf der dieser Kontakt gewesen sein könnte?
- Könnte es ein bekannter Kontakt sein, der einen falschen Namen eingegeben hat?

Können Sie keine der Fragen mit Sicherheit mit „Ja“ beantworten, ignorieren Sie die Anfrage.

Zusätzlich können Sie sich bei jeder Preisgabe von Daten die folgenden Fragen stellen:

- Warum veröffentliche ich gerade diese Daten?
- Könnte ich die Veröffentlichung später bereuen („das Internet vergisst nicht“)?
- Könnten Angreifer Informationen erlangen, die mir schaden?

Weitere Hinweise zu „Gefahren in sozialen Netzwerken, die primär Ihre Daten sammeln und deren spätere Nutzung unbekannt ist“

- Das Bundesamt für Sicherheit in der Informationstechnik hat Informationen über Gefahren in sozialen Netzwerken veröffentlicht: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/SozialeNetze/Sicherheitsrisiken/sicherheitsrisiken_node.html sowie einen Basisschutz zusammengestellt: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/SozialeNetze/Schutzmassnahmen/Basisschutz/Basisschutz_node.html.

Teil 2:

Wie soziale Netzwerke Ihre Meinung beeinflussen können

Wer versucht Sie oder Ihre Meinung zu beeinflussen?

Diejenigen wollen Sie beeinflussen, die davon direkt oder indirekt profitieren können:

- Der Betreiber des sozialen Netzwerks könnte Sie mit gezielten Nachrichten beeinflussen wollen, damit Sie Ihre Meinung ändern.
- Werbenetzwerke, die in das soziale Netzwerk eingebunden sind, könnten zum Beispiel Ihr Kaufverhalten beeinflussen wollen.
- Ein sog. Fake-Profil könnte bekannte Personen vortäuschen und Sie in Bezug auf die richtige Person beeinflussen wollen.
- Kriminelle können gezielt Informationen streuen, um Sie zum Beispiel auf gefährliche Webseiten zu leiten.
- Freunde könnten Sie und Ihre Meinung beeinflussen.

Konsequenzen von Beeinflussung in sozialen Netzwerken

Wenn Sie in sozialen Netzwerken beeinflusst werden, gibt es verschiedene Arten von Konsequenzen. Im Folgenden eine Beispielauflistung:

- Sie könnten so beeinflusst werden, dass Sie bestimmte Produkte bevorzugt kaufen und damit Vorurteile gegenüber anderen Produkten haben.
- Sie könnten zum Beispiel für eine bevorstehende Wahl so beeinflusst werden, dass Sie eine bestimmte politische Richtung wählen.
- Sie könnten nur selektierte Nachrichten präsentiert bekommen und dadurch glauben, dass die Wahrheit so ist, wie sie Ihnen präsentiert wird.
- Kontakte könnten Sie negativ gegenüber anderen Kontakten beeinflussen, so dass Sie aufgrund dieser Beeinflussung andere Entscheidungen treffen.

Arten der Beeinflussung in sozialen Netzwerken

Es gibt verschiedene Methoden, die genutzt werden können, um Sie in sozialen Netzwerken zu beeinflussen:

- Angreifer könnten versuchen, Sie mit sogenannten Fake-Profilen zu beeinflussen. Diese Fake-Profile werden nur dafür angelegt, um Personen zu beeinflussen. Häufig verbreiten sie sog. „nicht verifizierten Content“ (z.B. Fake-News).
- Ein Zensurverfahren zeigt Ihnen nur die Informationen an, die laut den Richtlinien des sozialen Netzwerks erlaubt sind. Diese Richtlinien werden häufig an länderspezifische Regularien angepasst. In manchen Ländern werden gezielt falsche News verbreitet und andere zensiert.
- Unternehmen könnten Ihre Meinung beeinflussen, um deren Image und Ihre Einstellung dem Unternehmen gegenüber zu verbessern.

Beschreibung „Beeinflussung durch Fake-Profile“

Angreifer erstellen Profile, welche sie dann nutzen um Inhalte zu streuen, die nicht vertrauenswürdig sind. Diese Inhalte werden in der Regel nicht überprüft (sog. „nicht verifizierter Content“).

Weiterhin kann die Annahme einer Freundschaft oder Bekanntschaft mit einem solchen Fake-Profil Ihre Bekannten beeinflussen, so dass Ihre Freunde denken könnten, dass sie diesen Kontakt auch kennen.

Es ist jedoch unwahrscheinlich, dass Sie eine reale Kontaktanfrage erhalten, wenn Sie vorher nicht in der realen Welt kommuniziert haben.

Beschreibung „Zensur in sozialen Netzwerken“

Soziale Netzwerke leben von den Inhalten in diesen Netzwerken. Häufig werden die Inhalte in sozialen Netzwerken für Werbung genutzt.

- Wenn das soziale Netzwerk nun gezielt diese Ein- bzw. Ausblendung von Inhalten einsetzt, werden bestimmte Personen manipuliert.
- In manchen Ländern gibt es gesetzliche Regulierungen, die dem Netzwerk vorschreiben, bestimmte Inhalte zu zensieren.

Bei beiden Varianten werden bestimmten Personengruppen Inhalte verborgen und somit verschiedene Informationen an verschiedene Personen freigegeben.

Beschreibung
„Beeinflussung durch Betreiber oder Werbung“

In sozialen Netzwerken hat der Betreiber die Möglichkeit, bestimmte Inhalte beliebig zu sortieren. Zum Beispiel kann das soziale Netzwerk Nachrichten so sortieren, dass es die wirtschaftlichen Interessen für andere Unternehmen widerspiegelt und diese Nachrichten somit weiter oben angezeigt werden als andere Nachrichten. Dieser Effekt wird verstärkt, wenn Inhalte bezahlt werden. Dies erkennt man häufig an Zusätzen wie „Gesponsert“ in der jeweiligen Nachricht. Durch gezielte Veränderung der Darstellung wird also Ihre Wahrnehmung beeinflusst.

Beschreibung „Beeinflussung durch Betreiber oder Werbung“

Eine weitere oder zusätzliche Variante der Werbung ist, dass bestimmte Werbearten so dargestellt werden, dass es sich um eine persönliche Empfehlung zu handeln scheint. Zum Beispiel könnte einer Ihrer Bekannten Ihnen etwas empfehlen, indem er etwas „geliked“ hat. In dem dargestellten Bild sehen Sie, dass Max Mustermann dem Paketservice ein Like gegeben hat und dadurch wird Ihnen eine Werbung mit Angeboten gezeigt.

Dies ist insbesondere dann ein Problem, wenn Sie nicht erwarten, dass das soziale Netzwerk Ihnen Werbung darstellt als käme Sie von einer bekannten Person. Werbung, die eine persönliche Empfehlung erhält, wird in der Regel als glaubwürdiger empfunden und somit ist der Kaufanreiz größer.

Empfehlung „Plausibilitätsprüfung“

Wenn Sie die folgenden Punkte beachten, können Sie das Risiko einer Beeinflussung minimieren:

- Überlegen Sie sich genau, ob eine Kontaktanfrage legitim ist und überprüfen Sie, ob Sie diesen Kontakt wirklich kennen.
- Melden Sie vermeintliche Fake-Profile sofort an die Betreiber des sozialen Netzwerks, damit auch andere geschützt werden.
- Lassen Sie sich nicht so einfach von Informationen anderer beeinflussen und verifizieren Sie deren Herkunft.
- Nutzen Sie die Funktionen, die anzeigen, dass Ihnen etwas gefällt, möglichst sparsam und lassen Sie somit das soziale Netzwerk weniger Informationen über Sie lernen.

Teil 3:
Wie soziale Netzwerke Ihnen finanziellen, sozialen oder einen Imageschaden zufügen können

Wer versucht Ihnen zu schaden?

Angreifer wollen Ihnen schaden, um direkt oder indirekt davon zu profitieren:

- Kriminelle könnten versuchen, Daten von Ihnen zu bekommen, die benutzt werden können, um sogenannte Social Engineering-Angriffe durchzuführen.
- Kriminelle könnten versuchen, Sie auf eine gefälschte Webseite zu bringen, um so persönliche Daten von Ihnen zu bekommen. Zum Beispiel könnten dies Benutzername und Passwort sein. Damit wäre ein Identitätsdiebstahl möglich.
- Angreifer könnten versuchen, Ihrem Unternehmen Schaden zuzufügen, um Beispiel durch gefälschte Nachrichten.
- Angreifer könnten versuchen, Sie zu mobben (Stichwort Cybermobbing).

Konsequenzen in Form von sozialen, finanziellen und Image-Schäden

Die Konsequenzen äußern sich häufig in einem sozialen, finanziellen oder Image-Schaden:

- Bei sozialem Schaden erleiden Sie einen Schaden, der sich im Umgang mit Ihren Mitmenschen äußert. Sie werden in einer bestimmten Gruppe beispielsweise nicht mehr angenommen.
- Finanzieller Schaden schlägt sich in der Regel direkt auf Ihre monetären Mitteln nieder, zum Beispiel durch eine Überweisung in Ihrem Namen.
- Imageschaden äußert sich in der Regel durch einen Wertverlust oder Aktiensturz Ihres Unternehmens.

Auf welche Arten können Schäden in sozialen Netzwerken entstehen?

Es gibt verschiedene Arten, wie ein sozialer, finanzieller oder ein Image-Schaden in sozialen Netzwerken entstehen kann.

- Es kann ein Image-Schaden entstehen, wenn Ihre Mitarbeiter oder andere Personen **negative Nachrichten** über Ihr Unternehmen veröffentlichen oder verteilen.
- Wenn Ihre Identifikationsdaten (wie zum Beispiel Benutzername und Passwort) in die Hände Dritter gelangen, kann dies zu einem **Identitätsdiebstahl** führen. Der Angreifer kann also Aktionen in Ihrem Namen durchführen (z.B. kostenpflichtige Buchungen).
- **Cybermobbing** ist die Veröffentlichung von negativen Nachrichten über Sie oder andere Personen.
- Angreifer können Nachrichten mit gefährlichen Links posten und dadurch auch **Schadsoftware** verbreiten.

Beschreibung
„Negative Nachrichten über Ihr Unternehmen“

Soziale Netzwerke werden immer häufiger auch im geschäftlichen Umfeld genutzt und dienen dort Marketingzwecken. Gut gewählte Marketingkampagnen, die auch auf sozialen Netzwerken genutzt werden, haben meist eine gute Außenwirkung.

Verärgerte Kunden und unzufriedene Mitarbeiter nutzen den Weg über soziale Netzwerke auch, um Ihre Unzufriedenheit auszudrücken. Nicht selten sind die Nachrichten sehr offensiv. Bei Mitarbeitern können sogar Interna an die Öffentlichkeit gelangen.

Diese Nachrichten bewirken je nach Außenwirkung einen negativen Impuls für Ihr Unternehmen.

Beschreibung „Identitätsdiebstahl“

Identitätsdiebstahl ist ein häufig anzutreffendes Problem in sozialen Netzwerken. Es bezeichnet die Übernahme eines Benutzerkontos durch eine unbefugte Person, so dass diese im Namen des Kontonutzers Nachrichten posten kann. Häufig sind diese Nachrichten nachteilhaft für den eigentlichen Kontonutzer.

Bedenken Sie auch, dass eine Kommunikation über integrierte Messenger möglich ist und somit Ihre Kontakte belästigt werden könnten. Weiterhin kann der Angreifer wichtige Informationen erfahren, die auch dazu genutzt werden können, Zugang zu Ihrem E-Mail-Account oder sogar zum Onlinebanking zu erhalten.

Beschreibung „Cybermobbing“

Der Begriff Cybermobbing ist die elektronische Variante von Verleumdung, Belästigung und Nötigung von Personen.

Häufig wird in sozialen Netzwerken Cybermobbing in verschiedenen Ausprägungen genutzt, um Personen sozialen Schaden zuzufügen, auch weil viele Personen annehmen, dass sie im sozialen Netzwerk allein durch die Wahl eines anderen Namens anonym sind..

Zum Beispiel können falsche Informationen über Sie veröffentlicht werden, die dann gegen Sie verwendet werden. Ein möglicher Schaden wäre zum Beispiel, dass Sie von Kontakten gehänselt werden.

Beschreibung „Verbreitung von Schadsoftware“

Unter Schadsoftware versteht man die Software, die Ihrem Computer oder Ihrem Netzwerk schaden kann.

Posts in sozialen Netzwerken können von beliebigen Personen getätigt werden, die einen aktivien Account haben. Dort können natürlich auch Verweise auf Schadsoftware verteilt werden.

Wenn nun also diese Gefahr in Verbindung mit Identitätsdiebstahl auftritt, kann Schadsoftware schnell an einen großer Kreis verteilt werden. Diese wird mit höherer Wahrscheinlichkeit angeklickt, da es sich um einen bekanntem Absender handelt. Zum Beispiel könnte ein Ihnen bekannter Absender einen Link zu einer schadhaften Webseite posten.

Empfehlung „Selbstkontrolle“

Folgende grundlegende Regeln sollten Sie zusätzlich zu den in den oberen Teilen genannten Regeln befolgen:

- Vergewissern Sie sich, ob Sie wirklich einen Account bei dem betreffenden sozialen Netzwerk benötigen.

- Bewahren Sie Ihre Zugangsdaten an einem sicheren Ort auf. Weitere Informationen dazu erfahren Sie in der Schulung zum Thema Passwortsicherheit.

- Überlegen Sie genau, welche Informationen Sie in einem Netzwerk hinterlegen.

Weitere Hinweise zum Angriff „Gefahren in sozialen Netzwerken, die Ihnen finanziellen, sozialen oder einen Image-Schaden zufügen können“

- Die Schulung zum Thema „Phishing und gefährliche Nachrichten“ hilft Ihnen dabei, Phishing und andere gefährliche Nachrichten zu finden und korrekt zu behandeln.

- Die Passwortschulung hilft Ihnen dabei, einem Identitätsdiebstahl vorzubeugen.

Tools, die Ihnen dabei helfen, sich gegen Gefahren in sozialen Netzwerken zu schützen

Soziale Netzwerke werden in der Regel über Ihren Browser aufgerufen. Somit sind alle Sicherheitstools nützlich, die Sie auch beim Surfen im Internet schützen, u.a.:

- Achten Sie darauf, dass Sie einen **Virenscanner** auf Ihrem Gerät installiert haben und dieser immer auf dem aktuellen Stand ist. Nur ein aktueller Virenscanner erkennt die meisten bekannten Viren und Malware.
- Viele **Browser** aktualisieren sich automatisch. Achten Sie darauf, dass dieser Mechanismus funktioniert und prüfen Sie von Zeit zu Zeit die Aktualität des Browsers. Aktuelle Browser erweitern ständig ihre Sicherheitsfunktionalität und können Sie somit vor Gefahren schützen. Ein Beispiel dafür ist die Anzeige unverschlüsselter Webseiten.
- **Werbeblocker** für Ihren Browser können Ihnen helfen, ungewünschte Werbung auszublenden. Beachten Sie aber, dass manche Funktionen bei eingeschaltetem Werbeblocker nicht funktionieren.
- **Cookie-Verwaltungstools** können Ihnen helfen, unerwünschte Cookies, die nur zum Zweck von Tracking in Ihrem Browser abgelegt wurden, zu entfernen.

Tools, die Ihnen dabei helfen, sich gegen Gefahren in sozialen Netzwerken zu schützen

- Überprüfen Sie stets, ob Ihre Zugangsdaten (auch von anderen Diensten) über gesicherte Verbindungen übertragen werden. Sie erkennen dies am **https://** in der Adresszeile.
- Nutzen Sie ein **Passwort** nicht bei mehreren Diensten, sondern verwenden Sie überall ein anderes Passwort. Wenn dann ein Dienst Passwörter unsicher speichert, sind nicht direkt alle von Ihnen genutzten Dienste betroffen. Passwortmanager helfen Ihnen bei dieser Aufgabe.
- Aktualisierten Sie Ihr Betriebssystem und aktivieren Sie die automatischen Aktualisierungsmechanismen, damit Sie stets die neuesten Sicherheits-Updates auf Ihrem Gerät installiert haben.
- Seien Sie vorsichtig mit Software, die nicht vertrauenswürdig ist. Im Zweifelsfall installieren Sie die Software nicht.