Sicherheit in sozialen Netzwerken

Schutz der eigenen Identität und Daten!

Methoden:

- 2-Faktor-Authentifizierung
- regelmäßige Überprüfung, der Geräte mit Zugriff auf das Konto
- Rechte von 3rd Party Apps überprüfen und anpassen
- Nachrichten nur an Personen Senden, die diese auch angeht
- Privatsphäreeinstellungen anpassen
- nicht jede Freundschaftsanfrage annehmen, evtl. Böse Absichten
- Nachrichten, auch von Freunden, die z.B. Gehackt wurden, sollen mit Vorsicht behandelt werden

Soziale Sicherheit

Security-Checkliste Social Media

Social-Media-Konten stellen de facto die digitale Identität vieler Nutzer dar. Die Plattformen bieten deshalb Schutzfunktionen, die Sie anwenden sollten. Und: Schalten Sie gerade bei auffällig attraktiven sozialen Kontakten nicht den gesunden Menschenverstand aus.

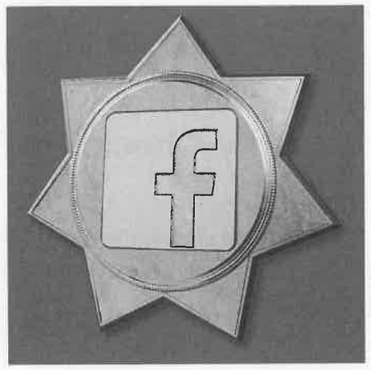

Bild: Andreas Martini

Von Holger Bleich

Zwei Faktoren nutzen

Werden Ihre Konten bei Facebook, Instagram oder LinkedIn gekapert, kann das nicht nur für Sie, sondern auch für Freunde und Kollegen katastrophale Folgen haben. Der Schutz solcher Accounts ist deshalb besonders wichtig. Nutzen Sie dazu alle Möglichkeiten, die die Plattformen bieten. Was in einigen anderen Checklisten bereits erwähnt ist (siehe auch Seite 82), gilt in besonderem Maße für soziale Plattformen: Sie sollten, wo immer möglich, weitere Zugangsbarrieren neben dem Passwort aufbauen, also auf eine Zwei-Faktor-Authentifizierung (2FA) setzen.

Auf der Facebook-Website gelangen Sie über einen Klick auf Ihr Profilbild oben rechts in die „Einstellungen", wo der Menüpunkt „Privacy Center" über „Sicherheit" zur „zweistufigen Authentifizierung" führt. Dort veranlassen Sie, dass bei jedem Zugriffsversuch von einem unbekannten Gerät oder Browser der zweite Faktor abgefragt wird, also etwa eine via SMS verschickte PIN oder der Anmeldecode einer zuvor mit dem Konto verbundenen Authentifizierungs-App. Ähnliche Einstellungen bieten inzwischen alle großen sozialen Netzwerke, also etwa Instagram, Twitter, Google (YouTube) und LinkedIn. Auch auf der Kurzvideo-Plattform TikTok lässt sich 2FA einrichten, allerdings nur in der mobilen App, dort in den Einstellungen unter „Sicherheit".

Damit die Abfrage nicht jedes Mal nervt, merken sich die Plattformen Geräte-IDs oder setzen Cookies und bleiben auf dem Gerät angemeldet. Dies kann zum Sicherheitsproblem werden, wenn sich mehrere Menschen einen Rechner oder ein Tablet teilen und ist definitiv gefährlich, wenn der Kontenzugriff von öffentlichen Terminals erfolgt. Sie sollten von Zeit zu Zeit prüfen, welche Geräte derzeit autorisierten Zugriff aufs Konto haben und deshalb von der 2FA ausgenommen sind. Bei Meta finden Sie diese Liste für Facebook und Instagram über die „Kontenübersicht" im Privacy Center unter „Hier bist Du aktuell angemeldet". Dort lässt sich der Zugriff selektiv unterbinden.

Zugriffe prüfen

Bei vielen sozialen Netzen können Sie externen Diensten und Fremd-Apps Zugriff auf Ihren Account gewähren, beispielsweise für Single-Sign-on-Logins auf verbundenen Websites. Bisweilen räumen sich Apps viel mehr Rechte als nötig ein. Sie sollten die Aktivitäten und Berechtigungen der Apps im Auge behalten. Facebook etwa gewährt Ihnen Kontrollmöglichkeiten in den Einstellungen unter „Apps und Websites". Besonders beliebt sind Apps bei Instagram-Nutzern. Unter „Apps und Websites" in den Profileinstellungen listet der Dienst die aktiven Apps auf. Kontrollieren Sie diese Liste ab und an und entfernen Sie nicht mehr benötigte Apps.

Gezielt teilen

Bei Facebook, aber auch bei anderen Anbietern wie LinkedIn kann man festlegen, mit wem man Inhalte teilen möchte. Behalten Sie Ihre Zielgruppen-Voreinstellung im Blick, um nicht versehentlich einen größeren Adressatenkreis anzusprechen als gewünscht.

So sollten Sie beispielsweise nicht öffentlich posten, dass Sie zwei Wochen im Urlaub sind, denn das legt nahe, dass Ihr Haus leersteht. Die Voreinstellung sollte eher defensiv sein. Sie lässt sich etwa bei Facebook in den Privatsphäre-Einstellungen unter „Deine Aktivität" ändern.

Anfragen checken

Freundschaft und Vertrauen sind auch auf Facebook, Instagram, LinkedIn oder TikTok ein begehrter Status. Befreundete Kontakte sehen je nach Profileinstellungen viel mehr Privates. Oft stecken daher hinter Freundschaftsanfragen Versuche, persönliche Daten abzugreifen, die Person zu stalken oder gar Geld zu ergaunern. Prüfen Sie jede Anfrage sorgfältig. Ist das Mitglied frisch dabei und hat viele neue Kontakte, kann das auf einen Betrug hindeuten – selbst wenn das Profil vermeintlich von einer Person stammt, die Sie persönlich kennen. Fake-Accounts haben oft Profilfotos von attraktiven Menschen.

Private Nachrichten

Lassen Sie Vorsicht walten, wenn jemand Sie anschreibt, es sehr dringend wirkt, und wenn er um Geld oder andere Gefallen bittet: Vielleicht wurde der Facebook-Account gehackt und übernommen, und nun versuchen Fremde, Ihr Vertrauen zu missbrauchen. Überweisen Sie keinesfalls Geld und rücken Sie nicht unbedacht Ihre Handynummer heraus, bevor Sie sich von der Identität überzeugen konnten – zum Beispiel mit einer Frage, die *garantiert* nur die befreundete Person beantworten kann.

(hob@ct.de) c't

Geldwerter Schutz

Security-Checkliste Onlinebanking

Auf Ihrem Bankkonto liegt Ihr Geld – logisch, dass Betrüger und Cyberkriminelle scharf darauf sind. Absolute Sicherheit gibt es beim Onlinebanking nicht, aber Sie können es Kriminellen ziemlich schwer machen.

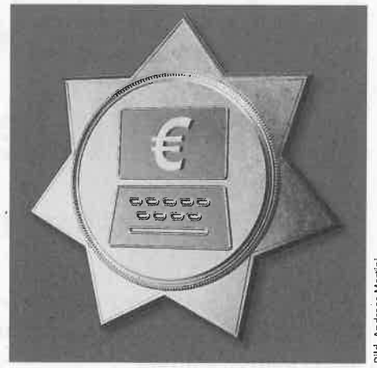

Bild: Andreas Martini

Von Markus Montz

Transaktionen checken

Viele Aktionen erfordern eine Zwei-Faktor-Authentifizierung (2FA), zum Beispiel durch eine PIN beim Login, gefolgt von einer TAN oder Push-Bestätigung bei einer Transaktion. Ähnliches gilt, wenn Sie ein neues Gerät für die 2FA freischalten. Checken Sie daher stets den Zweck dieser Bestätigung und brechen Sie ab, wenn er nicht stimmt. Bei Online-Überweisungen prüfen Sie außerdem, ob Empfänger-IBAN und Betrag korrekt sind – sie müssen auf sämtlichen beteiligten Geräten (PC, Smartphone, TAN-Generator) übereinstimmen.

Banking virenfrei

Für Banking auf dem PC oder Smartphone muss das System frei von Schadsoftware sein. Sorgen Sie auf einem Windows-PC dafür, dass ein Virenscanner mit aktuellen Updates mitläuft. Der bei Windows 10 und 11 mitgelieferte Defender bietet hinreichenden Schutz (siehe auch S. 80). Laden Sie Anwendungen nur von seriösen Websites herunter. Installieren Sie auf dem Smartphone allgemein nur Apps aus vertrauenswürdigen Quellen. Im Zweifel ist das Google Play für Android und der App Store für iOS.

Phishing erkennen

Bei vielen Betrugsversuchen verschicken Betrüger manipulativ gestaltete Mails oder Textnachrichten. Ein Beispiel sind Mails, die angeblich von einer Bank stammen. Diese enthalten in der Regel schädliche Anhänge oder Links auf Fake-Websites. Darüber schleusen die Täter Schadcode ein oder greifen Zugangsdaten ab (Phishing).

Prüfen Sie alle Mailanhänge sorgfältig, selbst wenn sie von bekannten Absendern stammen. Eine Bank schickt Ihnen wichtige Dokumente postalisch oder stellt sie in Ihr Onlinebanking-Postfach. Mails oder Textnachrichten mit Links, um Ihr Konto mit PIN und TAN zu „bestätigen", sind fast immer Betrugsversuche. Prüfen Sie bei allen Links zuerst die Ziel-URL. Schöpfen Sie Verdacht, wenn eine persönliche Anrede fehlt, Rechtschreibfehler enthalten sind oder Sie zur Eile getrieben werden. Geben Sie Ihre Zugangsdaten im Browser nur auf der Webseite der Bank ein, nachdem Sie die Adresse selbst eingetippt oder per Lesezeichen angesteuert haben. Sicher sind auch die App der Bank oder eine seriöse Onlinebanking-Anwendung.

Mitunter rufen Betrüger auch mit gefälschten Absender-Rufnummern an und geben sich als Bankberater oder Polizist aus. Eine Masche besteht darin, Sie vor einer angeblich drohenden Gefahr zu warnen, um Sie zu unüberlegten Handlungen zu provozieren (Social Engineering) [1]. Beenden Sie das Gespräch und rufen Sie die Bank über die Telefonnummer in Ihren Unterlagen (!) zurück.

Belege überprüfen

Insbesondere Kreditkartennutzer sollten jede Abrechnung kontrollieren und unbefugte Abbuchungen umgehend bei ihrer Bank reklamieren. Prüfen Sie auch Ihre Kontoauszüge regelmäßig. Noch besser ist es, alle paar Tage im Onlinebanking am PC oder in der Smartphone-App die Umsätze auf Ihrem Kreditkarten- und Girokonto zu verfolgen. Je nach Bank können sich Nutzer außerdem per Mail, SMS oder Push-Nachricht über neue Transaktionen oder Ereignisse wie das Unterschreiten eines bestimmten Kontostands benachrichtigen lassen.

Handy nicht rooten

Rooten oder jailbreaken Sie Ihr Smartphone oder Tablet nicht, mit dem Sie Onlinebanking betreiben. Andernfalls legen Sie wichtige Schutzfunktionen lahm. Das ist besonders dann gefährlich, wenn Sie beim Smartphone-Banking den zweiten Faktor über eine Sicherheits-App auf dem gleichen Gerät beziehen. Viele Sicherheits-Apps von Banken, teilweise aber auch deren Banking-Apps, starten unter modifizierten Betriebssystemen deshalb gar nicht erst.

Generell ist es empfehlenswert, ein ungerootetes Smartphone mit einem Betriebssystem zu verwenden, das noch Sicherheitsupdates bekommt. Dennoch sind ältere Betriebssysteme nicht per se unsicher. Aus Haftungsgründen empfiehlt es sich, den Vorgaben Ihrer Bank zu folgen: Solange Sie ein Betriebssystem nutzen, das die App Ihrer Bank offiziell noch unterstützt, kann Ihr Kreditinstitut zumindest daraus keine grobe Verletzung der Sorgfaltspflichten ableiten. Ohne solch eine grobe Verletzung haften Sie für Schäden mit maximal 50 Euro [2].

(mon@ct.de) c't

Literatur

[1] Mirko Dölle, Bei Anruf: Geld weg! Wie Telefonbetrüger die Zwei-Faktor-Autorisierung aushebeln, c't 14/2023, S. 66

[2] Stefan Hessel, Datenfänger und Haftungsflüchtlinge, Smartphone-Banking aus rechtlicher Sicht, c't 11/2020, S. 66