TELE-CREW

solutions for your business!

Zehn Regeln für Ihre digitale Sicherheit

Die aktuell geleakten Datensätze von Politikern und Journalisten zeigen: Selbst, wer sich selbst für vollkommen uninteressant hält, besitzt Daten über Dritte, die er schützen muss. Wir zeigen Ihnen hier die wichtigsten Grundregeln.

Die Meinung 'Ich habe doch nichts zu verbergen' ist unglaublich gefährlich und falsch. Selbst, wer sich selbst für vollkommen uninteressant hält, besitzt Daten, die weder Kriminelle noch staatliche Geheimdienste irgendwas angehen - nämlich Informationen über Dritte: Adressbücher mit Telefonnummern, E-Mail-Konten mit Nachrichten, Messaging-Apps mit Fotos und Chatverläufen, all das wird einem Angreifer in die Hände fallen.

Würden Sie nur einen Schlüssel für Haustür, Wohnungstür, Tresor und Fahrradschloss zu verwenden? Diese analoge Vorsicht scheint im digitalen Leben bei den meisten Nutzern außer Kraft gesetzt zu sein: Viele Menschen nutzen dieselben Passwörter für mehrere Konten. Das ist nicht nur fatal, sondern auch grob fahrlässig: Wenn Hacker Zugangsdaten erbeuten, versuchen sie und die Käufer der erbeuteten Daten fast immer, sich damit auch bei anderen Seiten einzuloggen.

Am sichersten sind natürlich komplett zufällige Kennwörter, die man sich nicht selber ausdenkt, sondern die man sich generieren lassen. Diese Funktion bringen die meisten Browser und Passwortmanager mit (aber auch auf tele-crew.com gibt es diese Funktion). Letztere sind übrigens sehr sinnvoll, denn einen Passwort-Manager sollten Sie ohnehin verwenden.

Die versprochenen 10 Regeln:

1. Verwenden Sie möglichst lange, zufällige und einzigartige Passwörter

Über sichere Passwörter kursieren viele Weisheiten: Neben der Einzigartigkeit ist tatsächlich die Länge mitentscheiden: Acht Zeichen sind das absolute Minimum, zwölf erhöhen die Sicherheit markant, für wichtige Konten sollten Sie 16 Zeichen verwenden.

2. Nutzen Sie einen Passwort-Manager

Das Gedächtnis ist der schlechteste Platz für Passwörter, Stift und Papier sind nur minimal besser - wenn Sie den Zettel verlieren oder unterwegs nicht dabeihaben, sperren Sie sich aus. Vertrauen Sie Ihre Login-Daten stattdessen einem Passwort-Manager an. Damit verwalten sie alle Anmeldeinformationen und synchronisieren diese im Idealfall über mehrere Geräte hinweg. Ein zentrales Master-Kennwort gibt Ihnen Zugriff auf alle anderen Zugänge - dass dieses Passwort besonders lang und sicher sein sollte, versteht sich von selbst. Dafür muss man sich nur dieses eine merken und alle anderen (auch die PIN Nummer der Bankkarte kann man im Passwortmanager speichern!) hat man dann dabei.

3. Vermeiden Sie "Single Sign-on"

Single-Sign-on (SSO) ist ein Verfahren, bei dem ein einzelnes Konto genutzt wird, um sich bei unterschiedlichen Diensten anzumelden. Google, Facebook und Twitter bieten etwa an, sich mit dem jeweiligen Account bei anderen Webseiten anzumelden. Sie müssen dann kein Passwort vergeben und keine zusätzliche Login-Daten speichern. Ist das eine Passwort gehackt, haben die Angreifer so auch Zugang zu anderen Diensten.

4. Misstrauen Sie Sicherheitsfragen

"In welcher Straße sind Sie aufgewahsen?" Oder: "Wie hieß Ihr erstes Haustier?" Manche Anbieter setzen solche Fragen als zusätzliche Absicherung ein, wenn Nutzer ihr Passwort vergessen haben oder zurücksetzen wollen. Grundsätzlich ist ein zweiter Faktor eine gute Sache, aber die Sicherheitsfragen bergen ein Risiko: Oft lassen sich die Antworten erraten oder aus öffentlich einsehbaren Informationen, zum Beispiel aus Profilen in sozialen Netzwerken, rekonstruieren.

Eine simple, aber effektive Strategie ist es, bewusst falsche Antworten zu geben. Eine Großmutter mit dem Namen des Wohnortes der Großmutter wird vermutlich kein Angreifer erraten, zumal die Zahl der Versuche begrenzt ist. Wenn Sie ganz sicher gehen wollen, generieren Sie als Antwort auf die Sicherheitsfrage ein zweites, zufälliges Kennwort, das Sie ebenfalls in Ihrem Passwort-Manager speichern.

5. Sichern Sie wichtige Konten mit einem zweiten Faktor

Immer mehr Dienste bieten mittlerweile Zwei-Faktor-Authentisierung (2FA) an. Leider sind viele Menschen zu bequem oder zu leichtfertig, um ihr Konto damit zu schützen. Sie verzichten ohne Not auf einen zweiten Faktor, der Angreifer auch dann aussperrt, wenn diese das Passwort erbeuten. Oft handelt es sich um einen Code, den Sie in einer separaten App empfangen oder per SMS zugeschickt bekommen.

6. Nutzen Sie nur Messenger mit Ende-zu-Ende-Verschlüsselung

Ende-zu-Ende-Verschlüsselung (E2E) klingt nach einer komplizierten Angelegenheit, aber das Gegenteil ist der Fall. Sie müssen sich keinen PGP-Key zulegen und Ihre E-Mails verschlüsseln, um sicher zu kommunizieren. Viele Messenger verschlüsseln Ihre Nachrichten, sodass weder Geheimdienste noch Kriminelle mitlesen können.

7. Prüfen Sie Links und Anhänge vor dem Öffnen

Moderne Phishing-Nachrichten sind auf den ersten Blick kaum noch von echten Nachrichten zu unterscheiden. Betrüger (man nennt sie Scammer) fälschen E-Mails und ganze Webseiten, die sich nur durch zufällige Kleinigkeiten vom Original unterscheiden. Meist versuchen die Betrüger, ihren Opfern mit Schadprogrammen verseuchte Anhänge unterzujubeln oder sie auf Webseiten zu lotsen, wo sie angeblich ihr Passwort zurücksetzen oder ihre Zugangsdaten eingeben sollen. Die wirksamsten Gegenmittel sind Vorsicht und gesunder Menschenverstand: Versichern Sie sich besser dreimal, ob Sie dem Absender vertrauen (und achten Sie dabei auf alle Zeichen der E-Mailadresse), bevor Sie einen Anhang öffnen oder auf einen Link klicken. Geben Sie Passwörter nur auf Seiten ein, deren URL Sie sorgfältig geprüft haben und öffnen Sie den Link zum Online-Banking nicht aus der E-Mail heraus sondern öffnen Sie ihn durch händische Eingabe oder durch Öffnen eines Lesezeichens. Lassen Sie sich dabei nicht von dem Schlosssymbol in die Irre führen, das viele Browser in der Adresszeile anzeigen, um eine sichere HTTPS-Verbindung zu markieren.

Das bedeutet nur, dass die Verbindung verschlüsselt ist! Aber auch Kriminelle können Ihre Verbindung verschlüsseln.

8. Halten Sie Ihr System aktuell und sicher

Fast jede Anwendung und jedes Betriebssystem enthält Sicherheitslücken. Die Frage ist nur, wann sie entdeckt und ausgenutzt werden. Die meisten Hersteller veröffentlichen deshalb regelmäßig Patches, um Schwachstellen zu schließen. Viele Apps und Systeme aktualisieren sich von selbst oder weisen auf Sicherheitsupdates hin. Nehmen Sie diese Warnungen ernst und verzögern Sie die Installation nicht. Und: Benutzen Sie einen guten, möglichst kostenpflichtigen, namhaften Virenscanner!

9. Ersetzen Sie alte E-Mailadressen

In Ihrem Google-Konto ist eine E-Mailadresse hinterlegt, die Sie seit Jahren nicht mehr genutzt haben? Das öffnet ein Einfallstor für Kriminelle: Falls diese den E-Mail-Account übernehmen, können sie das Google-Passwort zurücksetzen und selbst ein neues vergeben. Die Vorsichtsmaßnahme ist natürlich nicht nur bei Google wichtig, sondern bei allen Konten, die private oder sensible Daten enthalten: Hinterlegen Sie dort aktuelle Kontaktinformationen und achten Sie insbesondere darauf, dass E-Mailadresse und Handynummer stimmen.

10. Nutzen Sie offene WLANs nur mit VPN

Um mal schnell die Lieferzeiten vom Pizza Lieferdienst nachzusehen müssen Sie keine VPN-Verbindung nutzen. Aber bei Online-Einkäufen, Kontostandsabfragen, etc. sollte in offenen WLANs Vorsichtig geboten sein.
Ein Virtuelles Privates Netzwerk (VPN) baut eine separate Verbindung zwischen Geräten auf, meist verbindet es den Rechner oder das Smartphone eines Nutzers mit dem Server des VPN-Anbieters. Es kann als zusätzliche Sicherheit dienen, wenn Sie Ihre Aktivitäten vor Ihrem Internetanbieter oder dem WLAN-Betreiber (bzw. den anderen Nutzern in dem offenen WLAN) verbergen wollen.

Das gilt insbesondere für offene Hotspots, wo man dem Betreiber nicht hundertprozentig vertrauen kann oder man unsicher sind, ob unsichtbare Dritte versuchen, das Netzwerk zu überwachen. Solche WLANs finden Sie oft an Flughäfen und Bahnhöfen oder in Cafés - das VPN verschleiert Ihre Identität und leitet die Daten durch einen virtuellen Tunnel.

Doch Vorsicht: Falls Sie ein VPN nutzen wollen, müssen Sie den Anbieter sorgfältig auswählen. Ein privates Netzwerk nützt nichts, wenn Ihre Aktivitäten dann bei einem zwielichtigen Unternehmen landen. Seien Sie vor allem bei denjenigen kostenlosen VPNs vorsichtig, die mit unbegrenztem Datenvolumen und hohen Geschwindigkeiten werben.

Sie möchten sich absichern und benötigen Unterstützung?

Sprechen Sie uns an:

Tel: 09405 / 95666-0 oder info@tele-crew.de