Sponsored

Anzeige

So leichtsinnig gehen wir mit unseren Daten um

Internetsicherheit Weil wir glauben, für andere nicht interessant zu sein, öffnen wir Cyberkriminellen Tür und Tor. Dabei gibt es einfache Vorsichtsmassnahmen, die auch Familie, Freunde und Arbeitskollegen schützen.

Schliessen Sie die Türe ab, wenn Sie Ihre Wohnung verlassen? Selbstverständlich. Und vielleicht haben Sie auch eine Zeitschaltuhr, die das Licht an- und ausmacht, um Einbrecher abzuschrecken. Oder gar eine Alarmanlage. Aber haben Sie damit wirklich alle Gefahren gebannt? Weit mehr als Ihr Hausrat und Ihre Wertgegenstände sind nämlich Ihre Daten im Internet in Gefahr. Während die Zahl der in der Schweiz gemeldeten Diebstähle und Wohnungseinbrüche im vergangenen Jahr bei rund 112 000 lag, kursieren die Zugangsdaten von 3 Millionen Online-Konten mit Schweizer Mailadressen bis heute frei im Web. Ob Sie betroffen sind, können Sie über die Website «Have I been pwned» überprüfen. Am sichersten sind Sie im Internet unterwegs, wenn Sie einen Passwort-Manager verwenden. Dieser speichert nicht nur Zugangsdaten an zentraler Stelle, sondern kann Ihnen für jedes Konto ein separates, sicheres Passwort vorschlagen.

Die Angst vor langen Passwörtern

Es ginge also durchaus bequem und sicher. In Umfragen geben allerdings zahlreiche Befragte immer wieder an, dass es ihnen schwerfalle, sich lange Passwörter zu merken, die bedeutend besseren Schutz böten. Sie befürchteten, sich selber aus ihren Konten auszusperren. Andere erklären, dass sie seit Jahren überall dasselbe Passwort benutzen – und es aus Gewohnheit nicht ändern. Im realen Leben käme dagegen wohl niemand auf die Idee, nur einen einzigen Schlüssel für Haustür, Bürotür, Tresor, Hobbyraum und Veloschloss zu benutzen.

Sichern Sie Ihre Daten mit einer Backup-Sofware.

Oft geht es zudem nicht nur um den Schutz der eigenen Privatsphäre. Vielleicht haben Sie auf Ihrem Rechner Familienbilder von den letzten Strandferien gespeichert, die nicht für die Augen Fremder bestimmt sind. Und wer möchte seine Familie nicht vor unerwünschten Einblicken schützen?

Es mag sein, dass Ihre privaten E-Mails, Facebook-Posts und WhatsApp-Nachrichten tatsächlich nicht so spannend sind für Cyberkriminelle. Diese können geknackte Konten aber dazu missbrauchen, in Ihrem Namen Viren-Mails an Verwandte und Freunde zu verschicken.

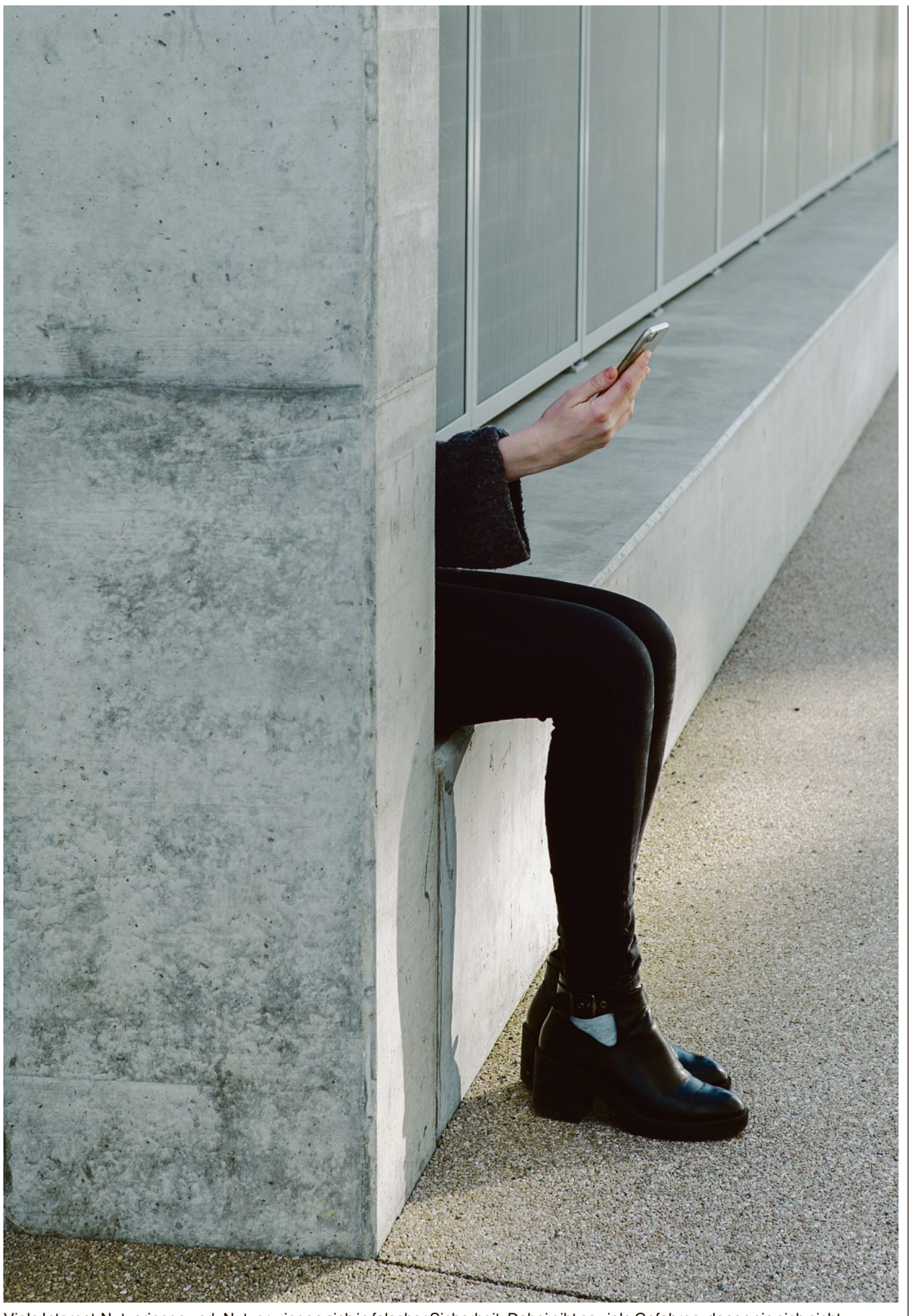
Und: Sichern Sie Ihre Daten regelmässig. Die Sicherung selbst sollte offline erfolgen. So sind die Daten nicht permanent über den Windows Explorer oder den Finder auf dem Mac zugänglich. Wenn Sie fürs Backup eine externe Festplatte verwenden, trennen Sie sie nach der Sicherung vom Computer. Ansonsten besteht das Risiko, dass Malware auch die gesicherten Daten befällt. Weil Online-Speicher gewöhnlich für Viren und Ransomware erreichbar sind, sollten Sie fürs Cloud-Backup einen dedizierten und eine Backup-Software wählen.

Netzwerkgeräte nicht vergessen

Setzen Sie Netzwerkgeräte wie Drucker, WLAN-Router, vernetzte Fernseher oder eine Überwachungskamera ein, sollten Sie diese ebenfalls schützen und zumindest das Standard-Passwort ändern. Auch regelmässige Firmware-Updates – also Aktualisierungen des Geräte-Betriebssystems – helfen mit, Sicherheitslücken zu schliessen. Der Grund für diese Schutzmassnahmen: Es gibt Malware wie beispielsweise Mirai, die es explizit auf schlecht geschützte Netzwerkgeräte abgesehen haben. Eine Antiviren-Software erkennt und blockiert solche Malware in vielen Fällen. Sie können den mit aktuellen Windows-Versionen mitgelieferten Windows Defender oder ein kostenpflichtiges Produkt verwenden. Wichtig ist, dass die Definitionen stets aktuell sind. Nutzen Sie hierzu automatische Updates. Für den Mac kursieren derzeit keine Viren. Weil sich das aber jederzeit ändern kann, sollten Sie präventiv eine Antiviren-Software nutzen. Da diese auch Windows-Malware erkennt, minimieren Sie das Risiko, versehentlich verseuchte Anhänge an Windows-Benutzer weiterzuschicken. Zudem sollten Sie eine Personal Firewall einsetzen, die den ankommenden und ausgehenden Netzwerkverkehr kontrolliert und so Malware allenfalls blockieren kann. Auch hier können Sie entweder auf die hauseigene Firewall von Windows und macOS setzen oder auf das Produkt eines Drittanbieters.

Aufgepasst bei E-Mail-Anhängen

Besondere Vorsicht ist bei E-Mails geboten. Etwa zwei Drittel der Malware landet über sie auf dem Computer. Seien Sie deshalb vorsichtig, wenn Sie in einem Mail auf einen Link klicken oder einen Anhang öffnen. Fahren Sie mit der Maus über den Link – ohne zu klicken! –, um das effektive Ziel anzuzeigen. Kommt Ihnen dieses verdächtig vor, löschen Sie das Mail oder melden es dem Provider als Spam respektive Phishing-Mail. Mail-Anhänge sollten Sie vor dem Öffnen stets mit einem Virenscanner prüfen. Und im Zweifelsfall beim Absender nachfragen, ob er Ihnen wirklich ein Dokument geschickt hat. Cyberkriminelle greifen auch Smartphones an. Sie sollten deshalb wie beim Computer regelmässig die Updates von iOS oder Android und jene Ihrer Apps durchführen. Die Apps beziehen Sie aus den regulären App-Stores von Apple und Google. Damit haben Sie die grösste Gewähr, dass Sie sich keine Malware oder Spionage-Apps einfangen.



Viele Internet-Nutzerinnen und -Nutzer wiegen sich in falscher Sicherheit. Dabei gibt es viele Gefahren, denen sie sich nicht bewusst sind. Foto: Stocksy

«Wir filtern 65 Millionen Spam-Mails pro Tag»

Interview Ein zuverlässiger, schneller Internet-Zugang ist längst selbstverständlich. Doch was braucht es, um diese Netzsicherheit zu gewährleisten? Philippe Vuilleumier, Chief Security Officer bei Swisscom, gibt im Interview Einblick in die meist unsichtbare Arbeit im Hintergrund.

Warum ist ein sicheres Netz für mich als Benutzer wichtig?
Ich mache eine Analogie zur Briefpost: Dort verlasse ich mich darauf, dass mein Brief in guten Händen ist und unversehrt beim Empfänger ankommt. Genauso ist es im Netz: Ich will mich darauf verlassen können, dass meine Telefongespräche, Daten und E-Mails sicher sind. Dazu kommt, dass die Netze der Telekomanbieter zur kritischen Infrastruktur der Schweiz gehören. Sie erfüllen wichtige Aufgaben für Private, die Wirtschaft und die Sicherheit unseres Landes.

Merken die Nutzer überhaupt etwas davon?
Der Grossteil der Netzsicherheit ist unsichtbar. Zum Beispiel filtern wir pro Tag rund 65 Millionen Spam-Mails heraus. Die Benutzer merken nur, dass weniger Spam in ihrem Posteingang landet. Gleichzeitig wird unser Netz etwa zwei Millionen Mal pro Monat angegriffen (siehe Infografik rechts). Oder anders gesagt: Während jemand dieses Interview liest, wehren wir 200 Angriffe ab. Weil wir dadurch viele Angriffsformen kennen, können wir effiziente Abwehrmassnahmen ergreifen.

Und wie bewerkstelligt Swisscom den Schutz des Netzes?
Das beginnt schon bei der Planung eines neuen Netzes. Wir überlegen uns auch, wie wir es absichern können. Ist das Netz in Betrieb, überwachen wir es natürlich. So können wir Störungen und Anomalien erkennen. Wir schützen Benutzer etwa acht Millionen Mal pro Monat vor dem Aufruf schädlicher Websites. Wenn wir feststellen, dass ein Kundenrechner wegen einer Malware beispielsweise Spam verschickt, weisen wir den Benutzer darauf hin und nehmen den Rechner in Quarantäne.

Bei Swisscom sind IT-Security-Profis am Werk. Aber was können Benutzer selbst unternehmen?
Wichtig ist, an die Sicherheit der Computer und Smartphones zu denken. Also alle Updates installieren, sichere Passwörter verwenden und zu Hause eine Firewall nutzen. Beim Surfen im Internet wachsam sein und in Mails nicht sorglos auf eingefügte Links klicken. Ein Problem sind die günstigen Router und Überwachungskameras. Sie sind oft ungenügend geschützt und leicht angreifbar. Auch hier sollten die Benutzer die Standard-Passwörter ändern und regelmässig Updates installieren.

Philippe Vuilleumier
Chief Security Officer
bei Swisscom