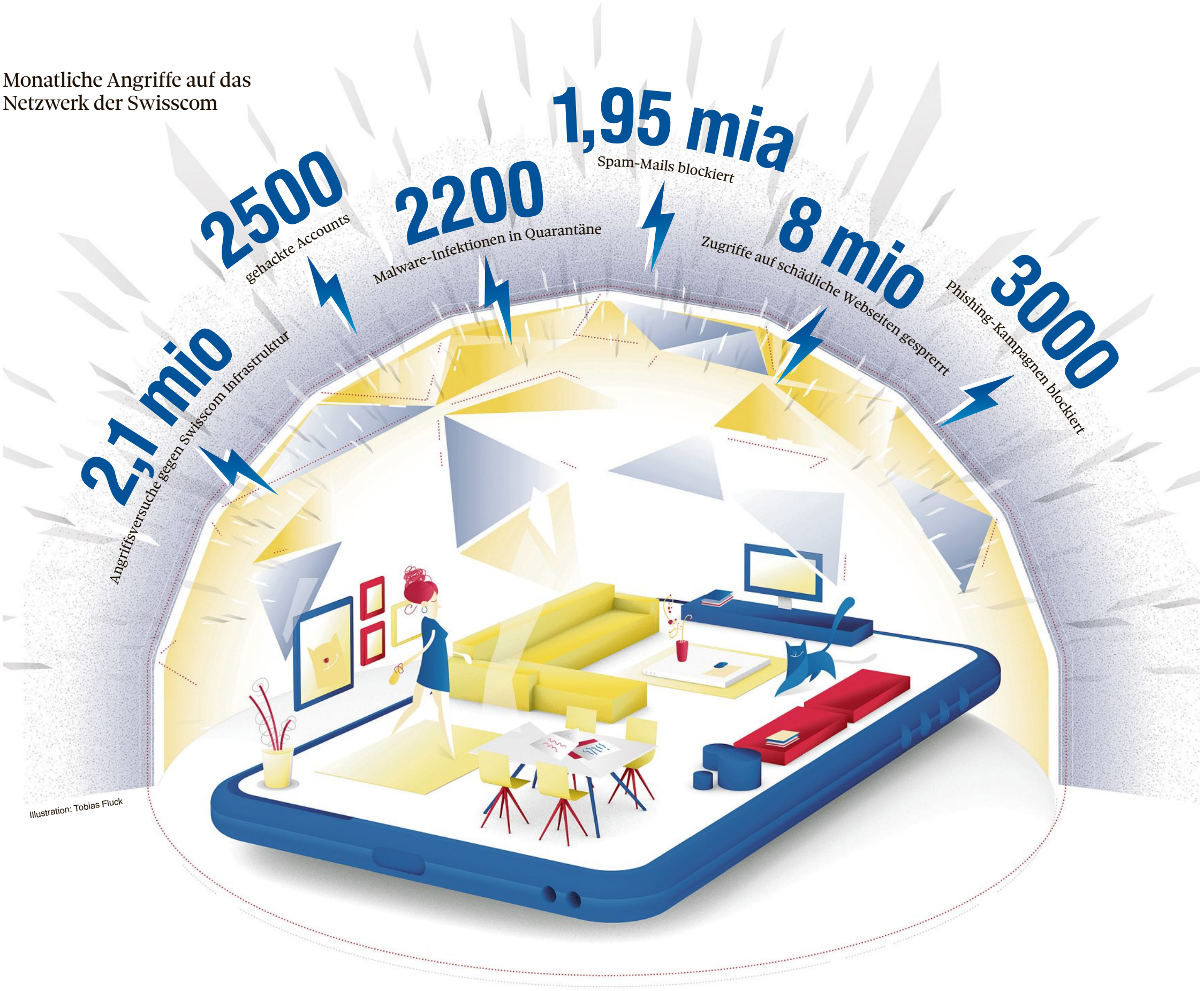
Sponsored

Fünf gefährliche Irrtümer im Netz

Daten schützen Hinter den Kulissen des Internets tobt ein komplexer Kampf. Die Angriffe sind so breit gestreut, dass sie im Prinzip jeden treffen können. Auch weil sich eine ganze Reihe von Irrtümern hartnäckig hält.



Irrtum Nr. 1: «Phishing-Mails erkenne ich an den Rechtschreibfehlern.»

Viele Phishing-Mails sind nicht nur inhaltlich, sondern auch sprachlich auffällig. Trotzdem bleiben sie der bevorzugte Weg, einen Computer mit Malware zu verseuchen. Ausserdem gibt es durchaus raffinierte Versuche von Cyberkriminellen, den Empfänger dazu zu verleiten, sowohl das Mail als auch den verseuchten Anhang zu öffnen. Zu den Tricks gehört es beispielsweise, Mails mit der Absenderadresse eines Bekannten zu verschicken.

Alleine Swisscom filtert laut Sicherheitschef Philippe Vuilleumier täglich 65 Millionen Spam-Mails aus. Doch es gibt eine technische Grauzone, in der sich legitime E-Mails kaum von Spam unterscheiden lassen. Diese digitale Post schlüpft durch die Maschen der Filter und landet im Posteingang. Oft erreichen Cyberkriminelle ihr Ziel: «Wir stellen monatlich rund 2200 Rechner in Quarantäne, die wegen Malware-Aktivitäten aufgefallen sind», erklärt Vuilleumier.

Irrtum Nr. 2: «Ich bin für Cyberkriminelle nicht interessant.»

Weil ein Grossteil der Phishing-Angriffe so breit gestreut ist, können sie im Prinzip jede beliebige Person treffen. Der Inhalt der Mails ist vielfältig: vorgegaukelte Probleme mit dem Bankkonto, unerwünschte Newsletter, Rechnungen, in denen sich Malware versteckt. Eine schwerwiegende Form des Cyberangriffs ist der Identitätsklau. Zum Beispiel der Einbruch in fremde Facebook-Konten. Man denke nur an die Bekannten, die auf diese Weise gehackt wurden und betonen, man solle ja nicht auf den Link klicken, den der Hacker in ihrem Namen verschickt hat. Die Möglichkeit des Zugriffs auf Online-Konten, den Computer oder Geld machen so ziemlich jede Person interessant als Ziel für Cyberangriffe. Bei Smartphones präsentiert sich die Bedrohungslage anders als bei Computern. So haben in letzter Zeit immer wieder Apps die Runde gemacht, die neben dem eigentlichen Zweck – beispielsweise Fotos mit Filtern aufzuhübschen – im Hintergrund heimlich Benutzerdaten und das Adressbuch an den App-Anbieter senden. Vor solchen Apps kann man sich bis zu einem gewissen Grad schützen – indem man nur Apps aus den offiziellen App Stores von Apple und Google installiert und immer die aktuellen System- und Sicherheits-Updates installiert. So schliesst man Sicherheitslücken, die Angreifer ausnutzen könnten.

> Phishing-Angriffe können jede und jeden treffen.

Irrtum Nr. 3: «Öffentliches WLAN ist praktisch.»

Praktisch ja. Aber sicher? Fast jedes Café und Restaurant bietet heutzutage Free Wifi an. Das Problem dabei: Man kann nicht überprüfen, wie sicher der Zugang ist und ob nicht jemand heimlich die Kommunikation mitliest. Das muss nicht einmal ein Angreifer von aussen sein. Vielleicht ist es ja der sympathische Herr am Nebentisch. Sicherer ist, zusätzlich mit einer VPN-App (Virtual Private Network) die Kommunikation abzusichern oder das Smartphone als Hotspot zu verwenden.

Irrtum Nr. 4: «Mit einem guten Passwort kann mir nichts passieren»

Grundsätzlich ist ein langes Passwort, das auch noch mit Zahlen und Sonderzeichen gespickt ist, schwer zu knacken. Immer wieder gelingt es gewieften Cyberkriminellen aber, bei Einbrüchen in Systeme Millionen von Benutzerdaten inklusive Passwörter zu erbeuten. Das jüngste Beispiel sind die sogenannten Collections 1-5. Sie enthalten rund 2,2 Milliarden Zugangsdaten, also eine Kombination aus E-Mail-Adresse und Passwort. Darunter befinden sich auch rund drei Millionen Schweizer E-Mail-Adressen, wie das Schweizer Fernsehen recherchiert hat. Sobald ein Passwort in einer Leak-Datenbank auftaucht, nutzen Kriminelle es für Angriffe.

Irrtum Nr. 5: «Wenn ich Computer und Smartphone schütze, bin ich auf der sicheren Seite.»

Viele Geräte in einem Haushalt sind mit dem Internet verbunden. Der PC, die diversen Notebooks der Familienmitglieder, die Smartphones. Und was ist mit dem neuen, intelligenten TV? Den smarten Lautsprechern? Die Zahl der vernetzten Geräte im Haushalt nimmt zu – und damit auch das Sicherheitsrisiko. Denn insbesondere günstige Netzwerkgeräte sind oft schlecht gesichert. Die Grundregel lautet also: Wenn etwas vernetzt ist, braucht es auch einen vernünftigen Schutz.

swisscom