Persönlich

Was zeigt Ihr erstes Handyfoto?

Die Sommerferienzeit ist angebrochen, zu tausenden zieht es uns in den nächsten Wochen an die entlegensten Ecken der Welt oder einfach ein paar Kilometer weiter als das vertraute Daheim. Doch egal, ob feinster Sandstrand in der Karibik, Party auf einer Mittelmeerinsel oder Ausspannen in der kühleren Schweizer Bergwelt – das Handy ist immer mit dabei. Und damit auch die Fotokamera.

Um seinen Liebsten daheim oder seinen Bekannten einen Hauch von Feriengefühl zu vermitteln – (oder, um sie vielleicht neidisch zu machen?) – knipst man alles Mögliche, was einem vor die Linse kommt. Der Cocktail an der Poolbar, das skurrile Häuschen auf dem Ausflug in ein landestypisches Dorf oder der eindrückliche Sonnenuntergang am Meer. Auf WhatsApp, Facebook, Instagram, Snapchat und Konsorten werden die Eindrücke fast im Stundenrhythmus hochgeladen. Und gleichzeitig steigt die Zahl der gespeicherten Fotos auf dem Handy an.

Bei mir sind es diese Woche schon 19 784 Fotos, die sich angesammelt haben. Doch wann habe ich eigentlich das erste Handyfoto geschossen und mit welchem Motiv? Also rasch das iPhone zücken und ganz weit zurück in die Vergangenheit. Die Auflösung: Mein erstes Foto datiert vom 8. Dezember 2008 und ist kein Ferienfoto. Es zeigt ganz banal eine unserer damaligen Katzen. Sie lebt übrigens heute noch. Vielleicht lichte ich sie heute Abend wieder einmal ab. So viel Speicherplatz muss dann doch sein.

Marc Ribolla
marc.ribolla@chmedia.ch

Apropos

Hawaii statt Davos

Sie gehören zu den Evergreens: Artikel über die Ferienpläne von Regierungsrätinnen und Regierungsräten. Gerne will man als einfacher Bürger wissen, was sie an freien Tagen machen, wie gross ihr Fernweh ist. Zumal die Ergebnisse oft tief blicken lassen. Während beispielsweise die meisten Luzerner Regierungsräte die letzten Sommer zu Hause in den Schweizer Bergen verbrachten, gibt es auch in der Aargauer Exekutive leidenschaftliche Wanderer.

Anders die St. Galler Regierung. Zwei von sieben Mitgliedern sind in diesem Sommer tagelang mit dem Velo unterwegs. Drei fliegen gar auf andere Kontinente. Stefan Kölliker (SVP) nach Florida, SP-Kulturministerin Laura Bucher nach Hawaii. Mit der wieder sinkenden Flugscham liegen sie voll im Nach-Corona-Trend. Und angesichts der exotischen Ferienorte und der Wahl ihrer Fortbewegungsmittel (Velo statt zu Fuss) bestätigt sich nur, was wir als Lokalpatrioten schon immer ahnten: Die St. Galler Exekutive ist die weltoffenste und schnellste von allen Kantonsregierungen.

Jürg Ackermann

Das sicherste Internet wird kaum genutzt

Nachrichten über Hackerangriffe reissen nicht ab. Dabei gäbe es eine neue Technologie, die Angreifer besser fernhält. Entwickelt hat diese ein ETH-Professor, durchgesetzt hat sie die Schweizerische Nationalbank zusammen mit den Telekom-Anbietern. Doch die weitere Verbreitung stockt.

Anna Wanner

Die Angriffe auf Unternehmen, nationale Institutionen und kritische Infrastrukturen häufen sich: Anfang Februar attackierte eine Ransomware-Gruppe die Universität Zürich, wenig später vermeldeten die SBB einen Cyberangriff, auch Gemeinden verzeichnen seit einem Jahr deutlich mehr Angriffe auf ihre Systeme. Zuletzt gehörten auch Kantone, das nationale Parlament und die Bundesverwaltung zu den Opfern von Cyberattacken.

So griffen russische Hacker mehrere Websites der Bundesverwaltung an – drei Tage vor der Rede des ukrainischen Präsidenten Wolodimir Selenski vor der Bundesversammlung. Gemäss Angaben des Nationalen Zentrums für Cybersicherheit (NCSC) galt der Angriff der ganzen Bundesverwaltung: Die Websites waren nicht mehr erreichbar, Anwendungen des Bundes nicht mehr verfügbar. DDoS-Angriffe (Distributed Denial of Service) auf die Informatiksysteme der Verwaltung legten die Systeme lahm.

Letzte Woche wurde das Ausmass des Lecks publik, welches ein Ransomware-Angriff auf die IT-Firma Xplain in Interlaken hatte: Baupläne von Polizei- und Armeesystemen, Adressen und Sicherheitsdaten von Bundesräten sowie Informationen über den Schutz von hiesigen Botschaften stellte die Hackerbande Play ins Netz.

Die Art der Attacken unterscheiden sich zwar. Unbestritten aber ist: Der Schaden ist einerseits finanziell gross und andererseits unterminieren die Angriffe das Vertrauen in die Behörden.

Bis zu 250 Milliarden Franken für Cybersicherheit

Die Schweiz ist nicht alleine. Weltweit wächst die Schadensbilanz in schnellen Schritten. Denn die Digitalisierung der Wirtschaft schreitet voran und damit auch die Interaktionen im Internet. Den Hackern bietet sich mehr Angriffsfläche. Die Unternehmensberater von McKinsey schätzen, dass der Schaden weltweit bis 2025 auf 10,5 Billionen Dollar pro Jahr wächst, also fast 10 000 000 000 000 Franken. Das sind drei Mal mehr als noch 2015.

Damit steigt auch das Bedürfnis nach Sicherheit. Private, Unternehmen und Behörden wenden jedes Jahr mehr Geld auf, um sich, ihre Daten, Systeme sowie Dienstleistungen zu schützen. Je nach Schätzung werden weltweit 150 bis 250 Milliarden Dollar pro Jahr in die Cybersicherheit gesteckt – bei einer jährlichen Wachstumsrate von über 12 Prozent. Grössere Unternehmen, die über höchst sensible Daten verfügen und kritische Dienstleistungen anbieten, schützen sich meist aufwendig.

Das Paradebeispiel dafür sind Geldtransfers der hiesigen Banken. Die Schweizerische Nationalbank (SNB) muss sicherstellen, dass die Transfers zwischen den Geldinstituten funktionieren, sie ist verantwortlich für das sogenannte Swiss Interbank Clearingsystem (SIC). 2022 wurden pro Tag im Mittel rund 3,7 Millionen Zahlungen im Wert von 200 Milliarden Franken über dieses System abgewickelt. An Spitzentagen können es über 12 Millionen täglich sein – mit Umsätzen von bis zu 403 Milliarden Franken.

Unvorstellbar, was passieren würde, wenn Überweisungen nicht übermittelt werden könnten und somit nicht mehr beim Adressaten ankommen. Unvorstellbar auch das Chaos, wenn das private Konto plötzlich und für längere Zeit nicht mehr zugänglich ist. Wer verfügt heute noch über genügend Bargeld, um sich mehrere Tage versorgen zu können?

Der Schweizer Bankenplatz als Wegbereiter

Um das Zahlungssystem vor Angriffen zu schützen und die Transaktionen ohne grössere Unterbrüche sicherzustellen, mieten die SNB sowie alle SIC-Teilnehmer Punkt-zu-Punkt-Verbindungen zum zentralen SIC-System. Über solche privaten Linien kommunizieren auch Militärs oder Nachrichtendienste, um Zugriffe von aussen auszuschliessen.

Die Verbindungen der Banken sind so zwar sicher, aber vergleichsweise wenig resilient: Fällt eine Netzwerkverbindung aus, dauert es bis zu drei Minuten für die Umschaltung auf eine alternative Verbindung. In Zeiten, da Kunden in Sekundenschnelle ihre Ware zahlen oder auch Geld erhalten wollen, ist Geschwindigkeit auch eine Sicherheitsfrage.

Die SNB zeigte sich offen und interessiert an neuer Technologie, die zukunftsfähig und mindestens genauso sicher wie das bisherige Verfahren ist. Das von der ETH Zürich unter Professor Adrian Perrig entwickelte SCION-Protokoll entspricht den strengen Kriterien, weil es eine wesentlich erhöhte Sicherheit und weitere wünschenswerte Eigenschaften verspricht (siehe Box). So beschränkt das geschlossene Netzwerk die Teilnahme auf einen Teilnehmerkreis aus der Finanzbranche und kann die Teilnehmer vor bestimmten Attacken wie DDoS, BGP-Hacking oder Re-Routing schützen.

Zusammen mit dem Finanzdienstleister SIX, welcher die Infrastruktur für den Schweizer Finanzplatz zur Verfügung stellt, entwickelte die Nationalbank das Projekt des Secure Swiss Finance Network (SSFN), über welches in Zukunft der Schweizer Finanzplatz grossmehrheitlich kommunizieren wird. Aktuell findet die Ablösung vom bestehenden Netzwerk bis Ende September 2024 statt.

Für das Projekt haben sich die Betreiber Swisscom, Sunrise und Switch mit ihren Netzwerken zusammengeschlossen, um einen neuen Sicherheitsstandard zu erstellen, eine wesentlich erhöhte Resilienz und Ausfallsicherheit. So ist beim Ausfall eines Providers die laufende Kommunikation nicht tangiert und der Kunde – beispielsweise eine Bank – bemerkt die Störung nicht.

Ein weiterer Vorteil der neuen Technologie gegenüber dem allseits zugänglichen Internet liegt laut SNB-Vertreter Sébastien Kraenzlin, Leiter operatives Bankgeschäft, auch darin, dass nur jene Finanzmarktteilnehmer und -dienstleister, die den strengen Zulassungsvorschriften zum SSFN entsprechen, daran teilnehmen können. Damit sei das Risiko für Angriffe von aussen auf das Netzwerk quasi eliminiert. «Jedoch müssen die Finanzmarktteilnehmer ihre eigenen Infrastrukturen weiterhin selbst schützen.» Das sichere Netzwerk schützt die Kommunikation und nicht den gesamten Betrieb.

Eine namhafte Bank wird täglich 80 000 Mal angegriffen

Konkret zeigen Messungen von Anapaya, dem ETH-Spinoff von Perrig und dem Vertreiber der SCION-Router-Technologie, eindrücklich, wie Netzwerke durch den Einsatz der neuen Technologie geschützt sind. Die Firma hat die Angriffe auf eine grössere Schweizer Bank im letzten Quartal 2022 gemessen und zählte 80 000 Versuche jeden Tag, über das Netzwerk ins System der Bank einzudringen. Davon sind 1000 Angriffe gezielt, also bösartig, sogenannte code injection attempts. «Mit der Umstellung auf die SCION-Technologie rechneten wir schon mit einer massiven Reduktion der messbaren Attacken», sagt Anapaya-CEO Martin Bosshardt zu den Tests. Das Resultat verblüffte gar die Entwickler: «Es gab keine einzige Attacke mehr, die über das SCION-Netzwerk erfolgte und von den Firewalls hätte geblockt werden müssen. Von den rund 1000 bösartigen Angriffen pro Tag sank die Zahl auf Null.»

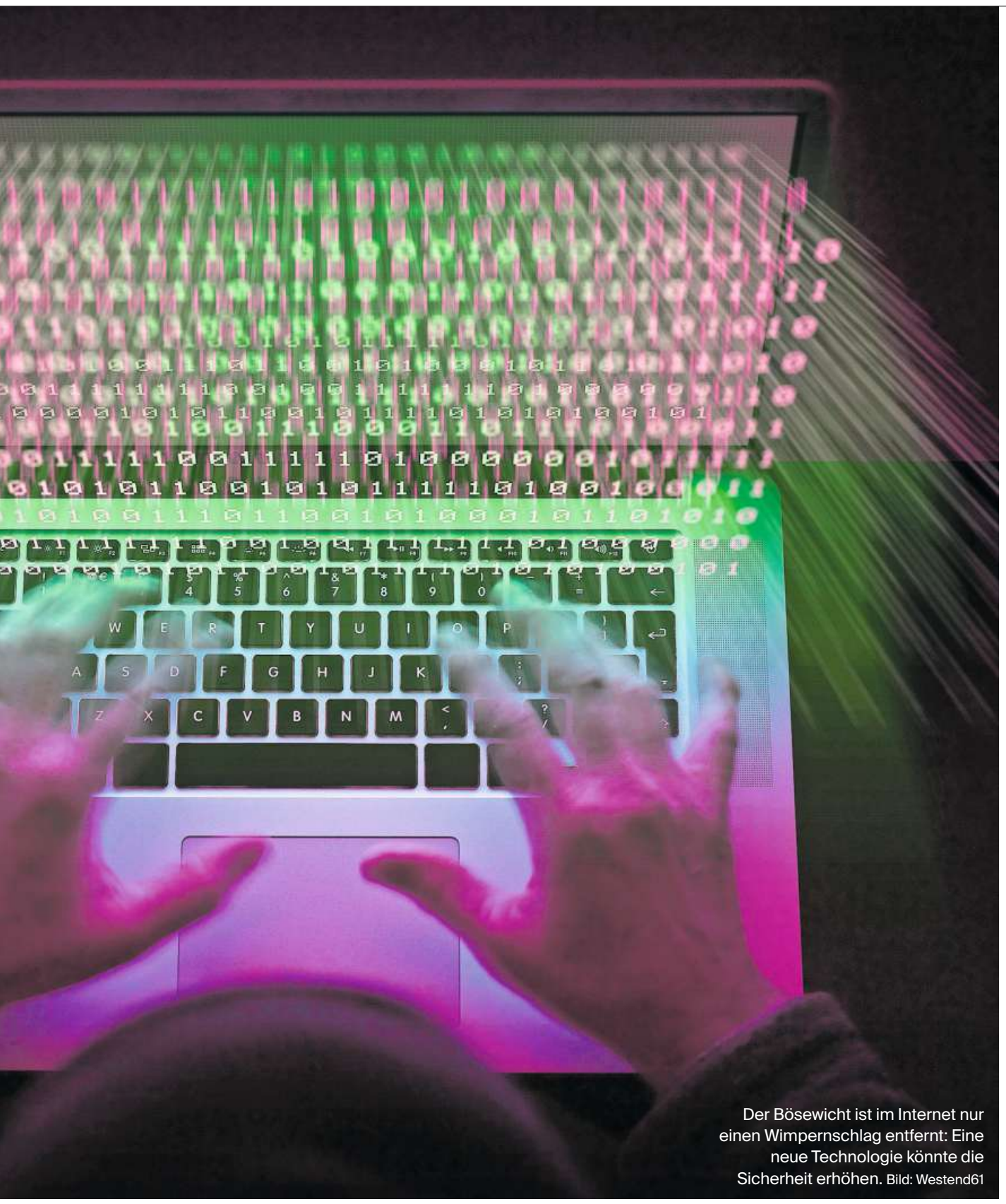
Einzig Fehlermeldungen, etwa falsch eingegebene Passwörter, erscheinen noch in der Statistik. Doch Angriffe, die einen Schaden hätten anrichten können, wenn der Zugang zum System nicht gut gewartet und gesichert ist, gab es keine mehr.

Der Grund für die erhöhte Sicherheit ist eine direkte Folge der Technologie, welche die Daten nur über vertrauenswürdige Router leitet: Für Aussenstehende, also Attacker oder deren Bots (Programme, die nach Schlupflöchern suchen), ist das Netzwerk sowie dessen Teilnehmer gar nicht mehr erkennbar, also nicht mehr sichtbar, wie Martin Bosshardt erklärt. Entscheidet also ein Netzwerkteilnehmer, dass er nur andere Teilnehmer aus der Schweiz als vertrauenswürdig erachtet, erscheinen sein Anschluss und seine im Netzwerk angebotenen Dienste für Anwender im Ausland nicht.

Und daraus leitet sich der grösste Sicherheitsvorteil ab: In der Regel verschaffen sich Kriminelle über gestohle-

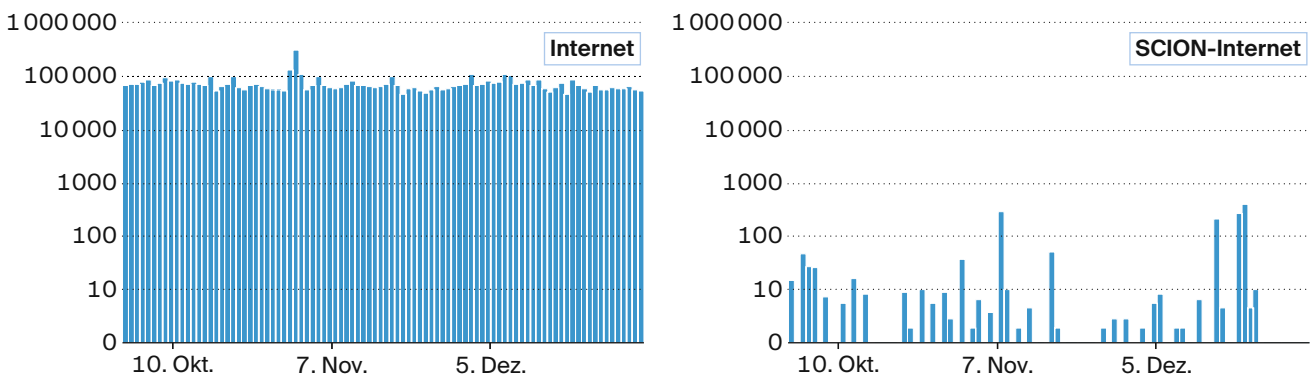
So funktioniert das SCION-Protokoll

Die Kommunikation übers Internet, der Austausch von kritischen Inhalten, kann heute nur mit viel Aufwand geschützt werden, weil weder Absender noch Empfänger kontrollieren können, wo ihre Daten durchgehen. Die SCION-Technologie steuert diesen Verkehr. Der Kunde bestimmt, welche Verbindung vertrauenswürdig ist und wo die Informationen durchgehen – und schliesst so potenzielle Angreifer aus.

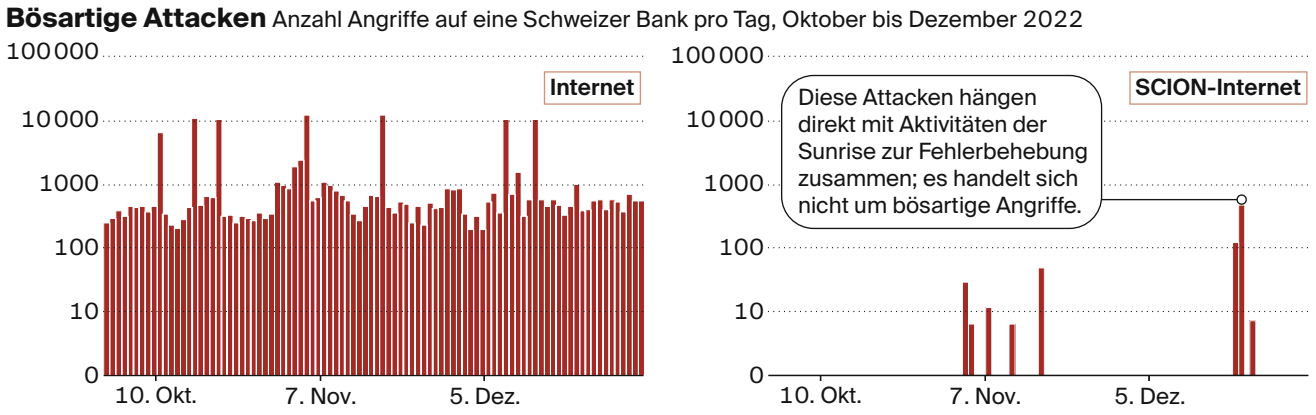


Der Bösewicht ist im Internet nur einen Wimpernschlag entfernt: Eine neue Technologie könnte die Sicherheit erhöhen. Bild: Westend61

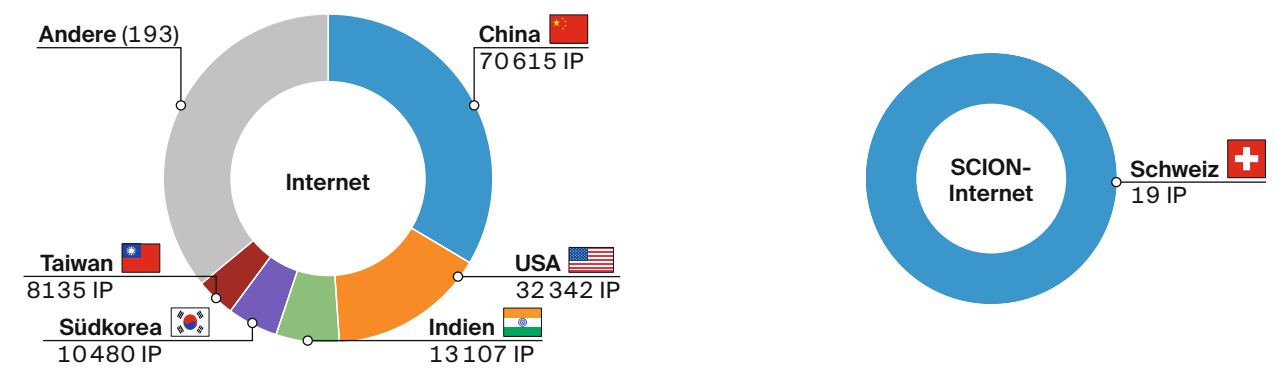
Unspezifische Attacken Anzahl Angriffe auf eine Schweizer Bank pro Tag, Oktober bis Dezember 2022



Bösartige Attacken Anzahl Angriffe auf eine Schweizer Bank pro Tag, Oktober bis Dezember 2022



Herkunftsländer der Hacker Auswertung der Angriffe Oktober bis Dezember 2022 für einen Tag



Quelle: Namhafte Schweizer Bank (CH Media bekannt)/Grafik: let

ne Passwörter und Logins Zugang zu Geschäftsnetzwerken oder auch zu privaten Computern. Wenn nun ein System gar nicht auffindbar ist, dann bringen dem Hacker auch die Logins, Passwörter und Zertifikate nichts, weil er das System nicht mehr erreichen kann. Martin Bosshardt spricht von einem «Riesenschritt in der Sicherheit», weil der einzelne Teilnehmer nun definieren kann, wer ihn selbst theoretisch überhaupt noch angreifen kann.

Der Vorteil bei der Anwendung der SCION-Technologie in der Schweiz: Indem Attacken aus dem Ausland verhindert werden können, bleiben den Cyberkriminellen nur noch Angriffsmöglichkeiten aus der Schweiz. Doch hier kontrollieren die Internetprovider Swisscom, Sunrise, Switch und Co. den Datenverkehr. Das heisst, die Adressen der Nutzer sind alle rückverfolgbar und identifizierbar. Das wiederum bedeutet eine grosse Hilfe für die Strafverfolgung, welche die Kriminellen besser auffinden kann.

Eine weitere Statistik von Anapaya zeigt, woher die Angreifer kommen. Die Firma hat die Herkunftsländer der insgesamt fast sieben Millionen Angriffe in nur drei Monaten auf die erwähnte Schweizer Bank ausgewertet: Der Grossteil der Angriffe stammte aus China. Die zweitmeisten Angriffe kommen aus den USA – aus den grossen Cloud-Providern, die Anonymität bieten.

In solchen Fällen ist die Identifikation der Täter so gut wie unmöglich. Auch weil sie teilweise von den Herkunftsstaaten gedeckt werden.

Auch die Bundesverwaltung testet die Technologie

Wieso ist diese Technologie also (noch) nicht weiter verbreitet? Einerseits ist die Gefahr wenig sichtbar: Weil Cyberangriffe in der Schweiz nicht generell meldepflichtig sind, lässt sich das Ausmass der Schäden nur schwer beziffern. So gelangen grosse Angriffe wie bei den SBB nur an die Öffentlichkeit, wenn sich Störungen bemerkbar machen – oder wenn gestohlene Daten veröffentlicht werden.

Weiter ist die Technologie noch wenig bekannt und trifft auf eine grosse Portion Skepsis, wie Martin Bosshardt feststellt. Doch die Cyber-Angriffe nehmen zu – auch auf die Homeoffice-Konten der Unternehmen. Dank dem Verbund Schweizer Internetprovider zur Umsetzung der neuen Technologie könnten globale Angriffe auf wichtige Systeme unterbunden werden. Die SNB hat beispielsweise ihre Homeoffice-Zugänge für die Mitarbeitenden mittlerweile auch grösstenteils über SCION abgesichert.

Unbekannt ist die Technologie aber nicht: Florian Schütz, Delegierter des Bundes für Cybersicherheit, bestätigt auf Anfrage mehrere Testversuche. So band das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) 2019 als Pilotversuch die Schweizer Botschaft in Deutschland über die SCION-Technologie an. Einen zweiten Pilotversuch startete das EDA 2021 mit der Anbindung der Botschaft in Südkorea und der Verbindung mit der demilitarisierten Zone an der Grenze zu Nordkorea.

Auch die Armee und das Nationale Zentrum für Cybersicherheit (NCSC) testeten die Technologie. Der Cyber-Defence-Campus von Armasuisse betreibt seit 2022 eine permanente SCION-Netzwerktest-Infrastruktur zur Verbindung seiner Standorte in Zürich, Lausanne und Thun. Diese Testinfrastruktur dient zur Forschung und Innovation und wird aktuell mit einem zusätzlichen SCION-Knoten in Estland am Exzellenzzentrum der Nato für Cyberabwehr erweitert, um 5G-Netze über SCION zu testen.

Ob und wann diese auch in anderen Bereichen angewandt werden kann, sei noch offen, sagt Florian Schütz. «Die Technologie ist interessant, bedeutet jedoch nicht die ultimative Sicherheit.» So seien die schützenswerten Systeme nie ganz isoliert. «Es gibt immer einen Eingang», erklärt Schütz. Die Technologie verkleinere aber die Angriffsfläche.

Gewisse Cyberattacken seien auch über andere Massnahmen in den Griff zu bekommen. Beispielsweise könnten DDoS-Attacken über mehr Leistung, also breitere Volumen bei der Verbindung, verhindert werden. Das sei letztlich aber eine Kostenfrage. «So ist der Risiko-Appetit für jedes Unternehmen steuerbar», sagt Schütz.

Ein gigantischer Vorteil für die Sicherheit der Schweiz

Dass die SCION-Technologie alle Probleme der Cyberkriminalität lösen kann, wird nicht postuliert. «Die granulare Kontrolle über die eigene Angriffsoberfläche ist ein fundamentaler Unterschied, was die Sicherheit angeht. Genügend Druck für eine DDoS-Attacke aufzubauen, ist mit SCION schlicht nicht möglich. Damit sind dann auch keine kostspieligen, laufend wachsenden Abwehrbandbreiten mehr notwendig», sagt Martin Bosshardt und präzisiert: «Zudem sind anonyme Angriffe über juristische Grenzen hinweg nicht mehr einfach technisch gegeben. Solche Risiken können ausgeschaltet oder dann gezielt eingegangen werden.»

Der Anapaya-CEO spricht von einer «sicheren Kommunikation», im Unterschied zu «sicheren Zugängen». Das bedeutet, gängige Sicherheitsanwendungen wie Firewalls, Virenschutz und Verschlüsselung von Informationen braucht es nach wie vor.

Martin Bosshardt ist sich denn auch bewusst: «Es braucht noch viel Energie und einen langen Atem, um die SCION-Technologie weiter zur Anwendung zu bringen.» Auch für die Zusammenarbeit mit der SNB musste sich der Anapaya-CEO gedulden.

«Die SNB agiert bei Sicherheitsfragen höchst konservativ», erklärt Sébastien Kraenzlin die lange Testphase. Dass die neue Technologie dereinst angewandt würde, war keineswegs klar. «Wir haben sie zwei Jahre lang auf Herz und Nieren geprüft.»

Der Entscheid der SNB, die Technologie für den Bankenplatz Schweiz anzuwenden, gleicht darum einem Ritterschlag: Die Technologie muss die höchsten Sicherheitsanforderungen erfüllen. Gleichzeitig ermöglichte die SNB die Ausbreitung von SCION-Verbindungen in der ganzen Schweiz, indem sie die ansässigen Internetprovider vom Projekt überzeugen konnte, wie Sébastien Kraenzlin sagt.

Swisscom, Sunrise und Co. haben Millionen in die Technologie investiert. Der SNB-Vertreter sieht für das Land darum ein grosses Momentum: «Der Finanzplatz mit seinen höchsten Sicherheitsanforderungen hat den Anfang gemacht. Jetzt hoffen wir, dass auch weitere Institutionen, Firmen und Behörden auf die SCION-Technologie setzen und damit einen neuen Sicherheitsstandard in der Kommunikation schaffen.»

Der Grundstein ist gelegt, bereits heute können Interessierte einen SCION-Zugang bei den Telekom-Providern bestellen und mit dem Einsatz der notwendigen Soft- und Hardware über ein sichereres Netzwerk (Swiss ISD) verbinden. Daraus erwächst dem Land ein gigantischer Vorteil, weil wichtige Systeme im «White Net» der SCION-Technologie sicherer sind: Dazu gehören nicht nur die Dienste des Finanzplatzes, sondern auch die Spitalversorgung sowie die öffentlichen Infrastrukturen – etwa der Schienenverkehr oder die Energieversorgung.

Die Telekomanbieter sehen ebenfalls eine grosse Chance, sie haben investiert. Die grosse Frage ist, sieht sie auch die Schweiz?