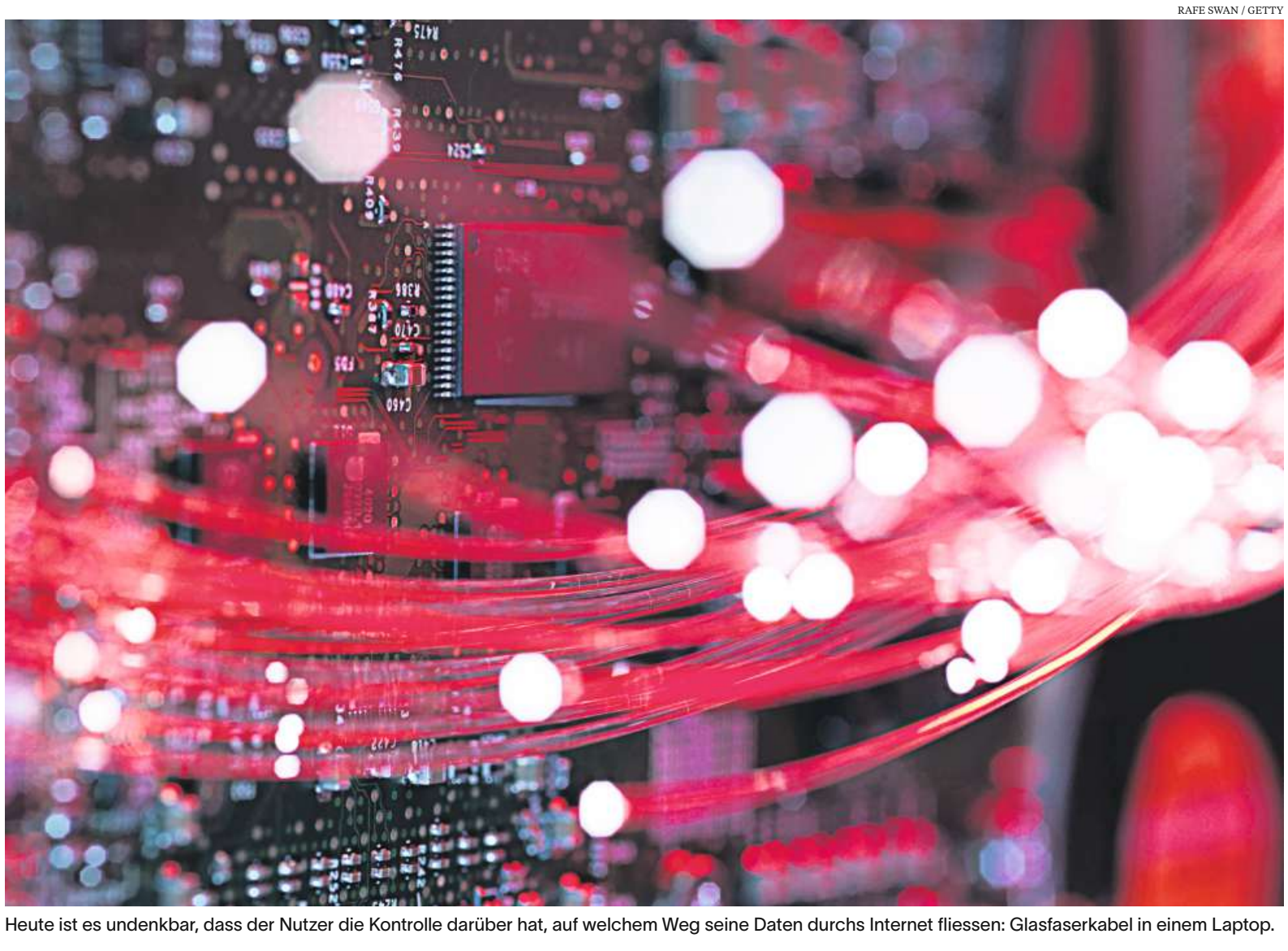
Es gibt ein besseres Internet

Internetanbieter schauen vor allem aufs Geld, wenn sie sich unsere Daten weiterreichen. Dafür muss der Nutzer ein langsameres, weniger sicheres Internet hinnehmen. Ein ETH-Professor will das ändern. **Von Leonid Leiva Ariosa**

RAFE SWAN / GETTY



Heute ist es undenkbar, dass der Nutzer die Kontrolle darüber hat, auf welchem Weg seine Daten durchs Internet fliessen: Glasfaserkabel in einem Laptop.

Ein Geburtstagskalender hängt im Wartezimmer vor Adrian Perrigs Büro an der ETH Zürich. Darauf sind aber nur einzelne Daten zu sehen, keine Namen. Für einen der wichtigsten Cybersicherheitsforscher der Welt reicht das als Erinnerung: Heute hat ein Kollege Geburtstag. Einem Aussenseiter bleiben die Details jedoch verborgen. Dem Besucher wird klar: In Sachen Datenschutz überlässt Perrig nichts dem Zufall.

Perrigs grösste Passion ist, die Gerüste des Internets nach Schwachstellen abzuklopfen. Mit seinem Wissen hätte er bereits als Teenager zum sagenumwobenen Hacker im schwarzen Kapuzenpulli werden können. Doch die Rolle des Türstehers ist ihm lieber. Perrig wirkt bescheiden, fast schüchtern. Kaum etwas in seinem Auftreten lässt erahnen, dass er dabei ist, ein besseres Internet in die Welt zu setzen. Aber seit 2009 tut der ETH-Professor genau das. Sein Ziel ist, den Bauplan für ein möglichst einbruchsicheres Internet zu zeichnen. Auf dem Reissbrett ist seine Arbeit grösstenteils fertig. Nun steht der Praxistest an.

Perrig ist der Erfinder von Scion, einer Netzwerkarchitektur, mit der bereits heute Banken, Stromversorger und Spitäler in geschlossenen Netzwerken geschützt Daten austauschen. Auch die Schweizer Regierung sieht darin eine vielversprechende Technologie. Und jetzt beginnen globale Internetanbieter, Scion auch für den Massenmarkt zugänglich zu machen. Damit bekommt das heutige Internet mehr als dreissig Jahre nach seiner Erfindung zum ersten Mal ernstzunehmende Konkurrenz.

Vom Krypto-Forscher zum Internetverbesserer

«Am Anfang wollte ich einfach ein besseres Routing-Protokoll erfinden», sagt Perrig. Das klingt bescheiden, ist es aber nicht. Denn Perrigs Vorhaben würde vieles ermöglichen, was im heutigen Internet undenkbar wäre: nämlich dass der Nutzer die Kontrolle darüber hat, auf welchem Weg seine Daten durchs Internet fliessen. Oder dass die Kommunikation nie ausfällt, weil ein Hacker den Datenverkehr in eine Endlosschleife umleitet. Schon als Gymnasiast macht Perrig Hackern das Leben schwer. Anfang der Neunziger, lange vor der Erfindung von Bitcoin, ist er bereits mit den allerersten Kryptowährungen vertraut. Perrig analysiert, wie sicher dieses frühe digitale Geld wirklich ist, und veröffentlicht sogar eine wissenschaftliche Studie dazu. Da ist er erst zwanzig.

Wenige Jahre später entwickelt er auch ein System für die Authentifizierung von Satelliten. Damit wird heute die Echtheit von Signalen des europäischen Satellitennetzes Galileo sichergestellt. Aber irgendwann hat Perrig nur noch ein Hobby: Er will verstehen, wie Daten im Internet von A nach B kommen. Schon bald fällt ihm auf, dass das gängige Internet-Routing-Protokoll – das Border Gateway Protocol, kurz BGP – erhebliche Schwächen hat. Daten werden von Angreifern auf ihre eigenen Server umgeleitet oder bleiben einfach unterwegs hängen; so finden die Daten oft nicht den Weg zum Empfänger, obwohl eine Route dafür verfügbar wäre – alles wegen Konstruktionsfehlern im BGP-Protokoll.

BGP kommt zum Einsatz, wenn sich Internetanbieter wie Swisscom, Deutsche Telekom oder Sunrise Datenpakete hin und her senden. Das geschieht, wenn Menschen online einkaufen, Videos streamen oder durch soziale Netzwerke scrollen. BGP gibt vor, wie die Datenpakete den Weg zwischen entfernten Servern und unserem Computer finden. Man kann sich das vorstellen, als würden die Daten auf eine Wanderung gehen und bei jeder Weggabelung einem Wegweiser folgen. Das BGP-Protokoll legt die Regeln fest, nach denen die Wegweiser beschriftet werden. Und diese Beschriftung ändert sich ständig, je nachdem, welche Wege gesperrt oder zugänglich sind. Entscheidend sind in den meisten Fällen jedoch die Kosten.

In Wirklichkeit leitet BGP die Daten fast immer an denjenigen Internetanbieter weiter, der den tiefsten Preis verlangt. Wenn wir also etwa in der Schweiz auf dem Smartphone ein Video schauen wollen, das auf einem Server in Deutschland liegt, kann es durchaus sein, dass die entsprechenden Datenpakete erst nach England oder in die USA fliessen und von dort in die Schweiz. Wenn der Umweg unter dem Strich weniger kostet, nimmt der Internetanbieter meist die Verzögerung in Kauf – so ärgerlich das für den Nutzer sein mag. Kritiker nennen BGP deshalb ein «Money Routing Protocol». Hier gehe es primär um die Weiterleitung von Geld, so der Vorwurf.

Das macht das Internet aus Sicht der Nutzer ineffizient. «In vielen Fällen legen die Datenpakete einen um zehn bis zwanzig Prozent längeren Weg zurück, als sie müssten», sagt Perrig.

Auch die Sicherheit leidet: Mit jedem zusätzlichen Anbieter, an den die Datenpakete weitergereicht werden, steigt das Risiko, dass Unbefugte darauf Zugriff bekommen. Und wer den Fluss der Datenpakete beobachtet, kann ohne grossen Aufwand erschreckend viel über unser Online-Verhalten herausfinden. Auch wenn die Daten verschlüsselt sind.

Denn die Metadaten – etwa die Grösse der Datenpakete oder die Zeitabstände zwischen ihnen – sind nicht verschlüsselt. So wird beispielsweise jeder Film als eine einmalige Reihe solcher Datenpakete übermittelt. An den Zeitabständen zwischen aufeinanderfolgenden Paketen allein lässt sich laut Perrig ablesen, welchen Film jemand gerade zu Hause schaut. Wer übers Internet telefoniere, sei auch exponiert, wenn die App nicht durch spezielle Sicherheitsvorkehrungen geschützt sei. «Trotz Verschlüsselung können in solchen Fällen aus den Metadaten Sprache und Geschlecht von Gesprächsteilnehmern sowie rund ein Drittel der gesagten Wörter abgeleitet werden», sagt Perrig.

Perrig könnte sich stundenlang über die Sicherheitslücken im BGP auslassen. Das Protokoll habe sich in den frühen neunziger Jahren gegen bessere Alternativen durchgesetzt, weil seine Entwickler die schnellsten gewesen seien. Als die BGP-Erfinder das Protokoll 1989 bei einem gemeinsamen Mittagessen auf ihren Servietten niederschrieben, sorgt sich niemand um die Datensicherheit im Internet. Rückblickend ist aber klar: Das Internet beruht auf einem Schnellschuss. Und die Folgen reichen bis in die Gegenwart. Perrig versucht jahrelang, die Sicherheitslücken im BGP zu schliessen. Doch mit jeder Lösung entstehen neue Schwachstellen. Rund um das Jahr 2005 begreift er, dass nur ein radikaler Neuentwurf des Internets die Probleme lösen kann. 2009 beginnt er an Scion zu arbeiten.

> Er hätte zum sagenumwobenen Hacker im Kapuzenpulli werden können.

PD

Adrian Perrig, Leiter der Network Security Group am Departement Informatik der ETH Zürich.

Perrig ist zu diesem Zeitpunkt Professor an der amerikanischen Carnegie Mellon University. Woche für Woche hält er mit seinen Studenten Sitzungen ab. Sie brüten über den Problemen des BGP, sammeln Ideen dazu, was ein gutes Protokoll können muss und wie man Hackerangriffe neutralisieren kann. Ein Jahr lang bleibt jeglicher Fortschritt aus. Perrig gibt aber nicht auf. «Ich dachte mir: ‹Wenn wir nur ein Drittel der Probleme lösen können, wäre das schon viel besser als das jetzige Internet.›»

Ein GPS-Gerät für Daten

Doch dann haben die Forscher einen Geistesblitz: Datenpakete sollen nicht mehr unzuverlässigen Wegweisern folgen. Stattdessen schlägt eine Art GPS-Navigationsgerät mehrere Routen vor. Der Nutzer wählt dann seinen bevorzugten Weg aus. Dadurch kann er entscheiden, ob der Pfad die Kosten, die Geschwindigkeit oder die Sicherheit priorisieren soll. Man kann den Datenverkehr beispielsweise auf ein Land beschränken oder bestimmte Länder meiden. Neben der Idee der «GPS-Navigation» baut Perrigs Internet auf sogenannten Isolationsdomänen auf. Diese sind wichtig, um die Schäden von Internetausfällen zu begrenzen.

Das heutige Internet besteht aus vielen Teilnetzwerken. Jede Firma, jeder Internetanbieter kann ein solches Teilnetzwerk verwalten, das mit dem Rest des Internets verbunden ist. Doch diese Selbstverwaltung hat Grenzen. Denn jedes Teilnetzwerk wird durch eine Art Adresse oder Ausweis identifiziert. So kann ein Empfänger den Sender eines Datenpakets verifizieren. Und dieses System ist stark zentralisiert und damit leicht angreifbar. Es gibt nämlich nur fünf regionale Autoritäten, die jeweils als «Passbüro» agieren und die Identitäten der Teilnetzwerke bescheinigen. Und wenn ein Angreifer eines dieser «Passbüros» hackt, kann das die Internetkommunikation der gesamten Region lahmlegen. Ein solcher Angriff hat kürzlich etwa das Netz der Telekomfirma Orange in Spanien unerreichbar gemacht.

Mit Scion kann jedes Teilnetzwerk eine Isolationsdomäne bilden und sein eigenes «Passbüro» bestimmen. Das ist nicht nur für die Verfügbarkeit der Netze relevant. Es bildet auch die Basis für das politisch brisante Thema der Datensouveränität. Für gewisse Daten ist es nämlich wichtig, dass sie stets innerhalb der eigenen Landesgrenzen bleiben. Nur so kann man sicher sein, dass nationale Datenschutzgesetze den Zugriff regeln.

Perrig ist überzeugt, dass Scion ein Game-Changer ist. Scion biete die Garantie, dass Daten immer einen Weg zum Ziel fänden, wenn es einen gebe. Und dass der Nutzer aus mehreren Wegen wählen könne, statt diese Entscheidung dem Internetanbieter zu überlassen. Das sei alles im heutigen Internet gar nicht möglich oder nur sehr schwierig zu erreichen. Aber Perrig gibt auch zu, dass Scion nicht alle Probleme löst: «Wir werden weiterhin Verschlüsselung, Firewalls und Spam-Filter brauchen.» Und Scion könne auch nicht verhindern, dass Apps oder Server infiziert würden und somit ganze Netze lahmlegten.

Von den Vorteilen von Scion sind aber inzwischen auch globale Internetanbieter überzeugt. Zurzeit laufen Gespräche etwa mit British Telecom. Die Firma plant, Scion über die nächsten Jahre als Standard-Dienst in 140 Ländern anzubieten. Die Wette des Türstehers Perrig könnte bald in grossem Stil aufgehen.