"Unsere Systeme sind inhärent unsicher"

«Unsere Systeme sind inhärent unsicher»

In der Theorie könnten Informatiksysteme viel sicherer sein, sagt Kryptologe Ueli Maurer. In der Praxis jedoch sind viele Sicherheitsmängel mit gewachsenen Strukturen und einem staatlichen Interesse an Einsicht zu erklären.

Interview von Jannik Belser

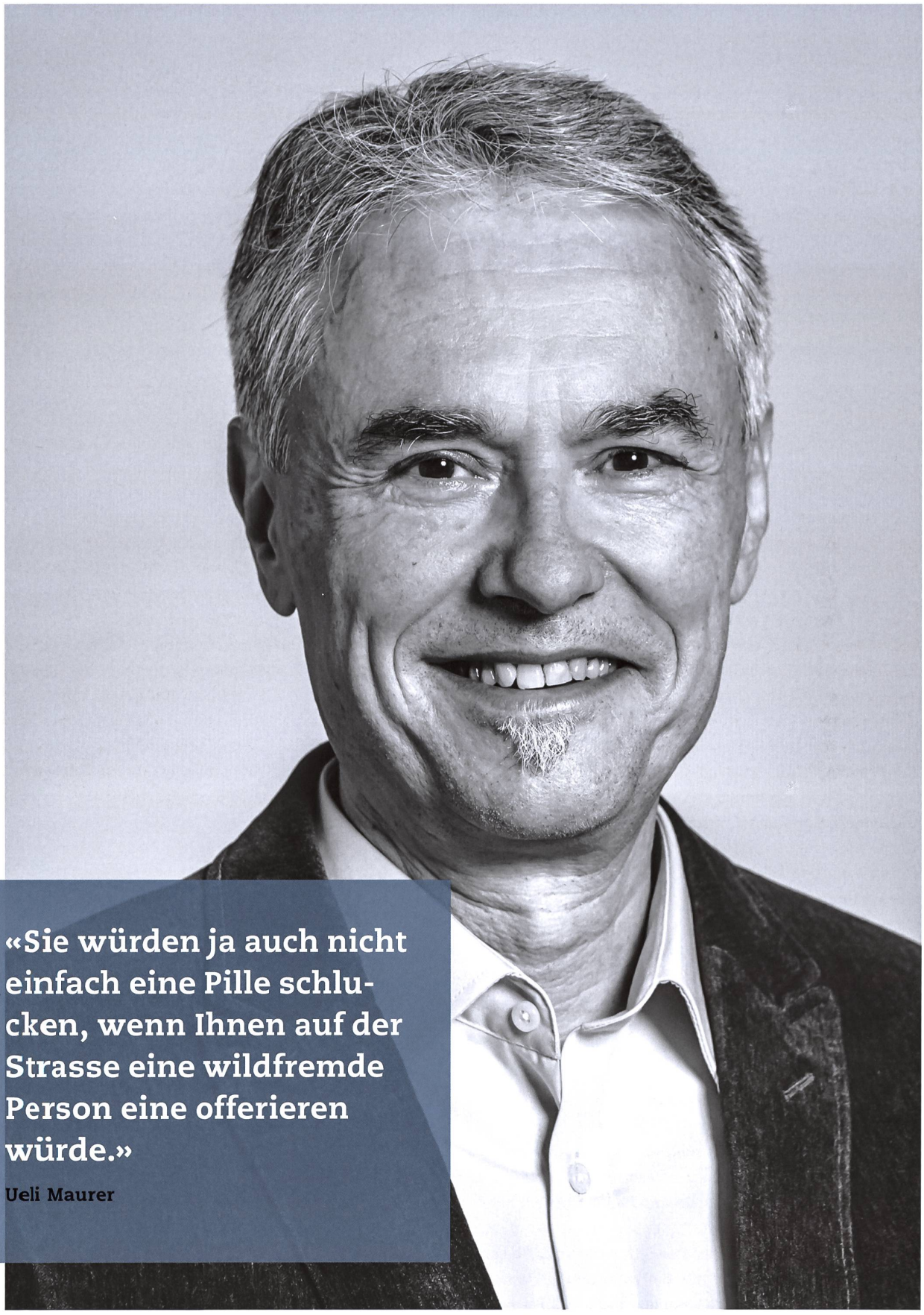
Herr Maurer, immer häufiger werden Privatunternehmen oder Behörden Opfer sogenannter Ransomware. Wie schützt man sich davor?
Indem Sie Ihre Systeme aktuell halten und die offensichtlichen Schwachstellen beheben. Zudem sollen Sie Backups haben. Ein Unternehmen kann sich durchaus auf den Angriffsfall vorbereiten – vielen kleinen und mittelgrossen Unternehmen fehlen jedoch die Ressourcen dazu. Der Staat hat hier sicher die Aufgabe, eine gewisse Unterstützung zu bieten.

Wer steckt hinter diesen Angriffen?
Es ist heutzutage möglich, Kriminalität zu betreiben, ohne sich dabei grossem Risiko auszusetzen, dafür verhaftet zu werden. Staaten wie Russland oder Nordkorea sind in der Internetkriminalität aktiv, für sie können Lösegeldzahlungen lukrative Einnahmequellen sein. Unsere Systeme müssen laufend gepatcht werden, da ist ganz früh in der Entwicklung der Informationstechnologie etwas schiefgelaufen: Unsere Systeme sind inhärent unsicher. Was angegriffen werden kann, wird auch irgendwann angegriffen.

Warum sind unsere Systeme nicht so sicher, wie sie eigentlich sein könnten?
Einerseits gibt es legitime Interessen, dass die Systeme für den einfachen User nicht sicher sind: Beispielsweise kann man so Terroristen einfacher verfolgen. Andererseits könnte die Begründung aber auch ökonomischer Natur sein: Bei den allermeisten Produkten kennen wir eine klare Haftpflicht beim Produzenten. Bei einem Bremsversagen beispielsweise haftet der Autohersteller. Bei Softwarelösungen ist das anders: Selbst die Crypto AG, die bei ihren Chiffriergeräten bewusst eine Möglichkeit zur Manipulation durch den amerikanischen Staat geschaffen hatte, musste nicht für diese Mängel im System haften. In den Anfängen der Informatikentwicklung hätte das auch anders gemacht werden können: Die Juristen hätten sich für eine Haftpflicht und Klagemöglichkeiten bei Fehlern von Softwareprodukten einsetzen können. Hätten sie das gemacht, hätten Technologieunternehmen ganz bestimmt mehr in die Sicherheit ihrer Softwaresysteme investiert. Hätte man Sicherheit wirklich gewollt, hätte man sie auch haben können.

Könnte man das Rad zurückdrehen?
Generell geben wir nicht gerne zu, dass viele Entwicklungen und Innovationen ziemlich chaotisch und willkürlich zustande kommen. Das moderne Internet ist so, weil es halt so gewachsen ist. Das Gleiche gilt für das Rechtssystem und auch für unsere Demokratie. Die Systeme sind mit viel Willkür und ohne einen zentralen Denker und Lenker einfach entstanden. Entwicklungen zurückzurollen, die einmal ihren Lauf genommen haben, ist sehr schwierig. Wir sind uns selber und unseren Schöpfungen gewissermassen ausgeliefert – das gilt auch im Bereich der Technologie.

Was leistet die Kryptografie?
Kryptografie ist viel mehr als Verschlüsselung, sie beschäftigt sich auch mit digitalen Signaturen oder komplexen Protokollen, zum Beispiel mit sogenannten Zero-Knowledge-Beweisen. Kryptografie ist ein Grundelement der digitalen Infrastruktur: Sie erlaubt es, ein virtuelles System



«Sie würden ja auch nicht einfach eine Pille schlucken, wenn Ihnen auf der Strasse eine wildfremde Person eine offerieren würde.»

Ueli Maurer

Ueli Maurer, zvg.

zu konstruieren – damit meine ich ein System, das man nicht zentral programmieren und kontrollieren kann. Ein solches virtuelles System ist dezentral verteilt, es erledigt einfach seinen Job. Denken Sie an Bitcoin, dort wird die Sicherheit im System durch die auf der ganzen Welt verteilten Miners garantiert: Unter der Voraussetzung, dass nicht zu viele aller involvierten Computer korrumpiert sind, kann so sichergestellt werden, dass die Transaktionen korrekt verbucht werden.

Wo werden solche virtuellen Systeme bereits eingesetzt?

Schon die normale Verschlüsselung kann man als die Konstruktion eines sicheren Kommunikationskanals verstehen: Wenn ich etwas verschicke, kann es niemand anderes als der Empfänger lesen, wenn die Nachricht von Ende zu Ende verschlüsselt ist. Das ist ein Paradigmenwechsel in der Art, wie man über IT-Systeme denkt. Nehmen Sie zum Beispiel E-Voting: Im Idealfall haben wir da ein virtuelles System, nicht einen Server in Bern, dem man vertrauen muss. Da kann sich jeder authentisieren und seine Stimme schicken. Das System zählt dann, per Definition, alle Stimmen zusammen und publiziert das Resultat. Wenn wir ein solches System bauen, ist E-Voting auf eine sichere Art möglich.

Wann ist so ein System wirklich sicher?

In der Theorie ist ein absolut sicheres System eines, dessen Sicherheit mathematisch definiert und mathematisch bewiesen wird. Allerdings gilt ein solcher Beweis nur unter bestimmten, klar definierten Annahmen, die sich in der Realität eventuell als falsch herausstellen können. So nimmt man zum Beispiel an, dass auch modernste Computer Millionen Jahre zur Lösung eines bestimmten mathematischen Problems brauchen – in der Realität ist es jedoch nicht ausgeschlossen, dass eine Informatikerin oder ein Mathematiker einen neuen, viel schnelleren Algorithmus entdeckt, der das Problem lösen kann.

«Hätte man Sicherheit wirklich gewollt, hätte man sie auch haben können.»

Ueli Maurer

Worin besteht Ihre Arbeit als Wissenschafter?

Ich versuche Theorien zu entwickeln, mit denen man solche virtuellen Systeme konstruieren kann. Wenn Sie ein System bauen, sagen wir zur Veranschaulichung ein Flugzeug, dann haben Sie zwei Typen von Anforderungen. Einerseits die Funktionalität: Das Flugzeug muss fliegen. Andererseits die Sicherheit, also die Anforderung, dass das System gewisse Dinge nicht machen darf: Das Flugzeug muss zum Beispiel geschützt sein gegen äussere Zugriffe und Manipulationsmöglichkeiten. Zwischen den beiden Anforderungen gibt es grosse Unterschiede. Die positiven Eigenschaften der Funktionalität kann man gut testen, etwa indem man ein Flugzeug unter verschiedenen Bedingungen Probe fliegt. Die negativen Eigenschaften kann man hingegen nicht vollständig testen: Man kann zwar einen Angreifer engagieren, der probiert, das Flugzeug zu knacken. Aber nur, weil er keine Schwachstelle vorfindet, heisst das noch lange nicht, dass es diese auch nicht gibt. Deswegen ist die Sicherheit eine intrinsisch mathematische Aussage: Man muss sie definieren und anschliessend beweisen.

Und die Theorie ist dann so lange gut genug, bis die Anwendungspraxis eine Schwachstelle findet?

Dann wäre der mathematische Beweis zwar nicht falsch, aber eine Annahme nicht erfüllt. Das sollte natürlich vermieden werden. Ich sehe die Kryptografie aber nicht aus der defensiven Perspektive. Es geht nicht darum, Löcher zu stopfen, sondern um eine konstruktive Disziplin, die neuartige virtuelle Systeme konstruieren kann.

Gerade im Bereich Kommunikation gibt es bereits verschiedene Applikationen, die Verschlüsselung einbauen.

Wenn man sich darum kümmert, dann findet man sichere Anwendungen. Dann aber stellt sich die Frage der Kompatibilität: Bei der Kommunikation bringt mir ein sicheres System nur etwas, wenn meine Freunde es ebenfalls verwenden.

Gibt es Tips, die Sie für normale Nutzer haben?

Eines der grössten Risiken ist, dass viele Leute wenig von Sicherheit verstehen: Es gibt Menschen, die fallen auf Telefonbetrüger rein und installieren auf Instruktion schädliche Software. Das ist unglaublich. Sie würden ja auch nicht einfach eine Pille schlucken, wenn Ihnen auf der Strasse eine wildfremde Person eine offerieren würde. Selbst wenn ein Polizist Ihnen eine anbieten würde, wären Sie wahrscheinlich sehr skeptisch. Genau diese Grundskepsis fehlt jedoch vielen, wenn sie sich im Internet bewegen. Hohe technische Kompetenzen kann man vom Normalbürger nicht erwarten. Die Sicherheit muss in der Technik verankert sein, wie beim Online-Banking: Es kommt dort nicht vor, dass ein Nutzer von sich aus Dinge installieren muss.

Sehen Sie es als Ihre Rolle, die Bevölkerung diesbezüglich aufzuklären?
Grundsätzlich empfinde ich das nicht als meine primäre Mission. Ich will grundlegende Wissenschaft machen. Auf komplexe Fragen gibt es nicht immer eindeutige Antworten. Aber wenn ich als Experte etwas zu sagen habe, dann mache ich das.

Nichtsdestotrotz teilen Sie Ihr Know-how immer mal wieder auch öffentlich. Was ist der ultimative Traum eines Wissenschafters?
Ein Tennisspieler will Wimbledon gewinnen. Die einfache Antwort wäre, dass auch Wissenschafter Preise gewinnen wollen, beispielsweise einen Nobelpreis. Viele treibt aber auch eine fast schon religiöse Komponente an: Man will etwas Bleibendes schaffen, ein Vermächtnis, das auch nach dem eigenen Tod signifikant ist. Andere hoffen, dass die eigene Forschung möglichst bald in der Realität einen konkreten Nutzen stiftet. Ich habe beide Ziele, bin aber eher auf das Ultimative aus: auf die Entwicklung einer Theorie, die lange Bestand hat und nicht in zehn Jahren durch eine neue abgelöst wird.

«Hohe technische Kompetenzen kann man vom Normalbürger nicht erwarten.»
Ueli Maurer

Verschlüsselung kann auch geknackt werden. 2019 hat Google einen Quantencomputer entwickelt, der offenbar Rechenprobleme lösen konnte, an welchen ein Supercomputer scheiterte. Was halten Sie davon?
Quantencomputer sind theoretisch in der Lage, gewisse Probleme sehr viel schneller zu lösen, als es klassische Computer können. In der Praxis wird bei der Realisierung der Basistechnologie von Quantencomputern zwar sehr viel Geld investiert, nach wie vor beschäftigt man sich aber immer noch mit den Grundlagen. Die Entwicklung von Google war sicher ein wichtiger Zwischenschritt, nicht jedoch ein Durchbruch. Das gelöste Problem war nämlich kein praxisrelevantes, sondern ein künstlich definiertes.

Viel Wirbel um nichts also?
Es ist nur eine Frage der Zeit, bis es Quantencomputer gibt, die wirklich schneller sind als die klassischen. Dann muss man allerdings auch noch untersuchen, für welche Probleme die Quantencomputer entwickelt werden: Ein Quantencomputer ist kein Computer, der einfach alles kann. Die Entwicklung erfolgt für ganz bestimmte Anwendungen, zum Beispiel die Simulation von Quanteneffekten in chemischen Reaktionen. Ich erwarte, dass die Entwicklung von Quantencomputern für das Knacken kryptografischer Probleme sehr spezifisch vorgehen müsste und dass sich das somit gar nicht als Business-Case rechnen würde, auch nicht für die NSA. Ein ideal funktionierender Quantencomputer, der auch die Errungenschaften der Kryptografie in Frage stellt, ist heute nicht zu erwarten – vielleicht wird es ihn gar nie geben. Trotzdem muss sich die Forschung mit Alternativen befassen, die auch für Quantencomputer unknackbar sind. Dies ist ein intensives Forschungsgebiet mit der Bezeichnung «Post-Quantum Security».

Bleibt die moderne Verschlüsselung also zumindest auf absehbare Zeit unknackbar?
Kürzlich war ich an einem Panel bei der Schweizerischen Nationalbank und wurde gefragt, wie schlimm diese Quantencomputer für die Sicherheit seien. Ich sagte, dass das für die Schweizerische Nationalbank eigentlich kein prioritäres Thema sei. Das echte Problem liegt viel eher darin, dass die normale Kryptografie, die heute verwendet wird, auch durch einen klassischen Computer gebrochen werden könnte: Für das Lösen des unterliegenden mathematischen Problems braucht es in der Theorie vielleicht nur eine clevere Idee – dann könnte das ganze Wirtschaftssystem bedroht sein. Das gesamtgesellschaftliche Risiko, dem wir uns so heute schon aussetzen, ist hier vermutlich höher als bei der Nukleartechnologie. Dass die Kryptografie auch ohne Quantencomputer ein reales Risiko mit sich bringt, ist vielen Leuten nicht bewusst.

Ist Ihr Alltag stark von Technik geprägt?
Ich wünsche mir nicht unbedingt mehr Technologie im Alltag und lebe auch heute relativ untechnologisch. Ich befürchte, dass uns die Technologieentwicklung in gewissen Aspekten entgleitet. Ich bin ein positiv denkender Mensch, habe aber Respekt vor der Zukunft. ❮

Ueli Maurer
ist Professor im Departement für Informatik der ETH Zürich. Er leitet die Forschungsgruppe für Informationssicherheit und Kryptografie.

Jannik Belser
ist Redaktor dieser Zeitschrift.