Inhärente Sicherheit statt Überwachung

Resiliente Computer | In einem Talk, den der Kryptografie-Experte Bruce Schneier in Lausanne hielt, gab er Einblicke in die Mechanismen, die zum Versagen von Sicherheitsparadigmen wie Patching, Authentifizierung und Lieferketten führen. Seine zentrale Frage lautete: «Können wir ein sicheres Netzwerk aus unsicheren Komponenten in einer unsicheren Welt aufbauen?»

RADOMÍR NOVOTNÝ

Studierende und IT-Interessierte strömten am 16. März 2023 an die ETH Lausanne, um den US-amerikanischen Kryptografie- und Computersicherheitsexperten, Dozenten und Autor Bruce Schneier zu hören und ihm Fragen stellen zu können.

«Ich möchte darüber sprechen, wie wir die Sicherheit in einer Welt gewährleisten können, in der alles ein Computer ist», so Schneier zu seiner Motivation, nach Lausanne zu kommen. Mit Beispielen illustrierte er, dass diese Aussage durchaus ernst gemeint ist, denn Computer verbergen sich auch in Dingen, die diesen Schluss nicht zwingend zulassen: Während es bei Mobiltelefonen noch ziemlich klar ist, dass sie eigentlich Rechner sind, die nebenbei zum Telefonieren verwendet werden können, ist die Sache bei Kühlschränken und Mikrowellengeräten weniger offensichtlich. Auch Bankomaten sind Computer, die Banknoten enthalten. Sogar Autos, die früher einfach mechanische Vorrichtungen zur Fortbewegung waren, können heute als Computer mit vier Rädern und einem Motor betrachtet werden. Oder, genauer gesagt, als verteiltes System mit Dutzenden vernetzten Rechnern. Wir leben also in einer Welt, die von unzähligen miteinander kommunizierenden Rechnern durchdrungen ist. Die Lektionen dieser Computerwelt können also überall angewendet werden.

Die universalen Lektionen

Schneier stellte zum Einstieg sechs Lektionen zur Computersicherheit vor. Seine erste Lektion: Die meiste Software sei schlecht geschrieben und unsicher. Der Grund dafür liege in unserem Wunsch, alles schnell, billig und mit allen möglichen Features haben zu wollen. Was an anderen Orten nicht funktioniert, schafft es

Bilder: Radomír Novotný

auch nicht, in der Informatik zu funktionieren, denn die zunächst nicht wahrnehmbaren qualitativen Abstriche wirken sich auf die Sicherheit aus: «Die Software ist voller Fehler. Einige dieser Fehler sind Schwachstellen. Einige dieser Schwachstellen können ausgenutzt werden und einige davon werden auch ausgenutzt», so Schneier.

Die zweite Lektion: Bei der Entwicklung des Internets spielten Sicherheitsfragen nie eine Rolle. Ende der 1970er-Jahre wurde das Internet nie für etwas Kritisches genutzt. Zudem hatte man nur Zugang, wenn man mit einem Forschungsinstitut verbunden war. Es wurde damals bewusst beschlossen, die Sicherheit im Internet zu ignorieren und sie den Endpunkten zu überlassen. In den 1980er- und 1990er-Jahren wurden dann aber Computer ans Internet angeschlossen, die nie für einen solchen Einsatz konzipiert waren, nämlich unsichere Personal Computer. Und das Ergebnis ist, dass nichts mehr sicher ist. Schneier betont: «Wir leben immer noch mit den Auswirkungen all dieser frühen Entscheidungen bezüglich Domänennamensystem, Internet-Routing-Paketen, E-Mail-Adressen und so weiter. Wir arbeiten immer noch daran, diese unsicheren Internetprotokolle nachzurüsten.»

Die dritte Lektion bezieht sich auf die Erweiterbarkeit von Rechnersystemen. Computer sollen möglichst für alle Zwecke einsetzbar sein. Der erste Slogan für das iPhone lautete: «There's an app for that.» Für alles gibt es eine entsprechende App – wobei bei jeder Erweiterung natürlich auch neue Sicherheitslücken entstehen. Die zu verteidigende Oberfläche wächst mit jeder Erweiterung.

Bei der vierten Lektion geht es darum, dass wegen der wachsenden Komplexität eine Attacke einfacher ist als die Verteidigung. Der Angreifer muss nur eine Tür finden, aber die Verteidiger müssen sich um alle Lücken gleichzeitig kümmern.

Die durch gegenseitige Verbindungen verursachten Schwachstellen standen in der fünften Lektion im Zentrum. Schneier erwähnte dazu mehrere Beispiele, wobei sein «Favorit» ein Angriff von 2017 auf ein Casino in Las Vegas ist, bei dem sich Hacker Zugang via einem Aquarium-Thermostaten mit Internetanbindung zum internen

Bruce Schneier im Rolex Learning Center in Lausanne.

Netzwerk verschafften. Daten der Casino-Datenbank wurden dann durch diese Lücke «abgesaugt».

Sechste Lektion: Die Attacken werden immer einfacher, besser und schneller. Es seien dabei nicht nur die immer leistungsfähigeren Rechner dafür verantwortlich, sondern die Angreifer, die sich anpassen und ihre Expertise unter anderem aus der Forschung holen. Dabei stehen drei Aspekte im Vordergrund, die vom Sicherheitsingenieur sichergestellt werden sollten: Vertraulichkeit, Integrität und Verfügbarkeit. Wenn in den Medien von Sicherheit die Rede ist, geht es meistens um Vertraulichkeit – Datenschutz, Datendiebstahl und Datenmissbrauch. Aber heute seien die Bedrohungen der Integrität und Verfügbarkeit viel schlimmer als die Bedrohungen der Vertraulichkeit, denn sie wirken sich gravierender aus. Jetzt besteht eine echte Gefahr für Leben und Eigentum. Schneier sagt: «Ich mache mir Sorgen, wenn jemand ein Krankenhaus hackt und meine privaten Krankenakten stiehlt. Aber ich mache mir noch viel grössere Sorgen, wenn jemand meine Blutgruppe in den Akten ändert. Das ist ein Angriff auf die Datenintegrität. Zudem möchte ich nicht, dass sich jemand in mein Auto hackt, das Bluetooth-Mikrofon einschaltet und meine Gespräche belauscht, aber ich möchte noch viel weniger, dass er die Bremsen deaktiviert.» Das Kritische ist, dass manchmal im Auto, im Kraftwerk und im Herzschrittmacher derselbe Prozessor mit dem gleichen Betriebssystem eingesetzt wird. Der einzige Unterschied bei einer Cyberattacke ist der Ort, an dem der Schaden entsteht.

Einige Sicherheitsansätze versagen nun

Anschliessend ging Schneier auf die Gründe für das Versagen gewisser langjähriger Sicherheitsparadigmen ein. Beim Patching schreiben meist die an der Software-Entwicklung beteiligten Ingenieure der grossen Softwarehäuser die Patches, sobald neue Schwachstellen gefunden werden. Die Anwender können bzw. sollten dann ihre Geräte entsprechend aktualisieren. Dies funktioniert aber bei billigen Geräten wie digitalen Videorecordern oder Home Routern mit eingebetteten Rechnern nicht, denn sie werden mit einer viel geringeren Marge entwickelt und meistens von Dritten im Ausland hergestellt. Ingenieurteams werden für einen konkreten Job zusammengestellt, schreiben den Code, und ihre Wege trennen sich wieder. Es gibt niemanden, der später solche Patches schreiben könnte. Bei Sicherheitsproblemen werden beispielsweise Home Router dann einfach durch neue ersetzt, was aus Ressourcensicht schlecht ist.

Das Gleiche gilt für IoT-Geräte, die, einmal in Häusern oder Autos installiert, jahrelang ihren Dienst ausführen, ohne je in den Genuss eines Patching zu kommen. Schneier konstatiert: «Es

gibt einen Grund dafür, wieso Apple und Microsoft ihre Betriebssysteme nach etwa einem Jahrzehnt einstellen: Es ist wirklich schwer, das alte Zeug zu warten. Und bei billigen Geräten ist es noch schlimmer. Die Firmen gehen Konkurs oder die Ingenieure sind längst weg. Keiner kennt den Code.» Dies sei ein grosses Problem, auf das es noch keine Antwort gibt.

Eine weitere Herausforderung ist die Authentifizierung. Passwörter, die man sich merken kann, funktionieren in den meisten Fällen nicht mehr. Zwei-Faktoren-Authentifizierung klappt auch nicht in jedem Fall. Aber das Schwierigste kommt erst noch auf uns zu: Die Anzahl künftiger Authentifizierungen steht kurz vor der Explosion, insbesondere dort, wo Geräte mit anderen Geräten im Internet-der-Dinge kommunizieren. Bei 100 IoT-Geräten, die alle miteinander Daten austauschen sollen, kommt man auf 10 000 Authentifizierungsvorgänge, bei 1000 sind es schon eine Million Vorgänge. Diese Skalierung, die beispielsweise bei Fahrzeugen untereinander und mit den Lichtsignalen vorkommen könnte, haben wir noch nicht im Griff.

Ein weiteres, praktisch unlösbares Problem sind die Lieferketten. «Können wir chinesischen Netzwerkkomponenten oder russischen Antiviren-Produkten vertrauen? Diese Frage wird natürlich auch aus der anderen Perspektive gestellt: 2014 hat China Kaspersky und die US-Firma Symantec verboten. Schneiers Fazit: «Man muss allen vertrauen und kann doch niemandem trauen. Wir haben hier keine guten Antworten.» Würde beispielsweise das iPhone ausschliesslich in den USA hergestellt, wäre man zwar sicherer – niemand wäre aber bereit, das Zehnfache dafür auszugeben.

Wie kriegt man die Situation in den Griff?

Für Bruce Schneier ist klar, dass der von der Gewinnmaximierung getriebene Markt alleine nicht in der Lage ist, die Sicherheitsherausforderungen zu meistern. Die Sicherheit ist der Aspekt, bei dem am ehesten gespart wird. Weil es um grosse Risiken geht, unter Umständen um Lebensgefahr, brauche es die Regulierung. Sein Motto lautet: «Wir haben nicht mehr die Wahl zwischen staatlicher Beteiligung und keiner staatlichen Beteiligung, sondern zwischen einer intelligenten Regierungsbeteiligung und einer weniger klugen.» Es ginge bei der Regulierung nicht darum, Innovation abzuklemmen, sondern darum, die wirtschaftlichen Anreize so zu verändern, dass die Unternehmen auch in Sicherheit investieren wollen.

Wie das funktioniert, illustrierte er mit einem Beispiel aus Kalifornien. Dort wurde 2020 ein IP-Sicherheitsgesetz verabschiedet und 2022 in Kraft gesetzt, das es verbietet, IoT-Geräte zu verkaufen, die mit einem Default-Passwort ausgestattet sind. Und da Hersteller von IoT-Thermostaten, Drohnen oder Spielzeugen nicht zwei Arten von Produkten – für Kalifornien und für den Rest der Welt – herstellen wollen, werden nun weltweit sicherere IoT-Geräte verkauft. «A good law in a big enough market moves the planet», so Schneier. Als Vorbild sieht er in dieser Hinsicht die Europäische Union, die indirekt auch die Sicherheit in den USA erhöht, beispielsweise durch die Datenschutz-Grundverordnung.

Dies sei auch der Grund, wieso sich Schneier als Dozent an der Harvard Kennedy School einsetzt, einer Schule für öffentliche Ordnung und Regierung der Harvard University in Cambridge, Massachusetts. Dort unterrichtet er nach eigenen Angaben Studierende, die der Mathematik während ihrer früheren Ausbildung bewusst aus dem Weg gegangen sind. Diese Studierenden, die später auf politischer Ebene einflussreich werden könnten, sollten sich mit den technologischen Zusammenhängen vertraut machen, um informierte Entscheidungen treffen zu können – Entscheidungen im politischen, technologischen und wirtschaftspolitischen Bereich. Dabei sollte der Sicherheitsfrage stets oberste Priorität eingeräumt werden, so lange das Internet bei kritischen Infrastrukturen eingesetzt wird. Das von Schneier vorgegebene Ziel klingt ansprechend: «We need to design for security and not for surveillance.»

Von Gebäuden, Restaurants, Apotheken und Technologien

Im Frageteil plädierte Schneier dafür, keinen Unterschied zwischen Technologien und anderen Aspekten des alltäglichen Lebens zu machen. Wenn man ein Gebäude betritt, muss man sich schliesslich auch nicht darum kümmern, ob beim Bau die Statik sorgfältig durchgerechnet wurde und ob die aktuellen Bauvorschriften eingehalten wurden. Oder wenn man mit einem Flugzeug fliegt, ob der Pilot seine Ruhezeit eingehalten hat, das Flugzeug korrekt gewartet wurde und über genügend Treibstoff verfügt. Wenn man in einer Apotheke ein Medikament kauft, ist es auch nicht erforderlich, ein Pharmakologe zu sein, um die Behandlung zu überleben oder ein Bakteriologe, wenn man in ein Restaurant zum Nachtessen geht. Bei einem verdorbenen Magen kann der Koch nicht einfach sagen, dass man genau dieses Gericht nicht hätte bestellen sollen. Aber bei Technologien scheinen gemäss Schneier andere Massstäbe zu gelten. Er fragt zu Recht: «Warum sollte es bei Computern anders sein? Warum darf man einen USB-Stick nicht in den Computer einstecken? Es ist ja schliesslich ein USB-Stick. Was soll ich denn sonst damit machen? Und klicken Sie ja nicht auf eine URL … Wir geben diesen Rat, weil wir unsere Systeme so schlecht konzipiert haben, dass es gefährlich ist, auf eine falsche URL zu klicken», so Schneier. Er rief dazu auf, solche Systeme von Grund auf sicherer zu gestalten, statt dem Benutzer die Schuld für Sicherheitsprobleme zu geben.

Aber bis diese Botschaft in der Forschung und der Industrie angekommen ist, wird man am Arbeitsplatz kaum darum herumkommen, sich als Anwender durch Kompakttrainings zur Bedeutung von Cyber-Sicherheit und typischen Sicherheitslücken wie Phishing am Arbeitsplatz von der eigentlichen Arbeit abhalten zu lassen. Der Hinweis, diese Skills können auch im privaten Bereich nützlich sein, ist da ein schwacher Trost, denn auch dort wünschte man sich inhärent sichere Computer. Möge Schneiers Plädoyer bei Software-Entwicklern also möglichst bald auf offene Ohren stossen!

Literatur

Bruce Schneier, A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend them Back, W. W. Norton & Company, 2023.

Autor

Radomír Novotný ist Chefredaktor des Bulletins Electrosuisse.

→ Electrosuisse, 8320 Fehraltorf

→ radomir.novotny@electrosuisse.ch