Kryptografie – Schlüsseltechnologie fürs Internet

Kryptografie war einst die Domäne von Mathematikern und Geheimdiensten. Heute ist Kryptografie eine der Schlüsseltechnologien für viele Internet-Dienstleistungen: E-Commerce und E-Banking sind ohne sichere Verschlüsselung undenkbar. Das ist aber erst der Anfang: Der Tag, an dem jedes Email verschlüsselt übertragen wird, dürfte nicht mehr weit weg sein.

In kaum 200 Kilometer Luftline von der Schweizer Grenze steht eine der geheimsten Einrichtungen auf dem europäischen Kontinent: Die Abhörstation von Bad Aibling bei München. Rund ein Dutzend Gebäude, die wie riesige Champignions aussehen, stehen dort. Darunter verbergen sich hochempfindliche Antennen, die in alle Richtungen zeigen. 750 Amerikaner, die zur geheimnisumwitterten National Security Agency (NSA) gehören arbeiten dort. Aber nicht mehr lange. Die Station wird bald geschlossen. Sie ist überflüssig geworden. Viele Signale lassen sich heute via Satelliten weit besser und billiger abhören. Aber sie rauschen auch durch die Kabel und auch diese lassen sich anzapfen.

Echelon heisst ein geheimnisumwittertes System, das all die gesammelten Daten auswerten soll. Betrieben wird es von ebendieser National Security Agency. Echelon soll mit mächtigen Filtern ausgerüstet sein und und mit akribischer Genauigkeit den weltweiten Telefon- und Datenverkehr auswerten.

Ist Echelon eine Spekulation, ein Gerücht oder gar eine der so beliebten Verschwörungsphantasien der Internet-Gemeinde. Dem scheint nicht so: Der Begriff ist allgegenwärtig - so auch im bisher umfangreichsten Buch, das wohl je über den NSA publiziert wurde. Geschrieben hat es der britische Journalist James Bamford, es trägt den Titel „NSA – die Anatomie des mächtigsten Geheimdienstes der Welt.“ (1)

Bestätigung für Echelon kommt auch aus der Schweiz: “ Wir müssen davon ausgehen, dass ein globale Abhörsystem namens Echelon tatsächlich existiert“. Das sagt Bruno Baeriswyl, Datenschutzbeauftragter des Kantons Zürich. Der Datenschutzbeauftragter ist in guter Gesellschaft. Echelon beschäftigt nämlich auch das europäische Parlament und einen nichtständigen Ausschuss. 120 Seiten dick ist das Papier, das dessen Berichterstatter Gerhard Schmid am 18.Mai in einer ersten Version publiziert hat (2). Die Schlussfolgerungen: „An der Existenz eines weltweit arbeitenden Kommunikationsabhörsystems, das durch anteiliges Zusammenwirken der USA, des Vereinigten Königrteiches, Kanads, Australiens und Neuseelands funktionniert, kann nicht mehr gezweifelt werden. Wichtig ist, dass das System nicht zum Abhören militärischer, sondern privater und wirtschaftlicher Kommunikation dient“.

Für den EU-Ausschuss ist klar: Das Abhören von Kommunikation stellt einen tiefgreifenden Eingriff in die Privatsphäre dar. Heute sind die Bürger nur unzureichend geschützt. Verschlüsselung ist darum ein Gebot der Stunde: „Die Kommission und die Mitgliedstaaten werden ersucht, geeignete Massnahmen für die Förderung, Entwicklung und Herstellung von europäischer Verschlüsselungstechnologie und –Software auszuarbeiten“. Verschlüsselung allein genügt aber nicht – denn sie kann auch ein trojanisches Pferd sein. Darum soll darauf geachtet werden, dass der Quelltext dieser Software offengelegt wird. Die Gefahr, dass auch Kryptografie-Software kompromittiert ist, ist sehr real.“ Wir müssen davon ausgehen, dass alle in den USA offiziell freigegebeneVerschlüsselungssoftware Hintertüren enthält und darum nicht sicher ist“, warnt der Datenschützer Bruno Baeriswyl.

Der Gedanke, dass Daten verschlüsselt werden müssen, hat sich heute noch nicht allgemein durchgesetzt. Verschlüsselung ist heute nur dort Standard, wo Geld im Spiel ist: Im Bereich des E-Commerce und des E-Banking. „Jeder Browser ermöglicht heute sichere Transaktionen“, sagt etwa der Netzwerkspezialist Peter Heinzmann im InfoWeek-Interview.

Und genau hier fehlt offenbar das Vertrauen der Benutzerinnen und Benutzer. Das Internet gilt heute ganz einfach nicht als sicher genug und das hält viele davon ab, Einkäufe übers Netz zu tätigen oder Transaktionen elektronisch abzuwickeln. Armgard von Reden, Chief Privacy Officer bei IBM in Brüssel brachte an einem Mediengespräch dramatische Zahlen ins Spiel: „Nach einer neueren Studie haben in jüngerer Zeit 12 Millionen Menschen aufgehört über das Netz einzukaufen, weil sie Bedenken hatten, ihre Daten preiszugeben. Das entspricht einem Verlust von 12 Milliarden Dollar."

Die Methoden für eine effektive Verschlüsselung sind bekannt – gute Produkte sind auf dem Markt. Gute Verschlüsselungsmethoden haben allerdings auch eine Kehrseite, denn sie erlauben auch dem organisierten Verbrechen effizient und unbelauscht zu operieren. Nicht zuletzt deshalb versuchen verschiedene Staaten den Export zu kontrollieren. Gerade die USA haben sich bis vor kurzem mit einem Exportverbot für die PGP Verschlüsselungssoftware unbeliebt gemacht. Weniger bekannt dürfte die Tatsache sein, dass Bedenken gegen den Export von solcher Software auch in Europa existieren: Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), zu der auch die Schweiz gehört, hat darum Richtlinien erlassen, die allerdings nicht bindend sind. Diese Richtlinien ermutigen einsereits die Staaten leistungsfähige Kryptografieprogramme einzusetzen. Gleichzeitig laden sie die Mitgliedstaaten aber auch ein, Instrumente für die Kontrolle dieser Technologien zu entwickeln.

Ein solches Instrument ist die Vereinbarung von Wassenaar, die in der Schweiz in der Güterkontrollverordnung umgesetzt ist. Demnach ist der Export von Kryptologieprodukten mit schwacher Verschlüsselung (56-bit mit symmetrischen und 512-bit mit asymmetrischen Schlüsseln) vollkommen freigegeben. Software mit stärkerer Verschlüsselung unterliegt gewissen Einschränkungen, die aber je nach Land unterschiedlich ausfallen.(3)

Dominik Landwehr

1) James Bamford: NSA – Die Anatomie des mächtigsten Geheimdienstes der Welt. München 2001. (Bertelsmann) – http://www.bodyofsecrets.com

2) Das Papier findet sich unter http://www.europarl.eu.int/tempcom/echelon/prechelon_en.htm

3) Eine Darstellung der Fragen der Kryptografie aus Sicht der Eidgenossenschaft finden sich hier: http://www.seco.admin.ch/Werwirsind/d_portrait/publi/kryptogr.pdf

„Verschlüsselung ist nur ein Teil der Sicherheit“

Peter Heinzmann ist Professor für Internet-Technologien und – Anwendungen an der Hochschule Rapperswil und Technischer Direktor der Firma cnlab Information Technology Research AG.

InfoWeek: Es gibt wohl nur zu wenigen Themen so viel Material auf dem Internet wie zum Thema Kryptografie? – Woran liegt das?

Prof. Peter Heinzmann: Ich glaube das hat mit der Natur des Menschen - mit der Faszination des Geheimen und der Neugier auf alles Verbotene zu tun Die Unübersichtlichkeit des Internet verstärkt einerseits die Befürchtung, dass jemand seine Daten mitlesen könnte Andererseits ist die absolute Meinungsäusserungsfreiheit des Internet eine idealer Nährboden für den Austausch von Informationen zu Themen, welche manche Stellen eher nicht zur Sprache bringen wollen.

IW: Und im Netz blühen auch die Verschwörungstheorien – hier dreht sich sehr vieles um den technischen Arm des amerikanischen Geheimdienstes, die geheimnisumwitterte National Security Agency (NSA). Was ist an diesen Theorien dran?

Heinzmann: Da sind die Meinungen eher zwiespältig. Einerseits nennen manche die NSA „the most overestimated agency". Auf der anderen Seite ist heute klar, dass der amerikanische Geheimdienst im Äther sehr genau hingehört hatte, was für Informationen übertragen werden. Noch einfacher als im Äther hinzuhören ist es, den Internet-Verkehr mitzuverfolgen. Allerdings gibt's da ein Problem: Es fallen immer grössere Datenmengen an und wer in diesem Gebiet operiert braucht extrem leistungsfähige Filtersysteme. Ich persönlich gehe davon aus, dass es solche Filter gibt und ausgeklügelte Abhörsysteme existieren. Man muss allerdings wissen, dass amerikanische Stellen und Firmen auch auf ganz legale Weise zu sehr viel Informationen über uns gelangen könnten: So gibt es beispielsweise amerikanische Firmen, welche verschiedene europäische Bundesstellen in strategischen Fragen beraten...

IW: Wer braucht die Verschlüsselung von Daten eigentlich?

Heinzmann: Ich würde die Frage anders stellen: Wann braucht es Verschlüsselung. Und hier gibt es ganz klare Antworten. Von Gesetzes wegen verlangt das Datenschutzgesetz (www.datentschutz.ch) die Verschlüsselung von besonders schützenwerten Daten – dazu gehören beispielsweise medizinischen Daten. Ich denke, dass gerade dies im Verkehr zwischen Aerzten und Spitälern noch keineswegs die Regel ist. Dann haben natürlich Firmen ein Bedürfnis, ihre Daten zu schützen. E-Commerce, E-Banking und Transaktionen via Bankomat sind ohne Verschlüsselung undenkbar. Zu den aktuellen Einsatzbereichen gehört sicher auch die Verschlüsselung in Funknetzwerken (Wireless LAN).

IW: *Brauchen auch Privatpersonen Verschlüsselung? – Wie halten Sie als Experte dies persönlich?*

Heinzmann: Persönlich benutze ich für die Übermittlung von Prüfungsaufgaben zwischen mir und meinem Assistenten Verschlüsselung. Der Zugang zu unseren Firmenrechnern erfolgt verschlüsselt und auch mit manchen Projektpartnern tauschen wir sensible Daten verschlüsselt aus. Im rein privaten Bereich habe ich kaum Grund zum Verschlüsseln, achte aber bei der Nutzung von E-Commerce-Internet-Angeboten darauf, dass meine Kommunikation mit den Servern verschlüsselt läuft.

IW: Wäre es nicht sinnvoll, den ganzen Mailverkehr verschlüsselt abzuwickeln?

Heinzmann: Ich denke, dass dies in Zukunft sicher einmal geschehen wird. Das Problem, dass es vorher zu lösen gilt, ist aber das Schlüssel-Management. Es braucht nämlich nicht nur effiziente Verschlüsselungsmethoden. Man muss auch garantieren können, dass die benutzen Schlüssel auch echt sind. Das hätte die Organisation Swisskey auch für Privatpersonen in der Schweiz übernehmen. Leider hat aber Swisskey diese Tätigkeit eingestellt. Inwiefern eine globales Schlüsselmanagement je realisiert werden wird, ist gegenwärtig schwer zu sagen.

IW: Welche Verschlüsselungsmethoden betrachten Sie als sicher?

Heinzmann: Sicher ist gar nichts. Man fühlt sich in einer Seilbahn sicher und trotzdem stürzt gelegentlich eine ab. Es gibt zwar Verfahren, die als sicher gelten aber es gibt immer auch Leute, die Zweifel an dieser Sicherheit anmelden. Entscheidend ist zunächst einmal die Schlüssellänge: Bei symmetrischer Verschlüsselung gilt 128 Bit als relativ sicher. Bei asymmetrischen Verschlüsselungsmethoden braucht es längere Schlüssel, hier gelten 2048 Bit als sicher.
In der Regel werden die beiden Verfahren kombiniert. Das muss man sich etwa so vorstellen: Man chiffriert vor der Verteilung den Schlüssel. Die

Schlüsselverteilung ist asymmetrisch, die Verschlüsselung der Dokumente ist dann aber wiederum symmetrisch. Das ist einfacher und schneller als wenn man alles mit dem asymmetrischen Verfahren verschlüsseln würde.

IW: Wie beurteilen Sie den Markt für kryptografische Produkte?

Heinzmann: Man darf diese Frage nicht bloss technisch anschauen. Nur mit einer ganzheitlichen Betrachtungsweise kommt man zu einem hohen Sicherheitsstandard. Es hat zum Beispiel keinen Sinn, ein leistungsfähiges Verschlüsselungsverfahren zu wählen und gleichzeitig den physischen Zugang zu den Servern nicht zu schützen. Manchmal ist schon der Portier die Schwachstelle. Trotzdem einige Worte zu den Produkten: Für den Privatanwender sind kostenlose Produkte wie beispielsweise das Programm „Pretty Good Privacy (PGP)“ eine gute Lösung. Es gibt auch kommerzielle Produkte mit diesem Namen, sie sind komfortabler in der Bedienung und erlauben es neben dem Mail auch ganze Dokumente und Disks zu verschlüsseln. Längerfristig dürften sich Produkte durchsetzen, welche in die weit verbreiteten E-Mail-Clients integriert sind. Für die generelle Verschlüsselung von Internet-Protocol-Paketen sind momentan „Virtual Private Networking (VPN)“ Produkte hoch im Kurs.

IW: Lange Zeit gab es gesetzliche Beschränkungen im Bezug auf Export und Verwendung von kryptografischen Verfahren.

Heinzmann: Das stimmt: Die Amerikaner haben früher alle Verschlüsselungsverfahren mit Schlüssellängen von mehr als 56 Bit als Kriegsmaterial deklariert. Wer solche Produkte exportieren wollte benötigte eine Exportbewilligung. Die Firma Network Associates hat vor einigen Jahren dieses Problem so gelöst, dass sie den Code für solche Programme in Büchern veröffentlichte. Um auch ausserhalb der USA zu völlig legalen starken Verschlüsselungsprodukten zu kommen, wurden wir bei cnlab AG beauftragt, für Network Associates den Code aus den Büchern zu rekonstruieren. Das wiederum war erlaubt, weil die Meinungsäusserungsfreiheit den Export von beliebigen Büchern zulässt.

Frankreich hat übrigens sogar den Einsatz von kryptografischen Verfahren lange Zeit untersagt. Die Amerikaner haben ihre Restriktionen erst vor einem Jahr fallengelassen. Bei uns in der Schweiz gab es bis 1999 keine restriktiven Vorschriften. Dies ist mit ein Grund für die lange „kryptografische Tradition“ mit Firmen wie der Crypto AG, der Gretag, der früheren BBC oder auch der Ascom , welche alle leistungsfähige Kryptografie-Produkte herstellten und auf dem Weltmarkt vertrieben. Ein Grund für die grosse Schweizer Crypto-Begeisterung im akademischen Umfeld war Prof. Dr. James Massey, eine weltweit führende Kapazität auf dem Bereich der Codierungstheorie, welche von 1980 bis 1998 an der ETH Zürich dozierte und verschiedenste Cryptospezialisten „produzierte“. Der bekannteste unter ihnen ist wohl Ueli Maurer, der heute selbst an der ETH lehrt und zu den weltweit führenden Kapazitäten auf dem Gebiet der Kryptologie zählt. Leider hat sich diese Begeisterung bisher nicht in der Form von kommerziellen Produkten auf dem internationalen Markt noch zu wenig manifestiert.

IW: Wie geht es in Sachen Kryptografie weiter? – In der Literatur ist viel von Quantencomputern die Rede, die auch in diesem Gebiet einen Riesenfortschritt bringen.

Heinzmann: Kryptologen wünschten sich schon immer praktikable Verfahren, welche eine beweisbare Sicherheit bieten. Bei der Quantenkryptographie bewegt man sich in diese Richtung. Quantenkryptographie ist heute mehr als Science Fiction, aber dennoch weit vom praktischen Einsatz entfernt. Im Bereich der breiten Anwendung geht der Trend heute in Richtung Integration von kryptografischen Verfahren in Standardsoftware. In den Internetbrowsern ist dies mit dem SSL (Secure Socket Layer) ja bereits eine Tatsache und das geschlossene Schlösschen im Browser zeigt uns an, dass gesicherte Verbindungen aufgebaut sind. Generell könnte der Sicherheitsproblematik und auch der systematischen Überprüfung der Sicherheit von Informatik-Systemen mehr Beachtung geschenkt werden. Im Rahmen von unseren Netzwerksicherheits-Vorlesungen und Weiterbildungskursen versuchen

wir deshalb, die Leute soweit zu bringen, dass sie sich schon beim Entwickeln oder bei der Konzeption von neuen Systemen Gedanken über die Sicherheit machen .

Alan Turing, Enigma und die Computergeschichte

Sie hätte einen Ehrenplatz verdient – aber im Deutschen Museum in München muss man sie fast wie die Stecknadel im Heuhaufen suchen: Die berühmte Enigma-Chiffriermaschine. Endlich gefunden – in einem kleinen, etwas versteckten Nebenraum der Informatik-Abteilung – gibt sie ihr Geheimnis kaum Preis. „Rotor-Chiffriermaschine mit Steckerfeld und Glühlampen Anzeige“, lesen wir auf einem vergilbten Zettel und weiter: „Ausführung für die Marine - Drei der vier Walzen konnten aus den acht Walzen I-VIII ausgewählt werden, die vierte aus den sogenannten Griechenwalzen β und γ . Im Zubehörkasten eingestempelt ‚Kommando der Marine-Station in der Ostsee, Druckschriftenverwaltung“.

1000 km westlich von München liegt Bletchley Park, fast genau in der Mitte zwischen London und Oxford. Dort hat die legendäre Enigma gleich ein ganzes Museum und dort erfährt der Besucher auch einiges mehr als in München: Engima war eine der raffiniertesten meschanischen Chiffriermaschinen, die je entwickelt wurden. Geschichte geschrieben hat allerdings nicht nur sie allein, sondern die Menschen, die ihre Signale nach jahrelanger Kleinarbeit entschlüsselt hatten.

Unter ihnen der geniale britische Mathematiker Alan Turing, der im Jahr 1937 den bahnbrechenden Aufsatz „On Computable Numbers“ publiziert hatte.Turing bewies darin, dass jede berechenbare Funktion auch von einer Maschine berechnet werden kann - damit war ein wichtiger Grundsteine für den späteren Bau von Computer gelegt.

Turing und seine Mistreiter - und das waren hunderte, viele von ihnen Frauen - arbeiteten in grösster Abgeschiedenheit in der parkähnlichen Landschaft des einstigen Herrschaftshauses von Bletchley Park. Unmöglich, dass sie alle Kombinationen und Permutationen, welche die mühsame Entzifferungsarbeit mit sich brachte, von Hand machen konnten – das Hilfsmittel, das ihnen zur Seite stand hatte ebenfalls Alan Turing entwickelt: Man nannte es „the bomb“ und die Geräte dürften als mechanische Form eines Computer gelten. So gelang es nach Jahren von vergeblichen Versuchen endlich, den Code von Enigma zu knacken. Die Operation trug den Namen „Ultra“. Ab 1942 konnten die Alliierten mit dieser Methode 39 000 deutsche Funksprüche pro Monat entziffern, später waren es sogar 84 000 jeden Monat. Der Operation „Ultra“ war auch die Tatsache zu verdanken, dass die Alliierten bei ihrer Landung in der Normandie im Jahre 1944 die genauen Truppenaufstellungen entlang der französischen Küste kannten. Die Leistungen von Alan Turing und Bletchley Park waren entscheidend: Es gibt Historiker, welche die Verdienste des schmächtigen und unauffälligen Mannes gleich neben jene des Titanen Winston Churchills stellen.

Turing blieb auch nach dem Krieg Mathematiker studierte weiter einer intelligenten Maschine nach. Der Intelligenztest für Maschinen, den er 1950 vorschlug, ist als Turing-Test in die Geschichte eingagangen. Er hat den Ruhm, der ihm gebührt, nie ernten können. Schuld daran war auch ein Gesetz, dass allen Angehörigen von Bletchley Park verbot, über ihre Tätigkeit währen des Krieges zu reden. Alan Turing hatte ein tragisches Ende: Seine Homosexualität brachte ihn im prüden England der 50er Jahre in eine so auswegslose Lage, dass er durch Freitod aus dem Leben schied.

Zahlreiche Background Infos zur Enigma auf der Seite von Frode Freirud vom CERN
http://mad.home.cern.ch/frode/crypto/index.html

Emulation einer Enigma
http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/

Engima im Museum

http://www.deutsches-museum.de/ausstell/meister/enigma.htm
http://www.bletchleypark.org.uk/

Eine äusserst lesenswerte Darstellung der Geschichte der Kryptografie bietet das kürzlich erschienen Buch von Simon Singh: Geheime Botschaften. Es ist im Jahr 2000 im Hanser Verlag herausgekommen und erscheint demnächst bei dtv als Taschenbuch.
http://www.simonsingh.com