SWR2 MANUSKRIPT
ESSAYS FEATURES KOMMENTARE VORTRÄGE

SWR2 Wissen

Kryptografie: Schutz vor Hackern und Geheimdiensten?

Von Kai Laufen

Sendung: Mittwoch. 29. März 2017, 08.30 Uhr
Redaktion: Sonja Striegl
Regie: Autorenproduktion
Produktion: SWR 2017

MANUSKRIPT

O-Ton 1 – Schulklasse:
(Daniela Neu): Guten Morgen!
(Schulklasse): Guten Morgen Frau Neu!
(Daniela Neu): Heute ist ein besonderer Tag… (runterblenden)

Autor:
Daniela Neu ist Lehrerin an der Grundschule im Kreuzerfeld in Rottenburg am Neckar. Mit ihrer dritten Klasse nimmt sie das Thema „Verschlüsselung“ durch.

O-Ton 2 – Schüler:
Aufgabe 14. Krypto hat von Kryptina eine verschlüsselte Nachricht erhalten. Kannst du ihm helfen, ihn mit der Skytale zu lösen?

Autor:
Thema in dieser Stunde: Die Skytale. Ein Klassiker der frühzeitlichen Verschlüsselungstechniken: Es wird den Spartanern zugeschrieben und ist das älteste bekannte Verfahren, mit dem militärische Geheimnisse gesichert wurden. Ein langer Papierstreifen wird mehrfach um einen Stab gewickelt und dann mit dem Text beschrieben, dessen Inhalt geschützt werden soll. Wer den abgewickelten Streifen in die Hände bekommt, erkennt nur eine vertikale Buchstaben-Abfolge. Erst wer den Streifen um einen Stab mit dem richtigen Durchmesser wickelt, kann die verschlüsselte Botschaft lesen.

O-Ton 3 – Daniela Neu:
Es ist, glaube ich, ein Papierstreifen der Länge 59 Kästchen. Breit ist es drei Kästchen und die Buchstaben sind in ein Zentimeter hohe Abteile eingetragen worden. Und diese Streifen werden nachher um diese Klopapierrolle umwickelt.

SPRECHERIN:
„Kryptografie – Schutz vor Hackern und Geheimdiensten?“. Eine Sendung von Kai Laufen.

Video:
Hallo Rekruten! Schön, dass ihr dieses Jahr wieder dabei seid. Es freut mich, auch neue Agentinnen und Agenten begrüßen zu dürfen. Mein Name ist Krypto… (abblenden)

Autor:
Schon zum zweiten Mal nehmen Daniela Neu und ihre Schulklasse an einer Aktion von IT-Sicherheitsunternehmen und der Pädagogischen Hochschule Karlsruhe teil: (**Video** aufblenden) Krypto ist eine Kunstfigur, die in kurzen Filmen durch die verschiedenen Aufgaben führt. Sein Name Krypto geht auf den altgriechischen Begriff für „verborgen, versteckt, geheim“ zurück: Kryptografie bedeutet „Geheimschrift“:

O-Ton 4 – Daniela Neu:
Also grundsätzlich so der Umgang mit Sachen-verschlüsseln find ich im Hinblick auf den Umgang mit dem Internet, mit dem Anlegen von sicheren Passwörtern, find ich das immer wieder wichtig, dass die Kinder eine Chance haben, ihre eigenen Passwörter zu kreieren auf Grund solcher Grundlagen. Und ansonsten finden die es einfach auch spannend, relativ niederschwellig ihre eigenen Botschaften innerhalb der Klasse zu verschlüsseln. Das war auch letztes Jahr total im Trend zwischen den Viertklässlern, dass sie sich Botschaften verschlüsselt haben.

Autor:
Auch wenn sich die Kinder in Rottenburg mit den Klassikern und nicht mit den aktuellen, digitalen Verschlüsselungstechniken beschäftigen: Der spielerische Umgang mit dem Thema könnte helfen, sie auf eine Welt vorzubereiten, in der Datensicherheit eine zunehmend wichtige Rolle spielt. Und Kryptografie hilft, unsere digitale Welt sicherer zu machen.

O-Ton 5 – Jörn Müller-Quade:
Tatsächlich ist es so, dass die Wenigsten schon in der Schule von Kryptografie wirklich was gehört haben.

Autor:
… weiß Jörn Müller-Quade, Professor für Kryptographie und IT-Sicherheit am Karlsruher Institut für Technologie, KIT. An seinem Lehrstuhl verbinden sich Theorie und Praxis: Die Theorie der Kryptografie, die auf viel Mathematik und ein wenig Mechanik aufbaut, geht eine enge Verbindung mit der praktischen Anwendung kryptologischer Verfahren ein:

O-Ton 6 – Jörn Müller-Quade:
Sehr, sehr viele Industriezweige machen sich im Moment enorme Sorgen. Wenn man allein mal daran denkt, dass die ganzen Autos vernetzt werden sollen, dass wir vernetzten Verkehr haben sollen, dass Industrie 4.0 für vernetzte Fabriken der Zukunft spricht…

Autor:
… zählt Müller-Quade Gebiete auf, die ohne sicheren Datenfluss gar nicht denkbar sind. Um zu verstehen, was Fabriken und selbstfahrende Autos der Zukunft mit Verschlüsselung zu tun haben, lohnt ein Blick in die Geschichte:

Atmo: Tastaturgeräusche

Autor:
In Jörn Müller-Quades Arbeitszimmer steht eine Glasvitrine. Darin: Das wohl bekannteste Gerät aus der Welt der Verschlüsselung – eine Enigma:

Atmo: Tastaturgeräusche

O-Ton 7 – Jörn Müller-Quade:
Dieses Exemplar hier ist eine kommerzielle Enigma. Die ist bei Sammlern nicht so gesucht, weil sie keine Nazi-Vergangenheit hat, sondern diese kommerzielle Enigma wurde in die Schweiz verkauft und dort in Regierungskreisen verwendet.

Autor:
Die Enigma war im Zweiten Weltkrieg die Standard-Verschlüsselungsmaschine des deutschen Militärs. Die komplizierte Maschine besteht aus einer Vielzahl verdrahteter Walzen und galt als absolut sicher – aber die deutsche Seite täuschte sich: Tatsächlich konnten zunächst polnische, dann britische Experten fast über die ganzen Kriegsjahre den chiffrierten Buchstabensalat der Wehrmacht mitlesen und entziffern.

Atmo: Tastaturgeräusche

Autor:
Willi Geiselmann, wissenschaftlicher Mitarbeiter am Lehrstuhl, erklärt das kompakte Stück Feinmechanik:

O-Ton 8 – Willi Geiselmann:
Das ist die Enigma. Technik ist, wir haben irgendwie in dem Fall vier Walzen, durch die Strom geschickt wird. In der einen Seite rein, permutiert durch die einzelnen Walzen.

Atmo: Tastaturgeräusche

O-Ton 9 – Willi Geiselmann:
Jetzt haben wir gerade den Fall … jetzt dreht sich einmal nur eine Walze und beim nächsten Tastendruck nimmt’s die nächste Walze mit…

Autor:
Die Enigma war ein technischer Meilenstein in dem jahrtausendealten Wettlauf zwischen Kryptografen – also den Erfindern von Verschlüsselungen auf der einen und Kryptoanalytikern auf der anderen Seite, also denjenigen, die verschlüsselte Texte so lange erforscht haben, bis sie die Verschlüsselung brechen und den Klartext lesen konnten. Das funktionierte zum Beispiel, indem man eine Tabelle mit allen vorkommenden Buchstaben erstellt hat – da in jeder Sprache bestimmte Buchstaben öfter verwendet werden als andere, konnten die Kryptoanalytiker aus solchen Tabellen oft schon ablesen, welcher der verschlüsselten Buchstaben wohl im Klartext etwa für ein „e“ stehen könnte. Auch Texte, die mit einer Skytale verschlüsselt werden, halten einer solchen statistischen Methode nicht stand. Sie konnten entziffert werden, auch wenn der Kryptoanalytiker den Umfang des Stabes, um den der Papierstreifen gewickelt werden musste, nicht kannte. War der verschlüsselte Text lang genug, ließen sich schon auffallend viele „e“ oder „s“ finden, oder Buchstabenkombinationen, die in einer bestimmten Sprache öfter vorkommen, wie etwa die Artikel im Deutschen. Nachweislich sicher ist dagegen das „One-Time-Pad“. Ein Verfahren, bei dem ein Schlüssel jeweils nur einmal zum Verschlüsseln und zum Entschlüsseln eingesetzt und danach vernichtet wird. So arbeitet zum

Beispiel die Hagelin-Maschine, die ebenfalls im Karlsruher Institut für Technologie steht.

O-Ton 10 – Willi Geiselmann:
Das ist eine Maschine aus dem Kalten Krieg, die in der deutschen Botschaft in Moskau stand.

Autor:
Erklärt Willi Geiselmann. Die Hagelin eignet sich allerdings auch um zu zeigen, dass es nicht ausreicht, ein besonders sicheres Verschlüsselungsverfahren anzuwenden, wenn es gleichzeitig andere Wege gibt, die Nachrichten heimlich mitzulesen:

O-Ton 11 – Willi Geiselmann:
Problem bei dieser Maschine ist, dass zum Verschlüsseln wird durch ein Stellmotor immer der einzelne, der entsprechende Buchstabe eingestellt und das verbraucht Strom. Und über den Weg kann man im Prinzip sehen, wie viel Strom verbraucht wird oder wie lang Strom verbraucht wird. Als man dann drauf kam, wurde an das Gerät noch ein Zusatzgerät, was sozusagen genau den Stromverbrauch und die ganzen Abstrahlungen, die damit sind, stört, dazu geschaltet worden. Das ist die kleine Kiste rechts daneben, die ziemlich unscheinbar aussieht und die hat, wenn man sie einschaltet, macht die so ein kleines piepsendes Geräusch, dass man weiß, dass sie eingeschaltet ist.

Atmo: Piepsendes Geräusch / Einschalten der Hagelin-Maschine

Autor:
Die Problematik der Hagelin-Maschine ist typisch für die Kryptografie. Es reicht nicht, wenn die Mathematik der Verschlüsselung nachweislich sicher ist. Auch ihre praktische Anwendung muss abgesichert sein.

Doch Geheimdienste etwa könnten versuchen, bereits die Herstellung kryptografischer Verfahren zu manipulieren, um heimlich mitzulesen, wenn sich andere vermeintlich sicher austauschen, meint Jörn Müller-Quade:

O-Ton 12 – Jörn Müller-Quade:
Man kann leider sehr gut verschleiern, dass ein System unsicher ist, weil ein System aus vielen Komponenten besteht, und eben eine Sicherheitslücke an einer Stelle unter Umständen schon ausreicht, um das gesamte System unsicher zu machen.

Autor:
Auch wenn es extrem schwierig ist, Daten mittels Verschlüsselung wirklich abzusichern – die Kryptografie hat in den vergangenen hundert Jahren große Fortschritte gemacht. Der wichtigste Schritt war möglicherweise die Erfindung der asymmetrischen Verschlüsselung. Asymmetrisch deshalb, weil Sender und Empfänger nicht über dieselbe Information verfügen: In den 1970er Jahren begannen US-amerikanische Mathematiker mit Formeln zu experimentieren, die sich leicht in die eine, aber fast gar nicht in die andere Richtung auflösen lassen – es sei denn, man weiß, welche Zahlenwerte jeweils einzusetzen sind. Solche Einmalfunktionen erlauben es, einen Schlüssel öffentlich anzubieten und die

Nachricht später mit einem privaten Schlüssel zu entschlüsseln. Dazu braucht es eine öffentlich einsehbare Datenbank, von der die öffentlichen Schlüssel abrufbar sind – eine sogenannte Public-Key-Infrastruktur. Diese bahnbrechende Erfindung hat Verschlüsselung im elektronischen Datenverkehr auf eine ganz neue Ebene gehoben:

O-Ton 13 – Jan Oetjen:
Wir beschäftigen uns mit dem ganzen Thema Verschlüsselung ja schon relativ lange.

Autor:
Sagt Jan Oetjen, Geschäftsführer von WEB.DE und GMX, also der in Deutschland führenden Email-Dienste. Emails zu verschlüsseln ist lange Zeit sehr kompliziert gewesen und wurde nur von wenigen Kunden genutzt. Aber durch die Enthüllungen von Edward Snowden wurde klar, dass Geheimdienste den gesamten Internetverkehr mitlesen, also auch Emails. Danach wuchs das Interesse an einfachem, aber wirksamem Schutz vor der Massenüberwachung.

O-Ton 14 – Jan Oetjen:
Wir haben uns hier für das Verfahren PGP entschieden und sind mit diesem Verfahren bisher sehr glücklich. PGP steht ja für „Pretty Good Privacy", also wörtlich übersetzt „ziemlich gute Privatsphäre". Jetzt im Nachhinein betrachtet, eine sehr bescheidene Wortwahl. Der Standard ist ja schon 1991 entwickelt worden. Also 25 Jahre alt und bisher zumindest kein Fall bekannt geworden, wo PGP geknackt wurde. Also von daher kann man hier auf jeden Fall von einem der sichersten Verfahren zur privaten Verschlüsselung sprechen.

Autor:
Damit PGP funktioniert, muss der einzelne Nutzer auf eine Public-Key-Infrastruktur zugreifen, mit der die öffentlichen Schlüssel verwaltet werden. Nutzer A nennt Nutzer B einen öffentlichen Schlüssel. Damit kann der Sender die Botschaft auf seinem Computer verschlüsseln und schickt diese – für Außenstehende unlesbare – Email an Nutzer B. Der kann sie mittels seines privaten Schlüssels auf dem eigenen Rechner wieder öffnen. Die Email ist also auf ihrem ganzen Transportweg geschützt. Die Deutschen wissen dieses Sicherheitsplus, das mittlerweile alle führenden Marken anbieten, offenbar zu schätzen, meint Jan Oetjen:

O-Ton 15 – Jan Oetjen:
PGP hat sich sehr positiv entwickelt. Wir sind mittlerweile bei 700.000 registrierten PGP-Keys bei uns. Das ist eine sehr beachtliche Zahl, wenn man bedenkt, dass es weltweit nach Schätzungen etwa so 5 bis 6 Millionen nur gibt aktuell. Also die Voraussetzungen sind sehr positiv dafür da, das große Problem ist natürlich noch, diesen Standard weiter zu verbreiten.

Autor:
Geht es beim Absichern von Emails vor allem um den Schutz des Inhaltes, tun sich in der Automobilindustrie noch andere Probleme auf:

O-Ton 16 – Christoph Krauß:
Meistens ist es noch viel wichtiger, dass wir wissen, mit wem wir überhaupt kommunizieren, das heißt also, die Authentizität der Kommunikationspartner gesichert ist.

Autor:
Professor Christoph Krauß vom Fraunhofer-Institut für Sichere Informationstechnologie in Darmstadt befasst sich nicht mit Emails, sondern mit Autos. Die sollen immer schlauer werden, sollen autonom im Straßenverkehr fahren, und dazu müssen sie „miteinander reden“. Oder auch mit den Verkehrszeichen oder der Ampel.

O-Ton 17 – Christoph Krauß:
Beispiel ist hier: Wenn wir eine Car-to-Car-Kommunikation haben, wenn ein Fahrzeug das andere warnt über ein Glatteis oder es warnt, dass ein Krankenwagen kommt, dann darf natürlich sich nicht irgendjemand anderes als ein Krankenwagen ausgeben, damit man eine freie Straße hat. Also, es heißt, da müssen wir sicherstellen, dass die Authentizität der Kommunikationspartner gewährleistet ist. Die Vertraulichkeit durch Verschlüsselung ist da weniger wichtig.

Autor:
Was passieren kann, wenn diese Kommunikation nicht 100 Prozent abgesichert ist, zeigt Christoph Krauß an einem straßentauglichen Kleinwagen: Dieser hat eine elektronische Schnittstelle, etwa für Diagnosen in der Werkstatt. Aber auch Versicherungen nutzen sie, um per Mobilfunk das Fahrverhalten des Kunden zu überwachen und daraus die Beiträge zu berechnen. Das Auto kommuniziert also – und ist dadurch für Hacker interessant:

O-Ton 18 – Christoph Krauß:
Man baut eine falsche Basisstation auf und dann konnte man beliebige Nachrichten einschleusen und dann gehen eben die Lampen an oder die Scheibenwischer wischen hin und her.

Autor:
Ein Hacker könnte so die Kontrolle über ein Fahrzeug übernehmen und schweren Schaden anrichten. Für die Entwicklung von autonomen Fahrzeugen ist daher die Echtheit, die Authentizität der Kommunikationspartner wesentlich.

O-Ton 19 – Christoph Krauß:
Oder auch ebenfalls das Thema Integrität. Also das heißt, wir schützen die Daten vor unberechtigter Manipulation. Das heißt, ein Angreifer gibt sich vielleicht als eine Ampel aus oder er verändert Daten einer Ampel so, dass der Empfänger denkt, die Ampel ist grün, obwohl sie tatsächlich rot ist. Also, es heißt, wir haben Authentizität, Integrität und Vertraulichkeit und dazu brauchen wir geeignete Maßnahmen.

Autor:
Ob es um die Kommunikation zwischen Fahrzeugen geht, um Emails oder geheime Botschaftsnachrichten: Stets soll Kryptografie helfen, Informationen vor fremdem Zugriff zu schützen. Aber was, wenn Straftäter die gleichen Techniken nutzen, um

Verbrechen zu planen? Die Polizei beklagt, dass verschlüsselte Kommunikation immer öfter dazu führe, dass sie nicht ermitteln kann, selbst wenn sie die Kommunikation an sich abhört oder mitliest: Wenn die Nachricht – wie bei dem PGP-Verfahren – jeweils von einem Ende bis zum anderen Ende des Kommunikationswegs verschlüsselt wird, hören und sehen die Ermittler in den Protokollen ihrer Telekommunikationsüberwachung nur Datenmüll. So wäre es auch im Fall der rechtsextremen Gruppierung Old School Society gewesen, deren Mitglieder sich über die Nachrichtenplattform Telegram austauschten.

Die Gruppe flog auf, drei Männer und eine Frau wurden vor wenigen Tagen zu Gefängnisstrafen verurteilt. Während der Gerichtsverhandlung war Rechtsanwalt Michael Rosenthal, der einen der Angeklagten vertritt, die Aussage eines BKA-Beamten aufgefallen:

O-Ton 20 – Michael Rosenthal:
Und der hat den Ausdruck „rückwärtserhobene Daten“ verwendet und dieser Ausdruck hat mich neugierig gemacht. Was heißt denn „rückwärts erhoben“? Nun hat er angefangen, zunächst mal nur in Umrissen, aber doch zu erläutern, dass das Bundeskriminalamt sich in diese Chats eingeblendet hat. Und zwar offenbar nicht dadurch, dass man es beim Provider ausgeleitet hat, sondern irgendwie anders.

Autor:
Normalerweise ordnet ein Ermittlungsrichter auf Bitten der Polizei eine Überwachungsmaßnahme ab einem gewissen Zeitpunkt X an. Damit tritt die Polizei an den Provider heran – also etwa die Telekom oder 1 & 1 – die dann die Kommunikation direkt an die Ermittler ausleiten – Telefongespräche, Emails oder auch Chats. Aber jene Kommunikation, die zeitlich vor dem Beginn der Telekommunikationsüberwachung lag, kann die Polizei eigentlich nicht kennen. Doch genau das meint "rückwärts erhobene Daten“. Stück für Stück rekonstruierte Anwalt Rosenthal den Trick des Bundeskriminalamtes:

O-Ton 21 – Michael Rosenthal:
Die wissen ja, dass die Chat-Accounts mit Mobiltelefonnummern verknüpft sind. Und die haben sich, diese Möglichkeit bietet Telegram tatsächlich, die haben sich dann mit der Behauptung, sie seien der eigentliche Benutzer, also mit der Telefonnummer der zu überwachenden Person selber bei Telegram angemeldet. Und daraufhin kriegt man von Telegram auf alle angemeldeten Endgeräte so einen Code zum Einloggen. Und da liegt jetzt der technische Mangel, der kommt ganz schnell per SMS noch hinterher. Und da greift jetzt die normale Telefonüberwachung nach 100a der Prozessordnung, also kann das Bundeskriminalamt die SMS abgreifen. Damit hat sie den Login-Code. Dann loggen die sich ein.

Autor:
So konnte das BKA ab diesem Moment die Chats mitlesen – aber auch in der Historie zurückgehen und den gesamten Chatverlauf nachvollziehen. Und das, obwohl die Chatteilnehmer sich sicher fühlten – ihre Kommunikation war ja schließlich verschlüsselt! Tatsächlich ist diese Verschlüsselung selber nicht zu knacken. Aber da die Anwender oft Fehler machen, haben Ermittler doch eine Chance. Diesen Umstand will Bundesinnenminister Thomas de Maizière nun

systematisch ausnutzen und hat zum Jahresbeginn die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich“ – ZITiS – ins Leben gerufen. Bald schon sollen 400 staatliche Hacker in München die Schwachstellen von Messengerdiensten wie Telegram und Whatsapp ausleuchten und die Informationen darüber allen Sicherheitsbehörden zugänglich machen. Stefan Grosse, Leiter des Referats „Grundsatzangelegenheiten der Cybersicherheit im Bereich der Polizeien und des Verfassungsschutzes“ beim Bundesinnenministerium nennt die umfangreichen Aufgaben von ZITiS:

O-Ton 22 – Stefan Grosse:
Das sind sämtliche Themen rund um Verschlüsselung, das sind sämtliche Themen der Entschlüsselung, das sind sämtliche Themen rund um das Thema Telekommunikationsüberwachung, das sind alle Themen im Bereich „digitale Forensik“. Dann die Themen im Bereich „Big Dater“, soziale Netzwerke – offene Auswertung und der fünfte Bereich ist alles, was im Bereich „Hacking Malware“ zusammenhängt. Also, Abwehr von Angriffen, auch da sind ja die Sicherheitsbehörden tätig.

Autor:
Auch wenn die Zentrale Stelle für Informationstechnik im Sicherheitsbereich nicht selber ermittelt, werden sich die 400 Mitarbeiter doch an realen Straftaten orientieren, um Prioritäten in ihrer Forschung zu setzen, versichert Stefan Grosse.

O-Ton 23 – Stefan Grosse:
Wenn jetzt die konkrete Anforderung ist, wir beobachten verstärkt die Nutzung eines Kommunikationsdienstes, ich nenne ihn mal X, um nicht irgendein Beispiel zu nehmen. Das wäre eine Anforderung, wie kann ich da rein, wie kann ich die Kommunikation im Zweifel rausbekommen? Dann wäre das ein typischer Auftrag für ZITiS, sich darum zu kümmern, zu gucken, gibt’s Schwachstellen, gibt’s Workarounds, gibt es Features, die man nutzen kann? Das wäre ein typischer Auftrag für ZITiS, ja.

Autor:
Aus diesem Auftrag ergeben sich aber auch mögliche Konflikte: Was tun die staatlichen Hacker von ZITiS, wenn sie auf Schwachstellen in Verschlüsselungsprogrammen stoßen, die noch nicht bekannt sind? Es gibt einen grauen Markt für solche Informationen. Auch für Informationen über Schwachstellen in Software oder Hardware. Soll der Staat, darf der Staat hier zugreifen und einkaufen?

O-Ton 24 – Stefan Grosse:
Das ist in der Tat ein Punkt, den wir wirklich noch diskutieren, wie man mit Angeboten umgeht. Wie sieht sozusagen der Prozess dazu aus? Wie ist auch die Abwägung nutzen versus schließen von Schwachstellen? Es ist eine Diskussion, die derzeit weltweit läuft. Ist es eine Schwachstelle, die in einem System liegt, die für kritische Infrastrukturen gesellschaftlich relevant ist? Gehe ich grundsätzlich anders mit einer Schwachstelle um, als wenn es eine Schwachstelle ist, die bei Ausnutzung keinen wirklichen Schaden, keine Risiken erzeugt.

Autor:
Es sind solche Überlegungen, die Datenschützern wie Constanze Kurz vom Chaos Computer Club Sorgen machen.

O-Ton 25 – Constanze Kurz;
Diese Behörde muss natürlich dann auch ein Interesse haben, wenn sie zum Beispiel Umwege findet oder Hintertüren kennt. Oder aber auch Werkzeuge von Dritten aufkauft, um Verschlüsselung zu umgehen, dass diese möglichst lange benutzt werden können. Damit hat man natürlich auch indirekt ein Interesse, dass Sicherheitslücken nicht geschlossen werden, die man ausnutzen könnte. Und diese Art des Vorgehens halte ich für falsch.

Autor:
Constanze Kurz sieht nicht nur die konkrete Arbeit der Zentralen Stelle für Informationstechnik im Sicherheitsbereich kritisch. Sie weist grundsätzlich darauf hin, wie viele sehr persönliche Daten über jeden Einzelnen ohnehin schon im Umlauf sind:

O-Ton 26 – Constanze Kurz:
Als sei in der vordigitalen Zeit jedes einzelne Datum und jedes Gespräch abhörbar gewesen. Was natürlich nicht der Fall ist. In Wahrheit bringt die Digitalisierung sehr große Vorteile. Insbesondere für Geheimdienste und Strafverfolger, weil wir zum einen alles digital tun und damit die Wege sehr viel leichter abhörbar sind und zusätzlich noch die Metadaten dazukommen, dass man also auch weiß, wo geht jemand hin, mit wem spricht er. Aber in der öffentlichen Debatte hat man oft den Eindruck: Oje, alles ist verschlüsselt. Aber so sieht die Wahrheit eigentlich nicht aus.

Autor:
Auch der Karlsruher Anwalt Michael Rosenthal stört sich an dem Anspruch der Strafverfolger, im Zweifelsfall jede Kommunikation, auch verschlüsselte, mitlesen zu können:

O-Ton 27 – Michael Rosenthal:
Das ist leider überall so. Es fängt ganz klein an und es wird versichert, wir brauchen das nur für die schlimmsten Straftaten, dann wird es immer weiter ausgeweitet, weil man behauptet, man komme sonst nicht zu Potte. Dahinter steht für meine Begriffe eine, ja so eine Art logische Lüge. Es ist Unsinn, denn selbstverständlich wird der, der etwas zu verbergen hat immer darauf sinnen, dass das nicht ans Licht kommt und Kommunikationswege benutzen, die nach Möglichkeit verschlossen bleiben. Und selbstverständlich werden die Bösen den Guten immer einen Schritt voraus sein.

Autor:
Einen Schritt voraus sein, will auch die Bundesdruckerei: Das Berliner Unternehmen im Besitz des Bundes stellt Banknoten und Steuerzeichen her. Dazu komplette Pass- und Ausweissysteme, die heutzutage ebenfalls kryptografische Produkte sind, etwa weil biometrische Daten verschlüsselt auf einem Chip gespeichert werden. Für die Personalausweise und Reisepässe hat ein Tochterunternehmen der Bundesdruckerei eine Public-Key-Infrastruktur aufgebaut.

O-Ton 28 – Kim Nguyen:
Ja, mein Name ist Kim Nguyen. Ich bin Geschäftsführer der D-Trust, Tochterunternehmen der Bundesdruckerei. Wir sind damit beschäftigt, im Prinzip diese berühmten Zertifikate zu erstellen, die dann eben digitale Identitäten halt darstellen, mit denen man dann verschlüsseln, signieren und andere Dinge machen kann.

Autor:
Man dürfe bei der Kryptografie niemals locker lassen, meint Kim Nguyen: Techniken, die gestern noch als utopisch galten, werden heute selbstverständlich in unsere Personalausweiskarten eingebaut. Weil diese Sicherheitsarchitektur in absehbarer Zeit wieder veraltet sein wird, müssen neue Verfahren entwickelt werden. Große Herausforderungen stellen sich durch neuartige Computer, deren Leistung schon bald einen großen Sprung machen werden, erklärt Walter Fumy. Er ist, Chief Scientist bei der Bundesdruckerei und international tätig im ISO-Komitee, das Sicherheitsstandards erarbeitet.

O-Ton 29 – Walter Fumy:
Eine dieser Entwicklungen ist am Horizont sichtbar. Es sind die Quantencomputer, die auf völlig neue Art letztlich ihre Berechnungen anstellen und manche der Kryptografie, wie wir sie heute kennen, im Prinzip wirkungslos machen.

Autor:
Quantencomputer, von denen bisher nur einzelne Prototypen existieren, nutzen quantenmechanische Effekte: Da, wo bisher ein Bit eindeutig für eine 1 oder eine 0 stand, steht künftig ein Qubit für eine ganze Reihe möglicher Zustände. Mit dieser Technik können große Datenbanken extrem schnell durchsucht und sehr große Zahlen in ihre Faktoren zerlegt werden. Quantencomputer könnten selbst asymmetrische Verschlüsselungen knacken. Die Public-Key-Infrastruktur, wie sie für Reisepässe, autonome Autos, Online-Banking sowie für die Email-Verschlüsselung eingesetzt wird, wäre nutzlos.

O-Ton 30 – Walter Fumy:
Bei Signaturverfahren oder bei Schlüsselaustauschverfahren, die auf asymmetrischen Verfahren beruhen und die ganz elementar sind, zum Beispiel für diese Zugriffsberechtigungsanfragen, wo ich authentifiziere, ob der Anfragende das Recht hat auf irgendein Datum zuzugreifen. Ja, und da brauchen wir neue Lösungen.

Autor:
Die Europäische Union hält die Quantentechnologie für so bedeutsam, dass sie im Mai 2016 ein „Quantum Manifest“ vorgestellt hat: Ein milliardenschweres Forschungsprojekt soll das volle Potenzial dieser Technologie ausschöpfen, so die offiziellen Erklärungen. Die Zeit drängt, denn es könnte sein, dass andere Staaten insgeheim längst weiter sind mit der Entwicklung von Quantencomputern.

O-Ton 31 – Walter Fumy:
Da bin ich völlig davon überzeugt, dass nicht alles offen gehandhabt wird. Dass bestimmte Institutionen an dem Thema forschen und nichts der Welt und der Wissenschaft mitteilen, wie weit sie sind. Die freie Wissenschaft glaubt, und da

gehen die Meinungen auch weit auseinander, glaubt, dass man in einem kleinen zweistelligen Jahresbereich soweit sein wird. Das können jetzt 10, 20, 30 Jahre bedeuten. Das weiß man nicht.

Autor:
Kurios erscheint dabei: Bereits lange vor seiner technischen Realisierung hat der US- amerikanische Mathematiker Peter Shor ein Programm für den künftigen Quantencomputer geschrieben, mit dem er dessen schier unglaubliches Rechenpotenzial theoretisch beweisen konnte. Das war in den 1990er Jahren. Nun trennen uns von dieser Realität wahrscheinlich nur noch zehn oder 15 Jahre:

O-Ton 32 – Fumy / Nguyen:
(Fumy): Ich rede von der Situation, wo wir eine Maschine bauen können, die universell genug ist, dass dieser angesprochene Algorithmus von Peter Shor darauf implementiert werden könnte und dass die heutige asymmetrische Kryptografie damit gelöst werden könnte, sage ich mal. **(Nguyen):** Also, es gibt ja Quantencomputer als Prototypen schon jetzt, aber die arbeiten dann zum Beispiel auf 4 bit oder so. Das ist jetzt noch keine echte Bedrohung, weil kryptografische Systeme dieser Größe können Sie selber im Kopf viel schneller lösen als der Quantencomputer braucht, um überhaupt gestartet zu werden. Aber darum geht es ja nicht, sondern es geht ja tatsächlich darum, ist es jetzt nur ein Skalierungsproblem, also kostet es nur noch Geld und Aufwand aus den vier Bit jetzt 1.000 Bit zu machen oder liegen da noch echte technische Fragestellungen dazwischen. Und das Letztere ist schon auch der Fall. Also, sonst könnte man das Ganze kommerziell ja jetzt auch schon beziehen, wenn es nur eine Frage von Geld wäre.

Autor:
Neue Verfahren müssen entwickelt werden, damit Verschlüsselung auch in Zukunft der Garant für Authentizität, Integrität und Vertraulichkeit im Datenverkehr ist.

O-Ton 33 – Schulklasse:
(Schüler): Ich hab halt nur ein bisschen was herausgefunden: Denk daran!
(Daniela Neu): Genau! Jetzt haben wir eine Idee davon, was du herausgefunden hast, aber wo hast du jetzt diese Buchstaben herausgefunden?

Autor:
„Denk daran, Plätzchen zu backen“ lautet die Botschaft, die die Drittklässler der Grundschule im Kreuzerfeld in Rottenburg am Neckar entschlüsselt haben: In der Vorweihnachtszeit haben sie an dem Wettbewerb „Krypto im Advent“ teilgenommen und erste Grundlagen in Kryptografie gelernt. Vielleicht sitzen unter ihnen zukünftige Ingenieure, die neue Verfahren erfinden, um Verschlüsselung auch im Zeitalter der Quantencomputer sicher nutzen zu können. Zum Beispiel Mohamed:

O-Ton 34 – Mohamed:
Man lernt vieles, um geheime Botschaften zu verschicken.

Atmo