
**GCHQ-DATENBANK „FLYING PIG“: Gesammelte Daten über TLS/SSL-Zertifikate dienen der Erleichterung von Angriffen etwa auf Onlinebanking.**



**Zentrale der National Security Agency in Fort Meade, US-Bundesstaat Maryland**

# Fliegendes Schwein

**Datenschutz** Die schlechte Nachricht: NSA und GCHQ knacken verschlüsselte Kommunikation im Internet – mit großem Einsatz und großem Erfolg. Das zeigen Dokumente Edward Snowdens. Die gute Nachricht: Es ist dennoch möglich, Daten zu schützen.

Wenn Weihnachten naht, können sich die Mitarbeiter der Überwachungszentrale GCHQ im englischen Cheltenham vom harten Alltagsgeschäft des Ausspähens erholen. Statt Verschlüsselungen in aller Welt zu knacken, spielen sie ihr „Kryptos Kristmas Kwiz“. Anspruchsvolle Zahlen- und Buchstabenrätsel sind zu lösen. Die stolzen Gewinner des Wettstreits erhalten eine besondere Teetasse, eine „Kryptos“-Tasse.

Verschlüsselung – die Nutzung mathematischer Methoden, um Kommunikation vor Ausspähung zu schützen – wird für elektronische Transaktionen aller Art genutzt, von Regierungen, Firmen und privaten Nutzern. Aber ein Blick in das Archiv des Whistleblowers Edward Snowden zeigt: Nicht alle Verschlüsselungstechniken halten, was sie versprechen.

Skype zum Beispiel, das von 300 Millionen Menschen genutzte Programm zum Videotelefonieren, wird als sicher gepriesen. In Wahrheit gibt es diese Sicherheit nicht. „Dauerhafte Skype-Sammlung begann im Februar 2011“ – so steht es in einem NSA-Schulungspapier aus dem Snowden-Archiv. Knapp ein halbes Jahr später, im Herbst 2011, meldeten die Spione laut diesen Unterlagen Vollzug. Daten von Skype sind seitdem für die Überwacher zugänglich. Software-Gigant Microsoft, dem Skype gehört, erklärt dazu: „Wir versorgen Regierungen nicht mit direktem oder freiem Zugang zu Kundendaten oder Codierungsschlüsseln.“ Das ist offensichtlich nur ein Teildementi: Direkte und bezahlte Übermittlung der Kommunikation der Skype-Nutzer ist damit nicht ausgeschlossen. Seit Februar 2011 ist Skype aufgrund der Anordnung eines geheimen Gerichts als Datenquelle für die NSA verfügbar.

Die „dauerhafte Skype-Sammlung“ ist ein weiterer Schritt der Behörde in dem Wettlauf, den sich Überwacher und Überwachte im Internetzeitalter liefern. Man-

FOTO: NATIONAL SECURITY AGENCY / DPA

che Codierungen sind allerdings auch so gut, dass sie Jahrzehnte überdauert haben und zu Standards geworden sind.

Für die NSA ist Kommunikation, wenn sie verschlüsselt abläuft, ein einziges Ärgernis. In einem internen Schulungsdokument, das der SPIEGEL einsehen konnte, fragt der Referent: „Wussten Sie, dass allgegenwärtige Verschlüsselung im Internet eine große Bedrohung für die Fähigkeit der NSA darstellt, Aufklärung in Datennetzen zu betreiben oder feindliche Schadsoftware zu bezwingen?“

Aus den Snowden-Dokumenten lässt sich ersehen, welche Verschlüsselungsverfahren wohl noch sicher sind und welche von der NSA geknackt wurden. Die Dokumente sind etwa zwei Jahre alt, aber Experten halten es für unwahrscheinlich, dass die Schnüffler mittlerweile wesentlich weiter gekommen sind. Snowden selbst erklärte nach seiner Flucht im Juni 2013 in Hongkong: „Richtig eingesetzte, starke Verschlüsselung gehört zu den wenigen Dingen, auf die man sich verlassen kann.“

Eine durchaus erstaunliche Bilanz: Trotz aller Bemühungen gibt es Programme, die teilweise mehr als 20 Jahre alt sind – und dennoch wohl bis heute sicher.

Aufgrund der digitalen Revolution ist Kryptografie nicht mehr ein exklusives Werkzeug von Geheimagenten. Inzwischen nutzt nahezu jedermann verschlüsselte Internetverbindungen, sei es beim Onlinebanking, beim Internetshopping oder beim Telefonieren. Netzaktivisten organisieren Kryptopartys, auf denen sie Interessierten das Verschlüsseln beibringen, um sicher und privat zu kommunizieren.

Kanzlerin Angela Merkel und ihr Kabinett nutzen Kryptotelefone. Und die Bundesregierung fordert auch die Bürger auf, sich zu schützen. Der Präsident des Bundesamts für Sicherheit in der Informationstechnik, Michael Hange, erklärte: „Wir schlagen Kryptografie vor, also konsequente Verschlüsselung.“

Das kann den Geheimdiensten nicht passen. Die Fünf-Augen-Allianz – die Geheimdienste Großbritanniens, Kanadas, Australiens, Neuseelands und der USA – verfolgt ein klares Ziel. Sie will Verschlüsselung im Netz an so vielen Stellen wie möglich aushebeln. Für ihren Feldzug gegen die Privatheit standen der NSA 2013 über zehn Milliarden Dollar zur Verfügung, der Etat des britischen GCHQ ist Staatsgeheimnis, dürfte aber bei über einer Milliarde Pfund im Jahr liegen.

Im vorigen Jahr berichtete der *Guardian* über eine Präsentation des NSA-Entschlüsselungsprogramms „Bullrun“ von 2010. Darin heißt es: „Im vergangenen Jahrzehnt hat die NSA einen aggressiven, vielschichtigen Ansatz verfolgt, um die verbreiteten Verschlüsselungstechniken zu knacken.“ Und: „Gewaltige Mengen verschlüsselter Internetdaten, die bislang weggeworfen wurden, lassen sich nun auswerten.“

Noch ist es eine Minderheit der Internetnutzer, die sich um ihre Privatheit sorgt und ihre Daten schützt. Den anderen erscheint das Verschlüsseln, das sie fälschlicherweise für eine Geheimwissenschaft halten, schlicht zu kompliziert. Oder sie glauben, dass die Experten der Geheimdienste ihnen haushoch überlegen seien und jede Verschlüsselung knacken könnten.

Dem ist nicht so. Wie ein Dokument aus dem Snowden-Archiv belegt, scheiterte die NSA zumindest bis 2012 an der Entschlüsselung mehrerer Kommunikationsprotokolle. Welche das sind, lässt sich diesem Dokument, einer NSA-Präsentation für eine Konferenz im Jahr 2012, entnehmen. Die NSA-Kryptologen teilten ihre Ziele in fünf Gruppen ein, entsprechend dem Schwierigkeitsgrad des Angriffs und entsprechend seinem Ergebnis – von „trivial“ bis „katastrophal“.

Als „trivial“ gilt demnach die Verfolgung des Weges, den ein Dokument im Netz nimmt. „Geringe“ Probleme bereitet es angeblich, Facebook-Chats mitzuschneiden; immerhin „mäßiger“ Aufwand ist zu betreiben, um Mails des Moskauer Anbieters Mail.ru zu entschlüsseln. Alle drei Schwierigkeitsstufen scheinen der NSA allerdings noch keinen großen Kummer zu bereiten.

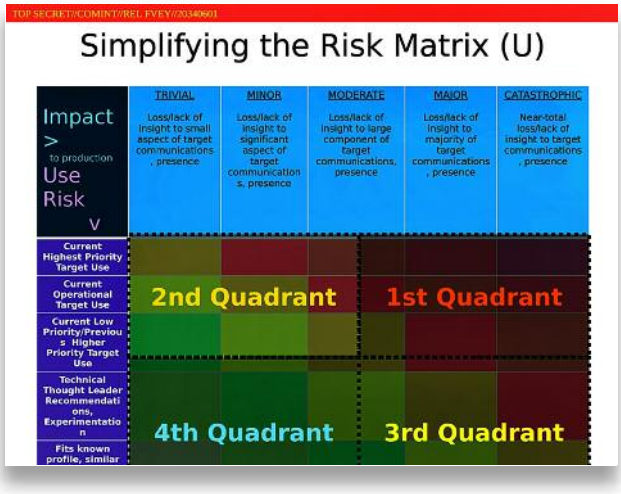
Der beginnt wohl auf Stufe vier. „Größere“ Probleme bereiten den NSA-Überwachern offenbar E-Mail-Dienstleister, die auf starke Verschlüsselung setzen, etwa Zoho oder das für anonymes Surfen im Internet entwickelte „Tor“-Netz. Tor steht für „The onion router“ und ist ein freie offene Software, mit der sich der Nutzer einen verschlungenen Weg durch mehr als 6000 Computer von Freiwilligen bahnt. Die Daten werden, wie bei einer Zwiebel, von einer Verschlüsselung nach der anderen umhüllt und wieder befreit. Für Überwacher ist so kaum zu rekonstruieren, woher der Aufruf einer bestimmten Website stammte.

„Größere“ Probleme hat die NSA auch mit Truecrypt, einem Programm zur Verschlüsselung von Dateien auf Computern, und mit dem sogenannten Off-the-record-Protokoll (OTR) zur Codierung von Chats. Beides sind Open-Source-Projekte, also Programme, deren Quellcode jeder Interessierte einsehen kann. Solche Software, darin sind sich die Experten einig, ist viel schwieriger von Geheimdiensten zu manipulieren als Systeme, die Konzerne wie Apple oder Microsoft entwickeln. Schließlich kann sich bei Open-Source-Projekten jeder den Programmcode ansehen, heimliche Hintertüren lassen sich kaum einbauen. Bei der Überwachung eines Chats stellte die NSA frustriert fest: „Keine Entschlüsselung verfügbar für diese OTR-verschlüsselte Nachricht.“

„Katastrophal“ – Stufe fünf – wird es für die NSA, wenn eine Zielperson beispielsweise eine Kombination aus Tor und einem weiteren Anonymisierungsdienst, wie dem quelloffenen Instant-Messaging-System Cspace, nutzt. „Fast vollständiger Verlust von Erkenntnissen über die Kommunikation und den Aufenthaltsort der Zielperson“ sei die Folge einer solchen Kombination.

Zur sicheren Verschlüsselung von Gesprächen und Textchats auf Mobiltelefonen gibt es das Protokoll ZRTP, das der NSA anscheinend größere Probleme macht. Es wird etwa in den Open-Source-Programmen RedPhone und Signal verwendet. Ihr Entwickler Moxie Marlinspike sagt: „Es ist sehr befriedigend, dass für die NSA die mit unseren Apps verschlüsselte Kommunikation wie ein Blick durch Milchglas ist.“

Entwickelt hat ZRTP unter anderen der Amerikaner Phil Zimmermann, der Mann, der den bis heute gebräuchlichsten Verschlüsselungsstandard für E-Mails und Dokumente geschaffen hat. Er ist bekannt unter der Abkürzung PGP, ausgeschrieben: Pretty Good Privacy – ziemlich gute Privatsphäre. Auch an diesem mehr als 20 Jahre alten Verschlüsselungsstandard bei-




**RISIKOMATRIX: So schätzt die NSA Verschlüsselungsverfahren und ihre unterschiedlichen Anwender ein: E-Mails sind „trivial“, Facebook ist ein „kleineres“ Problem. Mit OTR, Tor und Truecrypt-Verschlüsselungen hingegen gibt es „größere Probleme“.**

ßen sich die NSA-Spione offenbar die Zähne aus. In einem weiteren Dokument, das der SPIEGEL einsehen konnte, heißt es über E-Mails, die sich die NSA vom E-Mail-Provider Yahoo verschafft hat: „Für diese PGP-verschlüsselte Nachricht ist keine Entschlüsselung verfügbar."

Phil Zimmerman schrieb PGP im Jahr 1991. Der Anti-Atomwaffen-Aktivist wollte sich unbehelligt mit Gleichgesinnten austauschen. Sein System erfreute sich schnell hoher Beliebtheit unter Dissidenten in aller Welt. Da es auch außerhalb der USA verwendet wurde, setzte die US-Regierung gegen Zimmermann Ermittlungen wegen des „Exports von Munition" in Gang. Zimmermann veröffentlichte daraufhin mit Freunden den Quellcode als Buch – dies war durch die in der Verfassung garantierte Meinungsfreiheit abgedeckt.

PGP gibt es heute in verschiedenen weiterentwickelten Varianten, die häufigste ist „GNU Privacy Guard" des deutschen Programmierers Werner Koch. Zu den Eigenheiten der Spionagewelt gehört es, dass auch britische und amerikanische Geheimdienstmitarbeiter eine PGP-artige Software zum Verschlüsseln nutzen.

Tatsächlich decken sich die Interessen von Hackern, die ihre Privatheit schützen wollen, und US-Behörden häufiger, als man erwarten könnte. Das Tor-Projekt – für das auch die Co-Autoren dieses Artikels, Jacob Appelbaum und Aaron Gibson, arbeiten – wurde ursprünglich mit Unterstützung der U. S. Navy entwickelt, um US-Geheimdiensten eine sichere Kommunikation zu ermöglichen.

Die Snowden-Dokumente können einerseits also all jene beruhigen, die der NSA alles zugetraut haben: Es scheint noch geschützte Wege zu geben. Andererseits belegen die Dokumente, dass die Überwachung schon sehr weit geht.

Ein Beispiel: „Virtual Private Networks", VPN, wie es vor allem Mitarbeiter von Firmen und Institutionen mit mehreren Standorten nutzen. Der Schutz des Netzes ist hier tatsächlich nur virtuell, nicht echt. Denn die NSA betreibt ein großes VPN-Projekt, um solche Verbindungen massenhaft zu knacken und die darüber ausgetauschten Daten mitzulesen – etwa das Netz der griechischen Regierung.

Schon für Ende 2009 ist in einem NSA-Dokument davon die Rede, dass tausend Anfragen zur Entschlüsselung von VPN-Verbindungen verarbeitet werden müssten – pro Stunde. Bis Ende 2011 sollte diese Zahl auf 100 000 pro Stunde gesteigert werden. „Mindestens 20 Prozent" dieser Anfragen sollte das System vollständig erfüllen, also den Datenverkehr „entschlüsseln und wieder einschleusen".

Mit anderen Worten: Bereits für Ende 2011 sahen die Pläne der NSA vor, 100 000 vermeintlich sichere VPN-Verbindungen pro Stunde parallel auszuspähen.

Als unsicher muss auch das Protokoll PPTP gelten, ein zentraler Bestandteil vieler VPN. In der NSA-Präsentation „Einführung in den VPN-Ausspähprozess" wird stolz vom Projekt „FOURSCORE" berichtet, das PPTP entschlüssle.

Dadurch sei der Zugang zu zahlreichen Netzwerken gelungen. Ausgespäht wurden etwa die russische Transaero Airlines, Royal Jordanian Airlines und die Moskauer Telekommunikationsfirma Mir Telematiki. Als Erfolg gepriesen wird auch die Überwachung der internen Kommunikation afghanischer, pakistanischer und türkischer Diplomaten.

Für die etwas besseren Verfahren wie IPSEC hat die NSA Angriffsmöglichkeiten entwickelt, mit denen nicht das Verfahren geknackt wird, sondern die Schlüssel entwendet werden.

Weniger Aufwand ist notwendig für einen Angriff auf all jene vermeintlich sicheren Verbindungen, die jeder Internetnutzer ständig verwendet: um Bankgeschäfte zu erledigen, online einzukaufen oder den Web-E-Mail-Account einzusehen.

Sicher ist nichts davon. Die NSA kann mit einem Programm sogar das Protokoll SSH („Secure Shell") knacken. Mit SSH-Verbindungen loggen sich Administratoren ein, um mit anderen Computern zu arbeiten und sie zu steuern. Die Schnüffler sammeln die so gewonnenen Daten zusammen mit anderen Informationen über geknackte Verschlüsselungen in einer Datenbank. Für andere Systeme gibt es ebenfalls Datenbanken.

Telefonsysteme in aller Welt beruhen auf entzifferter Verschlüsselung und sind so gestaltet, dass sie für das Abschöpfen anfällig sind. In den Snowden-Dokumenten lässt sich nachvollziehen, dass die NSA sich Zugang zu Daten verschafft hat, die von Strafverfolgern bei Ermittlungen beschafft wurden, zum Beispiel in Russland und im Irak. Die NSA erklärt zu diesen und allen anderen Vorwürfen, dass sie sich strikt an die US-Gesetze halte.

Die NSA reklamiert für sich und ihre Verbündeten, solche Verbindungen routinemäßig und millionenfach zu knacken. Für Ende 2012 sieht ein NSA-Dokument zehn Millionen geknackte https-Verbindungen pro Tag vor. Besonders interessieren sich die Überwacher für den Moment, in dem ein Nutzer sein Passwort eintippt: 20 000-mal im Monat sollte das System Ende 2012 jeweils „mindestens 100 Passwort-basierte Verschlüsselungsanwendungen entdecken". Erkenntnisse über Verschlüsselungen mit den verbreiteten Protokollen TLS und SSL sammelt der britische Geheimdienst in der Datenbank „Flying Pig", fliegendes Schwein.

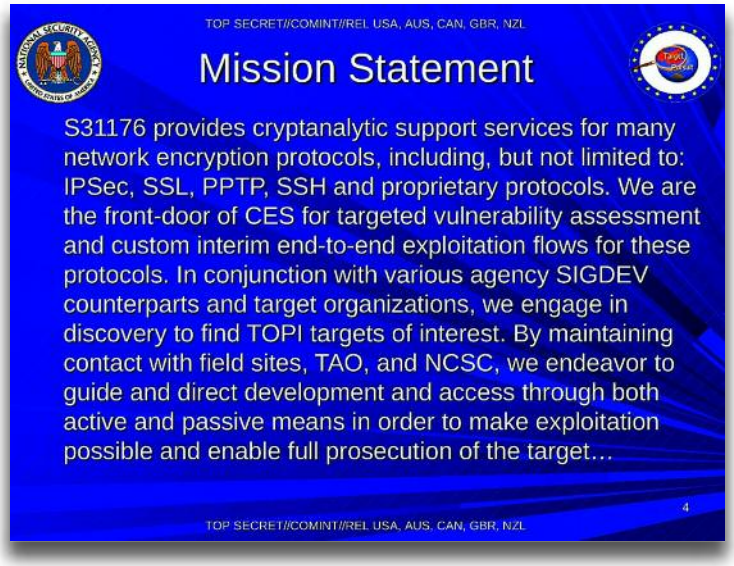
Die Spione Ihrer Majestät speichern in dieser Datenbank alle Informationen über die Nutzer von Verschlüsselungsprogrammen, deren sie habhaft werden können: wann wer mit wem und mit welcher Verschlüsselung telefoniert oder E-Mails austauscht.

In der Schattenwelt der Geheimdienste amüsieren sich die Überwacher wahrscheinlich köstlich darüber, was arglose, normale Internetnutzer für sicher halten. Allein im britischen Geheimdienst GCHQ waren vor rund vier Jahren 832 Personen über das NSA-Projekt „Bullrun" informiert, dessen Ziel dieser Großangriff auf die Internetverschlüsselung ist.

Skype jedenfalls macht den Spähern offenbar keine Mühe mehr. Wer sich darüber unterhält, sollte allerdings nicht glauben, dass nur amerikanische Spione mithören und mitschauen können.

Auch der russische Geheimdienst hat laut verlässlichen Berichten Skype schon vor Jahren geknackt.

Jacob Appelbaum, Aaron Gibson, Christian Grothoff, Andy Müller-Maguhn, Laura Poitras, Michael Sontheimer, Christian Stöcker




**LEITSPRUCH EINER NSA-ENTSCHLÜSSELUNGSABTEILUNG**
**„Aktive und passive Maßnahmen, um Auswertungen und volle Verfolgung von Zielen zu ermöglichen."**

**Lesen Sie weiter auf Seite 80**
**Die geheimen Todeslisten: Wie Amerikaner und Briten in Afghanistan Taliban jagten – gezielte Tötungen gehörten zum Alltag.**