Inhalt

Ist **das Ende von Verschlüsselung** und Datensicherheit eingeläutet? Mit dieser Frage sieht man sich aufgrund jüngster Enthüllungen Edward Snowdens zwangsläufig konfrontiert.

Das Ende von Verschlüsselung

Als Sicherheitsexperte und Hersteller von Verschlüsselungstechnologie steht man vor einem Problem. Der ausgesprochene **Generalverdacht** gegenüber Verschlüsselungsverfahren und Firmen, die Geld mit diesen Technologien erwirtschaften, sorgt bei Anwendern für ein Klima extremen Misstrauens.

> Verschlüsselungsverfahren sind „geknackt“, alles kann mitgelesen und mitgeschnitten werden. Firmen bauen auf Bitten von NSA (*National Security Agency*) und GCHQ (*Government Communications Headquarters*) Hintertüren (*Backdoor*) in Software ein und gewähren den Geheimdiensten willfährig Zugriff auf die Daten ihrer Anwender.

So die Behauptungen! Doch was steckt wirklich dahinter?

Offensichtlich betreibt die NSA ein geheimes Spähprogramm namens **Bullrun**, welches mit jährlich 250 Mio. US Dollar finanziert wird. Ziel dieses Programmes ist es, allgemeine gesprochen, den Zugang zu verschlüsselten Daten zu ermöglichen. **Ich staune über das Staunen.** Schon immer gab es solche Bestrebungen und schon immer versuchte die NSA verschlüsselte Daten zu „knacken". Es gehört zur Aufgabe eines Geheimdienstes, sich Zugang zu solchen Informationen zu beschaffen. Wer anderes denkt oder dachte, der liegt und lag falsch.

Betrachten wir, welche Möglichkeiten es für den Geheimdienst überhaupt gibt, um eine Verschlüsselung zu „knacken" *

1. **Der mathematische Weg**
   Mathematisch geknackt würde konkret bedeuten, dass man zum Entschlüsseln einer Nachricht nicht 100 Jahre benötig, sondern nur eine Stunde, weil man eine Formel gefunden hat, die die Berechnung erheblich verkürzt. Es ist jedoch davon auszugehen, dass die zugrundeliegenden mathematischen Verfahren, die eigentlichen Verschlüsselungsalgorithmen wie RSA (*Rivest, Shamir und Adleman*), AES (*Advanced Encryption Standard*) und andere, weiterhin in der Reinform sicher sind und **nicht geknackt** wurden. Die zugrundeliegenden Verfahren überfordern selbst die Supercomputer der NSA. Eine Unzahl an Fachleuten (*ich meine Fachleute!*) hat die Verfahren analysiert, ohne wirklich praxisrelevante Schwachstellen gefunden zu haben.
2. **Gezielter Einbau von Schwachstellen in Hard- und Software**
   In meiner Laufbahn bin ich sehr oft mit dem Begriff **Backdoor** (*Hintertür*) konfrontiert worden. Dabei handelt es sich um eine Möglichkeit, mit der man ohne Kenntnis des verwendeten Passwortes/Schlüssels (*oder von Teilen des Schlüssels*) Zugang zu den vermeintlich sicher verschlüsselten Daten hat.Ein Beispiel aus meiner Erfahrung: Im Rahmen eines Projektes arbeitete ich vor vielen Jahren mit dem System Lotus Notes/Domino. In diesem System kam eine Verschlüsselung zum Einsatz, die einen 64 BIT Schlüssel verwendete. Durchaus State-of-the-Art zur damaligen Zeit. Ich kann mich noch an den Schock erinnern, als plötzlich bekannt wurde, dass in der zum

Einsatz kommenden Version von Lotus Notes eine Hintertür für die NSA entdeckt wurde. Die NSA musste keinen 64 BIT Schlüssel brechen, sondern, Dank der Hintertür, nur noch einen 40 BIT Schlüssel. [NSA kann Bundeswehr Email knacken].Auch Hardware kann manipuliert sein. So wurde der Verdacht geäußert, dass Intel einen Baustein (*Intel Secure Key*), der für die Generierung von Zufallsdaten zuständig ist, derart manipuliert haben könnte, dass die Zahlen nicht so zufällig sind, wie dies nötig wäre. Greift eine Anwendung auf diesen Chip zu, um Zufallszahlen zu erzeugen, ist sie automatisch geschwächt.Derartige Manipulationen sind, sofern sie geschickt gemacht sind, kaum nachweisbar.Auch ohne den Einbau von Schwachstellen kann man mit Hilfe spezieller Programme, die eine Unzahl an gängigen Passwörtern und Passwortkombinationen durchtesten (*Wörterbuchattacke*), beachtliche Erfolge erzielen. Hier liegt die Verantwortung beim Anwender, der bei der Vergabe eines Passwortes nicht auf den Namen der Katze und das Geburtsdatum der Frau zurückgreifen sollte. Daten, die mit Passwörtern wie Mieze160494 oder Sommer2013 verschlüsselt wurden, sind in Nanosekunden geknackt.

3. **Besetzen von Schaltstellen**
   Warum sollte man den Aufwand betreiben, eine Verschlüsselung zu brechen, wenn man auf den Servern der Großen im Internet Zugriff auf die unverschlüsselten Daten der Anwender hat. Auch dann, wenn die Dienstanbieter (*Facebook, Google, Microsoft, Apple, WEB Maildienste, Clouddienste, etc.*) vorgeben, dass die Daten verschlüsselt abgelegt werden, haben Sie keine Sicherheit, dass dies wirklich der Fall ist. Zum Beispiel könnte Ihr 100 Zeichen langes Passwort einfach auf ein Standardpasswort gesetzt werden oder, wie im Beispiel von Lotus Notes gesehen, einfach gekürzt werden. Wie sollen Sie das merken?Gerade im Zusammenhang mit den jüngsten Enthüllungen zu **SSL** (*Secure Sockets Layer; veraltet – heute TLS*), der Basis für sichere Online-Kommunikation, kann man das Prinzip der Vorgehensweise der Geheimdienste sehr gut nachvollziehen. SSL ist ein Verfahren, welches für den sicheren verschlüsselten Datenaustausch zwischen Ihrem Rechner (*Client*) und einem Rechner im Internet (*Server*) sorgt. Wenn Sie zum Beispiel Geld überweisen, werden PIN, TAN und weitere Details zwischen Ihrem Browser und dem Bankrechner verschlüsselt übertragen. Nicht nur hier kommt das TLS Verfahren zum Einsatz. Auch beim sicheren Abrufen von E-Mails, beim Zugriff auf Cloud Dienste und bei s.g. VPN Verbindungen kommt das Verfahren zum Einsatz.Verschlüsselte Online-Kommunikation basiert auf dem **Prinzip des Vertrauens**. TrustCenter stellen, als Zertifizierungsstelle, Zertifikate aus, mit denen dann, vereinfacht ausgedrückt, die verschlüsselte Kommunikation eingeleitet wird. Und genau hier liegt das Problem. Der Markt für digitale Zertifikate wird von US Firmen beherrscht. Ein mathematischer Angriff ist schwierig und kaum zu gewinnen. Viel einfacher ist es, direkt Einfluss auf

die Zertifizierungsstellen zu nehmen. Dort lassen sich wunderbar geheime Schlüssel abgreifen, mit deren Hilfe man mitlesen kann!
Die Enthüllung, Edward Snowdens bestätigt eine Vermutung, die bereits im Jahre 2010 durch die Electronic Frontier Foundation (EFF) geäußert wurde. Eine Forschungsarbeit enthielt deutliche Indizien für das, was jetzt zu Tage tritt. SSL ist unsicher!Ein Grund, warum bei entsprechenden ArchiCrypt Verschlüsselungsprogrammen (*ArchiCrypt Online Disk und Passwort-Zentrale*) , niemals auf die Sicherheit von SSL und die der Server alleine gesetzt wird. Hier wird mit einem symmetrischen Verfahren zusätzlich auf dem Client (*Rechner des Anwenders*) verschlüsselt. Niemals landen also vermeintlich mit SSL geschützte Daten im Klartext auf einem Server. Selbst wenn die SSL geschützte Leitung abgehört wird oder ein direkter Zugriff auf die Daten des Servers möglich ist, muss sich ein Angreifer mit der symmetrischen Verschlüsselung plagen.

Wie können Geheimdienste Firmen zu einer solchen Mitarbeit bewegen? *

Es gibt viele Wege!

Die NSA kann über Strohmänner selbst Firmen betreiben, sie kann „Fördergelder“ bereitstellen, sie kann einzelne Mitarbeiter erpressen und bestechen, sie kann OpenSource Projekte infiltrieren, die alleine aufgrund des hohen Verbreitungsgrades von enormem Interesse sind und, sie kann Firmen die Pistole auf die Brust setzen und per Gesetzt zur Mitarbeit zwingen.

Leider werden in den Medien keine Firmen- und keine Programmnamen genannt. Die allgemein gehaltenen Formulierungen führen genau zu dem Generalverdacht, der eine komplette Branche, darunter viele Gute, trifft, wie ein Hammerschlag. Wäre für den Anwender klar erkennbar, dass Firma X mit Produkt A mit der NSA zusammenarbeitet, könnte man gezielt eben auf die „saubere“ Firma Y mit Produkt B zurückgreifen.

> **Erst dann, wenn Ross und Reiter genannt werden, kann man gezielt handeln! Wir brauchen die Firmennamen derjenigen, die unser Vertrauen missbraucht haben!**

Wie soll man sich verhalten? *

Ein großer Fehler wäre es, künftig auf jede Art von Verschlüsselung zu verzichten. Sie würden auf der Baustelle des Berliner Flughafens auch nicht ohne Helm herumspazieren, nur weil Sie wissen, dass der Helm Sie vor den herabfallenden Stahlträgern (*Geheimdienste*) nicht schützt. Denken Sie an Schrauben und Steine (*Hacker und Datendiebe*).

> **Wie oben erwähnt, halte ich es für eine Tatsache, dass die mathematischen Verfahren (*Verschlüsselungsalgorithmen*) NICHT geknackt wurden.**

Dafür spricht eindeutig der Umstand, dass die Geheimdienste Firmen zur Mitarbeit bewegen müssen und damit zumindest immer riskieren, dass diese Kooperation an die Öffentlichkeit gerät. Wären die Verfahren an sich geknackt, müsste man sich dieser Gefahr nicht aussetzen, sondern könnte entspannt in der stillen Kammer mitlesen.

Daraus kann man jetzt zwei konkrete Maßnahmen ableiten: *

1. Angenommen, die Geheimdienste haben Zugriff auf die privaten Schlüssel in den Zertifikaten. Der Verdacht liegt, wie oben erläutert, sehr nahe! Ja, NSA und GCHQ können dann Daten bei verschlüsselter Internetkommunikation mitlesen. Bei diesen Verbindungen muss man, die potentielle Gefahr des Abgehörtwerdens im Hinterkopf habend, von Fall zu Fall entscheiden. Wer beim Online-Shoping, beim Online-Banking ausschließen möchte, dass er grundsätzlich ausgespäht werden könnte, muss darauf verzichten! Wenn Sie sich entschließen, die Online-Dienste zu nutzen, verwenden Sie unbedingt Verschlüsselung. Denken Sie an die Schrauben und Steine (*Hacker und Datendiebe*).
2. Seien Sie bei der Wahl geeigneter **Verschlüsselungsprogramme sehr wählerisch**!

Internationale Projekte sollten Sie mit äußerster vorsichtig nutzen, eher meiden. Setzen Sie auf **rein deutsche Projekte und Produkte**.Hier kann ich Ihnen ein paar Fakten nennen, die mir im Zusammenhang mit Geheimdiensten und Behörden in besonderer Erinnerung geblieben sind und deutlich untermauern, dass **die Welt in Deutschland zurzeit noch in Ordnung** ist.Über die vielen Jahre hinweg erhielt ich unzählige E-Mails und Anrufe, in denen Mitarbeiter des LKA oder des BKA um Hilfe baten, weil ein Verdächtiger Daten mit ArchiCrypt Live verschlüsselt oder Spuren mit ArchiCrypt Shredder beseitigt hat. Niemals wurde in irgendeiner Weise gedroht oder Druck ausgeübt, wenn ich bedauern musste, nicht helfen zu können. [*Anm.: In diesen Situationen geht es mir oft wie dem Hersteller von Steakmessern. Man kann nicht verhindern, dass jemand auf die Idee kommt, das Messer als Waffe zu verwenden. Deshalb aber das Messer stumpf machen?*]Nie in all den Jahren trat der Geheimdienst mit der Bitte an mich heran, eine Hintertür in irgendein Softwareprodukt einzubauen. Gleichzeitig verwenden einige Behörden die ArchiCrypt Produkte.Vor allem als ich den **Anti-Bundestrojaner** geschrieben habe, rechnete ich fest damit, dass man in irgendeiner Weise auf mich zukommt. Was ist passiert? Nichts!

FAZIT *

Verschlüsselung ist NICHT am Ende. Verschlüsselungsverfahren sind mathematisch nicht geknackt und Sie sollten selbstverständlich weiter auf Verschlüsselung setzen. Ein Verzicht darauf bringt sie unter Umständen in Teufels Küche und spielt den Diensten und anderen (*Datendiebe*) in die Hand. Achten Sie darauf, dass Sie möglichst Produkte rein deutscher Firmen einsetzen. In Deutschland gibt es keine gesetzliche Grundlage, die Firmen zum Einbau einer Hintertür zwingt. Deutsche Geheimdienste und Behörden üben keinen Druck auf die Firmen aus. Geht es um sichere Online-Kommunikation via SSL, seien Sie sich darüber im Klaren, dass der amerikanische und britische Geheimdienst Ihre Daten vermutlich mitlesen kann!

Was wir dringend benötigen sind die Namen der Firmen die uns hintergangen haben. Erst dann wissen wir, wem wir weiter trauen können!