Presseinformation

# Ist Verschlüsselung noch sicher?

*München, 12. September 2013. Praktisch alle gesicherten Vorgänge im Internet basieren auf der SSL-Verschlüsselung. Während Firmen und Privatleute noch auf SSL vertrauen, deuten aktuelle Medienberichte an, dass Verschlüsselung für den amerikanischen Geheimdienst NSA kein Hindernis mehr darstellt. Der NSA soll es gelungen sein, gängige Internet-Verschlüsselungsmethoden zu umgehen. Damit sei es möglich, große Teile des verschlüsselten Internet-Verkehrs zu überwachen. Das entsprechende Programm zur Entschlüsselung des Internet-Verkehrs soll den Namen Bullrun tragen und 255 Millionen US-Dollar pro Jahr gekostet haben. Inhaltlich verraten die Berichte in den allgemeinen Medien jedoch nichts, was in der Fachwelt nicht schon seit Jahren Allgemeingut wäre.*

Der deutsche Sicherheitsexperte Dr. Hubert Jäger, Geschäftsführer des IT-Sicherheitsdienstleisters Uniscon (1), fasst den derzeitigen fachlichen Stand zum Thema Verschlüsselung wie folgt zusammen:

Generell galt und gilt, dass es keine absolute Sicherheit gibt, daher vermeiden ernsthafte Sicherheitsdienstleister wie Uniscon auch Formulierungen, die so verstanden werden könnten. Sicherheit/Privatheit ist vielmehr die Ökonomie des Schutzes: Hohe Sicherheit und in Folge zuverlässige Privatheit bedeuten, dass die Attacke deutlich teurer kommt als die Beute wert ist.

Außerdem galt und gilt, dass eine Sicherheitskette nur so stark ist wie ihr schwächstes Glied. Häufig neigen Sicherheitstechniker aber dazu, gerade die Glieder der Kette, von denen sie glauben, sie nicht sicher gestalten zu können, in ihrem Konzept zu verdrängen. An dieser Stelle setzen wir bei der Uniscon GmbH auf unserem Spezialgebiet, Sicherheit in der Cloud, an: In einer „ABC-Analyse“ der Sicherheitsketten liegt die Sicherheit beim Betreiber von Cloud-Diensten, E-Mail-Diensten und Webservern, an erster Stelle bei möglichen Lecks. Das heißt also das Risiko ist besonders hoch. Die Sicherheit der Endgeräte ist das zweitgrößte Sicherheitsloch. Die verschlüsselte Übertragung über SSL/TLS ist

dann nur noch das drittwichtigste Leck.

Bislang werden oft ohne echten Beweis die Dienstanbieter sowie die Geräte-, Betriebssystem- und Anti-Virus-Hersteller als vertrauenswürdig angesehen. Die Datenskandale sind jedoch überwiegend auf Untreue und Lecks bei den Anbietern zurückzuführen, nicht auf geknackte Verschlüsselungen. Es ist also geboten, sich erst um das schwächste Glied in der Sicherheitskette und dann um das zweitschwächste usw. zu kümmern. Also sind zuerst Betreibersicherheit und vertrauenswürdige Endgeräte zu verbessern, dann ist eine besonders sichere Verschlüsselung zu entwickeln.

Nun zur Verschlüsselung: Wenn in den Medien über „geknackte“ Verschlüsselungen berichtet wird, so wird in der Regel nicht zwischen den verschiedenen Methoden unterschieden.

1. Bei SSL/TLS ist die einfachste Methode des Abhörens, sich als Mann in der Mitte zwischen Sender und Empfänger zu stellen. Man muss dazu eine zweite verschlüsselte Verbindung aufbauen, von der – und das ist das Problem – der normale Nutzer in gewöhnlichen Browsern nichts mitbekommt, während Experten die Zertifikatsdetails anschauen und den Angriff erkennen können. Die Geheimdienste beherrschen diese Methode wahrscheinlich, da sie bei manchen Zertifikatserstellern so genannte Root-Zertifikate erhalten haben, oder vielleicht auch in den Browsern eigene Root-Zertifikate deponiert haben. Deswegen enthält das Firefox-Add-in für IDGARD eine automatisierte Angriffserkennung.
2. Eine zweite Methode des Abhörens ist, den verschlüsselten Datenstrom zu kopieren und dann alle möglichen Schlüssel automatisiert durchzuprobieren. Das dauert bei guter Verschlüsselung sehr lange. Bei mangelhafter Verschlüsselung kann das bei hohen Rechenleistungen und entsprechenden Kosten für die Geheimdienste aber inzwischen auch sehr schnell bewerkstelligt werden. IDGARD besitzt für seine Verschlüsselung ein A-Rating. Das bedeutet, alles, was im Bereich SSL/TLS sicherheitstechnisch erreichbar ist, wurde erreicht. Mittelfristig wird IDGARD optional eine weitere Verschlüsselung „on-top“ anbieten.
3. Eine weitere Möglichkeit, Verschlüsselung zu knacken, sind der Fachöffentlichkeit unbekannte bzw. geheime „Back Doors“, also bislang unentdeckte Einfallstore oder

Schwächen der Implementierung. Diese können Angreifer zur Entschlüsselung nutzen, wenn sie den Datenstrom kopiert haben. Hiergegen helfen nur „Open Source“-Implementierungen, die beispielsweise bei IDGARD eingesetzt werden, wo immer es geht.

Dass Privat- und Geschäftskommunikation abgehört wird, sollte mittlerweile jedem klar sein. Heute geht es in erster Linie darum, dass das verdrängte Sicherheitsproblem beim Betreiber, zum Beispiel von Cloud-Diensten, E-Mail-Diensten und Webservern, angegangen wird. Die meisten Sicherheitskonzepte von Cloud-Anbietern berücksichtigen den Unsicherheitsfaktor „Mensch“ nicht in umfassender Form. Um Vertrauen und Integrität in der Cloud umsetzbar zu machen, hat Uniscon die Sealed-Cloud-Technologie entwickelt.

Unternehmensdaten, die auf Sealed Cloud Servern gespeichert sind, sind technisch so abgesichert, dass sie vor den Blicken Außenstehender und sogar vor den Blicken des Cloud-Betreibers geschützt sind. Mit dem auf der Sealed Cloud entwickelten Dienst IDGARD können Nutzer über ein Web-Interface oder eine der IDGARD Apps für Smartphones und Tablets auf geschützte Daten in der Sealed Cloud zugreifen und mit ihren Partnern sicher kommunizieren. Seit wenigen Wochen stellt der Dienst zusätzliche Funktionen, wie beispielsweise einen abhörsicheren Chat, als sichere Alternative zu den Chats in Skype oder WhatsApp zur Verfügung. Auch bei der Nutzung von E-Mails arbeiten viele Nutzer ohne einen angemessenen Datenschutz und legen täglich eigene und fremde Informationen offen. Mit IDGARD lässt sich das vermeiden, da der Dienst sichere Kommunikationsräume schafft, die von allen üblichen Plattformen aus nutzbar sind.

**Über Uniscon GmbH –**

Uniscon – The Web Privacy Company entwickelt technische Lösungen zur sicheren und bequemen Online- Geschäftskommunikation. Der Service ID|GARD für Unternehmen basiert auf der weltweit patentierten Sealed Cloud Technologie. Dabei werden die Daten in der Cloud geschützt, so dass selbst der Betreiber des Portals keinen Zugriff auf die Daten seiner Kunden hat. Die Unternehmensdaten bleiben damit ausschließlich im Besitz des Eigentümers. Die Sealed Cloud Technologie wird durch ein von Uniscon geführtes Konsortium im Rahmen der

Presseinformation

Trusted Cloud Initiative des BMWi zur generellen Nutzung durch die deutsche Industrie weiter entwickelt. Weitere Informationen finden Sie unter www.uniscon.de, www.sealedcloud.de und www.idgard.de.

**Pressekontakt**
Uniscon GmbH/Claudia Seidl
Agnes-Pockels-Bogen 1
80992 München
089 / 41 615 988 110
presse@uniscon.de
www.uniscon.de

PR-Agentur Xpand21 GmbH
Doris Loster
Romanstr. 10
80639 München
089 / 71 68 07 35
uniscon@xpand21.com
www.pr-agentur-xpand21.de