

Daten unknackbar verschlüsseln

Ideales Tool für Unternehmen

Die Dominanz US-amerikanischer IT-Produkte ist in Sachen Datenschutz von Nachteil, wie nicht zuletzt die NSA-Affäre zeigte, die der Whistleblower Edward Snowden ins Rollen brachte. Unternehmen, die per E-Mail sensible Unterlagen versenden müssen, sollten daher auf Sicherheit setzen. Diese wird von ›Xchange‹ gewährleistet, einer Verschlüsselungssoftware, die vom Unternehmen Remus angeboten wird.

Ob Krieg im Nahen Osten, VW-Abgasaffäre oder Abhören des Handys der Bundeskanzlerin, die Fäden laufen oft in den USA zusammen. Doch haben auch die Geheimdienste anderer Staaten ihre Finger mit im Spiel, wenn es gilt, Ereignisse zum eigenen Vorteil ins Rollen zu bringen. Alles was dazu nötig ist, sind Daten, Daten und nochmals Daten.

Da deren Beschaffung per Internet besonders einfach vonstattengeht, hat nicht zuletzt China in diesem Bereich ein riesiges Heer an Mitarbeitern geschult, die durch Wirtschaftsspionage alleine in Deutschland einen Schaden von rund 50 Milliarden Euro pro Jahr verursachen.

Kritische Abhängigkeit

Vor diesem Hintergrund ist es extrem bedenklich, dass mittlerweile fast alle Computer-Prozessoren in Asien produziert werden. Es sollte auf der Hand liegen, dass es problemlos möglich ist, in diesen Chips Funktionsblöcke unterzubringen, die per Codesignal mit einem Schlag sämtliche damit bestückten Anlagen ausschalten können. Ob CNC-Maschine, Roboter, selbstfahrendes Auto oder westliche Waffen, alles könnte lahmgelegt werden.

Angesichts der Aktivitäten östlicher wie westlicher Geheimdienste müssen sich heimische Unternehmen fit in Sachen ›Schutz der eigenen Daten‹ machen. Wenn es mangels Alternativen schon nicht mehr möglich ist, den Einbau von Chips, Computer-

platinen oder Steuerungen aus zweifelhafter Produktion zu verhindern, sollten wenigstens die eigenen Betriebs- und Konstruktionsdaten optimal geschützt werden.

Schützen ist Pflicht

Es ist grob fahrlässig, wenn wichtige Unterlagen ungeschützt per E-Mail an Tochterunternehmen oder Zulieferer verschickt werden. Die Wahrscheinlichkeit ist hoch, dass die Daten als Kopie auch auf der Festplatte eines Geheimdienst-Rechenzentrums landen. Wer vor dem Versand die Daten jedoch verschlüsselt, hat schon einen großen Schritt in Richtung Datensicherheit gemacht. Doch gilt es hier ge-



Einfache Bedienung: Per Drag & Drop werden die zu verschlüsselnden Daten zusammengetragen.

nau hinzuschauen, welches Softwareprodukt dafür verwendet wird. Amerikanische Produkte sind mit Vorsicht zu genießen. Die Vielzahl an Bemühungen der amerikanischen Geheimdienste, direkt

oder indirekt Einfluss auf Firmen mit dem Betätigungsfeld ›Datensicherheit‹ zu nehmen, zeigt eindeutig, wohin die Reise geht. Auch hat man sich über Beteiligungen und Firmengeflechte den Zugriff auf wichtige Knotenpunkte der Internet-Infrastruktur gesichert, um Daten abgreifen zu können.

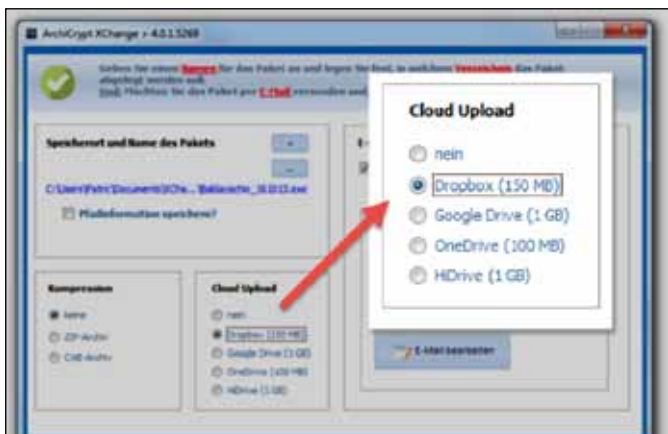
Fragwürdiges Handeln

Der ›Patriot Act‹ lässt Spekulationen mehr als zu. Unter dem Deckmantel der Terrorbekämpfung wird Verschlüsselung zum nationalen Feind erklärt. Die Haltung der Trump-Regierung zum Thema ›Verschlüsselung‹ ist eindeutig. Das Problem an einer Abschwächung von Verschlüsselung ist, dass derartige Schwächen nicht nur von vermeintlich guten Mächten verwendet werden.

Sicherheitsexperten sind sich einig, dass Hintertüren in Sicherheitssoftware nicht unentdeckt bleiben und im Zweifelsfall genau denen Zu-



Mit ›Xchange‹ bietet das deutsche Unternehmen Remus eine Verschlüsselungssoftware an, an der sich selbst Geheimdienste die Zähne ausbeißen.



Um sehr große Dateien versenden zu können, werden Cloud-Dienste verwendet.



Zur Information des Empfängers können eigene Themes erstellt werden, die sogar über QR-Code verfügen können.

griff gewähren, denen man eigentlich gezielt den Zugriff verwehren wollte.

Sicherheit zuerst!

Die Verschlüsselungssoftware ›ArchiCrypt XChange‹ wird ausschließlich in Deutschland entwickelt und nur im deutschsprachigen Raum vertrieben. Für Patric Remus, Inhaber der Firma Softwareentwicklung Remus, ist es eine Selbstverständlichkeit, dass seine Software niemals Möglichkeiten besitzen wird, Nachrichten mitzulesen oder wichtige Dokumente zu sichten. Er stellt klar, dass Sicherheitslösungen mit Backdoor, egal für wen, keine Sicherheitslösungen sind.

ArchiCrypt XChange setzt den Advanced Encryption Standard (AES) ein, der in den USA sogar für staatliche Doku-

mente mit höchster Geheimhaltungsstufe zugelassen ist. Ein sogenannter Brute Force-Angriff auf ein verschlüsseltes Dokument wäre selbst mit den derzeit schnellsten Rechnern aussichtslos.

Die Bedienung des Programms ist ein Musterbeispiel an Eleganz und Einfachheit: Es muss lediglich das zu versendende Dokument per Drag & Drop auf das Programmfenster geschoben werden und kann anschließend verschickt werden.

Geniale Software

Absolut genial ist, dass die Mails einen Umfang von bis zu einem Gigabyte haben dürfen, was keineswegs selbstverständlich ist. Üblicherweise ist die Größe pro Mail im Schnitt auf einige Megabyte begrenzt. Der großzügige Umfang

kommt durch die Nutzung von Cloud-Dienstleistern, wie etwa Dropbox, Google Drive oder HiDrive zustande. Diese Dienste können direkt und ohne lokale Installation genutzt werden. Auch Geheimdienste haben keine Chance, die Daten bei den Cloud-Diensten mitzulesen, da diese ja verschlüsselt sind. Wer auf Nummer Sicher gehen möchte, nutzt HiDrive, den Cloud Dienst der Strato AG, da das entsprechende Rechenzentrum in Deutschland steht.

Nachdem alle nötigen Eingaben getätigt sind, genügt ein Klick auf ›Fertigstellen‹, woraufhin das verschlüsselte Paket erstellt und an den Empfänger verschickt wird. Dieser muss zwar nicht ArchiCrypt XChange doch den kostenlosen Viewer besitzen, um das verschlüsselte E-Mail-Paket öffnen zu können. Diesen Viewer bietet Remus zum freien Download für Microsoft Windows und Mac OS an. Nach Empfang des Pakets genügen die Kenntnis sowie die Eingabe des Passworts in das deutlich sichtbare Eingabefeld. Dieses Passwort kann vorab per Telefon, in einem Meeting, per Brief oder auch per SMS mitgeteilt werden.

Sicher kommunizieren

Auch die Rückantwort ist für den Empfänger möglich, was zeigt, dass diese Software sich vorzüglich in den Workflow

von Unternehmen einfügt, schließlich haben Unternehmen zahlreiche Kunden, die nicht unbedingt die Vollversion von XChange im Einsatz haben, dennoch auf eine dringliche, vertrauliche Anfrage rasch eine Antwort geben müssen.

Erwähnenswert ist, dass es XChange erlaubt, sogenannte Arbeitskreise zu bilden. In den Arbeitsgruppen arbeitet jeder mit seinem individuellen Passwort. So erhalten beispielsweise alle Mitglieder einer Arbeitsgruppe eine verschlüsselte Datei, die jeder mit seinem Passwort öffnen kann. Jedem Mitglied ist es möglich, mit den anderen Mitgliedern unter Verwendung seines Passworts beliebige Daten verschlüsselt auszutauschen. Dieses Feature ist allerdings nur in der Pro-Version von XChange möglich.

Unternehmen sollten sich angesichts dieser Möglichkeiten die Software ArchiCrypt XChange von Remus einmal ausführlich ansehen und im Fall einer Kaufabsicht gleich zur leistungsstarken Pro-Version greifen, da diese gegen einen geringen Mehrpreis einen gewaltigen Mehrwert, wie etwa die Bildung von Arbeitskreisen und die Möglichkeit der Rückantwort, bietet.

Die garantierte Unknackbarkeit der Daten gibt es dann kostenlos dazu.



www.archicrypt.de



Um ein verschlüsseltes Paket öffnen zu können, muss der Empfänger lediglich das Passwort kennen und eingeben.