Verschlüsselt durch den Tag

Beim Thema Verschlüsselung stöhnen viele Internetnutzer, weil sie hohen Aufwand fürchten, andere denken gar an kriminelle Machenschaften. Doch wir nutzen täglich ausgefeilte Kryptografie – ohne es zu bemerken. Am sichersten dabei ist die Ende-zu-Ende-Verschlüsselung

Wenn Matthias Müller etwas von Verschlüsselung und Kryptografie hört, denkt er unweigerlich an Geheimdienste, Spione, Militär und düstere Machenschaften. Dabei sendet und empfängt er selbst täglich Dutzende verschlüsselte Botschaften: Egal, ob er eine Mail verschickt, im Internet surft oder im Supermarkt mit seiner EC-Karte zahlt. Er merkt nur nichts davon. Dabei begleiten ihn meist im Hintergrund verschiedene Verschlüsselungsformen durch den Tag.

Das beginnt schon morgens beim Frühstück, als Müller nebenher auf seinem Tablet noch schnell eine Mail an seine Versicherung schreibt. Eigentlich ist die elektronische Post so problemlos lesbar wie eine Postkarte für den Briefträger. Daher werden die Nachrichten von dem meisten Mail-Diensten verschlüsselt, damit sie niemand auf dem Übertragungsweg mitlesen kann. Üblicherweise wird der Text zumindest auf dem Transportweg durch kryptische Zeichen ersetzt, mit denen niemand etwas anfangen kann. Doch Müller geht auf Nummer sicher und codiert seine Nachricht mit einem extra Programm mit der Ende-zu-Ende-Methode. Erst beim Empfänger wird das Zeichengewirr wieder entschlüsselt, also in den Klartext verwandelt. Nichts anderes ist Verschlüsselung: die Umwandlung von einem lesbaren Klartext in einen unleserlichen Text. So können nur Müller und die Sachbearbeiterin bei seiner Versicherung lesen, was sein Anliegen ist. Daher spricht man von Ende-zu-Ende- Verschlüsselung. Das ist sozusagen ein Informationsaustausch in Geheimsprache.

Selbst wenn jemand auf den Servern seines E-Mail-Anbieters herumschnüffeln würde, bekäme er nur sinnlos erscheinende Zeichen-und–Ziffer-Kombinationen zu sehen.

Müller muss los, ins Büro. Dort fährt er den Rechner hoch und öffnet in seinem Browser eine Seite mit wichtigen Branchennachrichten. Er achtet nicht weiter darauf, doch in der Adressleiste steht https und nicht http - ein Hinweis darauf, dass er eine sichere Seite besucht.

Die Abkürzung mit dem „s“ steht für sicheres Hypertext- Übertragungsprotokoll (Hyper Text Transfer Protocol Secure). Dadurch werden Informationen im Internet abhörsicher übertragen. Dafür sorgt die sogenannte SSL-Sicherung (Secure-Socket-Layer- Protokoll). Sie bewirkt, dass sich der Browser eines Computers und der Webserver der angesteuerten Internet-Seite gegenseitig authentifizieren. Die Daten, die sie miteinander austauschen, werden von Anfang an verschlüsselt. Davon hat Müller schon gehört, doch Gedanken hat er sich darüber noch nicht gemacht. Wenn das gesperrte Vorhängeschlosssymbol in der Statusleiste seines Browsers als Zeichen für eine sichere Datenverbindung erscheint, geschieht im Grunde etwas ganz Simples: Dann machen sich zwei Rechner miteinander vertraut, so ähnlich, als ob Müller einem neuen Kunden die Hand zur Begrüßung gibt und sich beide mit ihrem Namen vorstellen.

Nachdem sich beide Rechner über das SSL-Protokoll bekannt gemacht haben, vereinbaren sie einen Sitzungsschlüssel. Jenen Code, mit dem sie alle folgenden Nachrichten verschlüsseln. Außerdem gibt es noch eine Art „Fingerabdruck“, mit dem jede Nachricht versehen wird – so wird sichergestellt, dass die Nachricht nicht unterwegs verändert wurde und sie tatsächlich von dem vertrauten Rechner stammt.

In der Mittagspause muss Müller rasch den Stand seines Online- Bankkontos checken und eine Rechnung bezahlen. Beiläufig fluchtet er diesmal über die Adresszeile seines Browsers: Okay, die Internetadresse beginnt mit https, er sieht außerdem das Vorhängeschloss und eine grün gefärbte Adressleiste. Müller kann daran sehen, dass die Extended Validation (EV) aktiv ist. Eine Methode, mit der Identitäten der Nutzer von SSL-Verschlüsselungen überprüft werden, wobei neben der Internetadresse noch Namen der Organisation und der Zertifizierungsstelle angeben werden. Müller weiß jetzt jedenfalls, dass er bedenkenlos seine Zugangsdaten und später eine TAN für seine Überweisung eingeben kann. Die Übertragung seiner sensiblen Daten ist sicher.

Nach der Arbeit kauft Müller kurz im Supermarkt ein. An der Kasse zückt er die EC-Karte. Sorgsam schützt er mit der Hand die Eingabe seiner PIN-Nummer vor allzu neugierigen Blicken. Könnte er hier einen kryptischen Code eintippen, denkt er sich, wäre ihm wohler. Das ist natürlich zu aufwändig – und wer möchte schon jedes Mal eine andere Zeichenfolge eingeben. Doch auf dem weiteren Weg seiner PIN geschieht genau dies: Keine der vierstelligen Zahlen, egal ob an der Kasse oder am Geldautomat eingegeben, wird als Klartext weitergegeben. Das verlangt der Datensicherheitsstandard des Zentralen

Kreditausschusses.

Währenddessen sind bei Müller schon diverse Mitteilungen über WhatsApp auf seinem Smartphone eingegangen. Er antwortet rasch – und auch diese Kurznachrichten werden Ende-zu-Ende verschlüsselt ausgetauscht. Seine Nachrichten können also nun nur noch von ihm und dem Empfänger gelesen werden. Auch hier merkt Müller nichts von dem Aufwand, der im Hintergrund betrieben wird. Der Tag neigt sich dem Ende entgegen. Zeit für Müller, im Bett mit seinem Tablet noch ein wenig Neues aus aller Welt zu studieren.

Sein Tablet ist über WLAN mit dem Heimnetzwerk verbunden. Wie fast alle neueren Router nutzt auch Müllers Box für die Funkverbindung zu seinem Tablet die Verschlüsselung namens WPA2. Die Abkürzung steht für „Wi-Fi Protected Access“, also „geschützter Zugang“, wobei die 2 aussagt, dass es die zweite Version dieses Standards ist. Um sich einzuwählen, hat Müller ein kompliziertes Passwort festgelegt, eine lange und wahllose Aneinanderreihung von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. So ist auszuschließen, dass sich Unbefugte in Müllers privates Netzwerk einwählen, ihn aushorchen oder gar über seinen Internetanschluss Schindluder betreiben. Müller kann beruhigt einschlafen.