Blindes Vertrauen

Wie gut kennen Sie eigentlich John Merrill? Nur dem Namen nach? Oder so gut, dass Sie ihm Ihr Geld anvertrauen würden? Letzteres tun Sie, wenn Sie mittels PayPal bezahlen, bei Amazon shoppen oder online eine Fahrkarte der Deutschen Bahn kaufen. Denn John Merrill ist der Chef von DigitalCert und DigitalCert ist das Unternehmen, das die SSL-Zertifikate von paypal.com, amazon.de, bahn.de und Millionen anderer Websites signiert hat.

Sie sind also fest davon überzeugt, dass Merrill und seine Mitarbeiter absolut integer und unbestechlich sind und niemals gegen Geld oder auf Druck staatlicher Behörden hin ein Zertifikat für PayPal, Amazon und die Bahn signieren würden, das nicht der jeweiligen Firma gehört. Sie vertrauen darauf, dass alle Zertifikate, die die Signatur von DigitalCert tragen, echt sind und nur Berechtigten ausgestellt wurden. Viele Vorschuss-Lorbeeren für eine Firma, deren Namen die meisten gerade zum ersten Mal gelesen haben dürften.

Sie vertrauen aber nicht nur Merrill und DigitalCert, sondern auch der Technik. Also darauf, dass der Verschlüsselungsalgorithmus der SSL-Verbindung zu Amazon & Co. sicher ist, wodurch niemand ihre Konto- oder Kreditkartendaten abgreifen kann, und dass sich die Signatur eines Zertifikats nicht fälschen lässt. Doch Verschlüsselungs- und Signaturalgorithmen sind längst Blackboxes geworden, die kaum noch jemand versteht und auf deren korrekte Funktion man mangels besseren Wissens vertrauen muss.

Mit der c't-Story auf Seite 188 in dieser Ausgabe verschaffen wir Ihnen einen kleinen Einblick in diese Blackboxes.

Der Krimi ist die Fortsetzung der Story aus c't 25/1999 (online unter ct.de/ypgv), in der das Schicksal zweier autistischer Zwillingsschwestern beschrieben ist, die in einem Sanatorium leben und RSA-verschlüsselt miteinander kommunizieren. Dabei erklärt der Autor Carsten Elsner, heute Professor für Informatik an der FHDW Hannover, einfach nachvollziehbar, wie der Zivi Martin den Dialog der Schwestern Schritt für Schritt entschlüsselt und so einem Skandal auf die Spur kommt, der langjährige Haftstrafen für die Täter zur Folge hat.

Heute, fast 20 Jahre später, gibt es Neues von den Schwestern. Die c't-Story auf Seite 188 zeigt anhand einer neuen, spannenden Geschichte, wie wichtig Signaturen sind - und wie sie berechnet werden, damit Sie der Technik nicht länger blind vertrauen müssen.

Mirko Dölle