

Warten auf den IT-Airbag

Die zweite Anti-Prism-Party in Karlsruhe macht deutlich: Absolute Sicherheit im Internet gibt es nicht. Eine Ausrede für Untätigkeit ist das aber nicht

Die Zahl der Nutzer innerhalb eines Tages verdoppelt. Nummer eins der kostenpflichtigen Download-Apps bei Apple. Und alles nur, weil Facebook den Nachrichtendienst Whatsapp gekauft hat. Die Angst vor Mark Zuckerbergs Datenmloch bescherte dem Schweizer Start-up Threema dieses extreme Wachstum. Wenig verwunderlich für Experten wie Kai Jendrian von der Karlsruher IT-Sicherheitsinitiative: „Ein sicherer Dienst, da die Nachrichten wirklich verschlüsselt werden.“ Ganz im Gegensatz zum Marktführer Whatsapp: „Der Betreiber hat alle Nachrichten in Klarform vorliegen“, erklärt er. Sicherheit, ein Fremdwort.

Mit der Sicherheit im Netz ist das gleich in vielerlei Hinsicht so eine Sache. Bei der zweiten Auflage der Anti-Prism-Party der Karlsruher IT-Sicherheitsinitiative drängten sich rund 600 Besucher im Karlsruher ZKM. Die Sensibilität ist da. Tipps und Empfehlungen gab es ebenfalls reichlich zum Vermeiden digitaler Fußspuren. Das Handeln jedoch hinkt hinterher.

Ein Grund: Bequemlichkeit. „Sicherheit bedeutet Disziplin und Aufwand“, macht David Hermanns, Geschäftsführer des IT-Netzwerks Cyber-Forum, deutlich. Beispiel gefällig? 30 Millionen Nutzer nutzen hierzulande Whatsapp, 400 000 Threema.

Zumal selbst mit den beiden Tugenden Disziplin und Aufwand Missbrauch möglich ist, denn: „Absolute Sicherheit gibt es nicht“, führt er weiter aus. „Die Fallstricke lauern in der Praxis“, ergänzt Jörn Müller-Quade, Lehrstuhlinhaber für IT-Sicherheit am Karlsruher Institut für Technologie. Zuweilen reicht ein Fetzen Klebeband, um ausgefeilte Technik zu schlagen. Ein zusätzlicher Chip auf der EC-Karte und der PIN-Klau durch das Kopieren des Magnetstreifens gehört der Vergangenheit an. Die schöne Theorie unterschätze jedoch das böse Verbrecherhirn. „Chip überkleben und schon klappt es mit dem Kopieren wie vorher. Wichtig ist es daher, Sicherheit als Prozess zu begreifen“, meint der Fachmann.

Wobei der Schutz der eigenen Daten viel mit Glauben und Ver-

trauen zu tun hat. Das verdeutlicht die Diskussion um den Browser-Anbieter Tor. Für die einen ist er der Inbegriff für anonymes Surfen. Für die anderen ist er ein Machwerk der NSA. Die Befürworter lieben ihn, weil er die eigene IP-Adresse umwandelt und eine falsche versendet. Zurückverfolgung zwecklos. Gleich, zu welchem Lager man zählt, an gewissen Grundregeln kommt keiner vorbei, findet jedenfalls der Datenschutzexperte Christoph Schäfer. „Alternative Dienste nutzen, Browser so einstellen, dass Cookies von Dritten nicht akzeptiert werden, Tracker blockieren, Chronik nach jeder Anwendung löschen“, lauten seine wichtigsten Hinweise. Selbst die beste Technik stößt jedoch an ihre Grenzen, wenn der Faktor Mensch ins Spiel kommt. Alle Grundregeln befolgt und dann im Online-Shop bestellt? Anonymes Surfen ade.

In der digitalen Welt lauern nicht weniger, aber auch nicht mehr Gefahren als in der realen Welt. Daran erinnerte David Hermanns: „Zuerst kam das Auto und dann der Airbag.“ *mh*



Herkunft verpflichtet

Christoph Bier vom Fraunhofer IOSB erklärt im Rahmen seines Vortrags „Data Provenance. Auch Daten haben ihre Geschichte“, warum in modernen Informationssystemen die Umsetzung datenschutzrechtlicher Transparenzanforderungen extrem schwer ist – und wie „Data Provenance“ das Problem lösen kann.



Wo Fraunhofer IOSB,
Max-Syrbe-Saal,
Fraunhoferstraße 1,
76131 Karlsruhe,

Wann 3.4., 18 Uhr

Mehr Infos unter
www.ka-it-si.de



Rund 600 Besucher kamen zur inzwischen zweiten Anti-Prism-Party ins Karlsruher ZKM