Erst denken, dann posten

Bei einer IT-Sicherheits-Veranstaltung im Zentrum für Kunst und Medientechnologie wird zur Selbstzensur geraten – eine Betrachtung

VON WILLY STORCK

KARLSRUHE. Klar, Spionage hat es immer schon gegeben. Nicht ohne Grund spricht man bei eingeschleuster Ausspähtechnik im Internet von „Trojanern", in Anlehnung an jenes hölzerne Pferd, das die Griechen den Einwohnern von Troja vor das Stadttor stellten. Worauf sich diese als ebenso unvorsichtig erwiesen wie viele heute im weltweiten Datendschungel. Das Ende ist bekannt: Heulen und Zähneknirschen.

Der IT-Hochburg Karlsruhe kann man nicht vorwerfen, dass dabei nur die Euphorie-Karte gespielt würde. Was die Gefahren des World Wide Web beziehungsweise Sicherheitsthemen angeht, gibt es hier starke Akteure. Da ist etwa der Verein Cyber-Forum , mit über 1000 Mitgliedern aus der Hightech- und IT-Branche das größte regionale Netzwerk seiner Art in Europa. Dann gibt es noch Kastel, am KIT angesiedelt und eines der drei deutschen Kompetenzzentren für Cybersicherheit. Und da ist die Karlsruher IT-Sicherheitsinitiative (KA-IT-SI), die immer wieder in auch allgemein zugänglichen Veranstaltungen auf Möglichkeiten hinweist, sich gegen Lücken, Datenklau und Infiltration im Netz besser abzusichern. Denn, so wird Dirk Fox, Chef der Karlsruher IT-Sicherheitsfirma Secorvo und Vorsitzender der Initiative, nicht müde zu betonen: „Es kann wirklich jeden treffen."

Denn längst geht es nicht nur um „meine" Daten, sondern auch um meine Kontakte. Jedes Fitzelchen kann da irgendwie für irgend Unternehmen oder einen „Dienst" nützlich sein. Und das kann Folgen haben

> Sehr Privates landet oft unnütz in der Cloud. Gut für Spitzel und Konzerne.

für Regierungen und Unternehmen bis hinunter zu Chantal und Kevin, die fröhlich posten und meinen, das sei doch alles völlig harmlos.

Die großartige Ausstellung Global Control and Censorship im ZKM bot da nun den oben genannten Initiativen eine besondere Plattform. „Eine kurze Geschichte der Überwachung" war die Veranstaltung überschrieben, deren erster Teil ein historischer Abriss war, den Dirk Fox mit Francis Walsingham begann. Der war im 16. Jahrhundert eine Art Innenminister der englischen Königin Elizabeth I. und richtete ein umfangreiches Überwachungs- und Spitzelsystem im In- und Ausland ein, das letztlich der katholischen Konkurrenz um Maria Stuart den Garaus machte. Der skrupellose Walsingham hat bekanntlich bis heute zahlreiche Nachfolger gefunden, nur dass diese über immer bessere technische Möglichkeiten verfügen und kaum noch auf Schlapphüte und Löcher in der Zeitung angewiesen sind, um an Informationen zu kommen.

Was heißt das für uns, die wir fröhlich bei Facebook posten, Privates gedankenlos preisgeben und jede uns angebotene Payback-Card abgreifen? Für den ganz normalen User, soviel machte dann Jörn Müller-Quade klar, ist das alles nur schwer durchschaubar. Der quirlige Professor, am KIT Lehrstuhlinhaber für IT-Sicherheit und Kryptographieexperte, hält WhatsApp auf Grund der Zugangsvoraussetzungen für Einfallstore für das ungebremste Datensammeln. Ein weiteres Problem seien etwa fehlerhaft konfigurierte Überwachungskameras, wofür er ein Beispiel aus einer Apotheke präsentiert. Und: „Hochprivate Daten werden zum Teil völlig unnütz erhoben und in die Cloud hochgeladen." Dort bleiben sie dann. „Wir können uns auf die Sicherheit heutiger Verschlüsselungen nicht verlassen", so Müller-Quade weiter. Ohnehin reiche Verschlüsselung allein nicht, die Sicherheit betreffe das gesamte System. Und es gehe dabei auch um Zensur. Das betrifft die handfeste Form, noch mehr aber die unterschwellige Beeinflussung von Meinungsbildung oder Kaufbeeinflussung.

So lange freilich Unternehmen und erst recht private Nutzer fahrlässig die Türen aufmachen, etwa gedankenlos der Weitergabe ihrer Daten zustimmen (auch hier steckt das Risiko im Kleingedruckten), haben Datensammler oder Kriminelle leichtes Spiel. Merke eben: Das Smartphone ist keineswegs dein bester Freund!