Einschaltung zur Förderung des Verfolgungswahns

Datensicherheit und Privatsphäre, was ist das?

netzknoten

Nun ist es offiziell: Gemäß einem EU-Report liest der größte Geheimdienst der Welt, die NSA (USA), europaweit e-mails, Telephongespräche und Telefaxe mit. Die Daten werden in Menwith Hill in Großbritannien gesammelt und von dort per Satellit in die USA übertragen. (Siehe auch: `http://www.heise.de/newsticker/data/ae-09.01.98-000/`) Die Daten werden dabei auf spezielle (länderspezifische) Schlüsselwörter untersucht. Auch Telephongespräche werden mit einem Spracherkennungssystem auf Schlüsselwörter untersucht.

Nun gut. Ist eben aus einem Gerücht eine Tatsache geworden. Was können wir dagegen tun? Nicht viel, das ist ja das Schlimme. Natürlich kann man seine Mails und Dokumente verschlüsseln. Mit dem Ergebnis, daß sich der Empfänger bei der Verwendung eines Entschlüsselungprogramms möglicherweise strafbar macht. (Was in welchen Ländern erlaubt bzw. verboten ist, findest Du unter: `http://www.gilc.org/crypto/crypto-results.html`). Oder aber mit dem Ergebnis, daß es Programme zu kaufen gibt (`http://www.accessdata.com`), die die Dokumente wieder entschlüsseln. (Details (und weitere Infos über die Sicherheit von Verschlüsselungsprogrammmen) gibt´s unter: `http://www.foebud.org/~christopher/pgp/pgp.1.7.html`).

Abgesehen davon wird die Nachricht vielleicht (im Klartext) mitgelesen, während sie getippt wird. Und zwar einfach, indem die Strahlung, die der Bildschirm aussendet, analysiert wird. (siehe auch: `http://www.computerwoche.de/archiv/1986/34/8634c080.html`). Der Datenklau geht problemlos mit Entfernungen von bis zu 300m (mit besserer Ausrüstung sollen auch Entfernungen von 1km kein Problem sein). Dabei erzeugt auch die Strahlung von mehreren Bildschirmen keinen „Datensalat", sondern kann voneinander getrennt werden.

Für dieses Verfahren gibt es auch ganz „tolle" neue Anwendungsmöglichkeiten, z.B. kann der Bildschirm auch andere Informationen abstrahlen als der Benutzer sieht, etwa kann die Farbe grau entweder durch einen grauen Bildpunkt oder durch abwechselnd schwarze und weiße Punkte erzeugt werden. Für den Benutzer ist das oft nicht zu unterscheiden, fuer das „Empfangsprogramm" ist die Unterscheidung hingegen kein Problem. Wozu das gut sein soll? z.B. könnte ein Programm seine Seriennummer abstrahlen, oder das Dokument an dem man derzeit arbeitet, oder beliebige Dateien, die sich auf der Festplatte befinden. (Dazu gibts mehr unter: `http://www.spiegel.de/netzwelt/themen/tempest.html` nachzulesen).

Natürlich gibt es auch für das Problem der Bildschirmabstrahlung eine Lösung. In diesem Fall heißt sie „abstrahlsichere Monitore". Die gibt es zwar, nur haben sie zwei Nachteile. Erstens sind sie natürlich teurer als gewöhnliche Geräte, und zweitens sind sie Privatpersonen und privaten Unternehmen nicht zugänglich.

Problematisch an den gängigen publickey-Verschlüsselungssystemen ist auch, daß das System nur auf der Annahme beruht, daß für gewisse Probleme (z.B. Faktorisierung von großen Zahlen) keine effizienten Algorithmen existieren. Und solange kein Beweis auf dem Tisch liegt, daß die Annahme richtig ist, kann man sich nicht sicher sein, daß nicht der Geheimdienst XYZ des Landes ABC oder der Typ, der am PC-Arbeitsplatz gegenüber sitzt, seit zwei Jahren die mühevoll verschlüsselten e-mails mitliest und sich über die Verschlüsselungsversuche halb tot lacht.

Natürlich „glaubt" kaum jemand, daß für gewisse Klassen von Problemen (NP-harte Probleme) effiziente Algorithmen existieren, aber das ist nur ein Argument, wenn ich diesen Artikel für die Zeitung der Theologie-Fakultät schreibe und nicht fürs TU INFO.

Weitere Infos findest Du auf etlichen Webseiten (einfach entsprechende Stichworte bei den diversen Suchmaschinen eingeben) und in den Newsgroups `de.soc.datenschutz` und `de.comp.security`. (Achtung: Verfolgungswahn ist nicht ausgeschlossen, wenn Du diese Newsgroups regelmäßig liest).
Übrigens: Wußtest Du, daß alle Newsartikel, die Du irgendwann mal gepostet hast, gespeichert werden?
(Siehe: `http://www.dejanews.com`)

• **Wolfgang Dautermann**