Die Angst vorm schwarzen Schirm

Cyberkriminalität: Sichtbar ist nur die Spitze des Eisbergs

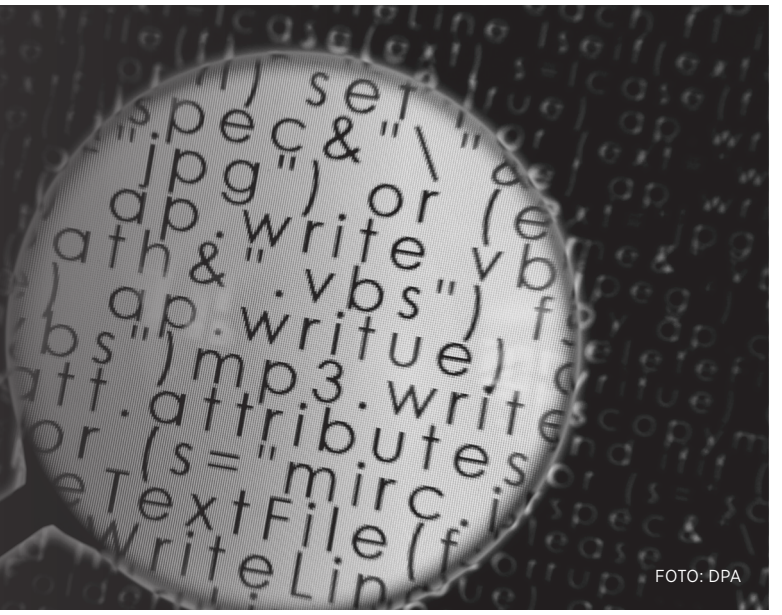

FOTO: DPA

Von Ulrich Nettelstroth

Von einem Moment auf den anderen geht gar nichts mehr. Der Bildschirm wird schwarz, mit einem Text in roter Schrift, der sich als Erpresserbrief herausstellt. „Ooops, your important files are encrypted“, beginnt das Schreiben, in dem die Zahlung einer Geldsumme von einigen Hundert Euro in der Internetwährung Bitcoin verlangt wird. Dann werde ein Code geschickt, mit dem die Verschlüsselung des Computers aufgehoben werde, so die Versprechung. Krankenhäuser haben solche Erpressungs-Trojaner erhalten, kleine und mittlere Unternehmen. Manche Firmen zahlen dann tatsächlich, weil die Blockade der Rechner für sie eine Existenzgefährdung bedeuten könnte. Ob sie ihre Daten wiedersehen, steht aber in den Sternen.

Fachleute gehen davon aus, dass solche offensichtlichen Fälle von Cyberkriminalität nur die Spitze des Eisbergs sind. Mehr als die Hälfte der Unternehmen in Deutschland (53 Prozent) ist in den vergangenen beiden Jahren Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden, mit einem Schaden von rund 55 Milliarden Euro pro Jahr, so eine aktuelle Studie des Branchenverbands Bitkom, für die 1069 Geschäftsführer und Sicherheitsverantwortliche quer durch alle Branchen befragt wurden. Der Anteil der Geschädigten könnte auch noch viel höher liegen, vermutet Ortwin Wohlrab, Vorstand des IT-Dienstleisters Netfox aus Kleinmachnow (Potsdam-Mittelmark). „Viele haben es nur noch nicht gemerkt“, sagt er.

Schadsoftware dringt meist über Links oder E-Mail-Anhänge in ein IT-System ein, sagt Wohlrab. Ein Computervirus kann als kleine Zeichensequenz etwa an eine Bilddatei angehängt sein, die der Nutzer unbedacht öffnet. Das Schadprogramm landet so unbemerkt auf der Festplatte. Eine Firewall wehrt zwar Attacken ab, die von außen kommen, lässt aber oft alles in das interne Netzwerk hinein, was der Nutzer selbst herunterlädt. Auch ein Antivirus-Programm entdeckt nur bereits gelistete Viren, aber keine noch unbekannten Schadprogramme.

Gerade der Internetbrowser ist ein Einfallstor für Hacker. „Sicherheitslücken im Browser öffnen Angreifern Tür und Tor“, erklärt Roman Maczkowsky, Geschäftsführer der M-Privacy GmbH, eines Berliner Spezialisten für IT-Sicherheit und Datenschutz. „Angriffe laufen im Hintergrund, ohne dass der Betroffene es merkt“, warnt er. So können Unbefugte auf Datenbanken mit Kundendaten und Geschäftskontakten im internen Unternehmensnetzwerk zugreifen, mitunter sogar im Auftrag von Konkurrenzunternehmen. Ein möglicher Schutz für Firmennetzwerke ist ein ferngesteuerter Internetbrowser. Dabei ist für den Internetzugang ein stark gesichertes Schutzsystem zwischengeschaltet, das so ähnlich arbeitet wie ein Terminalserver, im Fachjargon Remote Controlled Browser System genannt oder kurz RCoBS. Mögliche Angriffe über den Browser bleiben auf dem vorgelagerten System stecken.

Bei einer anderen Masche kommen Cyberkriminelle ohne große Programmierkenntnisse aus. Sie durchforsten die Webseite eines Unternehmens nach Personaldaten, ziehen auch soziale Netzwerke wie Xing hinzu, um etwa die dienstliche Mailadresse eines Buchhalters herauszufinden. Der bekommt dann eine täuschend echt gefälschte Mail des Firmenchefs mit der Aufforderung, eine vier- oder fünfstellige Summe auf ein bestimmtes Konto zu überweisen, vielleicht sogar noch mit dem Zusatz, die Zahlung diskret abzuwickeln. „Uns ist ein solcher Fall bekannt“, sagt Netfox-Vorstand Wohlrab. Weil die Buchhalterin nachgefragt hat, ist der dreiste Versuch aufgeflogen. In manchen Fällen aber kommen die Täter damit durch. Und geschnappt wird nur selten ein Cyberkrimineller. E-Mail-Absender sind oft schon nach Stunden nicht mehr am Netz.

Nicht einmal jede dritte betroffene Firma schaltet laut Bitkom-Studie die Polizei ein. Netfox-Vorstand Ortwin Wohlrab bedauert das. Er wünscht sich die Entstehung einer IT-Sicherheitskultur, ähnlich wie sie in den 1970er Jahren im Straßenverkehr entstanden ist.

Sicherheitsregeln im Web

Für alle installierten Programme regelmäßige Sicherheitsupdates durchführen.

E-Mail-Anhänge und Links nur bei vertrauenswürdigen Quellen öffnen.

Routinemäßig eine Datensicherung auf externem Speichermedien durchführen.

Vorsicht bei kostenlosen Angeboten, etwa bei Clouddiensten.

Wer wissen will, ob sein E-Mail-Zugang bereits gehackt wurde, kann sich mit dem Identity Leak Checker des Potsdamer Hasso-Plattner-Instituts kundig machen (hpi.de).