KRIMINALITÄT IM INTERNET

Betrüger im Netz

Das weltweite Datennetz bietet auch Betrügern und Saboteuren eine neue Plattform. Oft ist es einfach, sich vor den Kriminellen zu schützen.

"Werden Sie Ihre Schulden los, holen Sie sich Ihre verpfändete Uhr zurück", warb ein dubioser Anbieter im Internet für ein "Pfandgutbeschleunigungs-Programm" und verschickte Hunderte E-Mail-Offerte Anfang April wurde er auf die Spam Block List des Providers EU-Net Austria gesetzt. Seither werden E-Mails dieses Anbieters automatisch abgewiesen.

"Spamming", eine Art virtuelle Postwurfsendung, ist seit Juli 1999 nach österreichischem Recht verboten, verhindert wird es dadurch nicht. Die Internetbranche hilft sich mit lokalen Blocks wie jener von EU-Net und einer "Blackhole List". IP-Adressen, die auf diese Liste gesetzt werden, sind weltweit gesperrt. Spammer, die auf anonyme Mail-Server ausweichen, werden vom E-Mail-Verkehr ausgeschlossen, indem der Mail-Server in das ORBS genommen wird, das Open Relay Behaviour Modification System (Zurechtweisungssystem). Am häufigsten werden Anbieter dubioser Geldanlagen gekappt und Anbieter von Kinderpornos. Zu den fleißigsten Spammern zählen Betrüger, die für einen Geldtransfer aus Nigeria Millionen versprechen. Bis vor kurzem verbreiteten sie ihre Offerte mit der Post und per Telefax. Jetzt nützen sie das Internet für ihre Betrügereien.

Einfluss auf Aktienkurse

Vor gezielten Falschmeldungen im Internet warnte Anfang April die deutsche Börsenaufsicht: Besitzer von Aktien mit geringem Wert verbreiten gefälschte Informationen in Newsgroups; unbedarfte Anleger, die das lesen, kaufen die betroffenen Aktien. Das treibt den Kurs in die Höhe und gibt den Verbreitern der Falschmeldung Gelegenheit, ihre wertlosen Aktien teuer abzustoßen.

Scheinauktionen

Betrüger veranstalten Online-Versteigerungen: Sie bieten Computer extrem günstig an, ebenso Drucker, Scanner, Fotoausrüstungen und Notebooks. In der Versteigerung bieten sie selbst mit und treiben den Preis in die Höhe; oder sie geben jedem Bieter den Zuschlag, kassieren von jedem den Kaufpreis und tauchen unter.

Lieferbetrug

Betrügerische Web-Anbieter locken mit aufwendig gestalteten Homepages, kassieren und liefern nicht: Einen Lieferengpass bei Prozessoren Anfang März nützte eine Briefkastenfirma in Hongkong (China). Sie versprach einer St. Pöltner Firma, die Computerteile prompt zuzusenden, ließ den österreichischen Geschäftspartner 330.000 Schilling auf ein Konto in Hongkong überweisen. Danach tauchten die Betrüger unter. "Man weiß im Internet nie, mit wem man es zu tun hat", sagt Leopold Schauer, Interpol-Ermittler im Innenministerium. "Geschäfte sind rasch abgewickelt, Überweisungsaufträge laufen parallel und Betrüger tauchen unter."

Öffentliche Sicherheit, Ausgabe 07-08/2000

Digitale Unterschrift

Wer sicher gehen will, dass eine Person auch derjenige ist, als der er sich ausgibt, muss über ein Verschlüsselungssystem kommunizieren: Er besorgt sich unter Vorlage eines amtlichen Ausweises bei einer Zertifizierungsstelle einen "Public Key" (öffentlicher Schlüssel) und einen "Private Key" (privater Schlüssel), die in einem mathematischen Zusammenhang zueinander stehen. Der Public Key wird veröffentlicht, meist auf der Web-Site der Zertifizierungsstelle, den Private Key hält der Besitzer geheim. Bei E-Mail-Verkehr, bei dem er sich zu erkennen geben will, verschlüsselt er die Nachricht mit seinem Private Key – der Empfänger öffnet sie mit dem Public Key des Absenders und weiß, von wem die Mitteilung kommt. Die Verschlüsselung gilt als digitale Unterschrift nach dem Signaturgesetz. Wer will, dass kein anderer die E-Mail lesen kann als der, für den sie bestimmt ist, muss den Public Key des Empfängers kennen (sofern er einen hat, also zertifiziert ist). Er verschlüsselt die Nachricht mit dem Public Key des Empfängers – und die E-Mail lässt sich nur mehr mit dessen dazugehörenden Private Key öffnen. Vorsicht mit Kreditkarten. Visa-Sicherheitsexperte Erwin Petsch warnt vor sorglosem Umgang mit Kreditkartendaten im Internet. Visa bietet seinen Kunden SET (Secure Electronic Transaction). Der Zahlungsverkehr mit Kreditkarten im Internet zwischen Kunden und Händler wird über eine Bank abgewickelt. Der Händler erfährt die Kreditkartendaten des Kunden nicht. Vom Kreditkartenunternehmen erhält er grünes Licht für die Lieferung, von der Bank bekommt er sein Geld. "Das hat auch den Vorteil, dass der Händler keine Kreditkartendaten am Server gespeichert hat. Und macht es unmöglich, dass die Daten bei einem Hacker-Angriff gelesen werden.", erläutert Dipl.-Ing. Robert Gottwald, Internet-Sicherheitsbeauftragter des Innenminsteriums.

Datenverschlüsselung

Erwin Petsch empfiehlt, mit Händlern, deren Computer das SET-System nicht unterstützen, über SSL zu verkehren (Secure Socket Layer). Dabei wird der Datenverkehr verschlüsselt. Erkennbar ist die Verschlüsselung durch ein Schloss-Zeichen am unteren Rand des Bildschirms und am Kürzel in der Web-Adresse s:// statt ://. "Ist weder SET möglich, noch SSL, sollten die Kreditkartendaten nicht im Internet verschickt werden", rät die Visa-Kreditkartenorganisation auf ihrer Homepage. Obwohl nur zwei Prozent der Visa-Kunden im Internet mit Kreditkarte bezahlen, beziehen sich 50 Prozent der Beschwerden auf Internet-Einkäufe. "Es muss kein Hacker-Einbruch in den Datenbestand eines Händlers stattfinden", sagt Robert Gottwald. "Es reicht, wenn ein gekündigter Mitarbeiter des Händlers einige Kudendaten mitnimmt und damit unauffällig geringe Beträge abbucht." Vor allem Anbieter von pornografischem Material und dubiosen Computerspielen verlangen Kreditkartendaten häufig für den Zugriff auf bestimmte Seiten, obwohl dieser angeblich gratis sei. Sie geben vor, die Daten würden als Bestätigung nötig sein, dass der Web-Besucher über 18 Jahre sei. "Es gibt keinen Grund, die Kartendaten bekannt zu geben – außer man bezahlt mit Kreditkarte", sagt Erwin Petsch von Visa. Doch Internet-Surfer gehen oft blauäugig mit den neuen Medien um.

Kinder sind besonders gutgläubig. Eltern sollten daher die Sprösslinge auf Tricks und Fallen hinweisen, etwa Sekten, Nazis und Betrüger, Kettenbriefe und Pyramidenspiele – das nimmt den Kindern und Jugendlichen die Neugier auf das Unbekannte und wappnet sie gegen Angriffe, etwa durch Viren, die durch den leichtfertigen Umgang der Internet-Nutzer verbreitet werden.

Virenschutz

Täglich kommen Dutzende neue Viren hinzu. "Allein das Einstellen der Sicherheitseinstellungen der Internet-Browser auf höchste Stufe bietet bereits einen gewissen Schutz", erläutert Robert Gottwald. Das wäre Deaktivieren von JavaScript sowie Java, Visual Basic Script (VBS) und ActiveX. Ebenso sollte bei Programmen wie z.B. WinWord, Excel u.ä. der Makro-Virenschutz aktiviert werden. Grundsätzlich gilt, vor allem auch bei E-Mails und Downloads aus dem Internet, unbekannten Programmen und Dateien ein gesundes Mißtrauen entgegenzubringen und diese im Zweifelsfalle ungeöffnet zu löschen. Gottwald rät Internetnutzern weiters, ein aktuelles Virenschutzprogramm zu kaufen und zu aktivieren sowie die dazugehörenden Virendatenbanken regelmäßig in kurzen Abständen zu aktualisieren. Am besten seien Programme, die im Hintergrund laufen und automatisch alle neuen Dateien auf Computer-Viren überprüfen.

Gerhard Brenner

www.bmi.gv.at/Kriminalpolizei

www.arge-daten.at/

www.a-sit.at/