Tatort Internet

Bericht VKÖ

Sie haben keinen Computer, das Internet ist für sie unbekanntes Land. Sie glauben also vor Internetkriminalität gefeit zu sein – weit gefehlt. Opfer von Kriminellen, die das Internet als Tatwaffe benützen, kann jeder werden.

Sie haben einen Herzschrittmacher, einen der neuesten Generation der per Funk mit dem Hersteller verbunden ist. Sie haben Glück gehabt, dass dieses an sich nützliche Gerät ihren Blutdruck nicht auf 200 gebracht hat. Glück deshalb, weil ein Hacker in den Computer des Herzschrittmachererzeugers eingedrungen ist und damit die Einstellung sämtlicher Geräte verändern hätte können. Todesfälle wären nicht ausgeschlossen gewesen. Nur einer von tausenden Fällen von Internetkriminalität, einer von etwa 112.000 die an einem einzigen Tag von der Uni-Bonn registriert wurden.

Eine Milliarde Opfer

Was die Zuhörer der Fachtagung „Tatort Internet“ (veranstaltet vom „Bund Deutscher Kriminalbeamter“ in Kooperation mit unserer Vereinigung) zu hören bekamen, ließ so manchen erschauern. Nicht nur Einzelpersonen, sondern auch Firmen, ja ganze Staaten sind zu Spielbällen von Internetkriminellen geworden. Problematisch dabei ist, dass den meisten Menschen nicht bewusst ist, welche Gefahr aus der virtuellen Welt droht. Es sind nicht nur die etwa eine Milliarde User des Internets weltweit, die Opfer sein können. Der eingangs erwähnte Fall beweist anschaulich, jeder und wirklich jeder kann Opfer werden. Wie der malaysische Innenminister Yb Dato Seri Hishammuddin Tun

Hussein bei der Tagung treffend formulierte: Es gibt bei der Internetkriminalität kein „lokal“ sondern nur ein „global“. Die lokale Bekämpfung von Internetkriminalität muss scheitern, denn die Täter können im Nebenhaus oder auf einem anderen Kontinent sitzen, sie agieren global und arbeitsteilig. Nicht nur Technologie, sondern internationale Kooperation ist der Schlüssel zur Bekämpfung.

Michael Bartsch, seines Zeichens Fachmann für Internetsicherheit, zeigte auf, wie das Internet auch die Wirtschaft, ja das persönliche Eigentum beeinflussen kann ohne dass eine kriminelle Machenschaft dahinter stehen muss. So wurden auf einer neuen Homepage die Zentren der Kriminalität in Berlin aktuell aufgelistet. Die Folge war, dass die Grundstückspreise in diesen Gebieten rasant gefallen sind.

Kreditkarten gefälscht

Mirko Manske, Ermittler im deutschen BKA, erklärte neueste Methoden der Internetkriminalität. 46% der Internetdelikte in Deutschland sind im Bereich Internetbetrug anzusiedeln, die Zahl stieg im Vorjahr um 35%. Identitätsraub und illegale Botnetze* sind weitere aktuelle Bedrohungen der Gesellschaft. Problemlos kann man heute in underground-shops Identitäten zum Diskontpreis kaufen. Der Verkauf von malware* ist Teil der kriminellen Arbeitsteilung im Internet. Laut Manske sind derzeit vor allem Kreditkarten ein vordringliches Ziel der Internetkriminellen. Mehr Sicherheit wäre hier möglich. Aber Sicherheit stört die Bequemlichkeit und so bremsen die Banken, denn es könnten Bankkunden vertrieben werden. In den USA soll bereits die Hälfte der Kreditkarten gefälscht sein, die Rückkehr des Bargeldes ist damit möglich. Wie bereits VKÖ Präsident Richard Benda in seinen Einleitungsworten sagte und Manske bestätigte, erleichtern die Opfer häufig selbst die Ausführung der Tat. Die gleiche

Codenummer bei allen Kredit- und Bankomatkarten gehören ebenso dazu wie die Offenlegung privater Details in sozialen Netzwerken.

Soziale Netzwerke - ein Selbstbedienungsladen

Soziale Netzwerke wie Twitter oder Facebook sind überhaupt zu einem Selbstbedienungsladen für Kriminelle geworden. Wer öffentlich bekanntgibt, dass er die nächsten Wochen auf Urlaub ist, darf sich nicht wundern, wenn bei der Heimkehr die Wohnung ausgeräumt ist. Auf der anderen Seite profitiert auch die Polizei von diesen Outings. Es wurden schon mehrere Kriminelle durch Durchforstung des Internets ausgeforscht. Dies trotzdem einige datenschutzbewegte Mitbürger meinen die Polizei dürfe das Internet nicht zu Ausforschungen verwenden. In Deutschland hat jedenfalls des Verfassungsgericht klargestellt: Wer seine Daten und Lebensverhältnisse öffentlich bekanntgibt, darf sich nicht in seinen Grundrechten beschränkt sehen, wenn auch die Polizei diese Daten verwendet.

Etwas Erfreuliches hat die Internetkriminalität doch, es sind auch Kriminelle nicht davor gefeit. So ist eine russische Mafiagruppe die Geldwäscher suchte von nigerianischen Internetkriminellen gelegt worden. Ihr krimineller Gewinn versickerte irgendwo in Afrika. Dass die Zentren der Internetkriminalität just in Russland und der Ukraine sind, ist dabei eine Ironie des Schicksals.

G.F.

„Im 21. Jahrhundert wird nicht mehr ein Tresor geknackt, sondern das Internet.“

Markus Ulbig, Innenminister des Freistaates Sachsen.

- · *Unter Bot versteht man Computerprogramme die weitgehend selbstständig gewisse, sich wiederholende Aufgaben abarbeiten, ohne dabei auf die Interaktion von Menschen angewiesen zu sein. Ein Botnetz ist eine Gruppe von Softwarebots die zu einem Netzwerk zusammengeschlossen sind. Bei Illegalen Botnetzen wird das Bot ohne Wissen des Inhabers installiert und der Rechner wird für eigene Zwecke des Botnetzbetreibers über einen Command- and Controll-Server benützt.*
- · *maleware wird in der Computersicherheitsbranche als Überbegriff für Schadprogramme verwendet.*