

# IM VISIER VON CYBER-GANOVEN

Handys abhören, Passwörter knacken, Bankdaten klauen? Alles kein Problem für die heutige Hackerszene. Kein Byte ist da noch sicher. Besonders gefährdet sind Android-Smartphones. Die sind wie ne' angelehnte Eingangstür: solange sicher, bis wer vorbeikommt. Wir sprachen mit IT-Marshall Alexander Tsolkas über die aktuellsten virtuellen Bedrohungen, vor denen selbst ganze Nationen nicht gefeit sind.

Text **STEFAN FROST**

Sommer 2010. Im iranischen Atomkraftwerk Busher surren die Alarmglocken. Der Grund: Kein Defekt. Kein Erdbeben. Sondern Stuxnet, ein extrem aggressives Computervirus zum Fernsteuern von Industrieanlagen. Gleichzeitig laufen im Westen hysterisch die Telefone heiß. Denn noch nie war es einem virtuellen Schädling gelungen solch sensible Bereiche anzugreifen. Was, wenn das in einem deutschen Atomkraftwerk passiert? „Die Cyberkriminalität hat eine ganz andere Dimension bekommen durch Stuxnet. Das war eine komplett neue Liga.“, erinnert sich IT-Experte Alexander Tsolkas. „Gegen solche gezielten Angriffe kann sich ein Land nur sehr schwer wehren“. Willkommen in der Realität, wo kein Staat, kein Unternehmen und keine Privatperson mehr sicher sind. Mittlerweile hat die NATO sogar ein eigens Cyberwar-Zentrum in Tal-

lin, Estland, eingerichtet. Auch in Deutschland wurde eigens eine Taskforce zur Abwehr digitaler Angriffe geschaffen, sozusagen als Firewall der Bundesrepublik. Aber allein aus China stehen der Kampftruppe rund 30.000 hochprofessionelle Tastaturklopfer gegenüber.

Für den privaten User gibt es Firewall und Co., um es gegen die Hackerarmee aufzunehmen. Jedoch wimmelt es nur so vor Sicherheitslücken, die nach einem gezielten Exploit schreien. Akut gefährdet sind Smartphones. „Hier sind wir auf dem Sicherheitsstand, wie wir es bei den Computern im Jahr 1999 waren“, warnt Tsolkas. Bei Handys mit dem Betriebssystem Android gilt Alarmstufe Rot. „Weil es eben relativ neu ist, sind hier viele Fehler drinnen. Die sind noch nicht alle gefixt und gepatcht“. Was soviel heißt, dass die Software ihren eigenen Lücken noch ständig hinterher läuft und Cyber-Piraten Angriffspotential bietet. Wie gefährlich das sein könnte, belegen Zahlen zur Handynutzung: 88% aller User speichern sensible Da-

ten auf dem Handy, mehr als 70% nutzen es für Online-Banking. Für Hacker ist es dann ein leichtes, zu virtuellen Bankräubern zu mutieren. Aber auch einfache Handy-Gespräche können mitgeschnitten werden. Man braucht nur ein Gerät mit dem ein gefaktes Netz erstellt wird, wo sich das Mobiltelefon der Zielperson dann automatisch einloggt. Mittels Loopantenne kann das Abhörspiel beginnen, funktioniert aus mehr als 100 Metern und kostet rund 450 Euro. Die gute Nachricht: Privatbereich kommt das selten vor. Das müsste schon ein krankhaft eifersüchtiger Liebespartner sein, der Geld in solch Spionagetechnik steckt. In der Wirtschaft ist dieses Bedrohungsszenario jedoch Realität. Der Autogigant Mercedes etwa schützt sich mit modernster Abwehrtechnik, produziert die Firma doch auch sensible Technik fürs Militär. Bei fast allen Großkonzernen ist es ähnlich. „Da haben dann Firmenvorstände spezielle Verschlüsselungs-Handys oder die Verhandlungsräume sind vor Lauschangriffen abgeschirmt“, berichtet Alexander

Fotos: fotolla.de

## CHECKLISTE FÜR DEN PC

Das reicht für groben Hacker-Schutz: eine Firewall (individuell konfiguriert, keine Basiseinstellungen verwenden) Virenscanner und Anti-Spyware. Bestmöglichen Schutz bieten nur kostenpflichtige Programme, Freeware deckt 90% der Risiken ab. Achtung bei WLAN: unbedingt WAP2 verwenden und verschlüsseln. WEP reicht nicht, hier können Passwörter in nur kurzer Zeit geknackt werden.



Tsolkas aus Erfahrung. Als Sicherheitsexperte war früher bei Opel und Schenker weltweit im Dienste des Firmen-Datenschutzes unterwegs. Heute verdient er sich erfolgreich als selbstständiger Berater und warnt ständig vor dem menschlichen Faktor. Denn ein guter Hacker ist heute mehr Psychologe als Codeknacker. Die Schwachstelle Mensch wird von gewieften Cyber-Banditen schamlos ausgenutzt. „Wenn man versucht einen Code-Schlüssel zu knacken, wird man alt und grau. Daher geht man den direkten Weg. Es gibt nichts, was über Social Engineering hinausgeht“, so Tsolkas. Hacker geben sich am Telefon zum Beispiel als Rechtsanwälte oder Kollegen aus. Oft kommt der Schmä, sie seien vom IT-Support-Team und bräuchten schnell mal das Passwort, weil der Computer zu viel Traffic blockiert. Echte Profis gehen sogar so weit, dass Freundschaften im realen Leben geschlossen werden. Was eignet sich da besser für Recherchezwecke als Facebook, das persönlichste Tagebuch auf Erden. Dort gibt jeder ganz freiwillig Sachen von

sich preis, die man einer fremden Person nicht mal nach dem zehnten Bier erzählt.

**Die gesammelten Daten** werden vom Hacker nach erfolgreicher Arbeit an den Meistbietenden oder den Auftraggeber weitergereicht. Wie schnell das gehen kann, hat Alexander Tsolkas bei einer seiner frühen Geschäftsreisen selbst erlebt. In Singapur checkt er in ein Hotel ein. Ein kurzes „Flutsch“ beim Durchziehen der Kreditkarte, mehr braucht der nette Lobby-Angestellte nicht für den Check-In. In der Nacht um drei Uhr früh dann ein unangekündigter Anruf aus Indien, direkt durchgestellt ins Hotelzimmer: „Herr Tsolkas, wollen Sie nicht einen Tata zum Vorzugspreis kaufen?“. Keine sechs Stunden also waren vergangen und schon waren die Kreditkarten-Daten vom Hotel in Singapur bis zur Vertriebsstelle von Tata Motors in Indien gewandert. Ein Glück, dass es beim bloßen Verkaufsgespräch für den Billigwagen geblieben ist. Nicht immer ist Spyware 2.0 so barmherzig.

## GEFAHR FÜR SMARTPHONES & CO.

IT-Experte Alexander Tsolkas: Android und Symbian-Systeme sind gefährdet. Daher unbedingt Updates ausführen und ein Anti-Viren-Programm besorgen. (Gefahr von Man-in-the-Middle-Attacken) Aus dem Schneider ist das iPhone. Außer man hat es gejaillbroken, d. h. so verändert, dass man alle Anwendungen – nicht nur die von iTunes – downloaden kann. Mehr dazu: Sectank.de und tsolkas.com.

