

Zombies, Würmer und Trojaner

Neue elektronische Gefahren und unzuverlässige Mitarbeiter gefährden die IT-Sicherheit von Unternehmen.

Organisierte Kriminalität, Geheimdienste und die eigenen Mitarbeiter seien für einen Großteil der Attacken auf die IT-Sicherheit von Unternehmen verantwortlich. Zu diesem Schluss kamen IT-Sicherheitsexperten am 26. April 2007 bei einer Podiumsdiskussion der *APA-E-Business-Community* in Wien. „Kriminelle haben den Marktplatz Internet mehr und mehr in Besitz genommen, wodurch sich die Situation grundlegend verändert“, sagte Mag. Leopold Löschl, Leiter des Büros für Computer- und Netzwerkkriminalität im Bundeskriminalamt. Cybercrime hat sich zu einer echten Bedrohung entwickelt. Waren früher die technische Herausforderung der Hauptsporn für Hacker, herrschen heute finanzielle Beweggründe vor. Außerdem können Angreifer inzwischen auf fertige „Bausätze“ zurückgreifen – und das birgt neue Gefahren für die IT-Sicherheit. Ein Beispiel dafür sind „intelligente“ Würmer, die mehr oder weniger selbstständig entscheiden, ob sie sich weiter verbreiten, Passwörter aus-schnüffeln oder den Rechner für spätere koordinierte Attacken vorbereiten.

Bot-Netze. Eine relativ neue Bedrohung sind Bot-Netzwerke, bei denen Computer gekapert und zu Zombie-Rechnern gemacht werden. „Wir haben einen Fall gehabt, bei dem Russen Unternehmen im Bereich Online-Gaming damit erpresst haben, ihre Websites lahm zu legen. Auch Österreich war davon betroffen“, berichtete Löschl. Durch Systemausfälle seien Schäden in sechsstelliger Höhe entstanden. „Das war einer der ersten Fälle, die zu einer Verurteilung in Russland geführt haben, weil es dort keine konkreten Cybercrime-Bestimmungen gibt. Die drei Haupttäter sind zu acht Jahren Haft verurteilt worden.“

Die Debatte über verdeckte Online-Ermittlungen durch deutsche Behörden werde auch hierzulande genau beob-



Hans-Jürgen Pollirer, Leopold Löschl, Christian Hohenegger, Michael Herdy, Michael C. Fritz, Maximilian Burger-Scheidlin.

achtet. „Natürlich wünscht man sich eine volle Werkzeugkiste und den so genannten Bundestrojaner als Ermittlungs-Werkzeug“, betonte Löschl. In Österreich gebe es aber keine passende Rechtsgrundlage für den Einsatz von Programmen, die ohne Wissen des Betroffenen auf dessen Computer installiert werden. „Wir setzen das nicht ein, schauen uns aber an, was in Deutschland passiert und ob dergleichen für Österreich in Betracht kommt. In der Schweiz wird meines Wissens im Bereich Internet-Telefonie etwas eingesetzt und auch die Amerikaner dürften was haben“, berichtete Löschl.

Sicherheitsrisiko Mitarbeiter. „Durch Abkommen mit den USA wird der Datenschutz unterlaufen. Das ist das Dilemma Europas. Auch bei den Flug-gastdaten ist die EU eingegangen“, sagte Hans-Jürgen Pollirer, Obmann der Bundessparte Information und Consulting in der *Wirtschaftskammer Österreich*. Sicherheitsrisiko Nummer eins seien aber die Mitarbeiter. „Alle Statistiken über die Ursachen von Computerausfällen und Datenverlusten zeigen den Menschen an vorderer Stelle. Es werden beispielsweise kaum Maßnahmen für den Fall definiert, dass jemand aus dem Unternehmen ausscheidet“, sagte Pollirer.

„Viele der technisch hervorragend geschützten Unternehmen sehen die Mitarbeiter und Kunden nicht als Mittelpunkt ihrer Aktivitäten. Daraus resultieren oft herrliche Angriffspunkte

für Kriminelle und Mafiosi“, ergänzte Maximilian Burger-Scheidlin, Geschäftsführer der *ICC Austria*, die Teil der Internationalen Handelskammer ist. Die Professionalisierung der Spionage und Produktpiraterie schreite munter voran. „Gut organisierte Gruppen wollen immer mehr Geld – nur das Management steckt vielfach den Kopf in den Sand, und glaubt mit tollen technischen Lösungen das Auslangen zu finden“, kritisierte Burger-Scheidlin.

„Der Fokus auf imaginäre Feinde, die von außen angreifen, ist nicht sinnvoll. Denn der Mitarbeiter sitzt direkt im Unternehmen und hat Zugriff auf eine Vielzahl von Daten“, sagte Christian Hohenegger, Experte für IT-Security bei *Capgemini*. Sicherheitsmaßnahmen seien meist auf technische Maßnahmen konzentriert, interne Bedrohungen würden hingegen unterschätzt.

„Viele Vorstände tauschen per E-Mail sensible Daten aus. Jeder, der will, kann mitlesen und keinen interessiert das“, bemängelte Michael Herdy, Geschäftsführer der *IT Solution GmbH*. Aber auch bei kleinen Unternehmen – etwa dem selbstständigen Finanzberater, der Informationen über Kunden auf seinem Laptop gespeichert hat – sei Vorsicht geboten. „Es stehen heute unzählige elektronische Methoden zur Verfügung, um an geheime Daten jeglicher Form zu gelangen“, sagte Herdy.

„Script Kiddies oder Hacking aus Spaß sind durch die Gefahr der Spionage von Mitbewerbern und Regierungen abgelöst worden“, berichtete Michael C. Fritz von *NextiraOne*. Weniger technisch raffinierte Angriffe sondern geplante und über Jahre hinweg genutzte Sicherheitslücken hätten zur Preisgabe von sensiblen Informationen geführt. Fritz: „Im Normalfall wurden die nationalen Geheimdienste dazu benutzt, wirtschaftliche Vorteile für Staaten durch ihre Spionage zu schaffen und das hat hervorragend funktioniert.“