Technologie

Im Visier der Datendiebe

Immer noch sind PC und Server die beliebtesten Angriffspunkte für Attacken über das Internet. Social-Networking-Plattformen wie My Space oder Xing werden wegen der Sorglosigkeit der Anwender zu beliebten Zielen.

Eine ganze Branche lebt von den Gefahren, die über das Internet verbreitet werden. Sie rüstet sich mit Experten und weltweit vernetzten Überwachungszentren gegen mögliche Pandemien. F.: Symantec

Klaus Lackner

Nicht jugendliche Hacker, sondern organisierte Kriminalität, Geheimdienste und eigene Mitarbeiter sind für einen Großteil der Attacken auf die IT-Sicherheit von Unternehmen verantwortlich. So lautete der einhellige Tenor von Experten bei einer Podiumsdiskussion im Rahmen der APA-E-Business-Community in Wien vor wenigen Monaten. „Kriminelle haben den Marktplatz Internet mehr und mehr in Besitz genommen, wodurch sich die Situation grundlegend verändert“, erklärte Leopold Löschl, Leiter des Büros für Computer- und Netzwerkkriminalität im Bundeskriminalamt.

Angriffe auf die IT-Sicherheit hätten inzwischen großteils einen wirtschaftlichen Hintergrund. Eine relativ neue Bedrohung seien Bot-Netzwerke, bei denen Computer gekapert und zu Zombie-Rechnern gemacht werden. „Wir hatten einen Fall, bei dem Russen Unternehmen im Bereich Online-Gaming damit erpresst haben, ihre Websites lahmzulegen. Auch Österreich war davon betroffen“, erzählte 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 eigentlich keine konkreten Cybercrime-Bestimmungen gibt. Die drei Haupttäter sind zu acht Jahren Haft verurteilt worden.“

Gefahr aus dem Inneren

„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 unser Management steckt vielfach den Kopf in den Sand und glaubt, mit tollen technischen Lösungen das Auslangen zu finden“, kritisierte Burger-Scheidlin.

> „Angriffe auf die IT-Sicherheit haben großteils einen wirtschaftlichen Hintergrund.“
>
> Leopold Löschl, Bundeskriminalamt

„Der Fokus auf imaginären Feinden, die von außen angreifen, ist nicht sinnvoll. Denn der Mitarbeiter sitzt direkt im Unternehmen und hat Zugriff auf eine Vielzahl von Daten“, gab sich Christian Hohenegger, Experte für IT-Security bei Capgemini, überzeugt. Die Umsetzung von Sicherheitsmaßnahmen sei nach wie vor auf technische Maßnahmen konzentriert, interne Bedrohungen würden hingegen unterschätzt.

Aber auch etablierte, häufig besuchte Internet-Portale sowie Social-Networking-Seiten rücken ins Visier der Cyberkriminellen. Davon ist die breite Masse betroffen. Das ist eine der Kernaussagen des aktuellen Internet-Sicherheitsreports von Symantec, einem Anbieter für IT-Sicherheitslösungen.

Web 2.0 birgt neue Risiken

Zwar bleibt der Computer Angriffsziel Nummer eins, um an finanziell verwertbare Anwenderdaten zu gelangen, doch das Vertrauen in etablierte Webseiten und der unbedarfte Umgang mit persönlichen Infos ermöglichen immer gezieltere Phishing-Attacken. Dementsprechend ist die Zahl der Server, auf denen betrügerische Webseiten gehostet werden, im zweiten Halbjahr 2007 weltweit um 167 Prozent auf 87.963 gestiegen. Zudem nutzen Angreifer seitenspezifische Schwachstellen aus, um über Shotgun-Angriffe (zeitgleiche Attacken über verschiedene Schwachstellen) Trojaner und Spionage-Tools in Computer einzuschleusen. Meist ist es nicht einmal notwendig, dass der Anwender bewusst etwas herunterlädt oder anklickt. Solche Drive-by-Downloads sind mittlerweile Standard der Angreifer.

„Professionell, organisiert und hochflexibel sind die Attribute, die den Wandel der Cyberkriminalität zu einer globalen Untergrundwirtschaft am besten beschreiben“, resümiert Symantec-Experte Candid Wüest.