



# Hacken als Hobby war gestern

*Der Hobby-Hacker ist Vergangenheit. Wo begabte Codeknacker früher aus sportlichem Ehrgeiz in Systeme grosser Unternehmen oder Regierungsstellen eingebrochen sind, hat sich die Motivation heute stark geändert.*

GIUSEPPE CRISTOFARO

**H**acking ist ein Geschäft geworden, in dem professionelle Hacker kriminellen Kreisen ihre Dienste für gutes Geld anbieten. Das bedeutet auch, dass professionelle Trojaner, Viren und elektronische Würmer die Bedrohung für Unternehmen und Privatpersonen grösser gemacht haben. Oft beginnen Attacks mit gut versteckten Aktivitäten, die den Angreifern die Kontrolle über fremde Maschinen geben. Dann können sie Daten entwenden, ohne dass der Endbenutzer dies merkt. Die gestohlenen Informationen übergeben oder verkaufen sie dann einem Auftraggeber. Der Hacker kann die kontrollierten PCs aber auch für weitere «Dienstleistungen» einsetzen. Zum Beispiel für das Versenden von Spam oder über Bot-Netze für gezielte Distributed Denial of Service-Attacks (DDoS).

Wie ausgewachsene Business-Profis hat die kriminelle Hacker-Gemeinde verschiedene Geschäftsmodelle entwickelt. Man kann Lösungen und Dienstleistungen

kaufen oder mieten, teilweise gibt es sogar Maintenance-Services dazu.

## **Eindringen, verbreiten, verstecken**

Aber auch die Hacker-Tools haben sich weiterentwickelt. Moderne Malware kombiniert heutzutage die besten Viren mit immer komplexeren technischen Tricks, um Schwachstellen auszunutzen. Sogar Plug-ins sind möglich. Über sie kann die Malware nahezu beliebig erweitert werden. Dahingegen wirkt die Verteilung fast schon klassisch: Hacker nutzen neben modernen Peer-to-Peer Mechanismen auch weiterhin konventionelle Methoden wie die Autostart-Funktion oder E-Mail.

Ein gutes Beispiel für einen modernen Angriff ist die Evolution des Conficker Wurms. Zuerst nutzte der Wurm eine Schwachstelle im Betriebssystem, um einzudringen. Danach begann der Code, sich sehr schnell und aggressiv zu verbreiten. Um sich zu verstecken, konnte der Wurm

alle Systeme lahmlegen oder neu konfigurieren, welche ihn entdeckt hätten. Um dem Angreifer möglichst viele Möglichkeiten zu bieten, Schaden anzurichten, kann Conficker mit Plug-ins erweitert werden. Über Peer-to-Peer Technologien kann er Daten mit anderen infizierten Geräten austauschen. Sein Schadcode nistet sich äusserst hartnäckig in infizierte Systeme in hunderten von Routinen ein. Der Normalnutzer merkt davon meist nichts. Selbst Firmen benötigen oft mehrere Wochen, um Clients und Server komplett zu säubern.

## **Trojaner aus dem Baukasten**

Um einen Angriff zu starten, muss man nicht einmal mehr IT-Freak sein. Heute verfügbare Malware-Development-Kits ermöglichen auch dem unerfahrenen Entwickler, einfach und effizient einen Trojaner zu schreiben. Im Tool stehen ihm Funktionen wie verschlüsselte Kontroll- und Kommando-Kanäle zur Verfügung,

Web-Services für das Hosting von Phishing-Inhalten, Man-in-the-browser Proxy-Engines für den Identitätsdiebstahl und zu guter Letzt auch Laufwerksscanner. Damit lassen sich kommerziell interessante Daten wie E-Mail-Adressen und Kreditkarten-Details erkennen und abfangen.

Bei diesen Malware Entwickler-Paketen handelt es sich um hochentwickelte Software zur kriminellen Nutzung. Die Entwicklerteams garantieren sogar Service-Levels wie zum Beispiel beim türkischen Trojaner-Kit «TURKOJAN». Es ist in drei Versionen zu unterschiedlichen Preisen zwischen 99 und 249 US-Dollar erhältlich. Je teurer der Preis, desto höher der garantierte Service-Level. Zum Beispiel garantieren die Entwickler je nach Preis, wie lange Antiviren-Software den Trojaner nicht erkennt. Bei der teuersten Variante ist technischer Support rund um die Uhr im Preis inbegriffen. Andere Malware beinhaltet mehrsprachigen Support oder Funktionen, mit denen man Trojaner in Würmer umwandeln kann. Mittlerweile müssen die bekanntesten Entwicklerteams ihre Lösungen sogar schon vor unerlaubtem Kopieren schützen, einen Ehrenkodex gibt es in der kriminellen Hackerszene nicht mehr.

Um auf die geballte kriminelle Energie vorbereitet zu sein, müssen Unternehmen schnell sein. Neue Malware nutzt Schwachstellen immer schneller aus. Der IBM ISS X-Force Trend & Risk Report zeigt, dass sogenannte Zero-Day Exploits immer häufiger werden. Darunter versteht man Angriffe auf Schwachstellen, die Hersteller erst am selben Tag veröffentlicht haben. Zum Teil nur wenige Minuten nach Bekanntgabe gibt es schon Malware, die diese Schwachstelle nutzt. Sowohl für Privatanwender wie auch für Unternehmen ist es unmöglich, das Loch rechtzeitig mit einem Patch zu flicken – oft weil es diesen noch gar nicht gibt. Laut dem Trend-Report haben sogar ca. die Hälfte aller Schwachstellen sogar nach einem Jahr noch keinen Patch.

## Um einen Angriff zu starten, muss man nicht einmal mehr IT-Freak sein.

### Geschützt ungeschützt

Sich effizient gegen diese Gefahren zu schützen, ist schwierig. Es ist ein Katz-und-Maus-Spiel: Der Schutz wird einen Schritt besser, die Hacker finden eine neue Lücke. Zum Beispiel haben Antivirus-Software Hersteller signaturbasierte Technologien um Funktionen wie «Advanced Heuristic» oder verhaltensbasierte Engines erweitert. Malware Entwickler umgingen diese Massnahmen, indem sie nicht erkennbare Malware entwickelten. Ausserdem stehen ihnen Dienstleistungen und Tools zur Verfügung, um ihre Kreationen auf Resistenz vor den wichtigsten



**Funktionsprinzip des virtuellen Patches: Auch bei unbekannter Malware sind die Systeme sicher, sobald die Schwachstelle bekannt ist.** Quelle: IBM ISS

Antiviren Produkten zu testen. Solange die Entwickler von Malware schneller neue Versionen entwickeln als Antiviren-Hersteller Updates liefern können, sind die Kunden effektiv ungeschützt.

Vor allem Unternehmen sollten deswegen nicht allein auf konventionelle Antiviren-Software setzen. Daneben sollten weitere Lösungen zum Einsatz kommen, welche Schutz vor unbekannter Malware ermöglichen. Diese Möglichkeit bieten sogenannte Intrusion Detection und Prevention Systeme (IPS). Sie überprüfen verdächtigen Code nicht nur auf bestimmte Muster (Signatur), sondern analysieren, was der Code bewirkt und worauf er zugreifen will. Möchte ein Code auf eine Schwachstelle zugreifen, kann man diesen Zugriff verhindern. Das geschieht oft schon auf der Netzwerkebene und nicht erst, wenn die Malware schon auf der Maschine ist.

### Schutz selbst vor unbekannter Malware

Für solche Systeme muss man die Malware selbst noch nicht kennen – aber die Schwachstellen müssen bekannt sein. Namhafte Anbieter beschäftigen dafür Spezialisten, die wie Spürhunde Anwendungen und Systeme danach durchsuchen. Bei IBM haben zum Beispiel Experten der sogenannten ISS X-Force letztes Jahr über 7000 Schwachstellen aufgedeckt oder dokumentiert. Diese Arbeit und die Erkenntnisse fliessen direkt in die Intrusion Detection und Prevention Systeme ein.

Solche Lösungen haben zwei Hauptvorteile: Erstens ist man auch vor noch nicht bekannten Viren, Trojanern und Würmern geschützt. Und zweitens gewinnen Unternehmen die nötige Zeit, die sie brauchen, bekannte Schwachstellen mit den Patches der Hersteller zu schliessen. Ihre Systeme sind gesichert, auch wenn das Sicherheitsupdate noch nicht ausgerollt wurde.

Zudem beinhalten diese IPS auch Funktionen, um sogenanntes Cross-Site-Scripting oder SQL Injection-Angriffe zu verhindern. Mit dem Aufkommen von Web 2.0-Technologien steigt die Anzahl solcher Angriffe wieder an. Dies auch dank immer kürzerer Entwicklungszyklen

von Applikationen und den damit verbundenen kurzen Testzyklen, die oft zu Qualitätsproblemen führen.

## Um auf die geballte kriminelle Energie vorbereitet zu sein, müssen Unternehmen schnell sein.

### Fazit: Schutz ist unumgänglich

Professionelle Hacker und leistungsfähige Malware machen den Einsatz von umfangreichen Sicherheitstechnologien in Unternehmen – sowie oftmals auch für Privatanwender – unumgänglich. Jeder ist ein mögliches Angriffsziel. Dass viele Nutzer bislang glauben, noch kein Opfer von kriminellen Aktivitäten aus dem Netz geworden zu sein, hat leider nichts zu bedeuten. Von einer Infektion mit einem Daten-Schädling erfährt der Nutzer oft nichts oder erst, wenn es zu spät ist. Absolutes Minimum sollten Firewall, Anti-spam/Antiphishing und Antivirensoftware auf jeder Maschine sein. Vor allem in Unternehmen werden aber immer stärker moderne Intrusion Detection und Prevention Systeme zum Einsatz kommen. Managed Security Services, welche von verschiedenen Anbietern zu haben sind, bieten eine weitere Möglichkeit, sich vor Attacken zu schützen. Sie ermöglichen einen hohen Sicherheitsstandard rund um die Uhr, ohne ein eigenes 24x7-Sicherheits-Kompetenzzentrum betreiben zu müssen. Oft ist das eine valable Alternative.

Welche Massnahmen die Richtigen sind, hängt jeweils stark vom Einzelfall ab. Es gilt, Faktoren wie Unternehmensgrösse, Branche und Bedrohungslage zu beachten. Dass sich eine gründliche Analyse aber lohnt, ist unbestritten. Die Netz-Kriminellen planen ihre Einsätze rund um die Uhr und wissen genau, wann der Security Operator einer Unternehmung Feierabend hat. ■

Der Autor: Giuseppe Cristofaro ist Manager ISS bei IBM Switzerland.