# Im Netz der Hacker

**CYBER-KRIMINALITÄT** Angesichts der zunehmenden Überwachung sollten gerade auch Unternehmen ihre Exponiertheit nicht unterschätzen.

**TEXT** ANDREAS WISLER

**Eine Firewall und ein Antivirenprogramm reichen zum Schutz vor Hackern meist nicht mehr aus.**

Bildquellen: zVg

Cyber-Kriminalität ist ein lukratives Geschäft. Der Hersteller von Antivirenprogrammen McAfee hat bereits vor einigen Jahren gemeldet, dass damit mehr Geld umgesetzt wird, als mit dem weltweiten Drogenhandel. Auch die Schweiz gerät immer mehr ins Visier der Cyber-Kriminalität, schreibt die schweizerische Melde- und Analysestelle MELANI* in ihrem halbjährlich erscheinenden Lagebericht. Aus diesem Grund hat der Bundesrat am 27. Juni 2012 die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken» gutgeheissen. Mit dieser Strategie will er in Zusammenarbeit mit Behörden, der Wirtschaft und den Betreibern kritischer Infrastrukturen die Cyber-Risiken vor allem dort minimieren, wo Betroffene Hackern täglich ausgesetzt sind.

## UNTERSCHÄTZTE GEFAHR

Aber auch «gewöhnliche» Unternehmen sind davon betroffen. Die Schweiz gilt nicht umsonst als ein sehr innovatives Land mit guten Ideen und den meisten Patentanmeldungen weltweit. Mit Ideen und Erfindungen lässt sich viel Geld verdienen. Zudem sind die technischen Infrastrukturen von kleineren Firmen im Normalfall nicht so gut geschützt, wie bei grossen Unternehmen, die teilweise über eigene IT-Abteilungen verfügen. Immer wieder hört man Aussagen wie «an meinen Daten hat niemand Interesse» oder «wir sind ja keine Bank».

Diese erweisen sich heute jedoch als falsch. Daten und Informationen bedeuten Geld. Es braucht lediglich eine geschickte Verknüpfung von verschiedenen Informationsquellen – und das Profil eines Menschen ist erstellt. Ein Beispiel dafür ist die Suchmaschine von Google: Die Suchresultate werden im Laufe der Zeit immer besser den persönlichen Vorlieben angepasst und beeinflussen so die freie Meinungsbildung. Nicht vergessen werden darf, dass diese Angaben «freiwillig» zur Verfügung gestellt werden, wie dies auch bei den verschiedenen Kundenkarten der Fall ist. Auch hier wird ein Profil erstellt und personalisierte Werbung verschickt.

## DREISTE PHISHING-FALLEN

Auf der anderen Seite sind Informationen vorhanden, die nicht freiwillig oder bewusst veröffentlicht werden. Eine Methode, an solche Informationen zu gelangen, ist Phishing. Beim klassischen Phishing per E-Mail wird versucht, das Opfer auf eine manipulierte Seite zu locken, auf der persönliche Daten abgefragt werden. Oft wirken diese Seiten täuschend echt und originalgetreu und es ist für den Nutzer schwierig zu erkennen, wo er sich tatsächlich befindet. Beliebt sind dabei Abfragen von Kreditkartendetails. Obwohl sehr viel über Phishing und die dabei angewendeten Methoden berichtet wird, ist es verblüffend, wie erfolgreich solche Angriffe immer noch sind. Bei unseren gezielten Phishing-Angriffen, selbstverständlich in Absprache mit unseren Kunden, ist die Erfolgsrate sehr hoch: Zwischen 50 und 70 Prozent der angeschriebenen Personen fallen auf den Angriff herein.

Das klassische Phishing wird neuerdings vermehrt mit anderen Methoden kombiniert. So wurden Schweizer E-Banking-Kunden zum Angriffsziel für das sogenannte Voice-Phishing. Dabei werden Phishing-Emails verschickt, mit dem Hinweis, dass ein neues Sicherheitssystem installiert wurde und sich ein Bankmitarbeiter telefonisch melden werde. Dazu müsse nur die Telefonnummer angegeben werden. Anschliessend werden die Opfer tatsächlich von den Betrügern angerufen. Aus «Sicherheitsgründen» muss nun das Login inklusive des zweiten Merkmals (SMS, Token) angegeben werden. Solche Anrufe sind sehr professionell und werden teilweise sogar auf Schweizerdeutsch geführt. Auch hier gilt es daher, sehr vorsichtig zu sein und nie persönliche Angaben weiterzugeben.

## MIT HÜRDEN GEGEN HACKER

Wie bereits erwähnt, sind auch Firmen ein beliebtes Angriffsziel. Eine Firewall und ein Antivirenprogramm reichen zum Schutz nicht mehr aus. Denn auf dem Markt sind verschiedene Tools verfügbar, mit denen innert weniger Minuten eine Schadsoftware (Malware) erstellt werden kann, die von den heutigen Antivirenprogrammen nicht erkannt wird. Gelingt es einem Kriminellen, diese Malware in die Systeme einer Firma einzuschleusen, sind keine Hindernisse mehr vorhanden und er kann sich auf der Suche nach interessanten Daten frei im Netzwerk bewegen. Um diese Hürde so hoch wie möglich zu setzen, ist es wichtig, das Betriebssystem und die installierten Programme immer auf dem aktuellen Stand zu halten. Auch hier gilt es, Emails genau zu prüfen, bevor man ein mitgeschicktes Programm ausführt. Auch der als Preis erhaltene USB-Stick sollte erst nach einer gründlichen Überprüfung mit dem Computer verbunden werden. Wie verschiedene Statistiken zeigen, sind auch Schweizer Firmen und Personen ins Visier der Cyber-Kriminellen geraten. Mit der notwendigen Vor- und Umsicht ist es aber realisierbar, die Hürden möglichst hoch anzusetzen. Aktuelle Antivirenprogramme und eine gesunde Skepsis helfen, nicht selbst Opfer eines Angriffs zu werden.


**ZUM AUTOR**

Andreas Wisler ist Geschäftsführer und Senior Security Auditor bei der goSecurity GmbH, welche IT-Sicherheitsüberprüfungen und -beratungen durchführt. Weiter unterrichtet er unter anderem an der Fachhochschule Nordwestschweiz FHNW IT-Sicherheitsthemen.
wisler@goSecurity.ch


* www.melani.admin.ch