

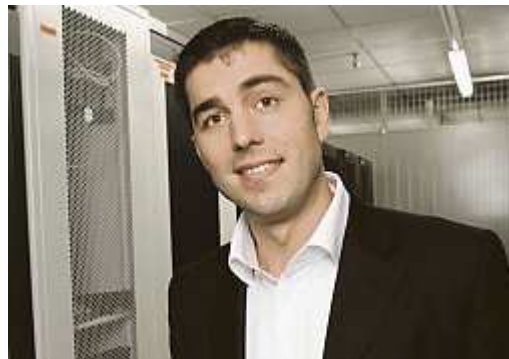
# Unternehmen im Visier der Web-Kriminellen

Von Stefan Meisterle

Computerschädlinge werden immer stärker auf ausgewählte Ziele angesetzt.

## Wien.

Eine lange Liste rattert über den Bildschirm. Kryptische Einträge aus Zeichen, Begriffs- und Zahlenketten bestimmen das Bild, werden überflogen oder angewählt. Hinter diesen scheinbar unerklärlichen Einträgen verbirgt sich freilich alles andere als Massenware: Es sind jene Computerschädlinge, die ausreichend raffiniert programmiert wurden, um die automatisierten Sicherheitsschleusen zu umgehen - und doch nicht raffiniert genug, um Warnmechanismen und geschultem Blick der Virenjäger zu entgehen. Was im Computerlabor des Wiener Antivirenspezialisten Ikarus unter die Lupe genommen wird, hat jedenfalls das Zeug dazu, reichlich Schaden anzurichten.



**Virenjäger Josef Pichlmayr rät Firmen zu einem "Plan B".**

Auf rund 281 Milliarden Euro beziffert das US-Unternehmen Symantec den jährlich durch die globale Internetkriminalität verursachten Schaden. Ein Großteil davon geht auf das Konto von Computerviren und anderen Schädlingsprogrammen. Den Rest teilen sich Phishing-Attacken, Kreditkartenmissbrauch und andere Formen des Online-Betrugs untereinander auf. Die Grenzen zwischen den Formen der Cyber-Kriminalität sind fließend, zur Anwendung werden sie häufig in kombinierter Form gebracht.

Doch es sind nicht nur die ausgeklügelten Werkzeuge, die Cyber-Crime immer bedrohlicher werden lassen - sondern speziell das Motiv, das dahinter steckt. "Angriffe aus dem Internet werden immer zielgerichteter, weil sie einer Ökonomie unterworfen sind. Es gibt inzwischen wesentlich mehr Attacken, die sich explizit gegen einzelne Opfer richten und dabei ein klares Ziel verfolgen", beobachtet Ikarus-Chef Josef Pichlmayr einen Trend weg von Massenattacken hin zur Online-Wirtschaftskriminalität, die ihre Werkzeuge verstärkt gegen Unternehmen einsetzt. Ziel dabei ist, an Kundendaten, Unternehmensgeheimnisse oder Verträge heranzukommen. Und sich dagegen zu schützen, fällt schwer.

## IT-Sicherheit betrifft alle

"Wenn es clever gemacht ist, schafft es ein manipuliertes E-Mail durch jeden Filter in den Posteingang des Opfers", ist Pichlmayr überzeugt. Häufig wird dabei Social Engineering als Vorarbeit geleistet, es werden also etwa Daten von Mitarbeitern per Google oder in sozialen Netzwerken ausfindig gemacht, die dann als Absender eingesetzt werden und beim Empfänger Vertrauenswürdigkeit suggerieren. "Es ist wesentlich einfacher, das Vertrauen der Mitarbeiter auszunutzen, als ein technisches System zu überlisten, wo man erst mühsam eine Lücke suchen muss", so der Ikarus-Geschäftsführer, der klarstellt: "Ist Wirtschaftsspionage das Motiv von Cyber-Crime und verfügt der Angreifer über genug Ressourcen, hat man keine Chance, sich dagegen zu wehren." Mit der Größe des Unternehmens hat das Bedrohungsbild dabei wenig zu tun: "IT-Sicherheit betrifft heutzutage jeden Unternehmer", so Hans-Jürgen Pollirer, Obmann der Sparte Information und

Consulting der Wirtschaftskammer.

Und doch gibt es Methoden, sich gegen Cyber-Crime abzusichern. Zum einen bedarf es einer Firewall und eines Antivirenprogramms. Zum anderen gilt es, sich bewusst zu machen, dass das nur bedingt schützen kann. "Ich muss einplanen, dass es jemandem gelingen kann, einzudringen. Und ich muss wissen, wie ich damit umgehe. Gibt es Dinge, bei denen keinesfalls etwas passieren darf, müssten diese eigentlich vom Netz", so Pichlmayr.

## **Cloud als Chance und Risiko**

In der Realität geht der Trend freilich in Richtung Verlagerung von Programmen und Daten aus lokalen Speichern ins Internet, der Cloud. Das wirft gerade in Sachen Sicherheit neue Fragen auf, wie eine Reihe von spektakulären Datenverlusten in den vergangenen Jahren verdeutlicht. Wenig überraschend sind folglich auch Sicherheitsbedenken die stärksten Vorbehalte, die viele Unternehmen noch vor Cloud-Diensten zurückschrecken lassen, wie Karl Mayrhofer, Geschäftsführer des Softwareanbieters Fabasoft, erläutert: "Wäre das Thema des Vertrauens in Cloud-Services nicht, würden heute schon viel mehr Unternehmen Cloud-Services nutzen." Dass die neuen Angebote Firmen auch in Sachen Sicherheit helfen würden, steht für Mayrhofer aber fest. "Von der Investition, die wir als Cloud-Provider investieren, um für Sicherheit und Zuverlässigkeit zu sorgen, profitieren auch unsere Kunden, insbesondere KMU", so Mayrhofer.

## **Die Schwachstelle Mensch**

Egal ob in der Cloud oder vertrauend auf lokale Speicher - aus der Verantwortung stehlen kann sich kein Unternehmen. Wichtig ist daher die Bewusstseinsbildung, sind Experten überzeugt. "Im Rahmen der Digital-ID-Initiative wollen wir 2012 bei den Unternehmen das Bewusstsein schaffen, dass Sicherheit und die sichere Nutzung von Internet- und Cloud-Diensten ein essentielles Thema sind", sagt Mayrhofer.

"IT-Sicherheit kann auch bei besten technischen Maßnahmen nur dann funktionieren, wenn die Mitarbeiter ein ausgeprägtes Sicherheitsbewusstsein besitzen", pflichtet Pollirer unter Verweis auf die seit 2005 bestehende Aktion "it-safe" bei. Und auch Pichlmayr stimmt zu: "Ein schwaches Glied in der Kette gibt es immer: Das sind wir Menschen." Denn selbst das akribischste Studium der neuesten Viren vermag eben nur bedingt zu schützen.

URL: [http://www.wienerzeitung.at/themen\\_channel/wz\\_digital/digital\\_news/431988\\_Unternehmen-im-Visier-der-Web-Kriminellen.html](http://www.wienerzeitung.at/themen_channel/wz_digital/digital_news/431988_Unternehmen-im-Visier-der-Web-Kriminellen.html)

© 2012 Wiener Zeitung