



Steckbrief

Name: Josef Pichlmayr
 Position: Geschäftsführer
 Unternehmen: Ikarus Software
 Mail: joe@ikarus.at
 Web: www.ikarus.at
 www.mymailwall.at

Josef Pichlmayr:

»Ein Katz-und-Maus-Spiel von Angreifern und Verteidigern«

Die Entwicklung der Cyberkriminalität hat im Jahr 2007 einen neuen Höhepunkt erreicht. output sprach mit Ikarus-Geschäftsführer Josef Pichlmayr über den enormen Anstieg von Schadcode und womit Unternehmen noch rechnen müssen.

output Welche Schädlinge stellen derzeit die größten Sicherheitsbedrohungen für Unternehmen dar?

Josef Pichlmayr Risiken verbergen sich im Prinzip hinter fast allen unter der Gruppe Malware subsummierbaren Codes. Die größten Risiken gehen aber eindeutig von der Trojaner-Gruppe aus.

Was macht Trojaner so gefährlich?

Pichlmayr Es gibt mannigfaltige Ausprägungen. Auch solche, die das Zielsystem komplett kontrollieren. Das ermöglicht eine Unzahl an Angriffsmöglichkeiten, sei es nur um die Identität des Opfers anzunehmen und Dritte damit zu schädigen oder dem Inhaber des infizierten PCs selbst Schaden zuzufügen.

Gerade im Unternehmensbereich kann das zu nachhaltig unangenehmen Konsequenzen führen – wenn etwa Informationen manipuliert werden, Forschungs-, Strategie- oder Finanzergebnisse in falsche Hände geraten oder schlicht und einfach irgendwelche Files – möglicherweise Kinderpornographie – zwischengelagert werden. Die Palette an Bedrohungsbildern und Risiken ist sehr vielseitig.

»Die Technologie ist nur Mittel zum Zweck. Immer wichtiger werden Verhaltensregeln und Awareness.«

JOSEF PICHLMAYR
GESCHÄFTSFÜHRER VON IKARUS SOFTWARE



Wie hat sich das Bedrohungsszenario in den vergangenen Monaten verändert?

Pichlmayr Das Prinzip heißt heute: »make money«. Waren es früher Motive wie Neugier, Langeweile oder Geltungsdrang hat sich mittlerweile eine effektive Cybercrime Community gebildet, die erstaunlich arbeitsteilig organisiert ist. Neben Daten und Informationen werden ganze Infrastrukturen – wie Bots, Webserver, Mailserver bis hin zu virtuellen ISPs –, spezielle Software wie Trojaner-Codes oder Hackertools und sogar Dienstleistungen wie Spamversand und DDOS-Attacken angeboten. Eigene Firmen – etwa das Russian Business Network – bieten »Komplettpakete« inklusive »Schutz« vor Gegenmaßnahmen allfällig Betroffener an. Das hat dazu geführt, dass wir mittlerweile über 10.000 neue Malware-Komponenten pro Tag registrieren.

Die nicht kontrollierbar sind?

Pichlmayr Diese Masse an neuen Mal-Codes macht es unmöglich, noch ein großes Bild zu zeichnen und zu erkennen, welche Trojaner-Systeme mit welchen Code-Teilen (Infektoren, Downloader oder Aktionsmodulen) interagieren. So darf es auch nicht verwundern, wenn die Qualität der Attacken um ein Vielfaches gestiegen ist. Neben professionellerer Infrastruktur zeichnen sich die Attacken des vergangenen Jahres durch zunehmende Komplexität aus und sind selbst für Spezialisten nicht immer auf den ersten Blick erkennbar oder nur zu einem Teil nachvollziehbar.

Die Virenschutztechnologie hinkt hinterher?

Pichlmayr Im Wesentlichen basiert das Katz-und-Maus-Spiel der Angreifer und Verteidiger auf einem Aktions-Reaktionsprinzip – jeder neuen Attacke wird mit neuen Sicherheitsmechanismen begegnet, die wiederum neue Attacken nach sich ziehen, die in der Lage sind, die getroffenen Sicherheitsmaßnahmen zu unterlaufen. Revolutionäres hat sich im Bereich der Sicherheitslösungen 2007 dabei nichts getan – jedoch lassen sich mehrere Trends ableiten, neben technologischen Neuerungen vor allem im Bereich der Umsetzung von Virenschutz- und Security-Maßnahmen.

Was sind die wirksamsten Schutzmaßnahmen?

Pichlmayr Aus Kostengründen, aber auch wegen der zunehmenden Komplexität, die sichere Systeme erfordern, sind UTM-Systeme (Unified Thread Management) stark im Kommen, also All-in-one-Systeme, die neben Firewall, Intrusion Detection und Virenschutz auch entsprechende »policy enforcement«-Lösungen beinhalten. Auf der anderen Seite wird aber auch immer mehr in den Bereich Managed Security Services investiert, wobei maßgebliche Sicherheitskomponenten ausgelagert werden.

Welche Fortschritte macht die Technologie?

Pichlmayr Auf technologischer Basis rückt das »behavioral blo-cking« als Hoffnungsträger in den Vordergrund. Es handelt sich

dabei um das Erkennen von Viren auf Grund ihrer Verhaltensweisen. Ähnliches wurde schon mit heuristischen Simulationsmethoden versucht. Neu ist jetzt, dass nicht nur der Virencode selbst bewertet wird, sondern auch eine Korrelation dieser Bewertung mit den Systemaktivitäten erfolgt.

Mit welchen Bedrohungen werden Unternehmen in Zukunft verstärkt rechnen müssen?

Pichlmayr Es ist eine klare Spezialisierung einzelner Angriffsbilder erkennbar. Attacken mit lokaler Ausprägung werden zur Regel und sind nicht mehr die Ausnahme. Angriffe, die sich gezielt gegen Einzelne richten, sind ungleich schwieriger zu erkennen und abzuwehren als der »high outbreak«, der neben Medieninteresse natürlich auch Vielzahl an Security-Experten auf den Plan ruft. Vereinfacht lässt sich sagen, dass sich die Anzahl der Risiken für Unternehmen vervielfacht.

Die Konsequenzen für die Betroffenen?

Pichlmayr Neuartige Bedrohungen werden einen veränderten Handlungsbedarf in elektronischen Geschäftsmodellen erfordern. Die Optimierung von Abläufen, Speed-to-market oder Just-in-time führen zu einer höheren Anfälligkeit dieser Prozesse. Einzelereignisse haben dabei unter Umständen weit reichende Kettenreaktionen zur Folge, die im Kontext der vernetzten Wirtschaft schwer überschaubar sind. So kann es zu sinkendem Vertrauen der Anwender bei allen Services im Netz kommen.

Wie sollen Unternehmen damit umgehen?

Pichlmayr Es gibt keine Patentlösungen. Die verwendeten Technologien sind nur Mittel zum Zweck. Immer wichtiger für Unternehmen werden Verhaltensregeln und Awareness – Letzteres steht aber in vielen Fällen fast diametral zur Anforderung, die leistungsfähige Sicherheitssysteme erfordern.

Welche Technologien bieten gegenwärtig die größte Sicherheit?

Pichlmayr Optional bietet sich an, die ausgetrampelten Pfade zu verlassen und mit alternativen Systemen weniger Angriffsfläche zu bieten. Ansonsten gibt es sehr leistungsfähige Firewall- und Virenschutzsysteme – neben den erwähnten UTM-Lösungen vor allem sehr starke dedizierte Systeme, die allerdings auch einen hohen Spezialisierungsgrad in der sicheren Anwendung erfordern. »Applications Layer Security« basiert auf kompletten Authentifizierungs- und Rechtesystemen und erlaubt eine ausgesprochen restriktive Handhabung von Sicherheitslösungen – vorausgesetzt man ist in der Lage das Pouvoir dieser Systeme auch voll einzusetzen und ihre Effektivität nicht am Altar der Usability zu opfern.

Das Gespräch führte Dietmar Boigner.