

# Internet-Security

**Sorglosigkeit ist der Nährboden für Angriffe im Internet. Die Angriffe aus dem Web werden immer schwerer erkennbar.**

Die Szene ist extrem lebendig“, sagt Josef Pichlmayr, Geschäftsführer der auf die Bekämpfung von IT-Schadsoftware spezialisierten Firma Ikarus. „In unserem Analyse-Lab registrieren wir pro Tag etwa 12.000 bis 20.000 Schadprogramme. Anfang 2008 waren es sogar an die 30.000 pro Tag.“

Wollten Hacker und die Schreiber von Schadsoftware zunächst nur sich selbst bestätigen und ihre Fertigkeiten erproben, ist seit 2004/05 ein massiver Motivwandel eingetreten. „Die Leute sind draufgekommen, dass sich mit Informationen, Manipulation und Betrug in vielfältiger Art viel Geld verdienen lässt. 2008 wurde mit Cybercrime bereits mehr Geld verdient als im internationalen Drogenhandel“, betont Pichlmayr. Waren die Schadprogramme in den Anfängen zumeist vom Angreifer selbst erdacht und geschrieben, ist nunmehr eine arbeitsteilige Organisation festzustellen.

Das – als Ausrede zur Unterlassung von Sicherheitsmaßnahmen vielfach gehörte – Argument „Wen interessiert schon mein PC?“ greift nicht. Interessant sind für einen Angreifer bereits die verwendete Hardware und der Speicherplatz – gleichgültig, ob virtuell auf einem Webserver oder dem PC. Auf diesem können Daten gelagert und Plattformen für weitergehende Angriffe geschaffen werden; es kann Rechenleistung in Anspruch genommen werden, etwa um Schlüssel zu errechnen. Interessant sind ferner Daten



**Schadprogramme benutzen ausgeklügelte Mechanismen, um sich vor Antivirensoftware zu tarnen. Sie lassen sich mit herkömmlichen Virenscannern nur schwer aufspüren.**

wie Kreditkartennummern oder Log-ins bei Online-Versteigerungshäusern, die es den Angreifern ermöglichen, die Identität ihrer Opfer anzunehmen. Der Angreifer, der genügend persönliche Daten gesammelt hat, kann in die virtuelle Identität des Angegriffenen schlüpfen, sich für ihn ausgeben, Einkäufe tätigen, Nachrichten abfangen, in Online-Casinos oder Online-Pokerrunden spielen – der Angegriffene wird zum Spielball.

**Soziale Netzwerke.** Informationen, die in Erfahrung gebracht werden können, wie Adressen, Arbeitgeber, welches Auto jemand fährt, welchen Hobbys er nachgeht, sind nicht nur für die Werbewirtschaft von Interesse. Mit derartigem Wissen können Angriffe auf der Basis von *Social Engineering* gestartet werden, indem

man sich über Netzwerke wie *Facebook*, *Xing*, *Myspace* mit Insiderwissen in das Vertrauen des Angegriffenen einschleicht.

„Man glaubt es nicht, was die Leute in derartigen Netzwerken alles von sich preisgeben“, erzählt Pichlmayr. „Bei Wirtshausgesprächen passt man mehr auf als in Bereichen des Web 2.0, wo man sich unter seinesgleichen wähnt.“ Je mehr man über sich erzählt, umso mehr Informationen erhält man über andere, was einen gewissen Druck erzeugt, mehr von sich preiszugeben, über Schulbesuch, Politik, Musik, Arbeitsverhältnis, persönliches Befinden. Bedenken sollte man, dass die Identität eines Teilnehmers in diesen sozialen Netzwerken nur in Ausnahmefällen überprüft wird, wenn sich etwa jemand auffällig als Prominenter ausgibt. Mit Insiderwissen über

das potenzielle Opfer können gezielte Angriffe gegen jemanden ebenso gefahren werden wie gegen das Unternehmen, in dem diese Person arbeitet. Liest man die Nutzungsbedingungen der Anbieter dieser Plattformen durch, erfährt man beispielsweise, dass die persönlichen Daten Eigentum des Betreibers des Netzwerks werden und man sich US-amerikanischem Recht unterwirft, Streitigkeiten also vor einem amerikanischen Gericht austragen müsste. Unternehmen sollten unbedingt eine Policy zum Umgang mit dem Web 2.0 entwickeln, rät Pichlmayr. Gesammelte Informationen können zum *Whaling* verwendet werden. Die „Wale“ sind Prominente, Politiker, Künstler, denen angedroht wird, sie zu kompromittieren oder deren Status missbräuchlich für andere Betrügereien zu verwenden – etwa insofern, dass bei einem vorgetäuschten Besuch einer Veranstaltung durch den Prominenten im Voraus kassiert wird.

„Joe-Jobs“ sind solche, die zum Ziel haben, durch gezielte Unwahrheiten die politische Meinungsbildung zu beeinflussen oder jemanden zu diskreditieren und die Meinung über ihn zu manipulieren, bis hin zu Nachrichten über seinen angeblichen Tod – was zu kurzfristigen Kurseinbrüchen an der Börse führen kann. Wie die Manipulationen um Steve Jobs als Gründer und CEO von *Apple* bewiesen.

Beim *Spear Phishing* werden gezielt Einzelne oder kleine Gruppen, über die man zuvor Informatio-



**Josef Pichlmayr, Ikarus:**  
**„Wir registrieren täglich etwa 12.000 bis 20.000 Schadprogramme.“**

nen gesammelt hat, mit glaubwürdig klingenden Phishing-Attacken angesprochen. E-Mails mit einem Attachment werden von Angreifern nur mehr bedingt eingesetzt. Man geht dazu über, auf einen Link zu verweisen, über den man angeblich zu begehrten Theater- oder Konzertkarten kommt oder gibt vor, dass ein Paket eingelangt sei.

**Virens Scanner** können den Inhalt von Links nicht erkennen. Bei Anklicken des Links geschieht dasselbe wie beim Öffnen des Attachments einer E-Mail mit Schadsoftware, etwa, dass sich ein Trojaner festsetzt. Ein solcher kann beispielsweise bei PCs von Finanzmanagern Stichwörter registrieren, die für den Kapitalmarkt von Interesse sind und verschickt selbstständig und unbemerkt Informationen mit derartigem Inhalt nach außen zu seinen Urhebern, die auf diese Weise einen Informationsvorsprung erhalten. Oder der Computer wird Teil eines „Botnetzes“ und zusammen mit vielen anderen dazu benützt, Angriffe auf andere Rechner zu fahren, um diese entweder völlig lahmzulegen (dDoS-Attacken; auch Wahlcomputer können davon betroffen sein) oder den Service zu beeinträchtigen. Angebliche Viren-

schutzprogramme, die prompt gefährliche Lücken aufzeigen, entpuppen sich als solche, die erst recht Schadsoftware enthalten. Oder es wird eine Überprüfung angeboten, ob die eigene Kreditkarte im Internet als gestohlen aufscheint – man brauche nur deren Nummer einzugeben. Eine andere „Masche“ ist es, eine Website zum Bezug von Nachrichten oder Leistungen perfekt nachzuahmen. Wenn dann, wie verlangt, die E-Mail-Adresse und das Passwort eingegeben werden, gehen diese Daten an eine im Adressfeld unauffällig veränderte Anschrift und werden auf die originale Website umgeleitet, so, als wäre nichts geschehen.

Eine gestohlene Kreditkartennummer wird ab 2 US-\$ aufwärts gehandelt, eine „aktuelle“ Liste von existierenden E-Mail-Adressen von 8 \$ aufwärts. Ein „Mailer“, um sechs Stunden lang Spam-E-Mails versenden zu können, kostet von 30 \$ aufwärts („Rent a Botnet“).

**Prävention.** „Die Top-100-Suchbegriffe in Google haben nichts mit Sicherheit zu tun“, weist Pichlmayr auf fehlendes Verständnis für IT-Sicherheitsfragen hin. Wichtig sei es, den Hausverstand einzuschalten, nicht allen Versprechungen zu glauben und ein gesundes Misstrauen zu entwickeln.

Das Betriebssystem sollte immer auf dem letzten Stand und ein tagesaktueller Virenschutz installiert sein. Man kann auch einem Provider eine Vor-Filterung überlassen. Wer ein Übriges tun will, arbeitet im Internet mit Open-Source-Systemen, die weniger verbreitet sind und daher weniger angegriffen werden. Regelmäßige Datensicherung sollte ebenfalls selbstverständlich sein.

Kurt Hickisch

## DÄMMERUNGS-EINBRÜCHE: SCHÜTZEN SIE SICH JETZT!



Neu und exklusiv bei uns:  
**DIAMOND 1000,**  
 die nächste Generation  
 der Alarmanlagen



GRUNDPAKET  
 AB **699,-**

- höchster Bedienungskomfort
- steuerbar über Internet
- ideal zum Nachrüsten  
 (kein Stemmen nötig)

Jetzt gratis  
 vor-Ort-Beratung  
 ausmachen!

Beratungs-Hotline: 0800 21 00 00  
 www.securityland.at

Shop Wien Nord, Sverigestraße 1b, 1220 Wien  
 Shop Wien Süd, Hubatschstraße 3, 2345 Brunn/Geb



**SECURITY  
 LAND**  
 Österreichs größtes  
 Sicherheits-Fachgeschäft



Rund 50% aller Einbrüche geschehen in Wohnungen und Einfamilienhäuser. Die Mehrzahl der Einbrecher dringt über die Fenster- und Fenstertüren in Wohnungen- und Einfamilienhäuser ein.

Unsichtbar, aber äußerst wirksam

**PROFILON SICHERHEITSFOLIE DER WIRKSAME SCHUTZ  
 NORMALES FENSTERGLAS WIRD ZUR  
 EINBRUCHSHEMMENDEN SICHERHEITVERGLASUNG**

- risikominimierend bei Blitzeinbrüchen
- durchwurfhemmend
- splitterabgangshemmend
- brandüberschlagshemmend

**Basisschutz – Aufhebelsperren**

Basisschutz für jedes Fenster ist dabei die Sicherung der Schlossseite einerseits und die Sicherung der Scharnierseite andererseits



FOL – TEC Sicherheitsfolien GmbH & Co. KG

1060 Wien, Haydngasse 4,

Tel.: 01/595 42 76, Fax: 01/595 42 76 -44, www.fol-tec.at

Unsere Firma ist Mitglied im

**KURATORIUM  
 SICHERES  
 ÖSTERREICH**