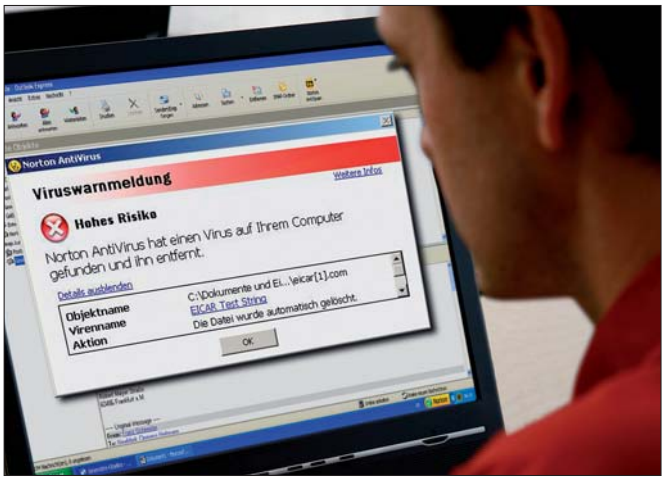
Firewall und Virenscanner sind wichtigste Schutzmaßnahmen für Computer, die mit dem Internet verbunden sind.



Schadprogramme via Internet nehmen zu: Ende Jänner 2008 war die Grenze von einer Million bereits erreicht.

Vom Opfer zum Täter

Auf der IT-Defense 2008 in Hamburg ist der unbedarfte Computer-Nutzer als Schwachstelle der Sicherheit des Internets hervorgehoben worden.

Computerkriminalität ist das am schnellsten wachsende Segment der Informationsindustrie", sagte Mikko H. Hyppönen, Chief Research Officer des finnischen IT-Security-Unternehmens *F-Secure*.

Hat es 1991 etwa 300 Schadprogramme gegeben, waren es 2004 schon 100.000, Ende Jänner 2008 war die Grenze von einer Million bereits erreicht.

„**Virenschreiber sind Leute,** die ihre Fähigkeiten im Berufsleben nicht zu Geld machen können", erläuterte Hyppönen. „Sie sitzen in den Slums von Sao Paulo, in China oder in den Nachfolgestaaten der ehemaligen Sowjetunion. Über das Internet steht ihnen die Welt offen, und Kriminelle bedienen sich ihrer."

Waren Virenschreiber zwischen 1986 und 2003 eher Leute, die das als Hobby betrieben haben, sind ihnen Kriminelle nachgefolgt, und seit 2006 rückt das Ausspionieren von Daten mehr und mehr in den Vordergrund. Mit Hilfe eingeschleuster Programme werden die Nummern von Kreditkarten in Erfahrung gebracht und in weiterer Folge sogar im Detail-Verkauf angeboten: Einer im Internet veröffentlichten Preisliste nach kostet eine deutsche Kreditkartennummer fünf Euro, eine aus den USA zwei Euro („gültig, frisch und noch nicht an andere verkauft").

Weitere Ausspähungsziele sind E-Mail-Adressen, Passwörter zu Online-Versteigerungen und zum Online-Zahlungsverkehr, zu Online-Banken, zu Aktienhändlern und zu Poker-Runden im Internet.

Im Besitz des Passwortes eines anderen, können Bankverbindungen geändert und Geldflüsse umgeleitet werden. Unter Verwendung einer fremden Kreditkartennummer können Online-Käufe getätigt werden und es kann an Poker-Runden teilgenommen werden – dies auch zum Zweck der Geldwäsche.

Mit der Drohung, die Computer durch gezielte Angriffe (DDos-Attacken) lahm zu legen, werden Unternehmen erpresst; Industriespionage wird zu einem kriminellen Erwerbszweig. Hyppönen erläuterte am Beispiel des „Storm Worms", der am 19. Jänner 2007 erstmalig aufgetreten ist, wie sich die Infektionswege verändert haben.

Mikko Hyppönen: „Virenschreiber können Fähigkeiten nicht zu Geld machen."

Adam Laurie:„RFID-Tags können geklont und umprogrammiert werden."

Internet-Nutzer werden über ausgespähte E-Mail-Adressen aufgerufen, bestimmte Websites zu besuchen, weil sie dort Love-Letters, Glückwunschkarten, Hilfe gegen Potenzstörungen oder ein Video erwartet, auf dem sie angeblich zu sehen sind.

Durch Anklicken dieser Internetadressen wird der Aufrufende unbemerkt Teil eines Netzes von fremdgesteuerten Roboter-Computern, eines BotNets, das ihn nun, ausgehend von den bei ihm gespeicherten Adressen, seinerseits nach anderen Opfern suchen lässt und gleichzeitig den Schadcode übermittelt, der beispielsweise in der Weiterleitung von Passwörtern oder Kreditkarten- und Bankkonten-

Fotos: Kurt Hickisch (2), Symantec, Alexander Tuma

INTERVIEW

Firewall und Virenscanner

Stefan Strobel, Geschäftsführer des IT-Sicherheitsunternehmens *Cirosec GmbH,* über den Schutz vor Gefahren aus dem Internet.

Vielen Internet-Usern sind die Gefahren nicht bewusst, die ihnen im „Haifischbecken“ Internet drohen. Welche Maßnahmen können Sie diesen Leuten zu ihrem und zum Schutz anderer empfehlen?

Strobel: Das Wichtigste ist sicherlich die Sensibilisierung der Anwender im Internet. Wer immer noch glaubt, dass ihn das Thema Sicherheit nichts angeht oder dass er sich keine Sorgen machen muss, da von ihm ja keiner etwas will, der wird schnell Opfer von kriminellen Subjekten. Im zweiten Schritt wird der ahnungslose Anwender dann auch noch eine Bedrohung für alle anderen, wenn sein Rechner zum Beispiel Bestandteil eines Bot-Netzes wird. Sicherheit im Internet geht wirklich jeden etwas an und die wichtigsten Schutzmaßnahmen für Privatpersonen, deren PC mit dem Internet verbunden ist, sind eine Personal Firewall und ein Virenscanner, der täglich aktualisiert wird.

Stefan Strobel: „Bei neuen Technologien wie Voice over IP oder WLANs wird häufig die Sicherheit zunächst vernachlässigt. “

Was kann getan werden, um die Verbreitung von Malware und Spam einzudämmen?

Strobel: Hier sind in erster Linie die Software-Hersteller gefragt. Die Sicherheit von Betriebssystemen wie *Windows XP* oder auch *Mac OS* hat einen entscheidenden Einfluss. Aber da auch Privatanwender, die sich selbst nicht ausreichend geschützt haben und deren PC deshalb schon unter der Kontrolle von Kriminellen steht, eine wesentliche Rolle bei der Weiterverteilung von Spam und Malware spielen, ist wirklich auch jeder Einzelne gefragt, seinen Beitrag zu leisten. PCs, die dauerhaft über DSL im Internet erreichbar sind und die nicht wenigstens durch eine Firewall geschützt sind, sollte es nicht geben.

Was kann der Einzelne tun, um seine Privatsphäre zu schützen?

Strobel: Es gibt spezielle Techniken, die für mehr Privatsphäre im Internet sorgen sollen, aber ich glaube, viele Leute müssten zunächst einmal über ihren eigenen Umgang mit ihrer Privatsphäre nachdenken. Wenn man sieht, wie viel Privates von Leuten in öffentlichen Internet-Foren oder Portalen wie *Xing* oder *Linkedin* preisgegeben wird, dann können Anonymisierungsdienste wie *Tor* auch nichts mehr retten.

Ihr Unternehmen ist auch auf dem Gebiet der Computer-Forensik tätig. Was sind die häufigsten Tatbestände, denen in Bezug auf Computerkriminalität nachgegangen wird?

Strobel: In der Praxis sind in Unternehmen vor allem Insider-Vorfälle das Thema. Angriffe durch Hacker müssen eher seltener nachverfolgt werden.

Wo sehen Sie sicherheitstechnische Schwachstellen in neuen Entwicklungen wie Voice over IP oder Videokonferenzen oder bei der Verwendung von WLANs? Was sollte bei deren Nutzung beachtet werden?

Strobel: Häufig ist es so, dass bei neuen Technologien die Sicherheit zunächst vernachlässigt wird. Voice over IP oder WLANs sind gute Beispiele dafür.

Während es bei WLANs inzwischen neuere Standards wie WPA-II gibt, die eine vernünftige Sicherheit bieten und in den heute verfügbaren Produkten auch meist implementiert sind, sieht es bei Voice over IP noch schlecht aus. Der Anwender sollte davon ausgehen, dass die Hersteller-Versprechungen zur Sicherheit ihrer VoIP-Produkte oft falsch sind.

Interview: Kurt Hickisch

nummern bestehen kann oder schlicht darin, dem Mastermind Adressen für Spam-Versand zur Verfügung zu stellen.

Während es früher ausgereicht hat, ein solches Netz dadurch zu zerstören, dass die Zentrale ermittelt und ausgeschaltet wurde, geht der „Storm Worm“ einen anderen Weg insofern, als keine Zentrale mehr besteht, sondern die einzelnen Computer untereinander („Peer-to-Peer“) vernetzt sind. Der Ausfall eines von ihnen schadet dem System nicht; im Gegenteil, dieses erkennt sogar Angriffe auf sich und schlägt mit Gegenmaßnahmen zurück.

Der unbedarfte Computernutzer, dem bei Durchsicht seiner E-Mails eine Glückwunschkarte gerade gelegen kommt, wird so vom unbewussten Opfer zum ebenso unbewussten, aber für die Sicherheit des Internets deshalb nicht minder gefährlichen Täter.

Abhilfe sieht Hyppönen in einer verbesserten internationalen Zusammenarbeit bei der Bekämpfung von Computerkriminalität und auch, dass Security im Computerbereich über den bloßen Verkauf von Software hinaus zu einer Dienstleistung umgestaltet werden muss.

Die Computer der unbedarften Benutzer als Gefahr gesehen hat auch Ryan Russell, der sich mit den der *Mac*-Welt drohenden Gefahren auseinandersetzt hat. „Jeder fürchtet sich vor Hackern, Spionen, Insiderdelikten und Diebstahl von Kundenkarten, aber Spyware macht diese Computer zu Robotern unter einer Million anderer.“

Kernel-Manipulation.
Wer den Kernel, die dem Prozessor unmittelbar überlagerte, maschinennächste

FOTO: KURT HICKISCH

Im Besitz eines Passworts können Kriminelle Bankverbindungen eines anderen ändern und Geldflüsse umleiten.

Softwareschicht und damit das Herz des Computers, in seine Gewalt bringen kann, kann beinahe unbeschränkte Macht über den Rechner ausüben. „Kernel sind zu cirka 90 Prozent in C und nur zu 10 Prozent in Assembler programmiert“, erläuterte Tobias Klein, IT-Sicherheitsberater bei *Cirosec*. „Schwachstellen, wie sie von der Programmierung üblicher Software her bekannt sind, können damit auch im Bereich des Kernel ausgenützt werden und wirken sich hier besonders fatal aus. Insbesondere lassen sich damit Sicherheitsfunktionen umgehen, die allesamt erst auf einer höheren Ebene, im Userland, greifen.“

Klein ist es gelungen, einige solcher Schwachstellen aufzuspüren. Es dauert aber Monate, bis die Schwachstelle behoben wird. „Der Trend geht dahin, bei der

IT-DEFENSE

Die IT-Defense wird seit 2003 alljährlich von der Firma *Cirosec* in Heilbronn *(www.cirosec.de)* in jeweils wechselnden Städten Deutschlands veranstaltet; die nunmehr sechste Veranstaltung hat vom 23. bis 25. Jänner 2008 in Hamburg stattgefunden.

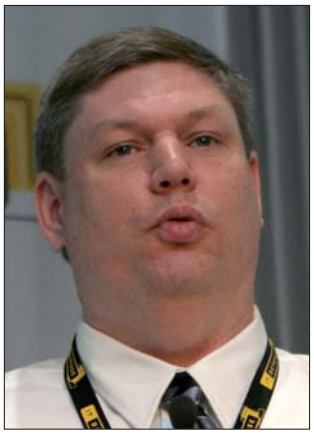
An ein zweitägiges Vortragsprogramm mit weltweit ausgesuchten Spezialisten schließt sich ein weiterer Tag an, an dem in Form von Gesprächsrunden (Round Tables) mit den Referenten Themen noch eingehender diskutiert werden können. Die mit 200 Teilnehmern limitierten Veranstaltungen sind Monate vorher ausgebucht.

Cirosec, ein Team von 20 Mitarbeitern, ist ein Beratungs- und Dienstleistungsunternehmen auf dem Gebiet der IT-Sicherheit und beschäftigt sich auch mit neu auftretenden Problemen und deren Lösung sowie mit Computer-Forensik und Sicherheitsüberprüfungen. Es werden auch Trainings und Seminare angeboten.

www.it-defense.de

FOTO: SYMANTEC

Käufliche Daten: Übersicht über Artikel, die über Untergrund-Server im Internet gehandelt werden.



Ryan Russel: „Spyware macht PCs zu Robotern."

Andy Müller-Maguhn: „Truppenübungsplatz Internet."

Programmierung von Malware Schwachstellen im Kernel auszunutzen", zeigte Klein künftige Tendenzen auf.

„Embedded Systems sind Computer, denen man es nicht ansieht", definierte Barnaby Jack, Security Researcher bei *Juniper Networks,* jene Schaltelemente und Steuerungsteile, die von der Küchenmaschine bis zum Handy und zur Spielkonsole ihre Dienste versehen, ohne dass man viel über ihre Funktion nachdenkt.

Gleichwohl sind sie Computer, die ausgelesen und umprogrammiert werden können. Dazu kommt, dass ihre Sicherheitsarchitektur durch die Massenherstellung und -verwendung derjenigen von PCs um Jahre nachhinkt. Mit dem Internet in Verbindung gebracht – das „denkende Haus" ist nicht mehr weit – können auch diese Peripheriegeräte Schwachstellen und Angriffspunkte darstellen.

RFID. Berührungslos arbeitende Erkennungssysteme (RFID-Technik) sind bereits weit verbreitet zur Warenkennung, als Zimmerschlüssel in Hotels, für Schipässe und zur Zutrittskontrolle, werden aber auch als Implantate zur Kennzeichnung von Tieren und – bislang eher ein Gag für Ferienclubs, um den Traum vom unbeschwerten Leben fernab von Ausweisen oder Clubkarten zu verwirklichen – unter die Haut platziert zur Identifikation von Menschen eingesetzt.

Die Behauptung, dass jede Identifikationsnummer eines derartigen RFID-Tags weltweit einzigartig ist, hat Adam Laurie, IT-Sicherheitsberater und Betreiber der Website *rfidiot.org,* widerlegt und dies auch demonstriert.

Mit Selbstbau-Geräten hat er nicht nur einen derartigen Chip geklont, sondern auch umprogrammiert, und den Inhalt eines Chips, wie er einer Kuh implantiert wird, auf seinen als Armband getragenen ID-Tag übertragen. Fortan hätten ihn berührungslos arbeitende Lesegeräte – die nur Daten auswerten, nicht aber auch sonstige Zusammenhänge erkennen – als Kuh ausgewiesen.

Was als unterhaltsame Demonstration gedacht war, hat einen ernsten Hintergrund, als (nur) auf dem Einsatz solcher Techniken beruhende Erkennungsmechanismen über Identitäten, von der Ware bis zum Menschen, getäuscht werden können, und dass auf alten Standards beruhende Sicherheitsmaßnahmen verbessert werden müssen.

Ähnliches gilt für das *Radio Data System (RDS),* dessen Standard 1997 festgelegt wurde und für Verkehrsdurchsagen verwendet wird. Zusammen mit dem *Traffic Message Channel (TMC)* wird eine Verbindung zu Fahrzeug-Navigationssystemen hergestellt, auf denen beispielsweise Staustrecken, Straßensperren oder überfüllte Servicestationen angezeigt werden. Zwei junge italienische Physiker, Andrea Barisani und Daniele Bianco, haben gezeigt, dass auch diese Systeme wegen fehlender oder mangelhaft ausgeprägter Sicherheitskomponenten beeinflusst werden können.

Darauf, dass nicht immer nur von der Informationstechnologie Gefahren drohen, hat der frühere Fernsehjournalist und nunmehrige Sicherheitsberater Stephan Schlentrich hingewiesen, und dass Unternehmen diesbezüglich nicht betriebsblind werden dürfen.

Es gibt auch genügend anderes Risikopotenzial in Unternehmen; die schwerwiegendsten aus einer Liste von etwa 1.400 Risiken sind etwa Produkterpressung und Produktrückrufe, Wirtschaftsspionage, Endemien, erpresserische Entführungen oder sonstige Kriminalität auf Auslandsreisen. Weltweit, hat Schlentrich ermittelt, gibt es jährlich 14.000 Entführungsfälle, von denen die meisten nicht publik werden. Auch dem privaten Auslandsreisenden empfiehlt er, sich vorzubereiten und zu informieren, nicht aufzufallen („Low Profil"), wachsam zu sein und nicht zu provozieren, Rückzugswege vorzubereiten („Wer sieht sich schon den Flucht- und Rettungsplan im Hotelzimmer an?") und Kontakt zu halten.

Die Informationssicherheit aus anderen Gesichtspunkten beleuchtet haben Annie Machon, die nach sechsjähriger Tätigkeit für den britischen Inlandsgeheimdienst als politische Aktivistin für den Schutz der Privatsphäre eintritt, und Andy Müller-Maguhn, Mitglied des Chaos Computer Clubs.

Auch wenn man nicht alle Auffassungen teilt, regt doch zum Nachdenken an, wenn Müller-Maguhn das Internet im Hinblick auf seine militärische Nutzung als Truppenübungsplatz und den Information Warfare als geradezu spottbillig im Verhältnis zu einem konventionellen Krieg bezeichnet, oder dass Trojaner auch mit marktwirtschaftlichen Mitteln verbreitet werden können, etwa im Zusammenhang mit konkurrenzlos billig angebotener Software.

Kurt Hickisch

Fotos: Kurt Hickisch (2), Symantec