Frühwarn-Systeme

Beim Security Forum 2008 des Hagenberger Kreises wurden Möglichkeiten vorgestellt, Malware-Angriffe im Internet möglichst frühzeitig zu erkennen und abzuwehren.

Malware ist ein Millionengeschäft“, sagte Andreas Lamm, Managing Director Europe von *Kaspersky Lab,* beim Security Forum 2008, das am 23. April 2008 in der Fachhochschule Hagenberg in Oberösterreich abgehalten wurde. „Bis Ende 2008 rechnen wir mit zehn Millionen Schadprogrammen. Der Spam-Anteil beim E-Mail-Verkehr liegt bereits bei 90 Prozent“, betonte Lamm. Die Entwicklung ist von „Script-Kiddies“ über Cyber-Hooligans und Berufshackern hin zu einer Underground-Economy gegangen, zu einem Wirtschaftszweig im Milliarden-Bereich.

Als neues „Geschäftsmodell“ hat sich C2C entwickelt – „Criminal to Criminal“. Sicherheitslücken werden an den Meistbietenden verkauft, Botnets werden zur Nutzung angeboten. Mit Spam lässt sich für Werbung Geld verdienen; mit Stock-Spamming werden über massenhaft verbreitete Nachrichten Aktienkurse manipuliert.

Im Online-Banking wurden im ersten Halbjahr 2007 40.000 Trojaner ermittelt; die Gesamtsumme von Trojanern im Jahr 2006 hat 12.000 betragen. Ziel dieser Trojaner ist es, Anwenderdaten von Bankkunden oder Kreditkarten auszuspähen, Passworte und PINs zu übermitteln, dem Hacker Zugriff auf die Konten zu ermöglichen. Zu Finanzdienstleistungen wird „Phishing all inclusive“ angeboten, Manipulation von Aktienkursen inbegriffen. Erpressung kann im Rahmen dieser Underground-Economy erfolgen über die

Heimanwender sind häufig Ziel von Datendieben. Mit harmlos wirkenden Downloads werden Schadprogramme in die Rechner eingeschleust, die Daten ausspionieren können.

Drohung, Verkehrssysteme oder lebenswichtige Infrastrukturen lahm zu legen.

Nach einer Studie des deutschen Bundesministeriums für Wirtschaft und Technologie (10. Faktenbericht 2007), hat der Schaden weltweit durch Malware im Jahr 2006 44,8 Milliarden Euro betragen, wobei auf Spam 39 Milliarden oder 87 Prozent entfielen, 9 Prozent auf Viren und 3 Prozent auf Trojaner. Bei Unternehmen ist auch der mittelbare Schaden durch Verlust an Reputation, an Vertrauen und in weiterer Folge durch den Verlust von Aufträgen zu bedenken – was mit ein Grund ist, dass Unternehmen mit Angaben über erlittene Schäden zurückhaltend sind und Anzeigen vermeiden. Die Kostenrechnung steht, selbst bloß Spam betreffend, erst am Anfang; eine weitere wissenschaftliche Durchdringung dieses Themas ist nötig, um rechnerische Nachweise für die Wirtschaftlichkeit des Einsatzes von Abwehrmaßnahmen zu erbringen.

Spam und Viren beeinträchtigen immer stärker das Medium E-Mail, erläuterte Dipl. Inf. (FH) Stephan Menzel aus der Sicht des E-Mail-Providers *GMX*.

Andreas Lamm: „Geschäft mit Sicherheitslücken.“

Norbert Pohlmann: „System zur Erkennung von Angriffen.“

Philipp Schaumann: „IT-Abteilung als Partner.“

Stephan Menzel: „Botnets verlangsamen den PC.“

Während Viren vielfach vom Provider abgefangen werden, nimmt die Bedeutung von Botnets wie Srizbi, Sturm, Mega-D, zu, die ihren Kunden zu Werbezwecken Versendekapazität zur Verfügung stellen. Die mittlerweile hohen Bandbreiten bei Endnutzern lassen bereits Spam mit Bildern, Audiowerbung und Videos zu.

Das Tätigwerden von Botnets lässt sich an Auslastungsprofilen erkennen, wenn sie sich nicht im üblichen Verkehr verstecken: Entweder in den Nachtstunden, wenn der allgemeine Netzverkehr nachlässt oder im Auftreten von Spitzenbelastungen. Ein Provider, der seine Kunden vor der Belastung mit Spam schützen will, steht vor dem Problem, dass zugesendete elektronische Post mitunter lediglich subjektiv als Belästigung empfunden wird.

Je „schärfer“ ein Spamfilter eingestellt ist, desto mehr steigt die Rate der unterdrückten Mails, die keine Spams sind. Am einfachsten kann eine Filterung über Blacklists erfolgen, also über IP-Adressen, die als Versender von Spam bekannt sind; damit können etwa 60 Prozent der unerbetenen Nachrichten abgeschöpft werden.

Bei Whitelists wird der umgekehrte Weg beschritten; durchgelassen wird nur, was aus einer bekannt sicheren Quelle kommt. Zwischen diesen beiden Extremen liegt beim Erkennen von Spam ein weites Feld. Beispielsweise kommt es auf das Verhalten des Rech-

FOTOS: KURT HICKISCH (4), SYMANTEC

Gefahr aus Brüssel

Vor rund einem Jahrzehnt hat uns die EU ein neues Waffenrecht beschert. Grundlage war ihre aus dem Jahr 1991 stammende „Waffenrechts-Richtlinie“. Sie mußte in österreichisches Recht umgesetzt werden und war wesentlich strenger als unser bis dahin geltendes Gesetz. Nun steht offenbar der nächste Schritt nach unten bevor. Zwar ist der formale Ablauf einigermaßen kompliziert. Der Effekt ist aber eindeutig: Dem zivilen Waffenbesitz wird der Hals ein weiteres Stück zugeschnürt.

Die EU beabsichtigt, ihre Waffenrechts-Richtlinie an die Vorgaben des UN-Protokolls anzupassen. Dazu hat die Kommission im März 2006 einen Vorschlag vorgelegt. Er betrifft bloß jene Punkte des Protokolls, die in den Anwendungsbereich der EU-Richtlinie (Ziviler Waffenerwerb und -besitz) fallen. Der Entwurf ist zur Stellungnahme ausgesandt worden. Gibt es nur mehr „genehmigungspflichtige Waffen“ (derzeit Kategorie B), dann können entsprechend restriktiv gestimmte Waffenbehörden den legalen Waffenbesitz formal einwandfrei in die Nähe von Null zurückschrauben, auch wenn sich das Gesetz einigermaßen freundlich lesen sollte. Wie das im Prinzip funktioniert, haben in der Vergangenheit manche Österreicher erfahren, die eine Erweiterung der Waffenbesitzkarte angestrebt haben, oder als Jäger einen Waffenpaß gebraucht hätten. Am Gesetzestext hat sich gegenüber früher nicht viel geändert. An seinem Vollzug schon. Wird auch das Gesetz prohibitiv, dann kann man sich vorstellen, was bei seiner übergetreuen Anwendung vom privaten Waffenbesitz übrig bleibt.

Vorstandsmitglied Heinz Krenn untersucht den Vorschlag der Kommission. Er betrifft nicht den Waffenbesitz als solchen und würde auch keine Änderung des Waffengesetzes 1996 erfordern, sondern nur Anpassungen in anderen Rechtsvorschriften, wie etwa dem Beschußgesetz oder der Gewerbeordnung. Dabei könnte aber auch einiges schief gehen. Zu den radikalen Plänen der Abgeordneten Kallenbach hat die IWÖ eine eingehende Stellungnahme erarbeitet. Sie ist auf unserer Homepage einzusehen.

In beiden Fällen ist das letzte Wort noch nicht gesprochen. Entscheidend werden die politischen Entscheidungsprozesse sein. In diese können die Staatsbürger – noch – eingreifen. Sie können die Abgeordneten zum Europäischen Parlament darauf hinweisen, daß mit einer weiteren Einschränkung des zivilen Waffenbesitzes in Europa das Los der zu Soldaten mißbrauchten Kinder in Afrika nicht besser werden wird. Die an allen Ecken und Enden der Welt stattfindenden Genocide wird es weiter geben, auch nachdem man den österreichischen Jägern, Sportschützen und Sammlern ihre Waffen weggenommen und das Laden von Patronen verboten hat. Kämpfe unter Drogenbanden werden nach wie vor unschuldige Opfer fordern, auch wenn österreichischen Bürgern nicht nur durch Behördenvertreter von bewaffneter Notwehr dringend abgeraten wird, sondern diese Möglichkeit schon von Haus aus durch ein restriktives Waffenrecht genommen ist.

Die österreichischen Waffenbesitzer haben erfolgreich den aus dem Inland kommenden Versuchen widerstanden, sie zu enteignen und zu entmündigen. Jetzt droht diese Gefahr

Campus der Fachhochschule Hagenberg.

ners des Versenders beim Aufbau des Dialogs an, wie sich der Sender authentifiziert, wie genau die Standards eingehalten werden oder wie viele Fehler beim Verbindungsaufbau erzeugt werden. Werden viele „Unknown Recipients“ erzeugt, deutet das darauf hin, dass Adressen nach Wörterbüchern generiert wurden.

Durch Vergleich mit käuflichen Adressenlisten kann erkannt werden, ob derartige Listen beim Versender eingesetzt wurden. Eine Prüfung des Inhalts kann erfolgen über statistische Textanalysen oder Ähnlichkeitsanalysen nach Checksummenverfahren.
Auch der Nutzer selbst kann mithelfen, indem er seinen Provider auf erkannte Spamquellen hinweist.

Internet-Frühwarnsystem. Prof. Dr. Norbert Pohlmann vom *Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen (www.internet-sicherheit.de)* hat mit dem Internet-Analyse-System (IAS) ein Frühwarnsystem vorgestellt, das helfen soll, Bedrohungen im Internet frühzeitig zu erkennen.

Wie Verkehrszählungen im System der Autobahnen Staus frühzeitig zu erkennen helfen, werden in den Internet-Verkehr (oder auch in das Intranet eines Unternehmens) passive Sonden eingelassen, die es ermöglichen, Angriffssituationen und Anomalien zu erkennen. Die über das Netz fließenden Nachrichten werden nur über ihren Header ausgewertet, was ohne merkliche Zeitverzögerung

HAGENBERGER KREIS

Security Forum

Der Verein „Hagenberger Kreis für digitale Sicherheit“ *(www.hagenbergerkreis.at)* wurde im März 2002 von Studenten des Fachhochschulstudiengangs „Computer- und Mediensicherheit (CMS)“ der Fachhochschule Hagenberg/Oberösterreich gegründet und hat sich zum Ziel gesetzt, das Bewusstsein für die IKT-Sicherheit in der Öffentlichkeit zu heben. Diesem Zweck dient unter anderem das seit 2003 jährlich abgehaltene Security Forum, auf dem namhafte Experten zu Fragen der Informationssicherheit referieren.

Die Folien und Unterlagen vom Security Forum 2008 stehen unter *www.securityforum.at/unterlagen.php* zum Download bereit.

www.securityforum.at

FOTO: KURT HICKISCH

erfolgen kann, wenig Speicherplatz erfordert und datenschutzrechtlich unbedenklich ist. Die auf diese Art gewonnenen Daten werden mit Durchschnittswerten verglichen. Wird beispielsweise ein signifikantes Ansteigen von E-Mails mit Attachments registriert, kann eine Wurm-Attacke gestartet worden sein, der mit einer Warnung begegnet werden kann, Anhänge von E-Mails vorerst nicht zu öffnen, bis die Hersteller von Anti-Viren-Programmen Abwehrmaßnahmen zur Verfügung stellen. Mit aktiven Sonden („Drohnen“) kann andererseits überprüft werden, inwieweit die Verfügbarkeit im Netz gegeben ist.

Unerwünschte Post: Der Spam-Anteil beim E-Mail-Verkehr liegt bereits bei 90 Prozent.

Security-Policy. Mit der hinter Benutzerregeln steckenden Psychologie hat sich Dipl. Phys. Philipp Schaumann, Berater für Informationssicherheit, in seinem Referat beschäftigt. Für die Sicherheit macht der Mensch etwas, wenn er sich bedroht fühlt. Eine relative Unsicherheit wird akzeptiert; oft geht Bequemlichkeit vor Sicherheit.

Gefahren für die Informationssicherheit bedrohen meist nicht persönlich; das persönliche Interesse, keinen Virus in ein System einzuschleppen, ist daher eher gering. Die sachlich-verstehende Haltung gegenüber der IT-Sicherheit ist vorhanden („wichtig und notwendig“), die emotionale Haltung weicht davon allerdings ab (vgl. Studie „Entsicherung am Arbeitsplatz“; *www.known-sense.de)*. Die Arbeitswelt läuft technisch-gelangweilt ab („wie ein Roboter“). Gut durchstrukturierte Prozesse, die störungsfrei ablaufen, aber keine Kreativität verlangen, führen, so nutzbringend sie für das Unternehmen sind, zu einer sinnlichen Verarmung und erzeugen, durch die Messbarkeit der Leistung, auch Druck. Es lockt das Abenteuer, der „Blick durch das Schlüsselloch“. Wenn eine Spam-Mail das einzig Interessante im Arbeitsablauf ist, kann das zu einem „emotionalen Ausbruch“ führen; sie verbotswidrig zu öffnen, könnte Abwechslung in die Eintönigkeit bringen.

IT-Security-Maßnahmen werden als einengend erlebt, indem sie das individuelle Ausbrechen verhindern. Die IT-Abteilung wird zwar als nützlich empfunden, wenn man das Passwort vergessen hat, wird aber auch als „Exekutive des Systemzwangs“ angesehen, als „Kontrollorgan mit Allwissenheit“. Eine Gegenstrategie zu dieser Einstellung könnte in „Tagen der offenen Tür“ bestehen: Die IT-Abteilung stellt sich als Partner vor – man wendet sich dann leichter an sie. „Für die IT-Sicherheit könnte viel getan werden, wenn IT-Rechte nicht als Statussymbol angesehen würden“, betonte Schaumann. „Es ist keinesfalls nötig, vom Abteilungsleiter aufwärts alle mit Administrator-Rechten auszustatten.“ Zu viele Administrator-Rechte erleichtern die Installation zweifelhafter Software und erhöhen die Gefahr für die Rechnersysteme bedeutend.

Passworte haben eine psychologische Komponente. Mit ihnen steigt man in die Arbeitswelt ein, so, als würde man eine Arbeitsbekleidung anlegen. Mit dem Passwort kann ein Zusammengehörigkeitsgefühl verbunden sein, aber auch das Gefühl, etwas zu besitzen, das niemand anderer hat, in dessen Erstellung man einiges an Gedankenarbeit hineingesteckt hat und worin man eigene Wünsche und Vorstellungen verstecken kann. Die für die Erstellung von Passworten aufgestellten Regeln sind kalt und unpersönlich. Es dürfen keine Worte und nichts Persönliches verwendet werden, Zahlen und Sonderzeichen sollen verwendet werden. Passworte sollen ständig erneuert und dürfen nicht aufgeschrieben, aber auch nicht vergessen werden. Nach diesen strengen Regeln erstellte Passworte werden als eigene kreative Schöpfung verstanden; dem Zwang zur Änderung wird nur widerwillig nachgekommen („Jetzt soll ich mein Passwort ändern, nachdem ich es mir endlich gemerkt habe?“). Schaumann warf die Frage auf, ob der häufige Passwortwechsel, der aus früheren Mainframe-Zeiten kommt, überhaupt noch notwendig ist. Dann sollten Anleitungen entwickelt werden, Passworte so zu gestalten, dass Eigenes untergebracht werden kann, verbunden mit konkreten Anleitungen zum Codieren.

Das Erfinden von Passworten soll zum Erlebnis, zum Wettbewerb um die kreativsten Ideen werden; man merkt sie sich dann leichter und kann Identität einbringen *(vgl. www.sicherheitskultur.at/Passworte.htm)*. Problemen mit Passworten bei der Vertretung im Urlaub oder im Krankenstand sollten im Rahmen von Workshops in den einzelnen Organisationseinheiten ge-löst werden; jede Alternative (zentrale Mailbox; Mailbox für Lesen freigeben) ist besser als die Weitergabe des Passworts.

Kurt Hickisch

FOTO: SYMANTEC