Spam-Mails sind nicht nur „lästig“, sie zählen zu den größten Bedrohungen für Unternehmen im Internet.

Fachhochschule Hagenberg: Zum fünften Mal Schauplatz des „Security Forums“.

IT-Schwachstelle Mensch

Zum fünften Mal wurde in Hagenberg im Mühlviertel (Oberösterreich) das „Security Forum“ abgehalten. IT-Experten berichteten am 25. April 2007 über neue Bedrohungen.

Technik allein kann die immer komplexer werdenden IKT-Systeme nicht effizient schützen“, stellte DI Robert Gottwald, IT-Sicherheitsbeauftragter und Leiter des Fachbereichs IKT-Sicherheitsmanagement im BMI, fest. „Sicherheit beginnt im Kopf“. Den Haustorschlüssel legt man ja normalerweise auch nicht unter die Türmatte, warum also findet man Passwörter notiert unter der Tastatur? Der Schlüssel zur Haustür ist komplex gestaltet – warum aber werden triviale, leicht zu knackende Passwörter zum Betreten der Rechnerwelt verwendet? Den eigenen Wohnungsschlüssel gibt man kaum aus der Hand, und auch daran, dass andere Wohnungen versperrt sind, hat man sich in der realen Welt gewöhnt – warum sollte das in der IT-Welt anders sein? Die IT-Sicherheit wird, in absteigender Reihenfolge des Grades der Bedrohung, von Viren und Würmern, Spyware, Phishing-Attacken, Industrie-Spionage und Spam-Mails beeinträchtigt, an der Spitze aber steht der Risikofaktor Mensch. Aus Bequemlichkeit werden einfachste Passwörter verwendet, werden Passwörter zur künftigen Verwendung abgespeichert anstelle einer jeweils neuen Eingabe, werden Standardeinstellungen in Programmen beibehalten. Unzureichende Ausbildung oder unterschätztes Risiko verleiten dazu, „Trojaner“-Geschenke anzunehmen oder Sicherheitshinweise zu übergehen. „Auf Gefahren sensibilisiert sein, erzeugt Verständnis für Maßnahmen“, zeigte Gottwald die Notwendigkeit einer Bewusstseinsbildung auf; Awarenessveranstaltungen und Kommunikation des Themas IT-Sicherheit können, zusammen mit umfassenden Richtlinien, dieses Bewusstsein steigern.

Mobiles Internet. Dadurch, dass das Internet in steigendem Maß auch über Mobiltelefone zugänglich ist und Datendienste auf diesem Weg zunehmend genutzt werden, erlangen die Risiken des Netzes auch für die Benutzer dieser Geräte mehr Bedeutung, wie DI Dr. Wolfgang Schwabl von der *Mobilkom Austria AG* erläuterte. Zu den allgemeinen Regeln für das Verhalten im Internet kommt für die Betreiber von Mobiltelefonen spezifisch hinzu, dass sie niemals ihre SIM-Karte hergeben sollen (sie könnte geklont werden) und auch ihre PIN geheim halten. Wegen der Gefahr bösartiger Manipulationen sollte auch das Handy nie „hergeborgt“ werden, es sollten keine zusätzlichen Installationen durchgeführt und Bluetooth-Übertragungen ausgeschaltet werden, wenn sie nicht benötigt werden.

Hilfestellung zu Problemen der IKT-Sicherheit bietet die Organisation *ISPA (Internet Service Providers Austria)*. Die österreichweite Initiative *Saferinternet.at (www.saferinternet.at)* unterstützt Internetnutzer bei der sicheren Nutzung des Internet. Die *Computer Incident Response Coordination Austria (www.circa.at)* hat ein landesweites Frühwarnsystem für Malware aufgebaut. Stopline *(www.stopline.at)* bietet ein Meldesystem gegen Kinderpornographie und Neonazismus an.

CyberCrime. Warum es zu einem Missbrauch der Möglichkeiten des Internet kommt, erläuterte Shimon Gruper, Vicepresident von *Aladdin Knowledge Systems (www.eSafe.com)* in seinem Referat „Why are we still infected“. Die Gewinne aus Cybercrime seien mittlerweile höher geworden als jene aus dem illegalen Drogenhandel; die Rechtsdurchsetzung könne damit nicht Schritt halten. Ein „Botnet“ einzurichten, erfordert nur einen geringen finanziellen Aufwand, der im Bereich von vielleicht 150 $ liegt, wie Gruper an Hand der gängigen Marktpreise für die gestohlene Kreditkarte zum Registrieren der Domain ($ 5), frische Spamlisten ($ 10) und unentdeckte

Fotos: Symantec, Kurt Hickisch

Vortragende beim „Security Forum“: Robert Gottwald (BMI), Shimon Gruper, Ulrich Fleck, Alexander Miserka.

„Botnets“ ($ 100) und deren Miete ($ 30 für sechs Stunden), vorgerechnet hat. Der Gewinn jedoch ist, wenn angenommen 5.000 Roboter Werbe-Spam versenden und für jede Installation nur 0,40 $ gezahlt werden, mehr als hundertmal höher als der Aufwand. Und selbst wenn nur 0,01 Prozent der Empfänger von Werbemails das Angebot aufgreifen, sind das bei 100 Millionen versendeter Mails immer noch 10.000 neue Kunden. „DDOS-Attacken“ werden im Internet um 50 $ pro Tag angeboten mit dem Versprechen, damit jede gewünschte Website niederzufahren. Stellt man sein Konto für Geldwäsche zur Verfügung, wird ein prozentueller Anteil am überwiesenen Geldbetrag versprochen.

Gegenüber 2005 ist, nach der „Malware Study“ des *Aladdin Content Security Response* Teams, 2006 die Zahl von Spyware-Programmen und Trojanern um mehr als 1.300 Prozent angestiegen, als Folge dessen, dass sich die organisierte Kriminalität statt auf physischen Diebstahl auf Cybercrime verlegt hat. Eine neue Gefahr stellen die sich tief im Betriebssystem verankernden und deshalb schwer zu bekämpfenden Rootkits dar. „Im Krieg zwischen Gut und Böse wird das Gute siegen“, meint Gruper, nicht ohne hinzu zufügen: „Ich hoffe es.“

Extrusion Prevention. Wie man dem unkontrollierten Abgang von Daten („Extrusion Prevention“) begegnen kann, hat Dipl.-Inf. Med. Christian Götz von *Cirosec (www.cirosec.de)* in seinem Referat dargestellt. Daten, die, wenn sie in falsche Hände geraten, einem Unternehmen schweren wirtschaftlichen Schaden zufügen können, gibt es viele: Konstruktionspläne und Messdaten aus der Entwicklung, Rezepturen; Strategiepläne der Geschäftsführung; Daten von Kunden. Von Bedeutung sind ferner interne Verwaltungsdaten wie Dienstverträge und solche über Gehälter oder Daten, die mit der Gesundheit der Mitarbeiter in Zusammenhang stehen, wie etwa über deren Krankheiten.

„Channels“ erfassen. Um unerlaubte Datenabflüsse zu verhindern, muss man zunächst die Wege („Channels“) erfassen, über die sie nach außen dringen können, nämlich beispielsweise über Drucker, CD-Brenner, USB-Sticks, mobile Endgeräte, und die Zugänge zum Internet.

Man kann diese Ausgänge sperren und dabei Differenzierungen treffen, etwa beschränkt auf Standorte, auf bestimmte Operationen („Speichern“) oder auf Ausgabemedien („USB-Sticks“). Diese Methode ist relativ einfach, weil es nur wenige Speicherorte gibt, hat aber den Nachteil, dass die freigegebenen Channels unkontrolliert bleiben.

Bloß den Zugang zum Internet zu überwachen, ist zwar ohne Softwareinstalla-

FOTOS: KURT HICKISCH

tion auf den Endgeräten möglich, hat aber, neben der Beschränkung auf den Channel „Netzwerk“, den Nachteil, dass ein solches Verfahren bei Verschlüsselung oder Kompression der Daten „blind“ ist.

Der zweite Ansatz baut auf dem Inhalt der Dokumente auf, etwa auf bestimmten in ihnen vorkommenden Wörtern oder Mustern.

Will man die Endgeräte erfassen, muss man zunächst alle möglichen Geräte, von denen aus ein Datenabfluss möglich wäre, hard- und softwaremäßig unter einen Hut bekommen. Ferner müssen Programme („Agenten“) installiert werden, die, entweder vom Inhalt her, von den vorgenommenen Operationen oder über die Ausgänge, der festgelegten Policy entsprechend die Datenausgabe steuern. Mit einem solchen System ist auch Verschlüsselung kein Hindernis und es werden alle Ausgänge erfasst, doch darf der Agent nicht umgehbar sein oder deinstalliert werden können. Ohne ihn erfolgt keine Kontrolle!

„Extrusion“. Auch ist die Frage, was zu tun ist, wenn eine „Extrusion“ festgestellt wird. Das Mitprotokollieren der oder aller Datenbewegungen und Erzeugen eines Nutzerprofils stellt eine Form der Mitarbeiterüberwachung dar und wirft datenschutzrechtliche Probleme auf.

Zudem kann diese Methode, wegen der möglicherweise anfallenden großen Datenmengen, zu „Datenfriedhöfen“ führen. Eine Möglichkeit ist, dem Benutzer vor einer nicht gestatteten Operation einen Warnhinweis zukommen zu lassen und alle daraufhin doch gesetzten Operationen zu protokollieren, oder aber, die beabsichtigte Operation als solche zu sperren.

Die größte Schwachstelle in Bezug auf die Sicherheit von Daten und Computerzugänge ist der Mensch.

Digital Rights Management. Eine Sonderform der Extrusion Prevention stellt das Digital Rights Management (DRM) dar, um das unerlaubte Kopieren urheberrechtlich geschützter Daten (Audio- und Videodateien) zu verhindern.

Die Nutzung der mit DRM geschützten Werke ist abhängig von den Vorgaben des Erstellers der Dateien und in der Regel an eine Applikation gebunden. Als weitere Methode überprüft die „Behavior Access Control“, ob das Zugriffsverhalten eines Nutzers „normal“ ist, und zeigt auf, wenn beispielsweise von der Buchhaltung aus auf Daten der Forschung gegriffen wird. Die „Data-in-Rest-Analysis“ durchsucht Datenbestände mit einer Suchmaschine danach, wo sensible Daten liegen, die „Data-in-Motion-Analysis“ kontrolliert Datenbewegungen.

„Der Markt auf dem Gebiet der Extrusion Prevention steckt noch in den Kinderschuhen und entwickelt sich stark“, stellt Götz abschließend fest, „die entwickelten Lösungen sind erst etwa zwei bis drei Jahre alt.“

Ausfallsicherheit. Die Hochwasser-Katastrophe im August 2002 hat dazu geführt, dass in Niederösterreich das EDV-Wesen im Zuge einer Disaster Recovery Planung in Richtung Ausfallsicherheit umorganisiert wurde. Darüber haben Ulrich Fleck von *SEC Consult (www.sec-consult.com)* als projektierendem Unternehmen und Alexander Miserka vom Amt der nö. Landesregierung berichtet.

Das Amt der niederösterreichischen Landesregierung hat neben dem Landhaus in St. Pölten 175 Außenstellen, 200 Server und 6500 Benutzer; die Datenmenge beträgt 25 TB. Auf Grund der Erfahrungen bei der Hochwasserkatastrophe wurde – zusätzlich zum Rechenzentrum im Landhaus – nach einer Risikoanalyse für den neuen Standort in drei Kilometern Entfernung ein paralleles Rechenzentrum installiert. Neben einer redundanten Koppelung dieser Standorte wurden die Internet-Anbindungen und die Anbindungen zu den wichtigsten Außenstellen (21 Bezirkshauptmannschaften) redundant installiert.

Neben eingeschränkteren Tests, die in kürzeren Zeitabständen durchgeführt werden, wird einmal jährlich der Ausfall eines Standorts getestet. Ferner wurde die Informationstechnik neu organisiert, wobei sich laut Fleck die organisatorischen Änderungen und das erforderliche Loslassen von „alten“ Tätigkeiten, „die Leute mitzunehmen“ und ein Problembewusstsein zu schaffen, als die größeren Herausforderungen herausgestellt haben.

Kurt Hickisch

FOTO: EGON WEISSHEIMER

DIGITALE SICHERHEIT

Hagenberger Kreis

Der Verein „Hagenberger Kreis – Verein zur Förderung der digitalen Sicherheit“ wurde im Jahr 2002 von Studierenden des Studiengangs „Computer- und Mediensicherheit (CMS)“ der Fachhochschule Hagenberg gegründet. Ziel des Vereins ist es, das öffentliche Sicherheitsbewusstsein in Unternehmen, aber auch in privaten Haushalten zu heben. Hiezu veranstaltet der Verein unter anderem alljährlich das „Security Forum“ und gibt das „HK Magazin“ als kostenlos beziehbares Online-Newspaper heraus.

Die Unterlagen zu den einzelnen Referaten des diesjährigen Forums stehen unter *http://www.securityforum.at/unterlagen.php* zum Download bereit. Die Unterlagen zu den früheren Foren (2003 – 2006) können über die Homepage des Forums ebenfalls abgerufen werden.

www.hagenbergerkreis.at