Fotos: Jochen Schreiner

Security

„Angriffe werden professioneller"

Bedrohungsanalysen, Ratschläge für den Aufbau einer Sicherheitsarchitektur und Szenarien für die Zukunft: Das waren die Themen des Round-Tables, zu dem businessUSER die Spezialisten führender Security-Unternehmen eingeladen hatte.

Kritisierten Risiken beim Homebanking: Raimund Genes (Trend Micro, l.) und Christian Weber (Sophos)

Inwieweit spielt das Thema Sicherheit eine Rolle, wenn Unternehmen in den E-Commerce einsteigen?

Cuenin: Unternehmen sehen Security in erster Linie als Kostenpunkt, so dass dieses Thema nur eine untergeordnete Rolle spielt. Selbst wo es gesetzliche Vorschriften gibt, etwa im E-Commerce, wird nur das Nötigste getan.

Weber: Die meisten Probleme gelangen nicht in die Öffentlichkeit, sondern werden von den Verantwortlichen unter den Teppich gekehrt. Beispielsweise gibt es bei einer großen Bank in Frankfurt seit zwei Jahren ein Sicherheitsloch, das es ermöglicht, direkt auf Kundenkonten zuzugreifen.

Genes: Wenn ich mich im Internet illegal bereichern will, hacke ich doch keine Banken-Firewall, sondern ich platziere auf dem PC des Bankkunden einen Trojaner, der mir dann die PIN und die TAN des Opfers per E-Mail zuschickt. Mit diesen Daten kann ich vom Konto des Opfers Geld abheben.

Wenn wir uns die Bedrohung für die Unternehmen ansehen: Können Sie hier eine Struktur, etwa nach Branchen, erkennen?

Fuhs: Innerhalb der letzten fünf Jahre ist nur ein einziger unserer Kunden zur Staatsanwaltschaft gegangen und hat Strafanzeige gestellt. Alle anderen bevorzugten eine diskrete Lösung des Problems. Uns sind zahlreiche Fälle bekannt, in denen der Täter das Unternehmen nicht nur um viel Geld betrogen hat, sondern hinterher auch noch Schweigegeld kassiert hat. Das Bundeskriminalamt geht von rückläufigen Zahlen im Bereich der Computerkriminalität aus.
Aber 90 bis 95 Prozent der Vorfälle kommen gar nicht zur Anzeige.
Zur Branchenverteilung kann man sagen, dass jeder, der in irgendeiner Weise am Internet hängt, betroffen ist.

Dr. Harlander: Das kann ich nur bestätigen. Sie müssen heute davon ausgehen, dass alle ein bis zwei Monate gezielte Angriffe stattfinden, das heißt, es werden nicht nur die üblichen Hackertools wie Portscanner eingesetzt, sondern hier sind Profis am Werk. Besonders betroffen sind kleine, innovative und hoch technisierte Firmen. Unternehmen, die in der Öffentlichkeit stehen, werden hingegen bevorzugt Opfer von Denial-of-Service-Attacken.

„Angriffe alle zwei bis drei Monate"

Welche Tätergruppen stehen hinter diesen Angriffen?

Fuhs: Es sind im Wesentlichen drei Gruppen: Vor der ersten, den so genannten Script-Kiddies kann ich mich zuverlässig schützen. Das sind Jugendliche, die immer über dieselben Wege und mit den selben bekannten Mitteln kommen. Die probieren einfach mal was aus, haben aber nicht das Know-how, um wirklich gefährlich zu sein. Profis aus Deutschland und anderen Ländern sind hingegen sehr schwierig zu fassen, da sie ein viel größeres Repertoire an Angriffsmöglichkeiten haben. Als dritte Gruppe sind Geheimdienste wie die amerikanische NSA zu nennen. Gegen Letztere hat man natürlich keine Chance. Sie dürfen vor allem nicht vergessen, dass Wirtschaftsspionage ein sehr lohnendes Geschäft geworden ist, in dem man schon mal 20 Millionen US Dollar für drei Tage Spionagearbeit verdienen kann.

Gelöste Stimmung beim ernsten Thema (v. l.): Achim Roth (businessUSER), Howard Fuhs (Fuhs Security Consultants), Raimund Genes (Trendmicro), Christian Weber (Sophos), Dr. Michaela Harlander (Genua), Christoph Fischer (BFK)

Pohlmann: Meiner Meinung nach ist die Motivation hinter den meisten Hackerangriffen eher sportlicher Natur. Ein Unrechtsempfinden fehlt den meisten Hackern fast völlig. Aber auch in der Wirtschaft ist es üblich geworden, zur Konkurrenzanalyse in fremde Firmennetze einzudringen, um zu sehen, woran die Mitbewerber gerade arbeiten.

Wie sollten Unternehmen vorgehen, die ein Sicherheitskonzept entwickeln wollen?

Fischer: Am besten ist es, verschiedene Szenarien durchzuspielen. Dabei sollten alle sicherheitsrelevanten Bereiche gleichermaßen gesichert werden. Viele Firmen begehen den Fehler, dass sie sich auf einen sehr einseitigen Schutz, etwa ausschließlich für ihren Web-Server, verlassen, der von Profis sehr leicht zu umgehen ist.

Cuenin: Ein entscheidender Faktor ist die Time-to-Market. Ausgefeilte Konzepte zu erstellen ist zwar sehr wichtig, dauert vielen Unternehmen aber zu lange. Durch den hohen Konkurrenzdruck sind viele Firmen gezwungen, mit halbfertigen Security-Lösungen in den E-Commerce einzusteigen. Sie nehmen bewusst in Kauf, noch nachbessern zu müssen.

Karpinski Ein weiteres Problem besteht darin, dass die in einer Analyse gewonnenen Erkenntnisse nicht konsequent genug in die Tat umgesetzt werden.

Ein ganzheitlicher Schutz ist bei den wenigsten Firmen gegeben. Halbherzigkeiten finden Sie überall. Eine intensive Beratung durch Sicherheitsfirmen kann helfen, die größten Sicherheitslücken zu schließen.

Die Teilnehmer

André Cuenin: Senior Vice President Network & Webmanagement von Computer Associates, Weltmarktführer bei Unternehmenssoftware.

Christoph Fischer: Geschäftsführer der BFK edv-consulting.

Howard Fuhs: Inhaber von Fuhs Security Consultants.

Raimund Genes: General Manager von Trendmicro, spezialisiert auf Security-Technologie für Netzwerke.

Dr. Michaela Harlander: Geschäftsführerin des Firewall- und VPN-Anbieters Genua.

Jörg Karpinski: Marketing und Sales Manager von Psp Net, Distributor von Security-Lösungen.

Günther Mußtopf: Geschäftsführer des perComp-Verlages. Vetrieb von der Antiviren-Software FP-Win, F-Secure und Command AntiVirus.

Norbert Pohlmann: Vorstand Marketing von Utimaco, Hersteller von zertifizierten IT-Sicherheitslösungen.

Christian Weber: Leiter Technologie & Kommunikation bei Sophos, Spezialist von Anti-Viren- und Verschlüsselungssoftware.

Karsten Wolf, Manager E-Business & OEM Sales von Symantec, Anbieter von Internet-Security-Software.

Zeitdruck führt zu neuen Sicherheitslücken (v. l.): André Cuenin (CA), Jörg Karpinski (Psp Net), Karsten Wolf (Symantec)

Aggressoren werden professioneller, warnen Dr. Michaela Harlander (Genua, l.) und Christoph Fischer (BFK)

Glossar

Aktiver Inhalt:
Bestandteil einer Webseite, der sich zeitabhängig oder auf Grund von Benutzeraktionen verändert. So können Systeme manipuliert werden, die die Website aufgerufen haben.

ASP (Application Service Providing):
Das Vermieten von Anwendungssoftware über das Internet.
Best of Breed: System, das aus den besten Einzellösungen unterschiedlicher Hersteller besteht.

DECT (Digital European Cordless Telephone):
Standard für die Datenübertragung zwischen Basisstation und Handgerät von schnurlosen Telefonen.

DoS-Attacke (Denial of Service):
Eine Dienstverweigerungs-Attacke überschüttet einen Internet-Server derart mit Verbindungsanforderungen, dass er seine Dienste verweigert oder abstürzt.

GSM (Global Systems for Mobile Communication):
Aktueller Mobilfunkstandard in 60 Ländern.

Makros:
Programmiersprachen, mit denen vor allem in Office-Programmen Funktionen automatisiert werden. Makroviren nutzen diese Funktionen, um sich auf Dokumentdateien zu verbreiten.

NSA (National Security Agency):
Amerikanischer Geheimdienst, der systematisch E-Mail- und Faxverkehr sowie das Telefonnetz überwacht.

Polymorphe Viren:
Sie verändern bei der Übertragung ihren Code, um Antivirenprogramme zu täuschen.

Portscanner:
Programme, die im Internet nach offenen Schnittstellen von internen Netzwerken suchen, über die ein Hackerangriff erfolgen kann.

Proprietäre Software:
Speziell für ein Unternehmen entwickeltes Programm.

TAN (Transaktions-Nummer):
Einmalige Zugangsnummer beim Online-Banking.

Trojaner:
Programm, das sich unter der Vorgabe von Nützlichkeit in fremde Systeme einschleicht. Dort ermöglicht es die Fremdsteuerung des Computers, etwa zur Datenmanipulation oder -spionage.

Wie sieht die Architektur einer solchen ganzheitlichen Sicherheitslösung aus?
Pohlmann: Unternehmen wollen Abhängigkeiten vermeiden, indem sie ihre Produkte von verschiedenen Anbietern kaufen. Diese Heterogenität der verwendeten Systeme ist ein großes Problem für eine umfassende Sicherheitsarchitektur. Ein möglicher Ausweg besteht darin, Sicherheitsfeatures zunehmend in die Anwendungsprogramme zu integrieren.

Wie steht es mit der Integration der einzelnen Security-Produkte? Was ist besser: Best-of-Breed oder Lösungen aus einer Hand?
Wolf: Best-of-Breed-Lösungen sind effektiver, da niemand alles anbieten kann. Die einzelnen Hersteller haben sich spezialisiert und setzen Schwerpunkte in ihrem Angebot.
Karpinski: Standards zu erreichen, in die sich verschiedene Produkte integrieren lassen, ist sehr schwierig. Bei der Datenverschlüsselung hat es 15 Jahre gedauert, einen Standard zu entwickeln.
Viele Hersteller haben natürlich auch kein Interesse an Standards: Kunden mit proprietären Lösungen können nicht so leicht den Anbieter wechseln.

Wo sehen Sie den größten Handlungsbedarf bei den Firmen?
Cuenin: Den allermeisten Firmen fehlt eine Internet Defense Strategie (IDS). Das richtige Konzept zu finden ist dabei meist das größte Problem. Die Frage dabei ist: Was ist für die Sicherheit des Kunden am wichtigsten? Viele Entscheider in den Firmen wissen nicht, worauf es ankommt.
Genes: Es gibt eine große Nachfrage nach MP3-Filtern, damit die Mitarbeiter keine Musikdateien aus dem Internet laden können. Dateien werden jedoch zum Versand oft umbenannt, um diese Filter zu umgehen. Sie können davon ausgehen, dass 80 Prozent der Attachments, die versendet werden, für die Firmen unproduktiv sind.
Weber: Allzu oft werden ganz einfache Passwörter verwendet, wie der eigene Vorname oder „ABCD“. Generell werden Informationen viel zu leichtfertig herausgegeben. Es fehlt in vielen Firmen noch die Sensibilität für mögliche Gefahren.
Fuhs: Biometrische Verfahren, also die Identifikation über den Körper, sind wesentlich sicherer und eindeutiger als ein Passwort, das jeder verwenden kann, der es kennt. In vielen Firmen ist das Administrator-Kennwort einer

Handy und Kühlschrank bringen neue Herausforderungen, sagen Karsten Wolf (Symantec) und Norbert Pohlmann (Utimaco)

Firmen werden aktiv, wenn der Schaden passiert ist, kritisiert Günther Mußtopf (perComp, l.) mit businessUSER-Chefredakteur Peter Steinmüller

Gruppe von bis zu 20 Personen bekannt, die sich theoretisch alle als Administrator einloggen und unerkannt Systeme manipulieren könnten. Die bisherigen Entwicklungen sind jedoch noch nicht ausgereift und müssen dringend verbessert werden.

Wolf: Wir brauchen einen verlässlichen End-to-End-Schutz zwischen Homebanking-Kunden und Online-Bank. Es gibt daher bereits Vorschläge, Homebanking-Programme mit einer Firewall auszustatten, um die Sicherheit zu erhöhen.

Wenn Sie ein Szenario entwickeln müssten: Wie sehen die Bedrohungen in zwei Jahren aus?

Karpinski: Die verwendeten Systeme werden immer komplexer, so dass auch die Security immer wichtiger wird. Durch die zunehmende Abhängigkeit vom Internet wird auch das Verständnis für dieses Thema zunehmen. Unternehmen sollten rechtzeitig Ausgaben für die Sicherheit in ihre Budgets mit aufnehmen.

Wolf: Die möglichen Szenarien werden immer vielfältiger: Mit neuen Technologien kommen auch neue Probleme auf uns zu. Ich denke da nur an den Kühlschrank, der automatisch via Internet Bestellungen aufgibt.

Pohlmann: Ich sehe einige klare Trends: Die Ausgabegeräte werden immer kleiner, so dass die Bedeutung der Datenbanken zunimmt, auf denen die Daten an einem zentralen Ort bereitgehalten werden. Hier entstehen neue Gefahren. ASP gewinnt an Bedeutung. Durch die permanente Verbindung zum Server des Anbieters entstehen neue Sicherheitslöcher. Die großen Firmen wie Sun oder Microsoft werden zunehmend mehr Sicherheits-Features in ihre Systeme integrieren, um dem Kunden ein größeres Gefühl an Sicherheit zu vermitteln.

„Virus verbreitet sich in drei Stunden“

Fuhs: Auf Grund des starken Wachstums der mobilen Endgeräte müssen möglichst schnell Lösungen gefunden werden. Sollten beispielsweise makrofähige Handys entwickelt werden, hätten wir ein großes Sicherheitsproblem. Die bisher als sicher geltenden DECT-Telefone können mittlerweile entschlüsselt werden, ebenso die Datenübertragung über GSM.

Genes: Die in PDAs eingesetzten Betriebssysteme EPOC und Microsoft CE werden mit zunehmender Verbreitung dieser Geräte für Hacker interessanter. Vor kurzem sind außerdem die ersten Viren für WAP-Handys aufgetaucht. Die Reaktionszeiten der Antivirenhersteller müssen insgesamt schneller werden, da auch die Verbreitungsgeschwindigkeit der Viren rasant zunimmt. Bei „Melissa“ hat die Verbreitung der Viren 160 Stunden gedauert, bei „I love you“ nur noch fünf Stunden. In Zukunft rechne ich damit, dass sich ein Virus in nur drei Stunden weltweit ausbreitet. Als mögliche Sofortlösung sehe ich in die Programme integrierte Panikknöpfe, die eine E-Mailverbindung sofort blockieren können.

Karpinski: Die Hersteller von Mobilfunkgeräten kommen den schnellen Entwicklungszyklen im Sicherheitsbereich nicht hinterher. Die Verschlüsselung beim Mobilfunk hinkt derzeit mit gerade mal 8 Bit den technischen Möglichkeiten von 128 Bit weit hinterher.

Dr. Harlander: Angriffe im Internet werden zunehmend über aktive Inhalte erfolgen, indem man die User auf den eigenen Webserver lockt, um ihnen dann unerwünschte Dinge unterzujubeln.

Fischer: Denial-of-Service-Attacken wurden bisher nur sehr unprofessionell ausgeführt. Sollten sich Profis zu konzentrierten Angriffen zusammentun, werden die Folgen katastrophal sein.

Mußtopf: Ich sehe in eine pessimistische Zukunft und behaupte, dass für die Mehrzahl der Unternehmen das Thema Sicherheit erst relevant wird, nachdem wirklich große Schäden aufgetreten sind. Für die Erkennung und Bekämpfung neuer polymorpher Viren müssen die Sicherheitsfirmen bessere und effektivere Lösungen finden.

peter.steinmueller@businessUSER.de
achim.roth@businessUSER.de
(Moderation/Dokumentation)