Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 81 (2003)

Heft: 4

Artikel: Interview : Sicherheit ist ein Prozess

Autor: Schneider, Bruce

DOI: https://doi.org/10.5169/seals-876644

Interview

Sicherheit ist ein Prozess

Im folgenden Gespräch äussert sich Bruce Schneier über Risiken und Präventivmassnahmen in der vernetzten Unternehmenswelt. Der 38-jährige Informatiker und Physiker ist Mitbegründer der Counterpane Internet Security Inc., einem Unternehmen, das auf Sicherheitsbeobachtung spezialisiert ist. Er hat die Verschlüsselungsalgorithmen «Blowfish» und «Twofish» entwickelt und sass im Direktorium der International Association for Cryptologic Research (IACR).

Bruce Schneiers Standardwerk «Angewandte Kryptografie» wurde in den USA ein Bestseller. Er hat zahlreiche Beiträge zum Thema digitale Sicherheit verfasst und ist ein gefragter Redner. Sein jüngster Erfolgstitel heisst «Secrets & Lies – IT-Sicherheit in einer vernetzten Welt».

Herr Schneier, wie gross ist das Risiko, Opfer einer Netzattacke zu werden?
Schon jetzt sieht die Realität schlimmer aus als in den düstersten Szenarios. Jedes Unternehmen wird attackiert, immer wieder. Früher pflegte ich zu sagen: «Die Frage heisst nicht, ob Sie angegriffen werden, sondern wann.» Heute frage ich: «Wie oft sind Sie in der letzten Woche angegriffen worden, und warum wissen Sie nichts über die Eindringlinge?»

Weshalb ist es so schwierig, seine Systeme zu schützen?
Der Grund liegt darin, dass die IT-Manager mit der Bedrohung kaum Schritt halten können. Letztlich ist das ein Wettrüsten, bei dem die Angreifer alle Vorteile auf ihrer Seite haben. Schliesslich muss sich der Verteidiger gegen jeden möglichen Angriff wehren, während der Gegenseite eine einzige Schwachstelle genügt.

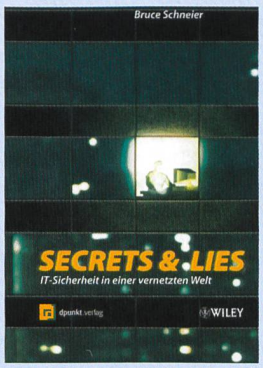
Aber es gibt doch jede Menge Experten, die sich mit Netzsicherheit beschäftigen. Genügen diese nicht?
Selbst Spezialisten können die Komplexität des Themas kaum noch überblicken, denn überall lauern neue Gefahren. Denken Sie nur an «Denial of Service»-Angriffe, die Web-Server lahm legen, oder an Sicherheitslücken in Mail-Programmen. Vor sechs Jahren wusste niemand etwas davon. Heute können sogar Laien mit Hacker-Programmen hantieren.

Wo befindet sich das schwächste Glied in der Sicherheitskette?
Es gibt Dutzende von Schwachstellen: angefangen von instabilen Betriebssystemen, ungesicherten Zugängen, fehlender Überwachungssoftware, schlecht konfigurierten Sicherheitsprodukten bis hin zu mangelndem Verantwortungsbewusstsein und menschlichem Fehlverhalten. Die Liste ist schier endlos.

Sind sich die Verantwortlichen wenigstens über die Risiken im Klaren?
Nein, sie haben keinen Schimmer. Die meisten Firmen nehmen sie auf die leichte Schulter und glauben, dass sie hinter einer Firewall unangreifbar sind. Sicherheit ist aber kein Produkt, sie ist ein Prozess. Was heute als sicher gilt, kann morgen ein Risiko darstellen.

Was halten Sie von Hochsicherheitstechnologien wie VPN, Smartcards,

Das Buch zum Thema
Secrets and Lies



In der Welt der digitalen Wirtschaft sind Informationen leichter zugänglich als je zuvor. Die vernetzte Kommunikation ist aus den Unternehmen nicht mehr wegzudenken und die Entwicklungen gerade in diesem Bereich sind rasant. In der Begeisterung für die neuen Technologien stellt kaum jemand Fragen nach Datenschutz und Datensicherheit. Erst im Mai dieses Jahres enthüllte der «Spiegel», wie unbedarft Unternehmen ihre Rechner über lokale Funkverbindungen vernetzen, ohne auf Sicherheitsvorkehrungen zu achten. Dabei gibt es sichere und einfache Systeme, sich vor unerwünschten Zugriffen zu schützen. In seinem neusten Buch «Secrets & Lies» führt der amerikanische Datenschutzexperte Bruce Schneier den Leser einmal durch das System der vernetzten Gesellschaft und zeigt ihm praxisnah, mit Spannung und Humor, die verschiedenen Facetten des Datendiebstahls; von den Ursachen der Sicherheitslücken bis zu den Motiven, die hinter den Angriffen der Hacker stehen. Er stellt die zurzeit vorhandenen Produkte und Prozesse zur Datensicherung vor, zeigt, wie sich Risiken feststellen lassen und wie man adäquate Sicherheitsmassnahmen implementieren kann. Der Autor wirft auch einen Blick auf die Entwicklungen der Zukunft und verschweigt dem Leser nicht die Grenzen der Technik. Unternehmen, die in der New Economy wettbewerbsfähig bleiben wollen, sollten nicht warten, bis findige Hacker ihre digitalen Sicherheitslücken ausspioniert haben.

Bruce Schneier, «Secrets and Lies», IT-Sicherheit in einer vernetzten Welt, Verlag Wiley VCH, 2001, geb., 408 S., Fr. 54.–, ISBN 3-527-50021-9. Das Buch kann bestellt werden über E-Mail: comtec@bams.ch oder Tel. 01 350 67 76.

Public-Key-Infrastrukturen oder Biometrie?
Sie leisten genau das, wofür sie konzipiert sind: Sie beseitigen punktuelle Probleme. Sicherheit ist aber mehr als die Summe von Einzellösungen.

Wo liegt der Ansatzpunkt für eine ganzheitliche Strategie?
Wir müssen aufhören, nach einer Wundertechnologie zu suchen, die jegliches Risiko ausschaltet. Es gibt auch keinen Rundumschutz gegen Krieg, Naturkatastrophen, Mord oder Diebstahl. Stattdessen müssen wir lernen, mit Gefahren umzugehen. Unternehmertum bedeutet immer Risikomanagement.

Also gibt es keinen absoluten Schutz?
Sicherheit ist ein relativer Begriff. Überbordende Vorsichtsmassnahmen sind nicht nur teuer, sondern behindern auch die Geschäftsabläufe. So lässt sich die Sicherheit in einer Bank erhöhen, indem man alle Kunden am Eingang kontrolliert – das würde sich aber niemand gefallen lassen. Was alle Unternehmer anstreben, ist ausreichende Sicherheit zu vertretbaren Kosten.

Worauf kommt es dabei an?
Auf drei Punkte: Es geht um die Verhinderung krimineller Handlungen, das Aufspüren von Regelverstössen und das Ergreifen von Gegenmassnahmen. Wären die vorbeugenden Mechanismen perfekt, müsste man die beiden anderen Punkte nicht beachten. Doch in allen Softwareprodukten gibt es Sicherheitslücken. Viele Firmennetze sind nachlässig konfiguriert, und Anwender machen alle möglichen Fehler.

Welchen Rat geben Sie IT-Managern?
Ich rate ihnen, die Alarmsysteme zu nutzen. Gibt es Bewegungsmelder, Kameras und Sensoren im Haus, schnappen sie jeden Einbrecher, egal wie er hereingekommen ist. Wenn sie ihr Firmennetz sorgfältig überwachen, spüren sie jeden Hacker auf, egal welche Schwachstelle er ausgenutzt hat. Und wer schnell und zielgerichtet reagiert, kann Angreifer abwehren, ehe ein Schaden entsteht. 4

Quelle: IC-World, Siemens

Wichtige Erfindung

Das Massachusetts Institute of Technology (MIT) hat wie jedes Jahr den Lemelson Invention Index für das Jahr 2003 erhoben, der über die nach Meinung der Befragten wichtigsten Erfindungen Auskunft gibt. In einer Multi-Choice-Abfrage standen zur Auswahl die Zahnbürste, das Auto, der PC, das Mobiltelefon und der Mikrowellenherd. Mehr als ein Drittel der Teenager und fast die Hälfte der Erwachsenen entschieden sich für – die Zahnbürste (erfunden im 15. Jahrhundert). An zweiter Stelle lag das Auto: bei den Jugendlichen fast gleichauf mit der Zahnbürste, bei den Erwachsenen deutlich dahinter. Fragte man die Jugendlichen, ob sie lieber ein berühmter Erfinder, ein bekannter Sportler, ein Bühnenstar oder Präsident der Vereinigten Staaten sein möchten, dann wollten die meisten jungen Männer mit weitem Abstand ein bekannter Sportler sein. Bei den Mädchen überwiegt deutlich der Bühnenstar. Erfinderin zu sein, kam fast nicht vor – dann noch lieber Präsidentin der USA.

Intelligenter Staub

Die DARA (Defense Advanced Research Agency, sie arbeitet dem Pentagon zu) hatte vor etwa fünf Jahren die Idee vom «Smart Dust»: winzige intelligente Sensoren, die sich zu einem Netzwerk ohne Hilfe von aussen organisieren können. Ursprünglich dachte man daran, solche Sensorennetze im Kampf gegen feindliche Einheiten einzusetzen. Sie sollten Informationen liefern über die Bewegungen des Gegners, ohne dass die Erkundung offenbar wurde. Heute hat man zivile Anwendungen im Auge, und der «Smart Dust» heisst nun «Motes». Das Ziel ist weiterhin ein funkgesteuertes Sensornetz, vor allem für Umweltmessung und für das Telemonitoring von Kranken, die mit Rücksicht auf anfällige Gesundheit fernüberwacht werden sollen, wenn sie sich frei bewegen. Auch im Strafvollzug für Freigänger wäre so ein Sensornetz einsetzbar. Wie die amerikanische Fachzeitschrift «EE Times» berichtet, wurden die Vorarbeiten von der Universität in Berkeley und von Intel geleistet. Einige hundert Motes sind mittlerweile bei der Crossbow Technology Inc. gebaut worden und werden derzeit vielfältig getestet. Crossbow gilt heute als einer der führenden Hersteller von digitalen und drahtlosen MEMS (Micro Electro Mechanical Systems). Die Prototypen bestehen aus anwendungsspezifischen Sensor-Arrays, die mit einer Steuerung verbunden sind. Der Aufbau ist hermetisch versiegelt, sodass Regen und Staub den Motes nichts anhaben können. Demnächst wird es dafür auch Ein-Chip-Lösungen geben, wobei dann die Motes etwa die Grösse von 1 mm^3 haben. Für die Motes wurde ein eigenes Betriebssystem geschrieben («TinyOS») und ein ebenfalls angepasstes Datenbanksystem («TinyDB»). Die Speicherkapazität der einzelnen Motes liegt bei einigen Tausend Byte. Die Grösse der zu speichernden Einzelinformationen beträgt bis zu 200 Byte. Das Geheimnis des Sensornetzes liegt in der Fähigkeit der Motes, sich selbst einen elektronischen Weg zu den benachbarten Motes zu suchen. Auf diese Weise entsteht von allein eine Hierarchie «von unten», die keine Steuerung «von oben» benötigt. Der modulare Aufbau der Motes macht die Anpassung an die jeweilige Anwendung leicht.
Homepage: www.eetimes.com/story/oeg20030128s0028

Crossbow Technology Inc.
41 Daggett Dr., San José
CA 95134
USA
Tel. +1-408-965 3300
Fax +1-408-324 4840
Homepage: www.xbow.com