Handelsblatt

Handelsblatt Nr. 046 vom 05.03.2012 Seite 52

Beilage oder Sonderseite

Datendiebe suchen neue Ziele

Internetkriminellen gelingt es immer wieder, Schutzmechanismen von Firmen zu knacken. IT-Forscher arbeiten an Software, die Angreifer noch früher erkennt.

David Meiländer Köln Die Schutzmauer hätte noch so hoch sein können - den Informationsdiebstahl bei der Firma RSA hätte sie nicht verhindert. Denn die Angreifer nutzten die Hintertür. Per E-Mail hatten sie ahnungslosen Mitarbeitern verseuchte Excel-Dateien geschickt und gelangten so ins interne Netzwerk der Sicherheitsfirma. Dort lagerte brisantes Material. Die Hacker stahlen die technischen Spezifikationen von automatischen Passwortgeneratoren, mit deren Hilfe die Systeme etlicher RSA-Kunden weltweit geschützt wurden. Millionen dieser Geräte mussten ausgetauscht werden.

Der Angriff auf RSA vor einem Jahr zeigte: Selbst eine der wichtigsten Sicherheitsfirmen kann Opfer von Datendieben werden. Auch der jüngst bekannt gewordene Passwortklau beim inzwischen zerschlagenen kanadischen Telekomausrüster Nortel, der jahrelang ausgespäht wurde, offenbart eine Schwachstelle der IT-Industrie: Die einstige Wunderwaffe, die Firewall, hat an Bedeutung verloren. "Sie allein reicht längst nicht mehr aus, um sich gegen Datendiebe zu schützen", sagt Jörn Müller-Quade, Leiter des Karlsruher Instituts für Kryptographie und Sicherheit. Der Schutz von Firmendaten werde immer schwieriger. "Die Branche vollzieht einen Paradigmenwechsel."

Bis vor wenigen Jahren hatten es Netzwerkadministratoren vergleichsweise einfach: "Angriffe kamen vorwiegend aus einer Richtung, nämlich von außen", erklärt Frank Fischer, Sicherheitsexperte des IT-Dienstleisters Accenture. Entsprechend ausgerichtet waren die Schutzmechanismen für Daten auf Firmenrechnern: "Man hat in Perimetern gedacht", meint Fischer. "Je wertvoller etwas war, desto weiter kam es nach innen." Die IT-Abteilungen schotteten so ihre Netzwerke von der Außenwelt ab.

IT-Abteilungen verlieren Kontrolle.

Eine solche virtuelle Schutzglocke wird in Zukunft immer schwerer zu verteidigen sein - auch, weil die Zeit isolierter Intranet-Systeme dem Ende entgegengeht. Zunehmend nutzen Beschäftigte private Computer und Smartphones für den Job. Ein Viertel der Firmen denkt zudem darüber nach, Rechenleistung und Speicher an externe Dienstleister auszulagern, so eine Umfrage der Deutschen Bank. "Für IT-Abteilungen bedeutet das einen enormen Kontrollverlust", sagt Frank Fischer von Accenture. Ihre sauber geordnete Sicherheitsinfrastruktur bricht auseinander und weicht einer milden Form der Anarchie. "Die Daten werden überall gespeichert und keiner hat einen genauen Überblick, wer genau darauf Zugriff hat", kritisiert Raimund Genes, technischer Leiter beim IT-Sicherheitsanbieter

Trendmicro. "Für viele Verantwortliche ist das ein Albtraum."

Unternehmen und Wissenschaft machen sich daran, das Konzept der IT-Sicherheit neu zu definieren. "In Zukunft müssen wir zunehmend kleinteiliger arbeiten", erläutert Forscher Müller-Quade. "Im Mittelpunkt wird nicht mehr nur der Schutz großer Netzwerke stehen, sondern der Schutz des gesamten Systems mit Endgeräten - bis hin zu einzelnen Dateien."

Doch das ist leichter gesagt als getan. Händeringend sucht die Branche nach Konzepten, die Sicherheit bieten und die Bedienbarkeit trotzdem nicht zu sehr einschränken. Die Entwicklung steht noch völlig am Anfang. "Es gibt sicherlich noch Spielraum nach oben", urteilt Accenture-Experte Fischer.

Deutlich wird das zum Beispiel beim Cloud-Computing. Hier werden etwa Datenbanken auf externen Servern gespeichert. "Weil die Mitarbeiter in den fremden Rechenzentren prinzipiell Zugriff darauf haben könnten, ergibt es Sinn, die Daten zu verschlüsseln", sagt Müller-Quade. "Dann ist es aber nicht mehr möglich, sie auf dem Server selbst zu verarbeiten." Eine wirtschaftlich tragfähige Lösung für das Problem gebe es noch nicht. "Hier muss man noch bereit sein, Kompromisse zu machen." Bei Smartphones und Tablets ist es ähnlich: Unternehmen verkaufen Applikationen, mit denen Beschäftigte per Fernzugriff auf den Firmenserver zugreifen können.

Smartphones bieten Angriffsfläche.

Die angezeigten Dateien bleiben im geschützten Unternehmensnetzwerk. Nur ein Abbild wird per sicherer Verbindung an das Handy gestreamt. "Die Technik gewährt den höchsten Schutz", bestätigt Jan-Frank Müller, Sicherheitsexperte beim IT-Dienstleister Computacenter. "Aber es gibt auch hier Einbußen bei der Bedienungsfreundlichkeit."

Gerade bei Mobilgeräten ist die Gefährdung hoch. Denn hier sind nicht nur gespeicherte Daten leicht abgreifbar. "Ungesicherte Laptops oder Smartphones sind ein Einfallstor für Angriffe ins Firmennetzwerk", erläutert Müller. Gerade das Google-Betriebssystem Android gilt als anfällig für Schadsoftware.

Schon arbeiten Sicherheits-Dienstleister an eigenen App-Stores, in denen sichere Programme angeboten werden sollen. "Doch völlig verhindern können wird man eine Infektion nie", glaubt Raimund Genes. "Ein Großteil der Arbeit der Sicherheitsleute wird deshalb zukünftig aus forensischer Analyse bestehen. Sie müssen lernen, Angriffe frühzeitig zu erkennen."

Auf der Cebit stellt Trendmicro dafür eine neue Anwendung vor. "Deep Discovery" überwacht das Verhalten von Computern oder Mobilgeräten, die ins Firmennetzwerk eingeloggt sind. Senden die zum Beispiel auf einmal große Datenpakete an bisher unbekannte Adressaten, schlägt die Software Alarm. So können die Administratoren die betroffenen Geräte isolieren und den Diebstahl von Firmendaten unterbinden. "Den perfekten Schutz gibt es aber auch damit nicht", warnt Genes. "Den findet man derzeit nirgendwo. Firmen, die das behaupten, sind nicht vertrauenswürdig."
Kasten: IT-SICHERHEIT
Unzufriedenheit Fast die Hälfte der Firmen und Behörden in Deutschland ist nicht zufrieden mit bestehenden Sicherheitslösungen. Laut einer Studie der Unternehmensberatung Steria Mummert hält aber nur ein Fünftel die eigenen Maßnahmen für unzureichend. Ein Viertel bezeichnet diese als überzogen.

Gefährdung Oft geschieht es unbemerkt: Fast jeden Tag werden Unternehmen aus dem Netz angegriffen. Laut einer aktuellen Studie des Sicherheitsanbieters

Fire-Eye sind es bis zu 100 Malware-Attacken pro Woche. 95 Prozent der Firmen fangen sich dabei einen Virus ein.

Meiländer, David

Quelle: Handelsblatt Nr. 046 vom 05.03.2012 Seite 52
Ressort: Beilage oder Sonderseite
Serie: Cebit (Handelsblatt-Beilage)
Dokumentnummer: 031205763