der Newsletter vom PC MAGAZIN vom 07. April 2008

Wirtschaftsspionage und Cyberwar – Trojaner Made in China

Chinesische Trojaner sitzen im Bundeskanzleramt und weit verbreitet auf einigen Festplattenmodellen von Maxtor. Doch nicht nur die Chinesen spionieren. Über das Internet werden Wirtschaftskriege ausgetragen, mit dem Ziel, geheimes Know-how zu erlangen oder Wirtschaftssysteme zu sabotieren.

von Cathrin Günzel am 31.03.2008

Eiskalte Krieger schleichen sich ins Pentagon, unsichtbare Spione lauern im Bundeskanzleramt. Die Eindringlinge brauchen keinen Nachschlüssel und keine Taschenlampen. Geräuschlos kommen sie über die Datennetze, genauso schnell verschwinden sie wieder, geheime Dokumente, Pläne und vertrauliche E-Mails im Gepäck. Ein neuer Kalter Krieg tobt unbemerkt im Internet, beteuern Geheimdienstler und Sicherheitsexperten.

"Ein Großteil der Webattacken geht von China aus"

Kenner vermuten vor allem China hinter einer aktuellen Welle von Online-Spionage, denn viele der gefunden Trojaner funken heim ins Reich der Mitte. Sogar auf in China gefertigten Maxtor-Festplatten fanden sich Hintertüren. „Internationale Spionage in Datennetzen von Behörden und Unternehmen wird sich im nächsten Jahr zu einem der größten Sicherheitsprobleme überhaupt entwickeln“, verkündet die interdisziplinäre Studie Virtual Criminology Report der Sicherheitsfirma McAfee. „Ein Großteil der Webattacken geht von China aus. Das Land gibt offiziell zu, dass seine Geheimdienste im Internet aktiv sind.“

Berichte der Financial Times verdächtigen Hacker der chinesischen Volksbefreiungsarmee, im Sommer in das Netzwerk des Pentagon eingedrungen zu sein. 1500 Computer soll das amerikanische Verteidigungsministerium aus Sicherheitsgründen vom Netz genommen haben. Bereits vor zwei Jahren sollen Eindringlinge aus dem Reich der Mitte Daten von Rechnern der US-Regierung geklaut haben. Auch das US-Militärlabor Los Alamos in New Mexico soll im Herbst 2007 Ziel von chinesischen Online-Attacken gewesen sein, ebenso das Oak Ridge National Laboratory (ORNL).

Auch deutsche, neuseeländische, britische und französische Regierungsrechner haben die Chinesen seit Jahren im Visier. Die chinesische Regierung hingegen weist alle Beschuldigungen als gegenstandslos zurück.

Falsche Schuldzuweisungen: China nur der Buhmann?

„Woher eine Attacke kommt, ob es sich um chinesische Hacker oder Trojaner handelt, lässt sich meist nicht feststellen. Auch wenn über einen chinesischen Rechner Angriffe gefahren werden, muss das gar nichts über den Verursacher sagen. Wer Illegales tut, schiebt das gern anderen in die Schuhe.“, betont auch der Karlsruher Sicherheits- und Virenexperte Christoph Fischer, Geschäftsführer des EDV-Sicherheitsunternehmens BFK edv-consulting. „Die Chinesen spionieren aggressiv, sie pflegen geradezu eine Kultur des Ausspähens und Nachmachens. Aber auf diesem Feld spielen auch viele andere mit. Nachrichtendienstliche Angriffe gegen Regierungen gehören zur Tagesordnung in der Politik.“ Der französische Vizepremier hat vor einigen Jahren schon zugegeben, dass Frankreich eine Hochschule für Industriespionage in Paris betreibt, die „Ecole de Guerre Economique“ („Schule für Wirtschaftskrieg“).

Dass China nicht als einzige Großmacht über Online-Spione verfügt, schreibt auch der Bericht von McAfee, dessen Autoren unter anderem Experten von NATO, FBI und der London School of Economics befragten: Weltweit nutzen rund 120 Länder das Internet zu Spionagezwecken und arbeiten an Strategien für Cyber-Angriffe – auch wenn ein Großteil der Webattacken von China ausgeht. Die Hacking-Operationen sind inzwischen professionell geplant und finanziert.

"Der volkswirtschaftliche Schaden ist beträchtlich"

Nicht nur Regierungen sind das Ziel von Bond 2.0, sondern Unternehmen und ihre Entwicklungsabteilungen. Der Generaldirektor des britischen Geheimdienstes MI5, Jonathan Evans, warnte Unternehmen vor chinesischen E-Spionage-Attacken und vor „hoch entwickelten technischen Angriffen". Der Kopf des MI5 hat Briefe an 300 Firmen- und Sicherheitschefs geschickt. Er vermutet aktive E-Spione gegen Großbritannien aus mindestens zwanzig Ländern. Kurze Zeit später wurden Attacken gegen Rolls-Royce und Royal Dutch Shell bekannt – angeblich wieder von chinesischen E-Spähern.

„Was wir brauchen, ist, dass bekannt gewordene Sicherheitslücken veröffentlicht werden und die Behörden die Unternehmen darauf hinweisen", fordert der Sicherheitsexperte Hartmut Pohl: „Denn der volkswirtschaftliche Schaden ist heute schon beträchtlich." Man müsse davon ausgehen, dass bundesweit mindestens 1500 Unternehmen heimlich ausspioniert wurden. „Wir müssen mit verstärkten Angriffen rechnen."