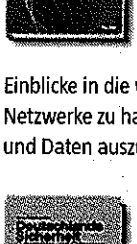
Klaren sein", sagt Pohlmann. Er sieht im Cloud-Computing aus Sicht der IT-Sicherheit auch Vorteile, weil die Daten beim professionellen Datenbankbetreiber gegen externe Angreifer häufig besser geschützt sind als im eigenen Unternehmen. Die IT-Sicherheit sieht Pohlmann unterm Strich sogar eher als Argument für als gegen die Cloud-Technik: „Sicherheit ist letztlich ein Treiber für Cloud-Computing, kein Hinderungsgrund", sagt der Experte. „Jedenfalls, solange sich die Unternehmen einen vertrauenswürdigen Anbieter aussuchen."

DENN DIE KLASSISCHE IT-Sicherheit mit Antivirensoftware, Malware-Erkennung und Firewall hat mit der Verschlüsselung der Daten nicht ausgedient. Wenn eine Schadsoftware installiert ist, die Passwörter und Zugangscodes ausspäht, können Eindringlinge damit auch die Verschlüsselung knacken. Sie ersetzt damit nicht klassische IT-Sicherheitskomponenten, sondern ergänzt sie. Allerdings ist die Zusammenarbeit der Systeme nicht immer einfach zu koordinieren. Unternehmen müssen sich etwa darauf einstellen, dass die Verschlüsselung der Daten die Überprüfung durch eine Antivirensoftware erschwert. „Die Verschlüsselung bremst die Datenhygiene aus", sagt von Faber. Und das bekannte Problem mit Computerviren und Schadsoftware wird Unternehmen auf unbestimmte Zeit weiter beschäftigen. Denn die Ursache für solche Unannehmlichkeiten sind Fehler in den Quellcodes der Programme und damit unvermeidlich. Bei umfangreicher Software und Betriebssystemen liegt die Fehlerquote im Promillebereich, macht bei einem Betriebssystem mit drei Millionen Zeilen aber immer noch eine Fülle von Mängeln. „Das können die Softwarehersteller bislang nicht verhindern, und die kriminellen Organisationen nutzen diese Schwachstellen immer professioneller aus", sagt Pohlmann. Denn die Fehler bieten Hackern Schlupflöcher, durch die sie auf fremde Rechner zugreifen können. Sind solche Einfallstore in der Szene bekannt, schreiben Hacker Programme, die auf fremde Rechner zugreifen und dort ganz unterschiedliche Sachen anstellen: heimlich E-Mails verschicken vom Account des Besitzers, Adressen klauen, Kennwörter mitschreiben. „Es gibt einen lukrativen Markt für solche Daten", sagt Pohlmann. Und viele Abnehmer, die gut für sie bezahlen. Denn die Hacker-Szene hat sich im Laufe der Zeit von ambitionierten Hobby-Cracks zu einer organisierten Kriminalität entwickelt, die vor allem eines will: Geld verdienen. Das Bundeskriminalamt beobachtet seit Jahren eine Zunahme der Internetkriminalität und gleichzeitig eine Professionalisierung der Branche. IT-Experte Pohlmann schätzt, dass jeder 25. Computer in Deutschland mit einer sogenannten Malware verseucht ist, die den Rechner fremd steuert. Und die Zahl solcher Schadprogramme wächst, laut einer

BUCHTIPPS

DER IT-SICHERHEITS-LEITFADEN Das Buch von Norbert Pohlmann und Hartmut Blumberg erscheint in diesem Jahr bereits in der dritten aktualisierten Auflage. Es liefert Unternehmen und Behörden die wichtigsten Grundlagen, um beim Schutz der IT mit laufenden Veränderungen Schritt zu halten.

NETWORK HACKING Nur wer weiß, wie sich ein Datenspeicher knacken lässt, kann auch geeignete Gegenstrategien entwickeln. Nach diesem Motto geben Peter Kraft und Andreas Weyert Einblicke in die wichtigsten Methoden um Netzwerke zu hacken, Lauschangriffe zu starten und Daten auszuspionieren.



DEUTSCHLANDS SICHERHEIT: CYBERCRIME UND CYBERWAR Autor Arne Schönbohm beschreibt, wie sich das Internet zum modernen Schlachtfeld entwickelt hat. Er skizziert, wer in Deutschland für die Cyberabwehr zuständig ist und mit welchen Maßnahmen sich der Bedrohung begegnen lässt.

gibt Fälle, in denen Hacker Computer vo
nehmen sperren oder Daten verschlüss
damit von den betroffenen Unternehm
erpressen", sagt Pohlmann. Immerhin
Deutschland die Zahl der unerwünsc
Mails. „Das Spam-Aufkommen verharrt
niedrigsten Niveau seit Jahren", sagt Hara
ma, Geschäftsführer beim Verband der d
Internetwirtschaft. Grund zur Entwarnu
der Verband allerdings nicht. Denn sobald
wehr schwächelt, kommen die Angreifer

IT-Forscher versuchen deshalb, A
programme weiter zu verbessern. Denn
haben solche Programme einen konst
Nachteil: Sie funktionieren rein reaktiv. E
bei mehreren Nutzern ein bestimmter An
bekannt wird, können die Anbieter dar
gieren. Pohlmann schätzt, dass Antiviren
derzeit nur rund 75 bis 95 Prozent der
programme abwehrt. IT-Forscher arbeit
halb seit Jahren an neuen Systemen. Das
Trusted Computing zum Beispiel verfo
Ziel, auf einem Computer, Laptop oder
mehrere virtuelle Maschinen laufen zu las
voneinander unabhängig funktionieren.
ternetbrowser würde dann als eigener Co
im Computer funktionieren, auf dem es,
geknackt wird, für Angreifer nichts zu hol
Außerdem sollen Betriebssysteme bei jede
en Start von einer identischen Grundkon
tion aus hochfahren. Eine Virensoftware
dann jedes Mal neu installiert werden, da
überhaupt Schaden anrichten kann.
müsste die Softwarearchitektur der Rechn
dings grundlegend anders aufgebaut sein
her", sagt Pohlmann. Zum Beispiel müss
einem Rechner neben einem großen auch
re kleine Betriebssysteme laufen. Die Entw
läuft schon seit mehreren Jahren unter
gung aller großen Anbieter. „Die Motivati
Koordinierung der monopolistischen He
ist allerdings nicht ganz einfach, deshalb
sich diese modernen Sicherheitssysteme
nicht etabliert." Auch bei Firewalls beob
Experten Fortschritte: „Der Schutz an der
nehmensgrenze wird immer intelligenter
von Faber. So würden die Filter immer bess
stehen, was der Nutzer gerade verschickt od
für ein Dienst aus dem Internet gerade Dat
dem Firmencomputer austauschen will.

DIE WAFFEN DER CYBERANGREIFER

SCHADSOFTWARE Experten entdecken immer mehr unterschiedliche Schadprogramme. Allerdings werden die Programme nicht mehr wie früher wahllos über das Internet gestreut, sondern meist gezielt verteilt.

Bedrohung aus dem Internet
Gefährdungstrends

	2009	2011	Pr
DDoS-Angriffe	↑	→	
Spam-E-Mails	↑	→	