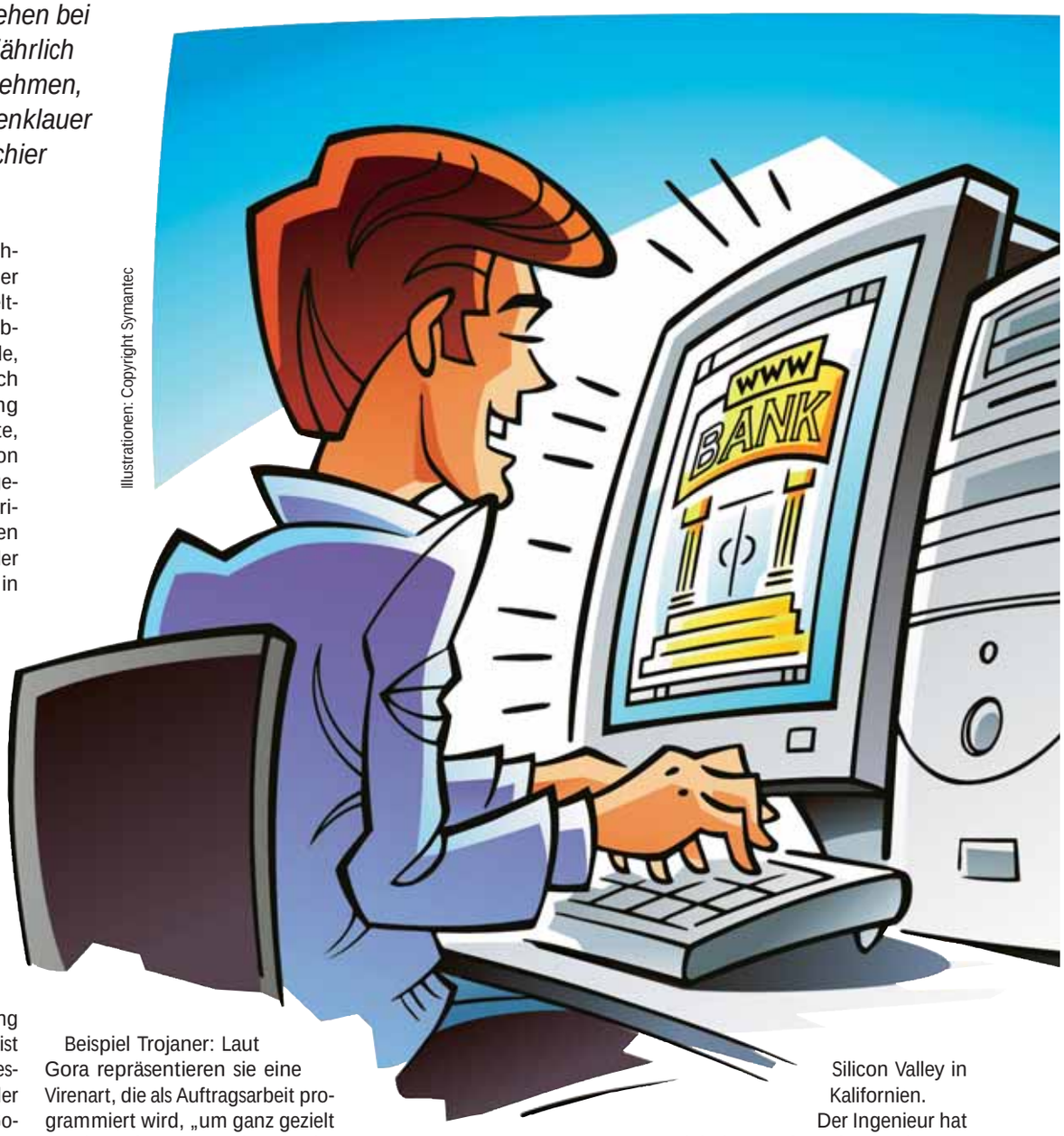
IT-Sicherheit Keine Angst vor

Schäden durch Hacker gehen bei der deutschen Industrie jährlich in die Milliarden. Unternehmen, Security-Firmen und Datenklauer befinden sich in einem schier unendlichen Kleinkrieg.



Illustrationen: Copyright Symantec

Vor etwa einem Jahr brachten die Computerwürmer „Sasser“ und „Netsky“ weltweit tausende von PCs zum Absturz. Der Autor der Störenfriede, ein 19-jähriger Hacker, der sich auf diesem Wege Anerkennung in der Szene verschaffen wollte, verursachte Schäden in Höhe von mehreren Millionen Euro. Insgesamt, so schätzt das Bundeskriminalamt in Wiesbaden, gehen die Schäden durch Hacker in der deutschen Industrie jedes Jahr in die Milliarden.

Gerade für mittelständische Unternehmen können die Folgen von Hacker-Angriffen gravierende Folgen haben. Ihr Problem ist jedoch ein anderes. Was aktuell wirklich „brennt“ ist, dass die so genannten Hacker nicht mehr zum Spaß oder einer vermeintlichen Anerkennung wegen agieren. „Inzwischen stehen ganz klare kommerzielle Interessen im Vordergrund“, bringt es Stefan Gora, Sicherheitsberater bei der Karlsruher Firma Secorvo Security Consulting GmbH, auf den Punkt. Wichtig ist für ihn nicht, wie die jeweils neueste Virenversion gerade mal wieder heißt, deutlich relevanter ist für Gora, „was die neueste Version tut“.

Christoph Fischer ist seit mehr als zehn Jahren Computer-Hackern auf der Spur.

Beispiel Trojaner: Laut Gora repräsentieren sie eine Virenart, die als Auftragsarbeit programmiert wird, „um ganz gezielt Wettbewerber auszuspähen“. Oder aber die Tatsache, dass hunderttausende von Endsystemen ahnungsloser Benutzer zu Bot-Netzwerken kombiniert werden, welche für Erpressungszwecke (Denial of Service) oder zur Spamverbreitung gemietet werden können.

Das hält eine ganze Branche auf Trab. Darunter auch Christoph Fischer, der schon seit Anfang der 90-er Jahre Computer-Hackern auf der Spur ist. „Cyber-Sheriff“ nennen seine Kunden den mittlerweile 45-Jährigen, der sich seine Nächte vor einer Vielzahl von Überwachungsmonitoren um die Ohren schlägt. Seine Firma, die BFK edv-Consulting GmbH in Karlsruhe, bietet Unterstützung bei Notfällen wie Hacking, Industriespionage oder Sabotage. Fischer ist in Moskau genauso gefragt wie in Peking oder im Silicon Valley in Kalifornien.

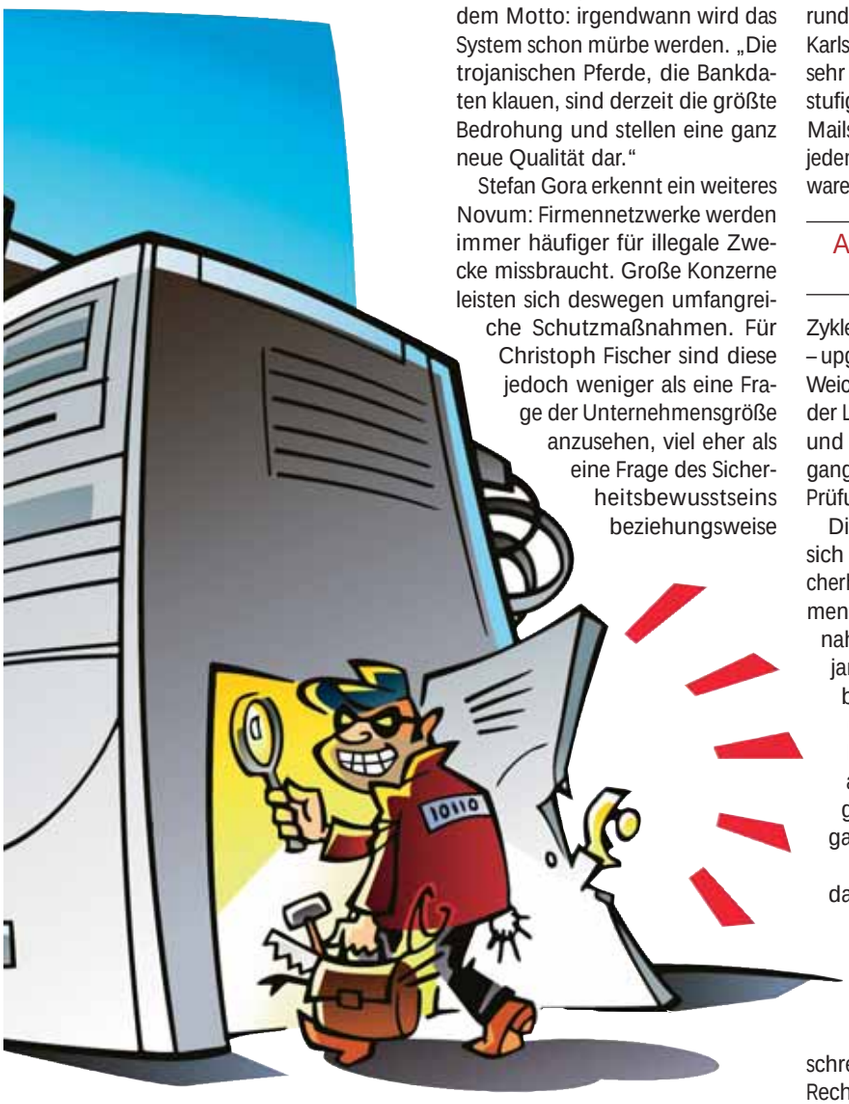
Der Ingenieur hat dabei trotz der mitunter langen Nächte durchaus Sinn für Humor – und für Symbolik: Mitten im

Mischung aus Kriminalistik, Puzzle und High-Tech

Überwachungsraum steht ein rotes Telefon, das dann klingelt, wenn einer seiner Kunden Hilfe braucht. Nicht weit von der Kaffeemaschine entfernt befindet sich eine olivgrüne

Foto: BFK edv-Consulting

Datenklau



Metallkiste, die an ein militärisches Waffenarsenal erinnert. Christoph Fischer nennt die wuchtige Kiste „Portable Nuclear Device“ – tragbare Nuklearausrüstung. „Mein Job ist eine Mischung aus Kriminalistik, Puzzle-Spiel und High-Tech.“

Derzeit befasst sich der Viren-Experte stark mit Sicherheitslücken bei Online-Banking-Systemen. Die Kombinationen von PINs und TANs, wie es jeder Privatnutzer kennt, sind für Hacker nur schwer durchdringbar. Folglich werden sie von Eindringlingen „regelrecht beschossen“, weiß Fischer. Nach dem Motto: irgendwann wird das System schon mürbe werden. „Die trojanischen Pferde, die Bankdaten klauen, sind derzeit die größte Bedrohung und stellen eine ganz neue Qualität dar.“

Stefan Gora erkennt ein weiteres Novum: Firmennetzwerke werden immer häufiger für illegale Zwecke missbraucht. Große Konzerne leisten sich deswegen umfangreiche Schutzmaßnahmen. Für Christoph Fischer sind diese jedoch weniger als eine Frage der Unternehmensgröße anzusehen, viel eher als eine Frage des Sicherheitsbewusstseins beziehungsweise der Kommunikationskultur. Unternehmen mit vielen Außendienstmitarbeitern etwa, deren Laptop oft außerhalb der Reichweite der EDV-Abteilung liegen, stellen Fischer zufolge ein besonderes Risikopotenzial dar.

Mit der Post kommt die Gefahr ins Haus

In den Unternehmen selbst sind vor allem die Posteingänge der E-Mail-Server relevante Sicherheitslücken. Die L-Bank, Förderbank des Landes Baden-Württemberg mit rund 900 Mitarbeitern am Hauptsitz Karlsruhe, geht mit diesem Thema sehr sensibel um. „Über ein mehrstufiges Antivirenkonzept auf dem Mailserver, den Fileservern und auf jedem Client wird eine Antivirensoftware gefahren, die in äußerst kurzen Zyklen – bei Bedarf alle 20 Minuten – upgedatet wird“, beschreibt Dieter Weick, zuständig für den IT-Bereich der L-Bank, den Umgang mit Mail- und Fileservern. „Jeder Schreibvorgang im Haus löst automatisch eine Prüfung auf Viren aus.“

Anscheinend gefährlich? Eintritt verwehrt!

Die Universität Karlsruhe hat für sich selbst ein ausgeklügeltes Sicherheitssystem entwickelt. Ankommende E-Mails werden vor der Annahme zum einen auf Viren, Trojaner und sonstige Schädlinge – beispielsweise Phishing-Angriffe, das Ausspionieren von Passwörtern – untersucht. Zum anderen werden als besonders gefährlich bekannte Anhänge gar nicht erst zugelassen.

Dies geschieht in der Form, dass eine solche Nachricht am Eingang erst gar nicht angenommen wird („Reject-Methode“), worüber der zuständige Provider automatisch informiert wird, beschreibt Hannes Hartenstein vom Rechenzentrum der Universität.

Ähnlich geht auch die Karlsruher Industrie- und Handelskammer vor. „Das System wird geschützt durch zwei Firewalls“, beschreibt IHK-Sprecherin Claudia Nehm. Derzeit installiert die Kammer einen Spamfilter, den der User allerdings selbst trainieren muss.

Bei allen Vorsichtsmaßnahmen warnt Sicherheitsexperte Stefan Gora von Secorvo Security aber vor Hysterie: Trotz Virenschutz und Vorsichtsmaßnahmen fallen den Angreifern immer neue Wege ein, in Systeme einzudringen. Auch Profis sind laut Gora davor nicht gefeit. **Stefan Jehle**

Sicherheits-Tipps

Hinweise über aktuell grassierende Viren und Sicherheitsstandards gibt es beim Bundesamt für Sicherheit in der Informationstechnik (BSI) im Internet: www.bsi.bund.de; www.bsi-fuer-buerger.de
Dort gibt es zudem Tipps zu Standardsicherheitsmaßnahmen wie Firewalls, Virenschutz, „gute“ Kennwörter etc. Auf dieser Philosophie basiert auch das IT-Grundschutzhandbuch des BSI. Eine abgespeckte Version insbesondere für den Mittelstand wurde 2004 als „Leitfaden IT-Sicherheit“ veröffentlicht. Die Broschüre umfasst 50 Seiten und liegt zum Download bereit unter: www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf

Viren-Top-Ten: *Listen zu den aktuell gefährlichsten Viren gibt es auch unter: www.sophos.de/virusinfo/*

Schadensschätzung: *Über Schäden bei mittelständischen Unternehmen geben aktuell IT-Security-Studien Auskunft, etwa die Untersuchung der silicon.de GmbH. Internetlink: www.silicon.de/cpo/studien/*

Grundsätzliches: *Christoph Fischer von der BFK Consulting: „Es gibt ein klassisches Portfolio an Protect-Detect-React-Maßnahmen und Werkzeugen, die firmenabhängig angepasst werden müssen.“*
Stefan Gora von der Firma Secorvo: „Sicherlich gibt es Standardsicherheitsmaßnahmen, wie eben Firewalls, Virenschutz, „gute“ Kennwörter etc. Allerdings reichen technische Maßnahmen ohne Unterstützung des Management nichts aus.“ **sj**