Privatanwender sind häufig Ziel von Bedrohungen aus dem Internet. Sie müssen selbst für ihre Sicherheit sorgen.

Strategien gegen Cyber-Crime

Angriffe auf IT-Systeme erfolgen von Tätern mit erheblichem Aufwand und großem Know-how. Neue Strategien und Technologien sind erforderlich, um Angriffe abzuwehren und die Systeme sicherer zu machen.

Der Kampf gegen Bedrohungen, die für die Wirtschaft und die Gesellschaft aus dem Internet erwachsen, ist in den letzten Jahren nicht einfacher geworden. Die Täter sind heute besser gerüstet denn je, sie verfügen über großes Know-how und sind in der Lage, beträchtliche Mittel in ihre Aktivitäten zu investieren.

Der „Stuxnet"-Virus, der im Sommer 2010 gegen industrielle Steuerungsanlagen gerichtet war, stellte das eindrucksvoll unter Beweis: Es dauerte Monate, bis Experten die Wirkungsweise dieses Virus herausgefunden hatten, und bis heute sind die Urheber unbekannt. Die herkömmliche Art erscheint problematisch, mit der Behörden, Unternehmen und Betroffene auf die Bedrohung reagieren. Bisher wurde abgewartet, bis die nächste Hacker-Attacke kam, und mit Warnungen und speziellen Tools vorgegangen. Es sollten aber strategische Antworten gefunden werden, die sich nicht mit der Lösung von Einzelfällen begnügen.

Netz- und Informationssicherheit. Die EU-Kommission verabschiedete Mitte 2010 „Vorschläge für Maßnahmen, die eine Politik zur Stärkung der Netz- und Informationssicherheit auf hohem Niveau zum Ziel haben". Die wichtigsten Punkte dabei sind:

- Schaffung eines Netzes von Computer-Notfallteams *(Computer Emergency Response Teams – CERT)* bis 2012
- Errichtung eines EU-Zentrums für Cyber-Kriminalität bis 2013
- Aufbau eines *Europäischen Informations- und Warnsystems (EISAS)* bis 2013.

Auf diese Weise wird ein institutioneller Rahmen für ein länderübergreifendes Vorgehen gegen Cyber-Kriminalität geschaffen. International operierende Banden entziehen sich einer nationalen Strafverfolgung, weil sie – beispielsweise bei der Abschöpfung von Gewinnen – die Schnittstelle zwischen virtueller und realer Welt in Länder verlegen, in denen sie vor einem Zugriff der Behörden sicher sein können. Regelungen auf EU-Ebene werden nicht ausreichen, da die Cyber-Sphäre nicht an den EU-Außengrenzen endet. Doch ohne Verankerung in der EU können die weiteren Schritte nicht erfolgen.

Cyber-Security-Assessment. Da Behörden weder im nationalen noch internationalen Rahmen Cyber-Crime in absehbarer Zeit mit juristischen oder polizeilichen Mitteln verhindern können, müssen Unternehmen und Privatpersonen selbst für ihre Sicherheit sorgen. Diese Verpflichtung ist derzeit umso ernster zu nehmen als Internet-Anwen-

FOTO: EGON WEISSHEIMER

der, die sich nicht ausreichend schützen, nicht nur sich selbst gefährden, sondern auch alle, die mit ihnen in Verbindung treten. In den letzten Jahren wurden eine Reihe von Regeln erlassen, etwa der *Sarbanes-Oxley-Act* oder der *PCI/DSS-Standard* für die Verarbeitung von Kreditkartendaten, die Normen für den sicheren Umgang mit Daten enthalten. Unternehmen können die Erfüllung solcher Vorschriften durch Zertifizierungen nachweisen.

Diesen wird künftig eine wichtige Rolle zukommen. Auch wenn es für Unternehmen nicht immer einfach sein mag, den komplexen Regelwerken zu entsprechen, wird auf Dauer daran kein Weg vorbeiführen, was auch in ihrem Interesse liegt. Unabhängig von Regeln und Zertifizierungen wird immer ein umfassendes Cyber-Security-Assessment notwendig sein, um festzustellen, wo Unternehmen angreifbar sind und wie Schwachstellen beseitigt werden können. Dabei sollte in allen Unternehmen und Behörden ein verantwortlicher Beauftragter für Cyber-Sicherheit etabliert werden.

Viren und Würmer verbreiten sich im Internet immer schneller. In wenigen Stunden können sie weltweit großen Schaden anrichten.

Die herkömmlichen Tools zum Schutz vor Malware sind auf absehbare Zeit unverzichtbar, aber nicht ausreichend. Die Unternehmen und Behörden verfügen nicht über das zur Abwehr nötige Know-how. Der Kampf gegen Risiken wie SQL-Injection-Attacs, gegen automatisierte Malware, gegen die Verwendung von SSL-Verbindungen oder der Einsatz von „Scareware“, also von irreführenden Warnhinweisen, setzt Know-how, Erfahrung und ständige Befassung mit dem Thema voraus. Das können nur IT-Sicherheitsspezialisten leisten, die sich ständig mit Cyber-Security beschäftigen. Kleinere Organisationseinheiten werden sich externes Know-how ins Haus holen und mit versierten Dienstleistern kooperieren müssen.

Neue Technologien. Als Strategie können auch diese Ansätze auf Dauer nicht zufrieden stellen, denn sie stellen immer noch Reaktionen auf Gefährdungen dar. Folglich müssen alle, die für Cyber-Security verantwortlich sind, auch die IT-Hardware- und Software-Hersteller, den Anwendern mit neuen Technologien bei Seite stehen. Dazu zählen:

- Integration von (zertifizierten) Sicherheits-Features in die Hardware und in die Applikationen; beispielsweise Verschlüsselung oder biometrische Verfahren zur Identifizierung von Nutzern;
- spezielle Betriebssysteme und Datenbanken für sicherheitskritische Aufgaben.

Der Einsatz neuer Technologien zum Aufbau „gehärteter IT-Systeme“ stellt einen zusätzlichen Aufwand dar. Cyber Security ist ein nicht unerheblicher Kostenfaktor, so dass für manchen IT-Verantwortlichen die Versuchung naheliegen mag, ein hohes Risiko in Kauf zu nehmen. Damit würden sie aber nicht nur sich, ihre Mitarbeiter und Geschäftspartner gefährden, sondern auch die gesamte IT- und Internet-Welt, zum Beispiel, indem die eigenen Rechner für Bot-Netze gekapert werden. Hier ist wieder die Compliance gefragt, und es gilt Cyber-Security-Standards auch auf technischer Ebene zu regeln. Ein Thema, bei dem die IT die Versicherungswirtschaft ins Boot holen sollte.

Auch im Rahmen bestehender Technologien lassen sich technische Lösungen finden. So bietet Cloud-Computing für Unternehmensdaten Möglichkeiten zur Risikobegrenzung, denn Unternehmen können kritische Daten zu einem Provider auslagern oder sie von einem Software-as-a-Service-Anbieter verarbeiten und pflegen lassen. Solche Spezialanbieter können mehr Sicherheits-Know-how einbringen als eine IT-Abteilung, die daneben eine Vielzahl anderer Aufgaben zu bewältigen hat. Voraussetzung ist, dass die Rahmenbedingungen stimmen, beispielsweise der Verbleib personenbezogener Daten in Einklang mit den Gesetzen geregelt ist. Zertifizierungs-Modelle sind denkbar. Die offenen Fragen sollten die Cloud-Anbieter zügig klären.

Für Hoch-Sicherheitsaufgaben, beispielsweise bei Regierungen, im militärischen Bereich und bei Infrastruktur-Unternehmen wie Kraftwerken oder Krankenhäusern, wird der Weg zu mehr Sicherheit nicht an der kostenintensivsten Lösung vorbeiführen. Getrennte Netze werden aufgebaut werden müssen.

In Deutschland wurde dies für Bundesbehörden beispielsweise mit dem Informationsverbund Berlin-Bonn (IVBB) realisiert. Bisher ist es Dritten nicht gelungen, in dieses Netz einzudringen, obwohl auch auf den IVBB ständig Angriffe unternommen werden.

Energieversorger steuern Kraftwerke und Umspannstationen in Deutschland nicht über das öffentliche Netz – im Unterschied etwa zu den USA, wo neuerdings auch über die Sicherheit dieser Anlagen vor Cyber-Angriffen diskutiert wird. *Bernhard Otupal*

FOTO: SYMANTEC