Viren, Hacker und Lauschangriffe – IT-Strukturen sind zunehmenden Gefahren ausgesetzt

Loveletter, Nimda, Code Red oder WTC – fast täglich tauchten in den vergangenen Monaten neue Computerviren, unbekannte „Trojanische Pferde“ oder E-Mail-Würmer auf. Hinzu kommen als weitere Gefahr Lauschangriffe, mit Hilfe derer sensible Informationen ausspioniert werden. Diese Palette von Bedrohungen können Unternehmen in ihrer Existenz gefährden.

„Je tiefer E-Technologien in Unternehmensabläufe eindringen, desto größere Bedeutung gewinnt das Thema Sicherheit“, ist Michael Adler, Leiter Practice Management bei Siemens Business Services in München, überzeugt. Denn Unternehmen seien durch die wachsende Anzahl von äußeren Angriffen in zunehmendem Maße gefährdet. Allein für das Jahr 2000 schätzt die Hamburger Unternehmensberatung Mummert + Partner die Schäden durch Viren und Würmer auf weltweit mehr als 17 Milliarden Dollar. „Viele Betriebe sind für diese Angriffe nicht ausreichend gewappnet“, warnt Michael Dickopf, Sprecher des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in Bonn. Deutsche Firmen und Behörden seien in der Vergangenheit nur deswegen meist recht glimpflich davongekommen, weil die Epidemien ihren Anfang in der Regel in Übersee nehmen und so wegen der Zeitverschiebung eine gewisse Vorwarnzeit für Europa existiert. Über 12.000 neue Schädlinge wurden im Jahr 2001 identifiziert. Im Vergleich zum Vorjahr – so die Studie „2001 Information Security Industry Survey" des amerikanischen Information Security Magazins – hat sich im vergangenen Jahr die Anzahl von Angriffen auf Webserver nahezu verdoppelt. Mehr als die Hälfte der befragten Firmen war davon betroffen. Ein reibungsloser Betrieb ist oft erst nach Stunden oder sogar Tagen nach einer solchen Attacke wieder möglich. „Schon kurzfristige Ausfälle können katastrophale Folgen haben“, betont Michael Adler.

Hacker hoch gefährlich

Neben der Bedrohung durch Viren werden Unternehmen zunehmend Zielscheibe der noch gefährlicheren Hacker. Denn diese bemühen sich aktiv, in ein Computersystem einzubrechen und dieses zu schädigen, wofür sie inzwischen viele Werkzeuge zur Verfügung haben. Die einfachsten sind Probes und Scanner, welche die angebotenen Dienste eines Systems prüfen und ein Profil daraus erstellen. Auf diese Weise lassen sich Schwachpunkte finden, an denen die Hacker in einen Computer eindringen und dort die Kontrolle übernehmen können. So besteht zum Beispiel die Möglichkeit, so genannte „Trojanische Pferde“ einzuschleusen. Dabei handelt es sich um Computer-Programme, die sich auf Rechnersystemen einnisten und dem Hacker den Zugriff auf sämtliche Dateien verschaffen oder gar die Kontrolle über den Computer oder über das gesamte Netz ermöglichen. Oft setzen die Angreifer auch Viren als Hilfsmittel ein. Der „QAZ-Wurm“ ist ein gutes Beispiel für die verschwimmende Grenze zwischen Viren und Hackern. Dieser Schädling fand ein großes Medien-Echo, weil er wichtige Firmengeheimnisse des von ihm angegriffenen Unternehmens offen legte. Er wurde im Sommer 2000 entdeckt und verbreitete sich durch Netzwerkverbindungen, wobei er ein „Backdoor“-Programm installierte, mit dem Passworte vom Rechner eines Opfers gestohlen werden konnten.

Schlecht gewartete Rechner und unvorsichtige Mitarbeiter tun ihr Übriges, um den Fortbestand der digitalen Schädlinge zu sichern. Harmlosere Viren und Würmer produzieren bloß unanständige Meldungen auf dem Monitor, andere spionieren sensible Informationen aus, wieder andere verursachen – bisweilen nach monatelanger Ruhephase – schlimme Verwüstungen und Datenverluste. „Die Ausfallzeiten und Datenverluste durch Viren und Hacker haben dabei weitreichende Folgen“, weiß der Leiter des Practice Managements Michael Adler. „Sie können neben den Aktienkursen beispielsweise auch die Finanzen oder die Produktivität eines Unternehmens beeinflussen oder äußerst negative Auswirkungen auf die Loyalität von Kunden haben.“ Nicht zu unterschätzen sei auch der generelle Imageverlust. Adler: „Zur Wiederherstellung eines positiven Images ist in manchen Fällen die Hälfte des Marketingbudgets eines mittelständischen Unternehmens aufzuwenden.“

„Lauschangriffe“ weiteres Problem

Teuer und geschäftsschädigend wird es auch, wenn es Unbefugten gelingt, sensible Informationen zu belauschen, auf deren Basis konkurrierende Unternehmen dann etwa günstigere Angebote beim Kunden abgeben können und so den Zuschlag für einen Auftrag erhalten. Solche Spionagetätigkeiten brachte man früher fast nur mit dem Militär in Verbindung, inzwischen sind jedoch auch zunehmend

Unternehmen von derartigen unlauteren Praktiken betroffen. Heute ist kein Unternehmen mehr vor diesen Bedrohungen gefeit. Neben Viren, Würmern und Hackern sind diese „Lauschangriffe“ zu einer besonders tückischen Bedrohung für den elektronischen Geschäftsverkehr geworden. Denn im Unterschied etwa zu einem Virus lässt sich eine Spionagetätigkeit nur indirekt und im Nachhinein ermitteln.

Vier Beispiele verdeutlichen anhand unterschiedlicher Szenarien, wie Informationen unerlaubt beschafft werden können und wie sich dieses verhindern lässt:

Szenario 1: Das „Belauschen“ des Mailverkehrs

Das Verschicken von E-Mails ist inzwischen zur Selbstverständlichkeit geworden – so mancher Geschäftsbetrieb würde zusammenbrechen, wenn es diese Form der Kommunikation nicht gäbe. Allerdings machen sich nur wenige Mitarbeiter in Unternehmen darüber Gedanken, dass E-Mails leicht auszuspionieren sind und somit firmen- oder personenbezogene Informationen, die Rückschlüsse auf Aktivitäten des Unternehmens zulassen, leicht in falsche Hände geraten können.
Eine Verschlüsselung elektronischer Daten ziehen sie gar nicht in Betracht, da sie davon ausgehen, dass dafür schon andere gesorgt haben.

E-Mails, die sich auf personen- oder projektbezogene Informationen beziehen, sollten jedoch grundsätzlich verschlüsselt werden. Für alle E-Mail-Anwendungen, die der Markt bereit stellt, gibt es Erweiterungsprogramme, die Verschlüsselungen oder oftmals auch Signaturen möglich machen.

Szenario 2: Das Eindringen in fremde Netzwerke (Hacking)

Durch die weltweite Vernetzung ist es nicht mehr notwendig, Kabel anzuzapfen oder sich in Verteilerkästen einzuklinken. Natürlich müssen Leitungswege auch weiterhin gegen Missbrauch abgesichert werden. Mittlerweile ist es jedoch nicht mehr erforderlich, einen bestimmten Ort aufzusuchen, um Zugriff auf Informationen zu erhalten. Eine Vielzahl von Internetseiten vermitteln Interessierten das notwendige Know-how, um sich den illegalen Zugriff auf Rechnersysteme zu erschleichen. Nicht zuletzt Viren und Trojaner, die per E-Mail versendet werden, unterstützen diese Hacker, da sie beispielsweise Hintertüren in den Systemen öffnen.

Es ist daher unbedingt erforderlich:
- bekannte Sicherheitslücken in den Systemen kurzfristig zu schließen,
- den Virenschutz ständig aktuell zu halten,
- den Zustand der Systeme regelmäßig zu überprüfen,
- definiert zu eskalieren, wenn es doch mal zu Problemen kommt.

Szenario 3: Das Vortäuschen einer falschen Identität

Das Belauschen des Mailverkehrs und/oder das Eindringen in fremde Netzwerke machen es neben dem Abgreifen von Daten möglich, eine falsche Person vorzutäuschen, um darüber noch einmal an sensible Daten zu gelangen.

Die einfachste Abhilfe schafft hier – wie oben bereits beschrieben – die Nutzung der persönlichen Verschlüsselung bzw. der Signatur des Mailverkehrs. Die Basis für das „who is who“ im Internet ist eine Public Key Infrastruktur. Geregelte Prozesse sorgen für die notwendige Transparenz beim Informationsaustausch.

Szenario 4: Das Stehlen physikalisch leicht zugänglicher Informationen

Nicht nur der fahrlässige Umgang mit sensiblen Daten birgt Gefahren. Ebenso leichtfertig ist es, im Bürogebäude wichtige Papiere unverschlossen herumliegen zu lassen oder vertrauliche Besprechungen in unsicheren Räumen durchzuführen.

Um das physikalische Abgreifen von Informationen zu verhindern, gilt es beispielsweise, Postfächer von Mitarbeitern unzugänglich und Besprechungsräume abhörsicher, also schalldicht zu machen. Im Einzelnen sollten Räume beim Verlassen verschlossen werden, ebenso Schränke oder Schreibtische. Vertrauliches Material darf nicht herumliegen.

Kontakt:
Siemens Business Services
Claudia Braun
Mail: claudiabraun@siemens.com
Tel.: +49-69-6682-1355
URL: http://www.sbs.de