Extremfall ist Erpressbarkeit

oder Tage lahm legen. Denial-of-Service-Attacken können eine Firma von der Aussenwelt isolieren.

Wer einem Unternehmen heute Schaden zufügen will, sei es von intern oder von extern, tut das am besten mit dem Computer. Ein paar Mausklicks und die Kundendatenbank ist bei der Konkurrenz. Dies ist möglich, weil umfassende IT-Sicherheitskonzepte in vielen Unternehmen fehlen. Gerade KMUs unterschätzen häufig die auch für sie bestehenden Gefahren und scheuen die für Informationssicherheit notwendigen Investitionen. Dies nicht zuletzt, weil ein unmittelbarer Nutzen selten ersichtlich ist. Derjenige, der in ein System eindringt, unternimmt alles, um keine Spuren zu hinterlassen. Er will sich ja seine Quelle nicht selbst abschneiden. Und der Geschädigte, wenn er es überhaupt bemerkt, wird dies nicht gross bekannt machen. Er will sich ja bei seinen Kunden nicht blamieren. Somit sind verlässliche Zahlen über angerichteten Schaden kaum erhältlich. Aber es muss einen nachdenklich stimmen, wenn jährlich geschätzte 20 bis 30 Milliarden Franken in Abhörsysteme investiert werden. Medienträchtigstes Beispiel dazu ist in letzter Zeit das so genannte ECHELON-System, welches im EU-Parlament zur intensiven Beschäftigung mit Wirtschaftsspionage führte. Diese Investitionen werden wohl nur dann getätigt, wenn damit Informationen von gleichem oder noch mehr Wert gewonnen werden können.

Schutz ist möglich

Er beginnt mit einer Risikoanalyse und anschliessendem Sicherheitskonzept für alle relevanten Geschäftsprozesse. Nebst technischen sind vor allem auch personelle und organisatorische Aspekte dabei zu berücksichtigen. Erst wenn diese Überlegungen abgeschlossen sind, beginnt die eigentliche Beschaffung und Implementation eines Sicherheitssystems sowie die Ausbildung der Benutzer. Immer komplexere Systeme ermöglichen auch immer wieder neue Attacken. Sicherheit ist deshalb kein zeitlich begrenztes Thema. Ein einmal implementiertes System muss regelmässig überprüft und gegebenenfalls an neue Bedrohungsformen angepasst werden. Wenn dies nicht erfolgt, befindet sich der Benutzer in einer trügerischen und gefährlichen Scheinsicherheit. «Knowledge is power!» Dieses Zitat von Francis Bacon hat unverminderte Gültigkeit. Gerade im Informationszeitalter. □

INFORMATIONSVORSPRUNG KANN ENTSCHEIDEND SEIN

Extremfall ist Erpressbarkeit

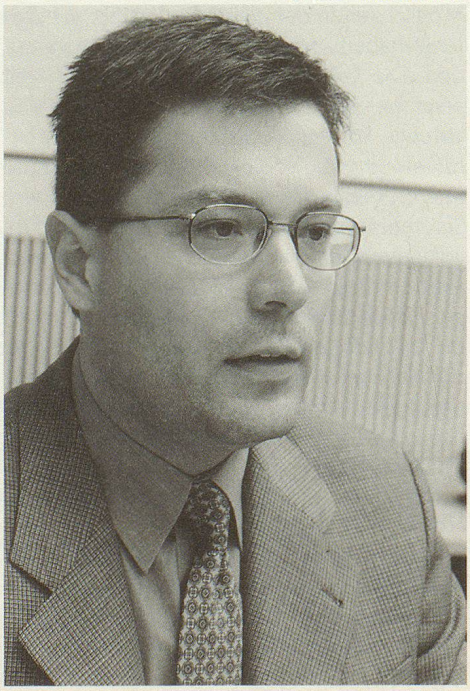
Zum Thema «Welche aktuellen Bedrohungen im Informationsbereich gibt es für Gesellschaft, Wirtschaft und Armee?» sprach an der Medienorientierung Riccardo Sibilia von der ETH Zürich.

In Militäroperationen erleben UAV (Unmanned Aerial Vehicles) eine wachsende Bedeutung. Neben den Aufgaben der Bildaufklärung, Zielbeleuchtung, Radar- und Signalaufklärung werden sie vermehrt als Mittel für die Durchführung von Computer-Netzwerk-Attacken eingesetzt. So zum Beispiel kann eine Drohne eine regelmässige Bahn längs dem Pfad einer Richtstrahlstrecke fliegen und dort Daten abhören oder manipulieren. Im Militär ist die Übermittlung per Richtstrahl immer noch eminent wichtig. Ungeschützte oder schlecht geschützte Strecken (ziviler und militärischer Art) sind grossen Risiken ausgesetzt.

Datenmanipulation auf diese oder ähnliche Art erlaubt einem Gegner, den eigenen Entscheidungszyklus aufzuklären und im schlimmsten Fall direkt zu beeinflussen. Das kann den Erfolg einer Operation bereits Tage vor ihrer Durchführung gefährden und muss aus diesem Grund in die Kategorie der strategisch relevanten Waffen und Methoden eingeordnet werden. Nur ein sehr guter Schutz, eine sinnvolle Ausbildung und ein tiefes Verständnis für die gegnerischen Möglichkeiten können hier Abhilfe schaffen.

In friedensunterstützenden Operationen ist die Unterstützung der lokalen Bevölkerung und der eigenen Mitbürger zu einem bestimmenden Element des Erfolges geworden. Deswegen sind psychologische Operationen heute Teil jedes grösseren Truppeneinsatzes. Während dem Kosovo-Krieg zum Beispiel, sind serbische TV- und Radio-Sender nicht nur deswegen zerstört worden, weil sie Milosevic's Propaganda ausgestrahlt haben, sondern auch damit eigene (zum Teil auch luftgestützte) Sender eine NATO-freundliche Programmierung auf denselben Frequenzen ausstrahlen konnten.

FOTO: E. REINMANN



Riccardo Sibilia: «Das Anzapfen von Daten- und Faxverbindungen ist heute alltäglich.»

In Privatwirtschaft und Verwaltung ist die Gefährdung durch «Information Warfare» noch grösser. Nicht nur ist die Informationsinfrastruktur sehr weniger systematisch geschützt (wenn überhaupt) wie beim Militär, sondern weist auch noch einen hohen Grad an Einheitlichkeit auf (Monokultur). Dies ist fruchtbarer Boden für potenziell noch gefährlichere Viren, als die bereits bekannten, und für mehr oder weniger gut gerüstete Hacker. Die Qualität der Softwareprodukte wird heute oft auf dem Altar einer zeitgerechten Markteinführung geopfert. Die Bedeutung der Qualitätsstandards bei sicherheitsrelevanten Komponenten muss deshalb enorm an Stellenwert gewinnen.

Die zunehmende strategische Wichtigkeit der Wirtschaftskraft eines Landes führt dazu, dass die enorm leistungsfähigen Aufklärungsmittel des Kalten Krieges vermehrt als Mittel der Wirtschaftsspionage genutzt werden.

Die moderne Gesellschaft ist so stark von den Informationstechnologien abhängig geworden, dass ein weitgehender Ausfall durch einen oder mehrere Viren und/oder durch einen strategischen Angriff auf kritische Infrastrukturelemente schwerwiegende Folgen für das Überleben vieler Unternehmen haben könnte. □