Zeitschrift: Action : Zivilschutz, Bevölkerungsschutz, Kulturgüterschutz = Protection civile, protection de la population, protection des biens culturels = Protezione civile, protezione della populazione, protezione dei beni culturali

Herausgeber: Schweizerischer Zivilschutzverband

Band: 48 (2001)

Heft: 4

Artikel: Information ist Wertsache

Autor: [s.n.]

DOI: https://doi.org/10.5169/seals-369408

Die Referenten

Tagungsmoderator:
Divisionär z. D. Peter E. Regli

1. Tag: Militärische Operationen in einem verschlechterten Informationsumfeld.
Hauptreferent: Generalmajor Bruce Wright, Kdt Nachrichtendienst der US Air Force, San Antonio, Texas (USA).
Weitere Referenten: Gérald Vernez, Untergruppe Operationen, Generalstab, VBS; Brigadegeneral z. D. Loup Francart, Paris; Hauptmann Cristian Rotaru, Verteidigungsministerium, Bukarest (Rumänien); McCallam, Firma Logicon (eine Gesellschaft der Northrop Grumman), Falls Chirch, Virginia (USA); Oberstleutnant im Generalstab Urs Lingg, Instruktor, Fachspezialist Übermittlung, Armee-Ausbildungszentrum Luzern.

2. Tag: Informationsoperationen. Einfluss auf die Wirtschaft und die Gesellschaft sowie mögliche Lösungen.
Hauptreferentin: Marit Blattner-Zimmermann, Regierungsdirektorin für kritische Infrastrukturen beim Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn (Deutschland).
Weitere Referenten: Brigadegeneral z. D. Loup Francart, Paris; H. A. M. Luiijf, Forschungsinstitut TNO, Den Haag (Niederlande); Kurt Haering, Geschäftsführer Stiftung InfoSurance (Stiftung für die Sicherheit der Informationsinfrastruktur in der Schweiz), Zürich; Daniel Bircher, Berater für strategische Fragen, Ernst Basler und Partner, Zürich.

Abendanlass 2. Tag: «Schnupperkurs» für Nichteingeweihte mit Einführung in die Problematik der Herausforderung «Informationsrevolution».
Hauptreferent: Divisionär z. D. Peter E. Regli, Chef des Schweizerischen Nachrichtendienstes von 1990 bis 1999.
Weitere Referenten: noch offen.

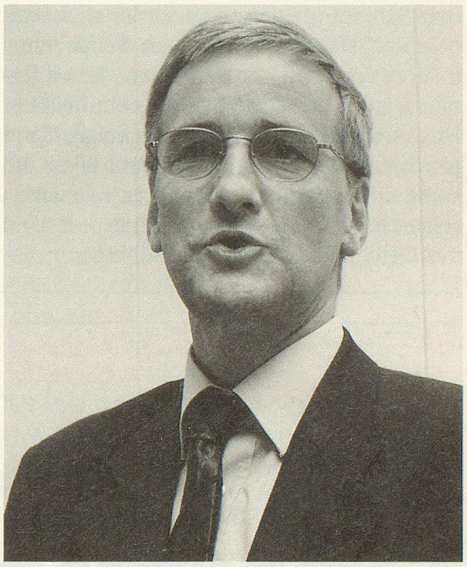
3. Tag: Schutz von Daten und Netzwerken; praktische Aspekte organisatorischer und technischer Natur für die Führungsebene.
Hauptreferent: Wolfgang Peter, Leiter Prüfstelle für Informationstechnologische (IT) Sicherheit, TÜV Informationstechnik GmbH, Essen (Deutschland).
Weitere Referenten: Roger Auinger, Fachspezialist für Mobile Sicherheit, ATAG Ernst & Young, Zürich, sowie weitere Referenten (noch offen) aus Hochschule und Industrie.

Peter E. Regli: «Die Information als Waffe wurde erst zu Beginn des letzten Jahrzehnts akut. In der Schweiz wurde die Problematik auf Stufe Bund ab 1997 ernsthaft in Angriff genommen.»

HÜTET EUCH VOR DATENDIEBSTAHL

Information ist Wertsache

Das dreitägige Symposium «Information Warfare» wird zu einer hochkarätigen Veranstaltung. Allein schon die anfangs Juni einberufene Medienkonferenz warf erste Glanzlichter voraus. Zum hoch aktuellen Thema «Welche Bedeutung haben die Informationsbedrohungen für das einzelne Unternehmen (speziell auch für KMU)?» sprach Armin Huber von der Crypto AG Zug.



Armin Huber: «Grossunternehmen und insbesondere Banken sind schon lange auf die Problematik sensibilisiert. Aber KMU?»

Wer hat es schon gerne, wenn jemand Fremder die eigene Post durchschnüffelt, wenn Dritte nachts durch die Büroräume gehen und die Aktenordner durchsuchen oder wenn die EDV plötzlich stillsteht und das Unternehmen dadurch praktisch handlungsunfähig wird? Um dies zu verhindern, verschicken wir unsere Post in Umschlägen, schliessen die Schränke und Türen ab und sichern den EDV-Raum mit speziellen Massnahmen. Was tun wir aber, wenn die Daten elektronisch übermittelt und abgelegt werden? Wenn unser Rechenzentrum mit Aussenstationen und mit dem Internet verbunden ist? Neue Computer- und Kommunikationssysteme dringen nach wie vor mit unverminderter Geschwindigkeit in unser Leben ein. Begriffe wie E-Business, E-Banking, E-Government werden für die nachkommende Generation bereits eine Selbstverständlichkeit sein. Wir stützen uns immer mehr auf die Möglichkeiten der digitalen Welt ab. Wenige Jahre haben unser Leben tiefgreifend verändert. Die virtuellen Komponenten der Welt ersetzen viele bisher physisch fassbare. Und virtuelle Formen sind schon jetzt oft kostbarer als physische. Die Bits und Bytes sind immer mehr die eigentlichen Wertsachen. Sie repräsentieren beispielsweise Anrechte auf Unternehmen, Verträge, finanzielle Transaktionen oder ganz einfach Wissensvorsprünge. Ein wichtiger Aspekt dabei werden auch die zukünftigen Rechtsformen sein, welche die elektronische Unterschrift der eigenhändigen gleichstellen. Information ist Wertsache geworden! Behandeln wir sie aber auch als Wertsache?

Die Gefahr ist unsichtbar

Durch die zur Verfügung gestellten kommunikativen Kanäle lassen sich heute alle Dimensionen und Hierarchien von Wirtschaft, Gesellschaft und Politik verknüpfen. Die Integration bezieht alle Dienste ein: von E-Mail zu Fax, vom GSM auf den Laptop, von Handheld auf die Datenbank. Faszinierend ist, dass dies alles immer einfacher und billiger wird. «Anything goes» erfasst uns mit einem Tempo, das Hinterfragen kaum zulässt. Aber gerade hier liegt das Problem dieser allumfassenden Integration: komplexe Netze sind sehr verletzlich. Diese Verletzlichkeit beruht darauf, dass komplexe Systeme auf Leistungsfähigkeit optimiert sind, nicht auf den Schutz der transportierten oder gespeicherten Information. Und so kann jede Schnittstelle auch eine Schwachstelle sein. Jeder Laptop, verbunden mit einem IT-System, kann zum Einfallstor für unbefugten Zutritt zu einem Rechensystem werden. Jedes E-Mail ist wie ein Brief, der ohne Kuvert verschickt wird. Jeder doch so praktische Anruf mit dem GSM, jederzeit und überall, kann mitgehört werden. Und Eindringen oder Manipulieren ist viel einfacher, als die meisten Benutzer annehmen. Das Erstellen einer elektronischen Kopie von Dutzenden oder auch Tausenden von Seiten dauert nur einen Augenblick und hinterlässt keine Spuren. Und ermöglicht die Einsparung von Millionen von Franken, wenn es sich zum Beispiel um Entwicklungs- oder Forschungsresultate handelt. Wissen, was die «andere Seite» plant, erhöht die Chance auf Erfolg bei Verhandlungen. Eine gefälschte Unterschrift unter einem modifizierten Dokument kann fatale Folgen haben. Durch einen Hacker können unersetzliche Daten für immer zerstört werden. Eingeschleuste Viren und Würmer können das EDV-System und damit die ganze Organisation für Stunden

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

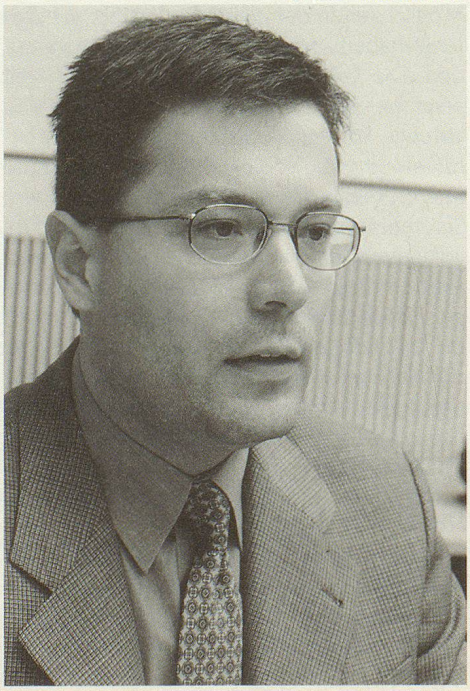
Zum Thema «Welche aktuellen Bedrohungen im Informationsbereich gibt es für Gesellschaft, Wirtschaft und Armee?» sprach an der Medienorientierung Riccardo Sibilia von der ETH Zürich.

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. □