Gefahr aus dem Netz – Bedrohung und Schutz kritischer Infrastrukturen

Thomas Berger

Thomas Berger ist Geschäftsführer von Compliance Investigations – Thomas Berger. Zuvor war er in Untersuchungs- bzw. Compliance Funktionen bei Global Security/Novartis Pharma AG sowie Compliance International/Credit Suisse AG und Office of Special Investigations/ABB Asea Brown Boveri Ltd. tätig. Thomas Berger begann seine berufliche Laufbahn als Polizei-Detetktiv bei der Staatsanwaltschaft Basel-Stadt in den Abteilungen Leib und Leben, Drogendezernat, Organisierte Kriminalität sowie später als Kriminalkommissar in der Abteilung für Wirtschaftsdelikte.

Thomas Berger absolvierte die Lehrgänge MAS Economic Crime Investigation sowie DAS Compliance Management und ist Certified Fraud Examiner.

Die Informations- und Kommunikationstechnologien haben heute einen massgeblichen Einfluss auf unser Leben. Sie sind die zentralen Elemente für das Funktionieren einer arbeitsteiligen Gesellschaft. Die Digitalisierung von Daten, die Computertechnik, sowie die neuen Übertragungstechnologien leiten eine – immer noch andauernde – Informationsrevolution ein. Stellvertretend dafür steht das Internet als globales Netzwerk, worin die Faktoren Raum und Zeit an Bedeutung verlieren, so dass vor allem für die Wirtschaft notwendige Informationen global und jederzeit verfügbar sind. Die Ware Information wird zum wichtigsten Produktionsfaktor und ermöglicht erst eine Globalisierung der Wirtschaft. Die Vernetzung eröffnet aber auch dem Privaten und sozialen Gruppen neue Formen der Kommunikation und Organisation. Nationale Grenzen verlieren somit an Bedeutung und ermöglichen das Aufkommen internationaler Interessengruppen.

Mit dieser Entwicklung nimmt auch die Abhängigkeit und Verwundbarkeit über den einzelnen Wirtschaftsbereich oder die Landesgrenze hinweg zu. Kein Wirtschafts- oder Verwaltungsbereich kann auf längere Dauer ohne Informations- und Kommunikationstechnik funktionieren. Jene Bereiche, welche bei einer Beeinträchtigung oder gar einem Ausfall eine existenzielle Bedrohung für Staat, Wirtschaft und Gesellschaft darstellen, werden als kritische Infrastrukturen bezeichnet (z.B. Energieversorgung, Bankwesen, Informations- und Kommunikationsinfrastruktur). Da durch eine Gefährdung auch die Grundrechte der Bürger beeinträchtigt werden, trifft hier den Staat eine Schutzpflicht zur Erkennung und Abwehr solcher Gefahren. Im Zentrum des Schutzes stehen die Informations- und Kommunikationsinfrastrukturen, welche alle anderen kritischen Infrastrukturen überlagern. Es gilt zu verhindern, dass im entscheidenden Moment eine Information falsch, fehlerhaft, nicht zugänglich oder gar nicht vorhanden ist. Ein wirksamer Schutz stellt hohe Anforderungen an das Abwehrkonzept dar, denn die Probleme sind vielfältig:

Die Informations- und Kommunikationstechnologien selber bergen besondere Risikofelder in sich (z.B. komplex, weltweit verbreitet, oft fehlerhaft aufgrund schnellen Innovationszyklen, Monokulturen infolge weniger Produzenten). Ständig neue Innovationen rufen immer umfangreichere Programme hervor, deren Verhalten in ausserordentlichen Situationen kaum jemand abschätzen kann. Der Staat kann infolge der Liberalisierung der diversen Märkte (Energie, Verkehr, Kommunikation) keinen direkten Einfluss mehr auf die betreffenden Sektoren ausüben. Neben dem Feld der passiven Gefährdungen (Feuer, Wasser, Strom, Blitz) gibt es ein breites Feld von aktiven Gefährdungen. Anders als bei Atom-/Bio- und Chemiewaffen ist das Instrumentarium der Informations- und Kommunikationstechniken zur Verursachung von Schäden für jeden zugänglich und einsetzbar. Die Akteure und deren Motive reichen vom "Script-Kiddie" bis hin zum Terroristen. Wenn Viren und Würmer von Jugendlichen mit den entsprechenden Tools hergestellt und innert weniger Minuten im Internet verbreitet werden können, so kann man sich vorstellen, zu was Terroristen in der Lage wären. Die neuen Technologien werden aber auch bei Unternehmen für Sabotage und Spionage eingesetzt und verursachen Schäden in Milliardenhöhe. Hinzu kommt, dass die Nationalstaaten die Bedeutung der elektronischen Kriegsführung erkannt haben und massiv ausbauen.

Mit der Vernetzung sind auch neue Schadenstypen entstanden. Die neuen Technologien ermöglichen eine Effizienzsteigerung, was bei einer Störung (sei es technisch oder durch einen Angriff) meist einen hohen Einzelschaden zur Folge hat. Die Vernetzung führt zu einer Multiplikation dieser Schäden und kann, je nach Verlauf, zu einer Katastrophe führen.

Die USA ergreifen 1996 als eine der ersten Staaten Massnahmen zur Risikoanalyse um zu verhindern, dass es zu einem "elektronische Pearl Harbor" kommen kann. Nebst repressiven Massnahmen (Militär, Geheimdienst) kommt ein präventiver Ansatz zusätzlich zum Zug, welcher auf ein enges Zusammenwirken von Staat und Wirtschaft setzt. Dieser Ansatz wird auch in der Schweiz, welche die neue Bedrohung ab 1997 wahrnimmt, anerkannt und konsequent weiterverfolgt, was im Abwehrkonzept eines 4- Säulenmodells mündet:

Die Störfall-Prävention ist Aufgabe eines jedes einzelnen Unternehmens, denn letztlich hängt das wirtschaftliche Überleben davon ab. Darauf aufbauend werden Unternehmen (vor allem KMUs) durch die Stiftung InfoSurance, welche einen präventiven Ansatz verfolgt, auf die neuen Bedrohungen sensibilisiert und in Form von "best practices" bei der Selbsthilfe unterstützt. Mit der vom Bund betriebenen Melde- und Analysestelle Informationssicherung (MELANI) wird der Bereich der Frühwarnung abgedeckt. MELANI stellt sicher, dass aufkommende Bedrohungen in Form von Lagebildern erkannt und entsprechende Präventiv- oder Gegenmassnahmen eingeleitet werden können. Für die Situationsanalyse ist MELANI auf Informationen der Wirtschaft und Schwesterorganisationen im Ausland angewiesen. Der Sonderstab Information Assurance (SONIA) stellt, analog dem

Sonderstab Geiselnahme, schliesslich die Bewältigung von Krisenereignissen sicher.

Der fortschreitende Einsatz der Informations- und Kommunikationstechnologien und die damit verbundenen Gefährdungen birgt, nebst wirtschaftlichen auch rechtliche und soziale Folgen in sich. Es kann von einer gesamtheitlichen Gefährdung gesprochen werden, welcher der Staat mit geeigneten Massnahmen Rechnung tragen muss. Durch das ständig wachsende Datenvolumen entstehen Kombinations- und Auswertungsmöglichkeiten, was einerseits der Wirtschaft umfangreiche Marktpotentiale ermöglicht, andererseits aber auch die Gefährdung durch Manipulation oder Überwachung des Bürgers in sich birgt. Der Datenschutz ist somit in die rechtlichen nationalen und internationalen Regelungen der IT-Sicherheit zu integrieren. Im repressiven Bereich wird mit der Unterzeichnung des Cybercrime-Abkommens durch 37 Staaten (Stand 18.03.2004) ein erster Schritt zur Förderung der internationalen Zusammenarbeit und Verfolgung einer gemeinsamen Strafrechtspolitik auf dem Gebiet der Internetkriminalität getan.

Hochschule Luzern - Wirtschaft
Institut für Finanzdienstleistungen Zug IFZ
Grafenauweg 10
Postfach 7344
CH-6302 Zug
+41 41 757 67 67
ifz@hslu.ch