Sachdokumentation:

Signatur: DS 1071

Permalink: www.sachdokumentation.ch/bestand/ds/1071

Zitierweise für graue Literatur

Elektronische Broschüren und Flugschriften (DS) aus den Dossiers der Sachdokumentation des Sozialarchivs werden gemäss den üblichen Zitierrichtlinien für wissenschaftliche Literatur wenn möglich einzeln zitiert. Es ist jedoch sinnvoll, die verwendeten thematischen Dossiers ebenfalls zu zitieren. Anzugeben sind demnach die Signatur des einzelnen Dokuments sowie das zugehörige Dossier.

Stiftung
LILIENBERG
Unternehmerforum

Januar 2014

10. Lilienberg Gedanken

Cyberrisiken – wachsende Gefahr für die moderne Informationsgesellschaft und die Privatsphäre

Erkenntnisse aus dem laufenden Lilienberg Zyklus
«Die strategischen Interessen der Schweiz und deren Auswirkungen auf die Sicherheitspolitik»

Cyber-Risiken: Mit wenig Geld und ohne grossen Aufwand können wenige Personen aus grosser Distanz aktiv sein. Dazu braucht es weder einen Staat noch teure Waffen – PC und Internetanschluss genügen.

Im laufenden Zyklus des Aktionsfeldes Sicherheit & Armee zur Sicherheitspolitik der Schweiz geht es darum, den Blick über die «klassische Landesverteidigung ab Landesgrenze» hinaus auf die modernen Bedrohungen unseres Kleinstaates zu richten. Der Zyklus geht vom Ansatz aus, dass die Schweiz zwar einwohnermässig ein Kleinstaat ist, aber unter anderen Gesichtspunkten – vor allem wirtschaftlich – eine Mittelmacht. So ist unser Land etwa als Drehscheibe für Finanzgeschäfte, Rohstoffhandel und Wissenstransfer weltweit bedeutsam. Wir sind damit aber auch besonders abhängig von den wachsenden globalen Verflechtungen. Die Sicherung der Energie-, Rohstoff- und Datenversorgung ist von zunehmender strategischer Bedeutung.

Immer mehr wird klar, dass sich die klassische Sicherheitspolitik des Staates nicht mehr von den wirtschaftlichen Verknüpfungen und Abhängigkeiten trennen lässt. Dabei kommt der Datensicherheit eine herausragende Bedeutung zu.

Cyberrisiken als neue und umfassende Bedrohungsform

Aus militärischer Sicht ist der sogenannte Cyberwar quasi die Fortsetzung der Rüstungsentwicklung von der Hellebarde über den Spiess zu den Schusswaffen, der Artillerie, den Flugzeugen und den Raketen. Oder man kann ihn sehen als neue Dimension eines Kriegsschauplatzes: also die Weiterentwicklung von Erdkampf, Luftkampf hin zum Kampf im elektronischen Raum oder eben im Cyber-Raum.
Dabei beginnt der Cyber-Raum schon mit dem Smartphone in der Hosentasche und umfasst letztlich die ganze Welt. «Cyberwar ist die Fortsetzung konventioneller Bedrohungen mit elektronischen Mitteln», würde heute der Militärtheoretiker Carl von Clausewitz sagen.

Cyberwar ist ein typisch asymmetrischer Krieg. Mit wenig Geld und ohne grossen Aufwand können wenige Personen aus grosser Distanz aktiv sein. Es braucht dazu weder einen Staat, ein eigenes Territorium noch teure Waffen – PC und Internetanschluss genügen!

Allerdings ist der Begriff «War» in diesem Zusammenhang nicht richtig. Es geht dabei nicht um eine zeitlich begrenzte, physische Attacke durch einen Staat gegen einen anderen Staat, sondern um permanente Bedrohungen, welche auch von nichtstaatlichen oder kriminellen Organisationen stammen können. Zudem ist die militärische Komponente der Bedrohung nur ein Teilbereich, auch wenn die Folgen einer Lahmlegung von Waffensystemen durch elektronische Einflüsse im Ernstfall natürlich sehr gravierend sind. Es geht um den Schutz sämtlicher kritischer Infrastrukturen einer Gesellschaft und einer Wirtschaft. Denken wir nur daran, wie abhängig beispielsweise Kommunikationsnetze, Energieversorgung, Zahlungsverkehr, Verwaltung oder Logistikdienste von funktionierenden Informatikanwendungen sind.

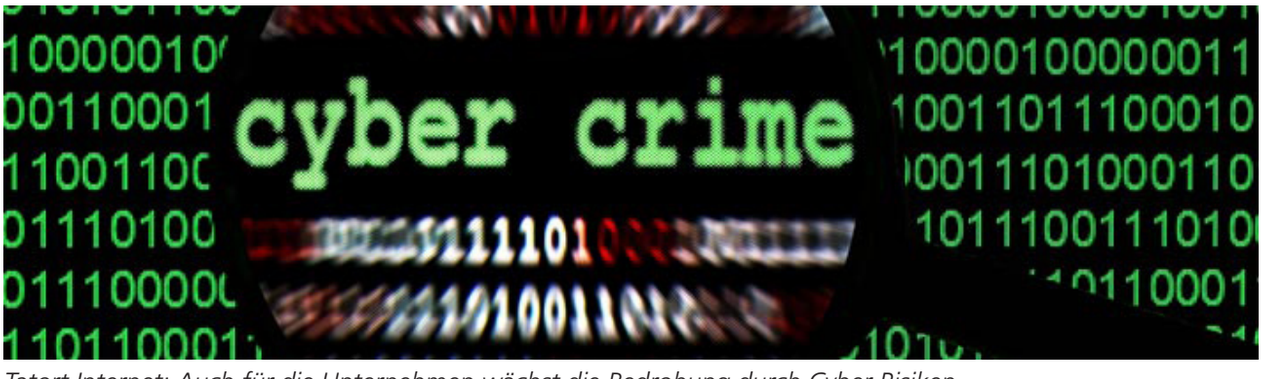
Cyber-Angriffe auf kritische Infrastrukturen können besonders gravierende Folgen haben, weil sie lebenswichtige Funktionen beeinträchtigen oder fatale Kettenreaktionen auslösen können. Den (oftmals privaten) Betreibern solcher Infrastrukturen kommt deshalb eine besondere Bedeutung zu. Behörden und Verwaltungen auf allen Ebenen können ebenfalls Opfer von Cyber-Angriffen sein und damit in ihrer Funktion beeinträchtigt werden. Cyber-Risiken betreffen letztlich aber auch alle Nutzer privater und beruflicher Informations- und Kommunikationssysteme sowohl Unternehmer als auch Privatpersonen. Systeme, mit denen wir wirksam einen Cyber-Angriff abwehren, geschweige denn mit denen wir feststellen könnten, welche Elemente angegriffen worden sind, gibt es heute auf dem Markt noch immer nur sehr wenige.
Informatiktechnologien können böswillig verwendet werden im Dienste der staatlichen Spionage, als Werkzeug des organisierten Verbrechens, der wirtschaftlichen Konkurrenz oder als taktische Option im Kriegsfall. Alle Anwendungen sind bereits Realität!

Paradigmenwechsel: Information als wichtigste Ressource

Die Informationstechnologie ist jene Technologie, die andere kritische Gebiete wie die Nukleartechnologie oder die Gentechnik an Brisanz zunehmend in den Schatten stellt. Der Fortschritt ist kaum aufzuhalten und erfolgt mit exponentieller Dynamik. Wenn wir die rasante Entwicklung der letzten Jahre extrapolieren, dann stehen wir heute in der Steinzeit der Informationsgesellschaft.
Der vielleicht grundlegendste Paradigmenwechsel, in dem wir uns befinden, ist die Tatsache, dass Informationen zur wichtigsten Ressource der Wirtschaft und der Gesellschaft schlechthin werden. Da die digitalen Objekte die physischen Gegenstände in ihrer Bedeutung zunehmend ablösen, kommt ihren besonderen Eigenschaften ein hoher Stellenwert zu. Ihre Charakteristik besteht darin, dass sie mit wenig Aufwand kopiert, mit Lichtgeschwindigkeit übermittelt und ohne Spuren zerstört werden können. Sie sind absolut stabil und nutzen sich nicht ab. All dies stellt neue Herausforderungen an den Schutz der Privatsphäre und des geistigen Eigentums.

Auf Vorrat abgehört und gesammelt

Wie durch die Enthüllungen des ehemaligen NSA-Mitarbeiters und Whistleblowers Edward Snowden bekannt geworden ist, setzen die Nachrichtendienste



Tatort Internet: Auch für die Unternehmen wächst die Bedrohung durch Cyber-Risiken.

die technischen Möglichkeiten des Abhorchens von Datenflüssen in einem bisher ungeahnten Ausmass ein. Dass Datenspionage zum Kerngeschäft jedes Geheimdienstes gehört, leuchtet ein. Die Ansicht, dass die Geheimdienste ihr technisches Repertoire jedoch nur in Einzelfällen einsetzen, ist aber blauäugig. Im Gegenteil: Es wird flächendeckend und auf Vorrat abgehört und gesammelt.

Elektronische Bauteile als Hintertür

Mit Hilfe frei zugänglicher und erschwinglicher Spionagesoftware bieten sich heute aber auch jeder Privatperson entsprechende Abhörmöglichkeiten bei der Nutzung von PC oder Mobiltelefon. Die Verschlüsselungstechniken werden deshalb immer wichtiger. Dazu gibt es absolut sichere Verschlüsselungsmethoden, die auch mit unendlich grossen Rechenleistungen nicht zu knacken sind. Die Anwendung solcher kryptographischer Methoden nützt letztlich aber nur etwas, wenn auch die verwendete Hardware sicher ist. Dazu gehört, dass die einzelnen elektronischen Bausteine von Computern oder Mobiltelefonen sicher gebaut sein müssen. Einen weiteren Schwachpunkt bilden die gängigen Softwareprodukte, die extrem komplex aufgebaut sind und somit genügend Möglichkeiten für (gezielte) Hintertüren der Datenschnüffler offen lassen. Da die USA in diesen Bereichen weltweit eine Monopolstellung einnehmen, wäre es naiv zu glauben, dass die entsprechenden Möglichkeiten nicht ausgenützt werden. Wenn Softwaregiganten und Telecomunternehmen mit den Geheimdiensten kooperieren, dann hat der einzelne Bürger trotz Kryptographie schlechte Karten gegen die Ausforschung seiner persönlichen Daten.

Spannungsfeld von Chancen und Risiken

Auf der einen Seite wird durch die modernen Informatikanwendungen, die wir gemeinhin mit dem Attribut «E-» zusammenfassen (E-Business, E-Cash, E-Gouvernement, E-Voting, E-Health etc.) eine Effizienzsteigerung erreicht. Andrerseits ergeben sich dadurch aber auch neue Risiken wie (elektronische) Virenepidemien, Hackerangriffe und Cyberkriminalität. Vielleicht muss auch der Begriff des geistigen Eigentums neu definiert werden. Durch Sicherheitstechnologien können diese Risiken zwar gemildert, aber nie ganz ausgeschlossen werden. Jedenfalls sind hochstehende Sicherheitstechnologien von entscheidender Bedeutung für die Entwicklung unserer Informationsgesellschaft.

Herausforderungen für die Schweiz und ihre Antwort darauf

Die Schweizer Behörden verwenden vorzugsweise die Bezeichnung «Cyber-Risiken» und nicht «Cyberwar». «Cyber-Risiken» betreffen nicht primär die Armee, sondern unsere gesamten Wirtschafts- und Gesellschaftsstrukturen und jeden einzelnen. Diese Erkenntnis zeigt sich auch in den Verantwortlichkeiten auf Stufe Bund: Die Federführung im Bereich Cyberrisiken ist kürzlich vom Verteidigungsdepartement ins Finanzdepartement übergegangen.

Das Informatiksteuerungsorgan des Bundes (ISB) koordiniert und vernetzt die Aktivitäten einer Vielzahl von Akteuren und ist daran, eine nationale Strategie zum Schutz vor Cyber-Risiken (NCS) umzusetzen. Massgeblich daran beteiligt ist auch der Nachrichtendienst des Bundes (NDB). Dabei werden jedoch keine Abwehrzentren oder Cyber-Armeen wie in anderen Staaten geschaffen. Die Schweiz setzt primär auf das Grundprinzip der Eigenverantwortung. Informationssicherung ist ein kontinuierlicher Risikomanagementprozess, der alle Unternehmensbereiche umfassen muss. Es handelt sich dabei um eine Aufgabe, die in der Verantwortung des Managements und nicht lediglich einer Unterstützungseinheit steht. Der Staat erbringt dazu subsidiäre Leistungen zum Schutz vor Cyber-Risiken, zum Beispiel durch Informationsaustausch oder nachrichtendienstliche Erkenntnisse. In diesem Sinn muss die Armee ihre wichtigen Infrastrukturen also genau so selbst schützen wie etwa die Banken oder andere Akteure der Wirtschaft.

Eine wichtige Rolle bei der Abwehr von Cyber-Bedrohungen spielt die Melde- und Analysestelle Informationssicherung (MELANI). Seit bald zehn Jahren betreibt sie ein eidgenössisches Lagezentrum zum Schutz kritischer Infrastrukturen und unterstützt deren Betreiber. Dabei ist sie vernetzt mit einer Vielzahl von nationalen und internationalen Quellen aus den Bereichen Nachrichtendienste, Ermittlungsbehörden und Computer Emergency Response Teams. Dies ist notwendig, um gegen Attacken via Botnetze, Verbreitung von Malware oder Datenausspähung gerüstet zu sein. Für EDV-Nutzer ist der Newsletter der MELANI zu empfehlen, der kostenlos abonniert werden kann unter der Internetadresse **www.melani.admin.ch.**

«IT-Sicherheit ist von ihrer Bedeutung her für ein KMU ebenso wichtig wie das Thema Liquidität». (Fritz Kläy, Inhaber SAFOS, Wangen)

Richtiges Verhalten des Einzelnen

Nicht vergessen werden darf, dass bei Cyber-Risiken nebst den technischen Gefahren immer auch der Mensch, sprich das Verhalten der EDV-Nutzer, ein bedeutendes Risiko darstellt. In diesem Sinn ist jede Behörde und jedes Unternehmen gefordert, eine umfassende Risikoanalyse unter Beurteilung der zu schützenden Werte, der Prozesse und der IT-Strukturen vorzunehmen. Dies gilt nicht nur für mittlere und grosse Unternehmen, sondern besonders auch für Kleinbetriebe wie Arztpraxen, Beratungsfirmen oder Gewerbetreibende. Gefragt ist also die persönliche

Der Cyber-Raum beginnt mit dem Smartphone: Nebst den technischen Gefahren stellt bei Cyber-Risiken somit auch der Mensch, also das Verhalten jedes einzelnen EDV-Nutzers ein Risiko dar.

Verantwortung jedes einzelnen. Doch wird es mittelfristig landesweit wohl unabdingbar, dass eine Art nationale Dachorganisation die verschiedenen Systeme und Anwendungsarten koordiniert und zielgerichtet zum Einsatz bringt.

Das Ende der Privatsphäre?

«Big Brother is watching you»: Mit der flächendeckenden Überwachung von Telefon- und Internetdaten durch den US-Geheimdienst NSA sind wir einem allmächtigen Überwachungsstaat, wie er von George Orwell in seinem damals utopischen Roman entworfen worden war, bereits sehr nahe gekommen. Zusammen mit neuen Technologien wie Videoüberwachung mit Gesichtserkennung, digitalen Signaturen oder fotografischer Erfassung der ganzen Welt führen selbstverursachte Datenfährten, etwa durch die Nutzung von Kreditkarten, Social Media, Mobiltelefon etc., unweigerlich dazu, dass die Datenspuren des Einzelnen immer engmaschiger werden. Das Leben jedes einzelnen ist durch eine Anhäufung von Daten dokumentiert. Die Technischen Möglichkeiten zur Beobachtung und Überwachung des Einzelnen wachsen fast ins Unermessliche, denn den Zugriffen auf Server und Glasfasernetze kann sich keiner entziehen. Das wird das Identitätsverständnis des einzelnen Individuums unweigerlich ändern. Zudem droht auch eine Spaltung der Gesellschaft in IT-Nutzende und IT-Verweigerer oder IT-Dilettanten, die es im bürgerlichen Leben zunehmend schwieriger haben werden. Über die technische Komponente hinaus geht es also um eine Frage der Werte, welche in einer gesellschaftlichen Diskussion erfolgen muss. Es geht nicht mehr um die Frage, welche Daten gesammelt werden können, sondern ob dies gemacht werden darf und welche wirksamen Kontrollmechanismen dabei bestehen.
In diesem Sinn haben wir vermutlich erst die Spitze des Eisbergs in dieser Thematik erlebt. Ein politisch brisantes Thema ist zudem die Frage, wie weit es den Untersuchungsbehörden gestattet werden soll, digitale Datenspuren zu verfolgen oder auf Vorrat zu erheben. Rechtfertigen einzelne Kriminalfälle oder Terroranschläge die schwerwiegende Beeinträchtigung der Privatsphäre für alle Menschen? Wird die freie, offene und deshalb verletzliche Gesellschaft durch die unkontrollierbaren Möglichkeiten der Datenspionage letztlich nicht nur nicht geschützt, sondern sogar zerstört?

Bei den Römern war der Toilettengang ein gemeinsames, öffentliches Ereignis, heute gehört er zur Intimsphäre jedes einzelnen. Wie sieht es wohl in der Zukunft aus?

Herausgeberin
Lilienberg Unternehmertum
Industriestrasse 1
CH-8340 Hinwil
Telefon +41 44 938 70 00
Fax +41 44 938 70 99
info@lilienberg.ch
www.lilienberg.ch

Text
Andreas W. Widmer,
Leiter Aktionsfeld Sicherheit&Armee
Redaktion
Christoph Vollenweider, Leiter Unternehmertum
Layout
Stefan Bachofen, Lilienberg Publikationen
Druck
Christian Walker, Repro Ferag AG