ISPSW Strategy Series: Focus on Defense and International Security
Cyber verändert die Welt –
Bürger und Gesellschaft, Wirtschaft und Staat vor neuen Herausforderungen
Ralph D. Thiele

Issue
No. 376
Sep 2015

Cyber verändert die Welt –
Bürger und Gesellschaft, Wirtschaft und Staat vor neuen Herausforderungen

Ralph D. Thiele

September 2015

Zusammenfassung

Staat und Unternehmen, Organisationen und Privatpersonen sind heute in vielfältiger Weise von Informations- und Kommunikationstechnologien abhängig. Insbesondere die Verfügbarkeit, Vertraulichkeit und Zuverlässigkeit von Informationen spielen eine Schlüsselrolle. Die enormen Möglichkeiten des Cyber-Raumes werden privat und gemeinnützig, unternehmerisch und staatlich genutzt. Auch deren Missbrauch boomt. Vermögen und geistiges Eigentum, Selbstbestimmung und Identität von Menschen und Unternehmen sind gefährdet, ebenso Freiheits- und Bürgerrechte. Es gibt erheblichen Regelungs- und Gestaltungsbedarf. Das IT Sicherheitsgesetz soll seit Mitte 2015 zu einer Verbesserung der IT-Sicherheit in Deutschland beitragen.

Aktivitäten im Cyber Raum werden sich in den nächsten Jahren vor allem auf Cloud-Dienste und Social Networks konzentrieren. Der stetige Zuwachs an mobiler Nutzung des Internets über Smartphones und Tablets wird diesen Trend verstärken. Mitten im rasanten Entwicklungsprozess der IT-Technik weiß niemand exakt, was in fünf Jahren kommen wird. Die Politik setzt Standards und Richtlinien, wie mit Daten umgegangen wird. Mit Blick auf technische Lösungen ist die IT-Wirtschaft in der Verantwortung. Insgesamt sind jedoch alle gefordert, die Nutzung des Cyber-Raumes zu gestalten - Bürger und Gesellschaft, Wirtschaft und Staat.

Das ISPSW

Das Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung (ISPSW) ist ein privates, überparteiliches Forschungs- und Beratungsinstitut.

In einem immer komplexer werdenden internationalen Umfeld globalisierter Wirtschaftsprozesse, weltumspannender politischer, ökologischer und soziokultureller Veränderungen, die zugleich große Chancen, aber auch Risiken beinhalten, sind unternehmerische wie politische Entscheidungsträger heute mehr denn je auf den Rat hochqualifizierter Experten angewiesen.

Das ISPSW bietet verschiedene Dienstleistungen – einschließlich strategischer Analysen, Sicherheitsberatung, Executive Coaching und interkulturelles Führungstraining – an.

Die Publikationen des ISPSW umfassen ein breites Spektrum politischer, wirtschaftlicher, sicherheits- und verteidigungspolitischer Analysen sowie Themen im Bereich internationaler Beziehungen.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analyse

Staat und Unternehmen, Organisationen und Privatpersonen sind heute in vielfältiger Weise von Informations- und Kommunikationstechnologien abhängig. Diese sind Lebensadern im Privatleben und sozialen Netzwerken, in Wirtschaft und Verwaltung. Insbesondere die Verfügbarkeit, Vertraulichkeit und Zuverlässigkeit von Informationen spielen dabei eine Schlüsselrolle. Die Analyse riesiger Datenmengen in Echtzeit hat ein unglaubliches Leistungsniveau erreicht. Bereits vor einem Jahrzehnt konnte man eine Nadel im Heuhaufen finden. Zwischenzeitlich haben sich die Möglichkeiten vervielfältigt. Welche Nadel darf es sein? Die mit dem roten Kopf? Die kurze Nadel? Die dünne Nadel? Niemand und nichts entgeht der Suche. Niemand und nichts wird vergessen.

Angriffe aus dem Cyberraum sind heute ebenso gefährlich wie physische Attacken. Sie können Staaten und Gesellschaften ins Wanken bringen, Unternehmen ruinieren, Privatpersonen bestehlen oder deren guten Ruf vernichten. Der Täter lauert nur einen Mausklick entfernt. Entsprechend wächst das Bewusstsein für mehr IT-Sicherheit. Im Jahr 2015 wird in Deutschland mit diesbezüglichen Umsätzen von knapp 4 Mrd. € gerechnet. Damit liegen wir aus internationaler Perspektive allerdings keineswegs an der Spitze des Fortschritts.

Der Boom von Cyberangriffen

Die enormen Möglichkeiten des Cyber-Raumes werden nicht nur privat und gemeinnützig, unternehmerisch und staatlich genutzt. Auch deren Missbrauch boomt – durch Einzelpersonen und Gruppierungen, Staaten und Unternehmen, insbesondere durch kriminelle Akteure. Vandalismus und kriminelle Aktivitäten, Sabotage und Spionage, die Manipulation der öffentlichen Meinung und die Ausforschung sozialer Netzwerke breiten sich wie Grippeepidemien aus. Die Akteure und die angewandten Methoden verändern wie ein Chamäleon permanent ihr Profil.

Die Gefahr ist ganz real. Bürger werden bestohlen und Banken beraubt. Unternehmen werden angegriffen und Energienetze abgeschaltet. Netze des Bundes in Regierung, Parlament und staatlichen Behörden erfahren laut Bundesamt für Sicherheit in der Informationstechnik jeden Tag zwischen 2.500 und 6.500 Attacken. Einige darunter sind auf einem derart hohen technischen Niveau, dass ein nachrichtendienstlicher Hintergrund angenommen werden muss. Insgesamt wurden im ersten Halbjahr 2015 bereits 4.353 Infektionen von Computern des Bundes mit Schadsoftware erfasst.

Angreifer konzentrieren sich insbesondere auf die Anwender. Der Mensch ist zugleich Ziel und vortreffliches Einfallstor für Cyber Angriffe. Viele Nutzer sind leichtfertig beim Umgang mit ihrem Passwort. Sie wählen gerne „12345". Das wissen auch Kriminelle. Die wiederholte Verwendung gleicher Passwörter ist eine weitere, gnadenlos ausgenutzte schlechte Angewohnheit von Anwendern. Auch wer seine Daten in einer kostenlosen Cloud speichert, sollte sich bewusst sein, dass der Betreiber seine Einnahmen aus der Verwertung der Daten des Nutzers für Werbung und andere Zwecke gewinnt. Zudem wurden in der jüngeren Vergangenheit wiederholt riesige Datenbanken mit Usernamen und dazugehörigen Passwörtern gestohlen – etwa 700 Millionen Datensätze – und weiterverbreitet.

Häufig bringen Angreifer die Anwender durch sogenanntes „Social Engineering“ – durch Eingriffe in und Ausspionieren des persönlichen Umfelds von Opfern – dazu, gegen ihre eigenen Interessen zu handeln. Vorzügliche Einstiegspunkte für kriminelle Delikte sind das WLAN im Zug, im Flughafen oder im Internet Café.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Im WLAN kann man sehen, dass nebenan Lieschen Müller und Joe Sixpack im Internet surfen. Deren Smartphone oder Tablet zu „knacken" und Daten zu stehlen dauert nur wenige Sekunden. Anschließend erfolgt dann z.B. der Anruf bei der Oma von Lieschen und die Bitte um einen Geldbetrag, weil Lieschen vorgeblich in einer Notlage ist. Oder man ruft Joe an, gibt vor Bankangestellter zu sein und berichtet von Unregelmäßigkeiten auf dessen Konto. Im Zuge der nachfolgenden Legitimierung erfährt der Kriminelle dann von Joe all die Daten, die er noch für einen Zugriff auf dessen Bankkonto braucht.

E-Mails gehören zu den meist genutzten Einfallstoren von Cyber-Angriffen. Und die Angreifer erzielen erhebliche Erfolge. Der jüngste Report des U.S. Unternehmens VERIZON – der 2015 Data Breach Investigation Report[1] – meldet, dass 23% der Empfänger Phishing-Emails öffnen und 11% sogar auf gefährlich Anhänge klicken. Laufende Software-Aktualisierungen sind ebenfalls ein massives Management-Problem. Das reicht von Browser-Plugins bei Privat-PCs bis hin zur Webserver-Software bei Unternehmen. Die massenhafte Nutzung von sogenannten „Apps" ermöglicht die massenhafte Verbreitung von Schadsoftware. Zudem wächst die Zahl der Angriffe auf Industrieanlagen und Steuersysteme (SCADA). Die physikalische Trennung zur Außenwelt allein ist kein wirksamer Schutz mehr. Neue Technologien, drahtlose Kommunikation und wiederum Social Engeneering ermöglichen den Zugang von Außenstehenden.

Wer sind die Akteure?

Wer betrachtet mich gerade durch die Kamera meines Handys, meines Tablets, meines Computers oder auch meines Fernsehers? Wer nutzt meinen Computer, um mich, meine Familie, andere Menschen oder Organisationen zuzumüllen oder anzugreifen? Wer gibt sich so viel Mühe, an meine Zahlungskartendaten und Passwörter zu kommen? Wer möchte meinen Geschäftsbetrieb stören? Wer führt Statistiken, wie oft und wo ich meine Jeans oder meine Kosmetikartikel ausführe, oder wie oft, wann und wo ich tanke? Die Erhebungs-, Analyse- und Angriffsmethoden werden immer ausgefeilter. Analysen erfolgen in Echtzeit. Angriffe werden mit atemberaubender Geschwindigkeit durchgezogen. Der Kriminelle bestellt seinen Ferrari eine Woche bevor er das Geld bei seinen Opfern kassiert, denn er überwindet Sicherheitsbarrieren in kürzester Zeit und mit Leichtigkeit. Privatpersonen und Unternehmen brauchen demgegenüber in vielen Fällen Monate oder gar Jahre, um zu entdecken, dass sie betroffen sind. Häufig sind sie machtlos. Zudem gibt es kaum hinreichende Rechtsgrundlagen, insbesondere wenn die Angreifer aus fernen Ländern und Kontinenten agieren.

Spätestens seit den Enthüllungen durch Edward Snowden weiß jeder, dass auch staatliche Konflikte im Cyber Raum ausgetragen werden. Generell nutzen Staaten den Cyber Raum zur Förderung ihrer politischen, militärischen und wirtschaftlichen Interessen. Die Aktivitäten der USA stehen derzeit im Vordergrund der öffentlichen Diskussion. Noch mehr Besorgnis sollten allerdings die Aktivitäten von Russland und Chinas erregen. Auch England und Neuseeland, Australien und Kanada, Brasilien und Indien, Iran und Syrien sind in diesem Feld hyperaktiv. Israel und Südkorea gehören in die Champions League der Cyberakteure. Nordkorea überfällt zu jedem seiner zahlreichen Jahrestage mit Cyberangriffen südkoreanische Banken, Medien und kritische Infrastrukturen, häufig auch in Verbindung mit physischen Attacken. Im Zuge der Ukraine-Krise wurde deutlich, dass sich über den Cyberraum im Zuge einer Informationskriegführung auch erfolgreich die Öffentliche Meinung beeinflussen lässt.

[1] http://www.verizonenterprise.com/resources/reports/rp_dbir-report-2015-executive-summary_de_xg.pdf

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Auf nichtstaatlicher Ebene spielen Cyber Kriminelle die wesentliche Rolle. Die Täter bedienen sich ausgefeilter Technologien und haben eine globale Reichweite – von Kleinkriminalität bis hin zu groß angelegten Kampagnen mit Schadenshöhen in der Größenordnung von einer Milliarde Euro. Opfer sind Bürger und Vereine, kleine mittelständische Unternehmen und High-Tech Start-Ups, Konzerne und öffentliche Einrichtungen. Das Motiv ist meist monetär. Die Wege zur Geldbörse sind einfallsreich und bunt. Nicht nur die Geldautomaten an der Bank, auch die Kasse beim Händler um die Ecke gehört immer öfter zu einem arbeitsteilig arbeitenden kriminellen Ökosystem.

Anzahl und Schwere der gezielten Angriffe auf die IT-Infrastruktur von Unternehmen nehmen dynamisch zu. Eine chinesische Hackergruppe steht im Verdacht, hunderte japanischer Unternehmen und Regierungsorganisationen seit 2013 auszuspionieren. Im Fokus dieser Gruppe stehen japanische High-Tech Unternehmen, darunter in den Branchen Chemie, Medizin, Ernährung, Automobil, Halbleiter, Robotik, Kommunikation, Energie, Satellitentechnologie und Finanzen. Für jedes Opfer gibt es eine eigens maßgeschneiderte Schadsoftware. Das macht es Analysten besonders schwer, diese zu entdecken.

Auch deutsche Firmen werden ständig Opfer von Cyberattacken. Demgegenüber herrscht insbesondere in kleinen und mittelständischen Betrieben eine Besorgnis erregende „digitale Sorglosigkeit". Einige bemerken Angriffe gar nicht erst. Andere verschweigen Vorfälle aus Angst vor Imageschäden. So findet sich das Wissen deutscher Mittelständler zur Solartechnologie heute weit verbreitet nicht nur bei vormals chinesischen Konkurrenten. Warum vormals? Nun, die betroffenen deutschen Mittelständler sind in Folge der Ausforschung längst Konkurs gegangen. Beim IT-Verband Bitkom geht man davon aus, dass nur knapp die Hälfte aller Firmen in Deutschland ausreichend auf IT-Notfälle wie Sabotage, Datendiebstahl oder Wirtschaftsspionage vorbereitet ist.

Grundsätzlich sind für Unternehmen sichere Cyber-Systeme heute eine grundlegende Voraussetzung für künftigen unternehmerischen Erfolg. Das wird sich im Zuge der dynamischen Entwicklung in Richtung Industrie 4.0 noch wesentlich verstärken. Kleinere Mittelständler, aber auch Kommunen sind aber mit dem Aufbau und Erhalt sicherer Datennetze oft überfordert. Für sie sind Selbstorganisation und Unterstützung dringend erforderlich. Es gilt, Kräfte zu bündeln, Expertise aufzubauen und kritische Systeme rund um die Uhr zu überwachen.

Auch Terroristen nutzen den Cyber Raum, bisher vornehmlich zur Radikalisierung, Rekrutierung und Finanzierung ihrer Operationen. Soziale Medien wie Facebook oder Twitter spielen in diesem Kontext eine zunehmend wichtige Rolle. Die Sorge ist, dass Terroristen künftig Großschäden in kritischen Infrastrukturen anrichten. Wenn dann der Strom ausfällt, gibt es kein Benzin in den Tankstellen, keine Lebensmittel in den Geschäften, keine Heizung im Winter und keine Kühlung im Sommer. Krankenhäuser und öffentliche Verwaltung stellen ihren Betrieb ein, die Wirtschaft Produktion und Handel.

Bis auf Weiteres ist davon auszugehen, dass sich die meisten der beschriebenen Aktivitäten rapide ausweiten. Da sich selbst politisch motivierte Attacken nicht eindeutig einer Organisation oder einem Staat zuordnen lassen, ist die Nachverfolgung von Angriffen und die Identifikation der Akteure im Cyber Raum – die sogenannte Cyber Forensik – ausgesprochen schwierig. Entsprechend gering ist die Hemmschwelle für solche Aktionen.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Auf dem Weg zur Cybersicherheit in Deutschland?

Bereits im Februar 2011 beschloss das Bundeskabinett die „Cyber Sicherheitsstrategie für Deutschland", um Cyber Sicherheit auf einem hohen Niveau zu gewährleisten, ohne die Chancen und den Nutzen des Cyber Raums zu beeinträchtigen. Zwei Ministerien sind primär für die Umsetzung verantwortlich: das Innenministerium und das Verteidigungsministerium. Daneben hat der Bundesnachrichtendienst eine wichtige Rolle. Er ist hauptsächlich für die Erstellung eines umfassenden Cyberlagebildes verantwortlich. Im Jahr 2013 wurde im Auswärtigen Amt ein eigener Sonderbeauftragter für Cyber Außenpolitik samt Arbeitsstab eingesetzt, der auf internationaler Ebene die deutschen Cyber Interessen vertritt.

Die Hauptverantwortung der Cyber Sicherheit liegt beim Innenminister. Das ihm nachgeordnete Bundesamt für Sicherheit in der Informationstechnik veröffentlicht Leitfäden und Richtlinien für den Schutz des privaten Sektors. Es zertifiziert Sicherheitsstandards. Es hat die Federführung im nationalen Cyber Abwehrzentrum – ein Abwehrverbund mit dem Bundesamt für Verfassungsschutz, dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, dem Bundeskriminalamt, dem Bundespolizei, dem Zollkriminalamt, dem Bundesnachrichtendienst und der Bundeswehr. Hier werden alle verfügbaren Informationen zu Cyber Angriffen zusammengeführt. Zudem soll ein Cyber Sicherheitsrat die Zusammenarbeit innerhalb der Bundesregierung sowie zwischen Staat und Wirtschaft stärken. Dieser konzentriert sich auf präventive Instrumente und ganzheitliche, umfassende Politikansätze für Cyber Sicherheit auf der politisch-strategischen Ebene zwischen Staat und Wirtschaft.

Mitte dieses Jahres verabschiedete der deutsche Bundestag das sogenannte IT Sicherheitsgesetz, das zu einer Verbesserung der IT-Sicherheit in Deutschland beitragen soll. Dessen Hauptziel ist es, kritische Infrastrukturen besser vor Cyberattacken zu schützen – darunter Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. Die wesentlichen Punkte dieses Gesetzes sind die verpflichtende Meldung von erheblichen IT-Sicherheitsvorfällen an den Staat, die Verbesserung des Schutzes der in den Kritischen Infrastrukturen eingesetzten IT und eine Stärkung der Aufgaben und Kompetenzen des Bundesamtes für Sicherheit in der Informationstechnik. Bei Energiefirmen spielen zudem Vorschriften der Bundesnetzagentur sowie ein neuer IT-Sicherheitskatalog eine wichtige Rolle. Diese verpflichten sie, schnell ein eigenes Management-System zur IT-Sicherheit aufzubauen.

Das Gesetz hat gute Elemente. In anderen Bereichen wird es bald überholt sein. Mitten im rasanten Entwicklungsprozess der IT-Technik weiß niemand exakt, was in fünf Jahren kommen wird. Die Politik setzt Standards und Richtlinien, wie mit Daten umgegangen wird. Mit Blick auf technische Lösungen steht die IT-Wirtschaft in der Verantwortung. Hier engagiert sich bereits die Deutsche Telekom. Sie hat jüngst mit dem Zusammenschluss von vier DAX-Konzernen – Allianz, Bayer, BASF und Volkswagen – , die gemeinsam gegen Cyberkriminelle vorgehen wollen und die ihr Angebot auch an kleine Mittelständler richten werden, eine Konkurrenz bekommen, die das Geschäft beleben wird.

Das zweite wesentliche Ministerium im Kontext der Cyber Sicherheit ist das Bundesministerium der Verteidigung. Hier war bisher das Kommando Strategische Aufklärung für Cyber Angelegenheiten zuständig. Zusätzlich soll in den kommenden Monaten ein Kommando aufgebaut werden, das die rund 15.000 mit Informationstechnologie befassten Soldaten und zivilen Mitarbeiter vernetzt. Eine Schnittstelle zur Wirtschaft und internationalen Partner sichert den Zugang zu und die Kooperation mit wesentlichen Partnern.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Entwicklungen und Fragen

Aktivitäten im Cyber Raum werden sich in den nächsten Jahren vor allem auf Cloud-Dienste und Social Networks konzentrieren. Der stetige Zuwachs an mobiler Nutzung des Internets über Smartphones und Tablets wird diesen Trend verstärken. Die rasanten Entwicklungen im Cyberbereich werfen eine Reihe fundamentaler Fragen auf:

- Wie bin ich betroffen?
- Kann ich mich schützen?
- Wie sichere ich meinen Geschäfts- bzw. Produktionsbetrieb?
- Wie sicher sind meine Daten in sozialen Netzwerken?
- Was kann ich tun, dass meine Kinder sicher im Internet navigieren können?
- Wo bleiben das Recht auf freie Meinungsäußerung und Informationsfreiheit, das Recht auf Privatleben und Privatsphäre?
- Wer gestaltet die Balance zwischen den Interessen der Strafverfolgung und der Achtung grundlegender Menschenrechte?

Die Fragen verdeutlichen den enormen Regelungs- und Gestaltungsbedarf, insbesondere auch hinsichtlich der Freiheits- und Bürgerrechte. Es gibt viel zu bedenken und viel zu tun. Bürger und Gesellschaft, Wirtschaft und Staat – alle sind gefordert.

***

Anmerkungen: Vortrag des Autors bei WirtschaftsForum Neuwied e.V. am 10. September 2015. Der Beitrag gibt die persönliche Auffassung des Autors wieder.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Über den Autor dieses Beitrags

Oberst a.D. und Diplom-Kaufmann Ralph D. Thiele ist Vorsitzender der Politisch-Militärischen Gesellschaft e.V. (pmg), Berlin und CEO von StratByrd Consulting. In seiner militärischen Laufbahn war Herr Thiele in bedeutenden nationalen und internationalen, sicherheits- und militärpolitischen, planerischen und akademischen Verwendungen eingesetzt, darunter im Planungsstab des Verteidigungsministers, im Private Office des NATO-Oberbefehlshabers, als Chef des Stabes am NATO Defense College, als Kommandeur des Zentrums für Transformation und als Direktor Lehre an der Führungsakademie der Bundeswehr.

Eine Vielzahl von Publikationen, regelmäßige Vorträge in Europa, Amerika und Asien sowie eine intensive Forschungstätigkeit im Kontext deutscher, österreichischer und europäischer Sicherheitsforschung unterstreichen sein ausgeprägtes Kompetenzspektrum.

Ralph D. Thiele ist Mitglied im Beirat Deutscher Arbeitgeber Verband e.V., Wiesbaden und im Defence Science Board, das von Gerald Klug, Verteidigungsminister der Republik Österreich, geleitet wird.

Ralph D. Thiele

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de