Globale IT-Bedrohungen

Die Entwicklung der Informationstechnologie und ihre Auswirkung auf Wirtschaft und Gesellschaft

Udo Helmbrecht[1]

Festkolloqium an der Universität der Bundeswehr München
anlässlich der Bestellung zum Honorarprofessor
Neubiberg 24. Januar 2011

Zusammenfassung

Informations- und Kommunikations-Technologien (IKT) sind das Rückgrat unserer Wirtschaft und Gesellschaft. Diese IKT-Infrastruktur wird ständig von Hackern und Kriminellen attackiert. Das bedeutet finanzielle Verluste (z.B. Produktionsausfälle, monitärer Diebstahl mittels Phishing), Abfluss von Informationen (Spionage) und Diebstahl geistigen Eigentums. Daher ist es notwendig, IT-Systeme und Infrastrukturen gegen Attacken zu schützen. Nur so sind Wachstum und Wohlstand in einer wettbewerbsorientierten, globalisierten Welt weiterhin möglich.

Alle Computerattacken bedienen sich derselben Technologie. Dies ist, verglichen mit herkömmlichen militärischen oder zivilen, kriminellen Attacken, eine neue Herausforderung an die Arbeitsteilung nach Taylor, wie sie von Regierungen und Industrieunternehmen praktiziert wird. Es ist Computerattacken nicht anzusehen, wer wen attackiert und warum bzw. mit welchem Ziel diese Attacke erfolgt.

Die Nutzung der Informationstechnologien in sozialen Netzwerken verändert das Verhalten von Individuen in unserer Gesellschaft. Es gilt, diese Entwicklung positiv zu gestalten.

Es werden vier Thesen aufgestellt, diskutiert und es werden Handlungsempfehlungen gegeben.

---

[1]Prof. Dr. Udo Helmbrecht http://de.wikipedia.org/wiki/Udo_Helmbrecht. Geschäftsführender Direktor der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) www.enisa.europa.eu und Honorarprofessor am Institut für Technische Informatik an der Universität der Bundeswehr München www.unibw.de/inf3/

Inhalt

Sehr geehrte Frau Präsidentin Niehuss,
sehr geehrter Herr Prof. Minas,
lieber Axel,
sehr geehrte Damen und Herren,

ein Festkolloqium dieser Art ist eine besondere Ehre für mich, da ich es als Wertschätzung meines Engagements an der Bundeswehr-Universität sehe.

Vielen Dank, lieber Axel, für Deine Laudatio. Herr Axel Lehmann war es , der mich vor einigen Jahren fragte, ob ich Vorlesungen und Seminare an der Bundeswehr-Universität halten könnte. Ich habe das sehr gerne gemacht, mir aber damals nicht vorstellen können, einmal Mitglied der Fakultät für Informatik zu werden.

Eine ganz besondere Freude ist es, meine Doktorvater Prof. J. G. Zabolitzky unter den Gästen begrüßen zu können. Unsere gemeinsamen Arbeiten in der theoretischen Kernphysik, nämlich physikalische Themenstellungen auf den seinerzeit schnellsten Vektorrechnern der Firma Control Data mittels numerischer Verfahren zu lösen, haben meine berufliche Karriere nachhaltig beeinflusst.

Einleitung

Die Entwicklung in der Computertechnologie des letzten Jahrhunderts ermöglichte neue Produkte und Dienstleistungen. Das erleichtert uns die tägliche Arbeit und hat Fortschritte in sehr vielen Branchen erst ermöglicht. Neue Unternehmensmodelle und Angebotsformen verändern unser Kaufverhalten. Aber: Sie verändern auch unser soziales Verhalten, wie die auf dem Internet basierenden sozialen Netzwerke zeigen.

In einer durch die Informationstechnologie weltweit vernetzten und von ihr unumkehrbar abhängigen Gesellschaft sind leider auch globale Bedrohungen möglich und real geworden: Die Kriminalität geht dorthin, wo viel Geld zu „verdienen“ ist. Früher wurden dazu brachial Banken überfallen, heute macht man das (viel risikoärmer) im Internet mittels der Methode des „phishing“[2], d.h. an die Stelle der einschüchternden Pistole tritt der heimtückische, weil unbemerkte Software-Trojaner , um an das Geld anderer Leute zu kommen. Die Internetplattform *WikiLeaks*[3] ist eine neue Entwicklung des Publizierens im Internet und der Virus *stuxnet*[4] ist eine negative Entwicklung von neuen IT-Bedrohungen. Ich werden darauf später zurückkommen.

Wenn wir von IT-Bedrohungen reden, denken wir zuerst an Viren, Würmer und Trojaner, das Ausspähen und Stehlen von Kredikartendaten oder personenbezogenen Daten. Ich möchte in meinem Vortrag den Rahmen weiter stecken und auch über Einflüsse und Bedrohungen auf unser Gemeinwesen, unsere Gesellschaft sprechen. Joseph Weizenbaum[5], war einer der scharfen Kritiker des unbedachten Umgangs mit der Computer-Technologie; schon 1972 hat er in der Wochenzeitung „Die Zeit“ gesagt: *„Unsere Zivilisation steht heute am Anfang einer schweren geistigen Krise.“*[66] 1972!

---

[2] Kunstwort aus *fishing* („Angeln“, „Fischen“[1]) in Anlehnung an *password fishing*
[3] http://213.251.145.96/
[4] http://de.wikipedia.org/wiki/Stuxnet
[5] gestorben 2008 in Berlin
[66] http://www.zeit.de/1972/03/alptraum-computer

Ich möchte in meiner Antrittsvorlesung die IT-Bedrohungen und deren Entwicklung in den letzten 40 Jahren betrachten und ihre Auswirkung auf unsere Wirtschaft und Gesellschaft erörtern. Dabei werde ich vier Thesen aufstellen und am Ende meines Vortrages auf das Zitat von Joseph Weizenbaum zurückkommen.

Informationtechnologie

Niemand wird heute die Abhängigkeit unserer Gesellschaft von der Informationstechnologie (IT) bestreiten. Wir kaufen online ein, wir buchen Flüge online, unsere Steuererklärung ist online möglich. Die Geschäftsprozesse in und zwischen Unternehmen werden „elektronisch" abgewickelt. Ausfälle dieser IT-Infrastruktur haben finanzielle Auswirkungen. Kurz um: Alle Bereiche in Wirtschaft und Gesellschaft sind von der Informationstechnologie abhängig. Daher sprechen wir heute vom Zeitalter der Informationsgesellschaft.

IT-Sicherheit

Sicherheit ist ein Grundbedürfnis des Menschen. Der Staat garantiert uns die territoriale Sicherheit. Im Straßenverkehr oder beim Hausbau gibt es Sicherheitstandards, die unser Leib und Leben und unseren Besitzstand schützen. Folglich beschäftigen wir uns in der Informationsgesellschaft mit IT-Sicherheit (IT-Security). Wir definieren[7]:

Definition: IT-System und IT-Infrastruktur

> Ein IT-System ist ein geschlossenes oder offenes, dynamisches technisches System mit der Fähigkeit zur Speicherung, Verarbeitung und Verbreitung bzw. zum Austausch von Informationen. IT-Systeme sind Bestandteile einer durch ihre Zusammenschaltung definierte IT-Infrastruktur, die insgesamt ein soziotechnisches System generieren.

Definition: IT-Bedrohung

> Eine Bedrohung des Systems zielt darauf ab, unter Ausnutzung einer oder mehrerer Schwachstellen oder Verwundbarkeiten einen Verlust der Datenintegrität, der Informationsvertraulichkeit oder der Verfügbarkeit herbeizuführen oder die Authentizität von Subjekten (Benutzern von IT-Systemen) zu gefährden.

Definition: IT-Sicherheit

> IT-Sicherheit bedeutet Schutz von Informationen, IT-Systemen und IT-Infrastrukturen vor den Gefahren, denen diese Systeme in einer global vernetzten Umgebung ausgesetzt sind. Durch den Einsatz von Sicherheitstechnologien und Verfahren für das Sicherheitsmanagement soll ein hohes Schutzniveau erreicht werden.
>
> Schutzziel ist die Gewährleistung der Integrität, der Vertraulichkeit, der Verfügbarkeit, der Verbindlichkeit, der Authentizität und der Privatheit aller in einer IT-Infrastruktur eingebundenen Informationen.

Effektive Sicherheitsrichtlinien und IT-Sicherheit durch Designvorschriften sind Beispiele dafür, wie dies erreicht werden kann. Dadurch werden z.B. die Integrität und Sicherheit der öffentlichen Kommunikationsnetze vor unbefugtem Zugriff und der Schutz Privatsphäre und personenbezogener Daten gewährleistet.

---

[7] Diese Definitionen stammen aus dem Buch von *Claudia Eckert, IT-Sicherheit , Oldenburg Verlag 2009*

In der Praxis orientiert sich die Informationssicherheit heute unter anderem an der ISO/IEC Standard-Reihe 27001, aber auch zunehmend an Kriterien zur Evaluierung von IT-Sicherheit, beispielsweise nach Common Criteria[8]).

Ich sprach in meiner Einleitung von der Entwicklung der Informationstechnologie der letzten 40 Jahre. Die ersten Schadprogramme tauchten bereits in den frühen 1970er Jahren auf: „Creeper“[9] gilt als einer der ersten Viren. Er „infizierte“ 1971 die DEC[10] Rechner des Arpanet (Advanced Research Projects Agency Network des amerikanischen Verteidigungsministeriums) und zeigte auf den infizierten Rechnern die Meldung „I'm The Creeper: CATCH ME IF YOU CAN.“ Der erste von den Medien beachtete Wurm war der „I-LOVE-YOU-Loveletter“, der sich am 4. Mai 2000 explosionsartig per E-Mail verbreitete. Es war eine eMail mit der Betreffzeile „I LOVE YOU“. Im Anhang dieser eMail war dann der Wurm beigefügt. Wer diese email von einem Bekannten bekam und sie mit einem Mausklick vertrauensvoll öffnete, der aktivierte unbewußt und automatisch das Schadprogramm[11]. Der Wurm verursachte weltweit Schäden in Milliardenhöhe. Der jüngste Angriff, der Medieninteresse erwecktete ging vom Virus *stuxnet*[12]*aus. stuxnet* hat gezeigt dass auch Steuerungssysteme, z.B. in Fertigungsanlagen oder Kraftwerken, das Ziel von Angriffen sein können. Bemerkenswert ist hier, das der Virius speziell für die dort eingesetzten SCADA[13]-Systeme geschrieben wurde. Dazu sind allerdings spezielle Kenntnisse der Steuerungssysteme Voraussetzung. Aufgrund der Komplexität dieser Systeme muss sehr viel Geld in hard- und softwaretechnische Ressourcen mit kriminellem Impetus invistiert worden sein, um solch einen Virus zu entwickeln und gezielt zu platzieren[14].

Einerseits erkennen wir mehr und mehr, wie empfindlich, wie angreifbar unsere IT-Infrastrukturen sind, andererseits fehlen uns hinlängliche Informationen, um Gefahren frühzeitig zu erkennen und ablocken zu können.

Ich werde nun vier Thesen aufstellen, die die heutige Situation und Entwicklung in der Informations-gesellschaft beschreiben. Daraus werden Handlungsempfehlungen für mehr IT-Sicherheit in der IT-Nutzung abgeleitet:

Thesen

These 1: Der Mensch wird zum Sklaven der Informationstechnologie

Die Telekommunikationsbranche und die ihr zugeordneten Technologien erlauben uns heute an jedem Ort und zu jeder Zeit – vorausgesetzt technisch verfügbar – sowohl im Privat- als auch im Berufsleben zu kommunizieren.

---

[8] www.commoncriteriaportal.org

[9] http://malware.wikia.com/wiki/Creeper_virus, Creeper (dt. "Schleicher, Unfugtreiber") ist eine von Steve Ditko (u.a. Spiderman) entworfene Comic-Figur. Auf den Bildschirmen infizierter Rechner erschien der Text „I am the Creeper – catch me if you can“

[10] Digital Equipment Corporation, 1998 von Compaq übernommen und gehört seit 2002, zu Hewlett-Packard.

[11] http://de.wikipedia.org/wiki/Loveletter Der Wurm löschte auf infizierten Rechnern alle Dateien mit bestimmten Dateiendungen und versandte sich automatisch weiter. Auf Grund seiner exponentiellen Verbreitung hat er in den ersten Stunden viele Mailserver überlastet.

[12] http://de.wikipedia.org/wiki/Stuxnet

[13] http://de.wikipedia.org/wiki/Supervisory_Control_and_Data_Acquisition

[14] Es wird spekuliert, dass *stuxnet* mit dem Ziel geschrieben wurde, die Leittechnik einer Anlage zur Uran-Anreicherung im Iran zu sabotieren.

Schüler kommunizieren per SMS. Wer als Schüler nicht Mitglied eines internetbasierten sozialen Netzwerkes ist, wird oder fühlt sich zumindest ausgegrenzt; das ist ähnlich der Subkultur, welche sich auf das Tragen von Markenkleidung gründet: sozialer Druck entsteht. Vom Berufstätigen wird erwartet, dass er jederzeit telefonisch erreichbar ist, es wird erwartet, dass eMails sofort gelesen und beantwortet werden. Damit verwischen die Grenzen von Berufs- und Privatsphäre: „das Rad dreht sich schneller". Wer sich beruflich nicht anpasst, ist „out".

Jedoch: Weltweit betrachtet partizipiert nur ein Teil der Weltbevölkerung an diesen Entwicklungen. Man spricht hier von „Digitaler Kluft" oder „Digitaler Spaltung"[15], denn der Zugang zum Internet und anderen digitalen Kommunikationstechnologien ist in der Welt ungleich verteilt und hängt stark von sozialen Faktoren ab.

Die Informationstechnologie erleichtert uns vieles und das Internet hilft uns, Aufgaben des täglichen Lebens schneller zu bewältigen. Aber was bedeutet das für unser Gehirn? Aus der Hirnforschung weiss man, dass sich bei jeder Benutzung unser Gehirn verändert. Neuere Untersuchungen zeigen: Viel „Surfen" schwächt die Kommandozentrale im Gehirn: in Studien wurde die Verminderung von Empathie und Intelligenz nachgewiesen. Martin Korte, Neurobiologie an der TU Braunschweig fasst das so zusammen: „Mit Multitasking droht die Verwahrlosung unseres Stirnlappens".[16]

Im Sinne der Weizenbaum'schen Kriktik führt dies zu folgender

Handlungsempfehlung: Wir müssen uns kritisch mit dem Einsatz der Computertechnik auseinandersetzen, dieser nicht blindlings vertrauen und uns nicht zum Sklaven dieser Technologie machen lassen. Es ist unsere Verantwortung den Technikeinsatz diesbezüglich zu gestalten.

Das mag trivial klingen, aber die Umsetzung in die Praxis ist schwierig und aufwändig, denn es geht um Transparenz, staatliche Interessen und teilweise gegensätzliche Wirtschaftsinteressen, Ausbildung von Schülern und Studenten sowie menschliches Verhalten. Ich werde später auf die Umsetzung dieser Handlungsempfehlung zurückkommen. Zunächst möchte ich die Frage, wie sich unsere Gesellschaft durch den Einsatz dieser Informationstechnologie weiter entwickeln kann, erörtern und stelle folgende These auf:

These 2: Das Internet ist eine neue Evolutionsstufe unserer Gesellschaft und IT-Sicherheit ist darin eine neue Herausforderung.

Die neuen Computer-Technologien und deren Implementierungen in verschiedenen Branchen haben unser Wirtschafts- und Gesellschaftsleben bereits heute verändert. Logistik, berufliche Mobilität oder Videokonferenzen sind einige Beispiele. Viele Beschränkungen sind aufgehoben. (Nur wenn gelegentlich ein Vulkan ausbricht[17] oder im Winter Schnee und Eis den Verkehr behindern, erkennen wir noch unsere Grenzen).

Das Internet ist nicht einfach nur eine technologische Neuerung, vergleichbar mit der Erfindung der Glühbirne oder der Dampfmaschine zuvor, vielmehr zieht es gesellschaftliche Veränderungen in globaler Dimension nach sich. Weltweite „Vergleichzeitigung" ermöglicht, ja erfordert neue Sozialisationen. Ich werde das an einigen Beispielen erläutern.

---

[15] http://de.wikipedia.org/wiki/Digitale_Kluft

[16] http://www.faz.net/s/RubC3FFBF288EDC421F93E22EFA74003C4D/Doc~ED6B19C9DFE0E424E8C7968156BD568FF~ATpl~Ecommon~Scontent.html

[17] http://www.spiegel.de/reise/aktuell/0,1518,689125,00.html

Beispiel *soziale Netzwerke*:
Wie eingangs erwähnt, ist es heute für viele Jugendliche ein Muss, Mitglied einer sozialen Plattform zu sein. Der Begriff „Freund" bezeichnet ursprünglich einen sehr nahestehenden Mensch, Partner, Gefährten oder Verbündeten. Es ist erstaunlich, wie gedankenlos Menschen heute private Informationen in *facebook* oder *twitter* ihren sogenannten Freunden geben. „Freund" wird damit, weil inflationär benutzt, vollkommen entwertet. Es kommt nur noch darauf an, wieviele sogenannte Freunde ich habe und welchen „Freund" meine „Freunde" haben. Niemals hätten die selben Menschen vor 15 Jahren solche Informationen weitergeben. Und gerade im Hinblick auf *twitter*[18] frage ich mich: wen interessiert es? Vergessen wird dabei, dass mittlerweile Personalchefs sich solche Plattformen anschauen, um sich ein Bild über Bewerber zu machen. Vergessen wird auch, dass das Internet keine Löschfunktion hat, und somit eine einmal veröffentlichte Informationen das ganze zukünftige Leben, im Besonderen das berufliche Leben beeinflusst.

Was ist nun neu an *facebook*, wenn ich sage, es ist mehr als der Einsatz einer neuen Technologie? Mark Zuckerberg, Gründer von facebook, hat Anfang 2010 gesagt: „The Age of Privacy is Over"[19]. Dies widerspricht dem Verständnis meiner Generation, die mit dem Volkszählungsurteil 1983[20] groß geworden ist. Zudem ist in der Charta der Grundrechte der Europäischen Union nach dem Lissabon-Vertrag von 2009 die Privatsphäre explizit geschützt[21]. Aber: die Gesellschaft verändert sich: Sind wir es, die die Jugend mahnen soll, verantwortungsvoll mit ihren privaten Daten umzugehen? Oder hat Zuckerberg recht, und unsere Gesellschaft kennt in der Zukunft keine Privatsphäre mehr?

Beispiel *Cloud Computing*:
„Cloud Computing" ist seit gut einem Jahr in aller Munde, es ist ein sogenannter Hype. Es handelt sich um eine neues Geschäftsmodell, quasi ein erweitertes Outsourcing Modell, in dem IT-Unternehmen Dienstleistungen, engl. Services, für Regierungen, Unternehmen und Bürger weltweit skalierbar zur Verfügung stellen. Alle Anwendungen und Daten sind im Internet (irgendwo auf der Welt), „in der Cloud", verfügbar. Da wir das Internet gerne als Wolke zeichnen, ist hierfür der Begriff Cloud Computing entstanden. Der Cloud Computing Provider kann seine Dienstleistungen heute auf verschiedene Standorte auf verschiedenen Kontinenten verteilen, was für den Kunden zu einer Intransparenz führt. Damit entstehen aber Fragen, die zum großen Teil noch unbeantwortet sind, z.B.:

- Über welche Wege (Leitungen) werden meine Daten transportiert?
- An welchen Orten sind meine Daten gespeichert?
- Wie kann ich meine Daten vor unbefugtem Zugriff schützen?
- Welche juristischen Rahmenbedingungen und allgemeinen Geschäftsbedingungen gelten, beziehungsweise: wie kann ich meine Interessen weltweit durchsetzen

ENISA hat hierzu eine Reihe von Positionspapieren und Empfehlungen veröffentlicht[22] und seit 2010 arbeitet ENISA mit dem Lehrstuhl von Frau Prof. Dreo Rodosek zum Thema Cloud Computing zusammen.[23]

---

[18] http://twitter.com/:"*Twitter* is without a doubt the best way to share and discover what is happening right now:
[19] http://www.youtube.com/watch?v=Z6TpmMdvSPM
[20] http://de.wikipedia.org/wiki/Volksz%C3%A4hlungsurteil
[21] http://www.europarl.europa.eu/charter/pdf/text_de.pdf:
Artikel 7: „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation."
Artikel 8 (1):„Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten."
[22] http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Alle neuen Geschäftsmodelle im Internet stammen überwiegend von amerikanischen Unternehmen, z.B.: ebay, amazon, google, facebook und auch die „alten global player“ wie IBM, HP, Microsoft stellen Ihre Geschäftsmodell auf das Internet um. Lesenswert ist in diesem Zusammenhang das Buch „Free“ von Chris Anderson[24]. Er beschäftigt sich mit der Frage, warum man im Internet mit kostenlosen Diensten Geld verdienen kann. Er zeigt, dass es dazu weltweit nur wenig zahlender Kunden bedarf. Damit würden die Grenzkosten gegen Null gehen.

Beispiel *WikiLeaks*:
Julian Assange, Gründer von WikiLeaks sagt auf seiner Internet-Seite „keep governments open“. Hier geht darum, wie sich diese Art von Journalismus weiterentwickelt. Setzt Wikileaks nur die Tradition des kritischen Journalismus fort. Geht es nur um die Transparenz von Regierungen? Oder wird es eine neue Art und Weise damit auch eigene politische Interessen durchzusetzen? Letzlich geht es um die Frage, sollen im Internet alle Informationen öffentlich verfügbar sein? Was bedeuten dann Privatsphäre, staatlicher Geheimschutz, Patente, Vertraulichkeit für uns, den Nutzer?

Diese Beispiele zeigen die neuen auf uns zukommenden Herausforderungen.

These 3: Es fehlt eine Sozialisation der Benutzer des Internets!

Vielen von Ihnen werden sich noch erinnern, wie Polizisten in die Schulen kamen um uns die Verkehrsregeln zu erläutern. Ich habe als Jugendlicher eine „Fahrradprüfung“ unter Aufsicht eines Polizisten auf dem Schulhof absolviert. Nach Bestehen der Prüfung bekam ich einen Ausweis!

Es ist für uns selbstverstandlich, dass wir, wenn wir das Haus oder die Wohnung verlassen, die Tür abschliessen. Machen Sie das gleiche mit Ihrem Computer/PC? In den meisten Fällen nein.

Ihr Auto waschen und pflegen Sie und Sie bringen es regelmäßig zur Inspektion in die Werkstatt. Führen Sie in gleicher Art und Weise updates auf Ihrem Computer/PC durch? Das heißt Update des Betriebssystems, der Textverarbeitung und anderer Anwendungen? In den meisten Fällen nein.

Damit ist Ihr Computer/PC „verkehrsunsicher“ und wird – ohne das Sie es merken! – kompromittiert. Vorhandene Schwachstellen werden von Kriminellen ausgenutzt.

An dieser Stelle erlaube ich mir eine kritische Bemerkung: Die Softwareindustrie hat es offensichtlich geschafft, den Begriff Fehler durch Schwachstelle zu ersetzen. Der englische Begriff „bug“25, zu deutsch „Insekt, Laus“ zeigt zumindest den Humor amerikanischer Software-Entwickler26, und die Fehlersuche heißt dann auch „de-bugging“ = „entlausen“. Und im Deutschen sprechen wir von Schwachstellen. Übrigens, im Maschinenbau gibt es machmal eine vorgesehene Schwachstelle, die man Sollbruchstelle nennt. Das gibt es auch in der Software: in der Krpytographie, d.h. wenn es um das Verschlüsseln und Entschlüsseln mittels Software geht, nennt man so etwas „Backdoor“, zu Deutsch „Hintertür.“, eine Möglichkeit, die Authentifizierung zu umgehen oder die Entschlüsselung zu vereinfachen.

Weitere Beispiele sind: Wenn wir eine offen stehende Haustür sehen, sind wir so sozialisiert, dass wir das Haus nicht betreten, wir respektieren fremdes Eigentum. Aber was tun wir im Internet?

---

[23] …lingk Vortrag Gabi Summerschool, Promotion Kretzschmar

[24] Chris Anderson, Free-Kostenlos, Geschäftsmodelle fuer die Herausforderungen des Internetsd, Campus Verlag, Frankfurt/NewYork

[25] http://www.focus.de/digital/videos/computergeschichte-der-allererste-computer-bug_vid_22091.html

[26] Häufig wird der Begriff *debugging* auf Grace Hopper zurückgeführt. 1947 hatte eine Motte für den Ausfall eines Relais im Mark II Computers der Harvard University gesorgt. http://de.wikipedia.org/wiki/Grace_Hopper

Wenn wir einen nicht gesicherten WLAN-Hotspot (=offene Haustür) finden, wird hemmungslos auf Kosten anderer gesurft.

Sie würden niemals in einer Großstadt nachts durch einen dunklen Park oder ein heruntergekommenes Viertel gehen. Aber im Internet wird schon in fahrlässigerweise auf jeden „link" geklickt. Meine Anregung ist, eine wöchentliche Sendung analog „Der 7.Sinn"[27] auch für die Computer-Sicherheit einzuführen. Ich begrüße daher ausdrücklich Initiativen wie „Deutschland sicher im Netz (DsiN)[28] und den - Europäischen Computer Führerschein (ECDL[29]).

Handlungsempfehlung: Die Bewusstseinsbildung und Bewusstseinsförderung von IT-Sicherheit muss flächendeckend in die Kurrikula der schulischen und der universitären Ausbildung einfließen.

Lassen Sie mich nun zur vierten und letzten These kommen:

These 4: IT-Sicherheit ist im Allgemeinen **KEIN** Geschäftsmodell!

Natürlich ist IT-Sicherheit ein Geschäftsmodell für die Firmen, die mit Virenschutzprogrammen, Firewalls oder Verschlüsselungs-Software Geld verdienen. Diese Firmen sind hier aber nicht gemeint.

Wenn wir uns die Entwicklung der Computertechnologie der letzten Jahrzehnte vor Augen führen, ging es im wesentlichen immer um schnellere Prozessoren, größeren Speicher, konstante oder sinkende Preise bei gleichzeitiger Leistungssteigerung. Und die Titelseiten der PC-Zeitschriften reflektieren dies. Unsere Mobiltelefone werden zu sog. PDAs (Personal Digital assistant): das Schreiben und Lesen von sms, emails, online-Bordkarten, Internet-Surfen steht im Vordergrund, Sprach-Telefonie wird zur Nebensache. Diese Geräte sind heute leistungsfähiger als die PCs in den 80er Jahren. Und die IT-Sicherheit? Der Wettbewerbsdruck und die Schnelligkeit der technologischen Entwicklung lassen dafür wohl leider keine Zeit. Wir müssen heute paradoxerweise auch auf den Handys Firewalls und Virenschutz als Nutzer selbst installieren. Da fragt man sich schon: „lernt die Industrie nichts dazu?" Andererseits ist es verständlich, dass ein Unternehmen nur in IT-Sicherheit investiert, wenn der ROI (Return on Investment) positiv ist. Gleiches gilt für andere Branchen, ein Beispiel: Wenn Bank A von Ihnen x% für einen Kredit verlangt und Bank B in IT-Sicherheit investiert, dafür aber (x+Δ)% für denselben Kredit verlangt, was meinen Sie, wohin werden die meisten Kunden heute noch gehen? In der Automobil- oder Versicherungsbranche ist das völlig anders. Es gibt gesetzliche Regelungen für z.B. den Sicherheitsgurt oder freiwillig eingebaute Airbags die Wettbewerbsvorteile sind. Der ADAC veröffentlicht beispielsweise die Ergebnisse von Crashtests und berichtet über Sicherheitsmängel in Autos. Ähnliches benötigen wir auch in unserer Branche.

Fazit: heute werden Investitionen in IT-Sicherheit aus betriebswirtschaftlicher Sicht nicht belohnt.

[27] „Der 7. Sinn" war eine Fernsehsendung zur Verkehrssicherheit, die von 1966 bis 2005 ausgestrahlt wurde. http://de.wikipedia.org/wiki/Der_7._Sinn

[28] https://www.sicher-im-netz.de

[29] ECDL = European Computer Driving Licence, www.ecdl.de

Darüberhinaus werden wir unsere privaten Daten auf unseren Computern nur dann gegen Kriminelle schützen könne, wenn wir in IT-Sicherheit investieren. Dies bedeutet aber auch, dass IT-Sicherheit früh im Softwareentwicklungsprozess berücksichtigt werden muss.

Handlungsempfehlung: Die Industrie muss Ihren Softwareentwicklungsprozess so definieren, dass IT-Sicherheit ein Designkriterium ist: „IT-Security by Design".
Geschäftsprozesse müssen die Investition in IT-Sicherheit belohnen.

Taxonomie

In den genannten Beispielen haben wir es immer mit derselben Technologie und Plattform – dem Internet – zu tun. Nutzen und Missbrauch der Informationstechnologie liegen dabei nahe beieinander. Leider wird in der fachlichen und öffentlichen Diskussion mit Schlagwörtern gearbeitet. Die Begriffsdefinitionen sind nicht klar und hängen vom Autor und Kontext ab. Wenn wir über Krieg sprechen, beziehen wir uns auf das Militär und wir bekommen militärische Lösungen: Sind die Bedrohungen krimineller Natur, bekommen wir polizeiliche Lösungen. Wie wir über das Thema IT-Sicherheit reden und wie die Schlagzeilen dazu aussehen, beeinflusst, welche Lösungen wir bekommen. Zusätzlich verwässern Anglizismen die Inhalte. Aus meiner Sicht ergibt sich folgende Klassifizierung:

A. Computerkriminalität (engl. Cyber Crime):

   Die Kriminalität hat im Internet ein neues Ausmaß. Im klassischen Verbrechen muss sich der Täter an den Tatort begeben. Beim Banküberfall muss er die Bank betreten. Im Internet sind ab er Ort und Zeitpunkt des Verbrechens unabhängig. Ich kann beim *phishing* illegaler Weise prinzipiell von einem beliebigen Ort auf der Welt aus das Bankkonto an einem beliebigen anderen Ort der Welt zu jedem Zeitpunkt ausrauben. Das bedeutet insbesondere, dass ich mich in unterschiedlichen Rechtssytemen befinde. Es kann für die Strafverfolgungsbehörden des Staates A unmöglich werden, einen Kriminellen im Staat B verhaften zu lassen
   Damit kann das organisierte Verbrechen seine illegalen Machenschaften beliebig skalieren.

B. Computerspionage (engl. Cyber Espionage):

   Spionage gibt es seit jeher, und es wird sie wohl auch weiterhin geben, so lange es nationalstaatliche Interessen und Nachrichtendienste gibt.
   Während man sich allerdings in der Vergangenheit als Spion in die Gefahr begeben musste, am Tatort enttarnt zu werden, kann man heute aus der Ferne ungesehen mittels sogenannter Trojaner spionieren. Auch muss man nicht mehr stundenlang geheime Akten fotografieren oder kopieren, ein einfacher USB-Stick oder eine CD genügt.

C. Computerunterstützte Kriegsfürung (engl. Cyber Warfare):

   Hier entsteht ein neues Feld asymmetrischer Kriegsführung. In der Vergangenheit standen sich Truppen gegnerischer Staaten gegenüber. Die Genfer Konvention[30] beschreibt z.B. Regeln für den Schutz von Personen, die nicht an den Kampfhandlungen teilnehmen.

   Terroristische Vereinigungen haben das Ziel, durch Handlungen, die unter rechtsstaatlichen Voraussetzungen als Straftaten bewertet werden, vor allem politische Ziele zu erreichen.

[30] http://de.wikipedia.org/wiki/Genfer_Konventionen

Mit der Internet-Technologie ist es möglich, Angriffe auf Infrastrukturen, sogenannte kritische Infrastrukturen[31], eines Staates als Einzelperson oder Gruppe mit oder ohne staatliche Duldung durchzuführen. Damit verwischt die Grenze zwischen Soldat, Terrorist und Kriminellem.

Folgende Beispiele zeigen, dass dabei die Grenzen verschwimmen: 2007 wurden Server der estnischen Regierung von Russland aus „angegriffen", d.h. per Distributed Denial-of-Service-Attack [32] (DDoS) lahmgelegt. Hintergrund war, dass die estnische Regierung ein Denkmal aus dem Zentrum der Stadt entfernte, was zu heftigen Protesten der in Estland lebenden russischen Bevölkerung geführt hatte. 2008 soll Russland DDoS-Angriffe auf die Internetseiten der georgischen Regierung ausgeführt haben. Viele georgische Server befanden sich unter fremder Kontrolle und Websites der georgischen Behörden sollen teilweise blockiert worden sein. Estland 2007 und der Georgien Konflikt 2008[33] sind noch keine computerunterstützte Kriegsführung, zeigen aber das Potential für mögliche zukünftige Konflikte.

Schlussfolgerungen

Lassen Sie mich meine Thesen zusammenfassen:

1. Der Mensch wird Skalve der Informationstechnolige
2. Das Internet ist eine neue Evolutionsstufe des Menschen und IT-Sicherheit ist darin eine neue Herausforderung.
3. Es fehlt eine Sozialisation der Benutzer des Internets
4. IT-Sicherheit ist im Allgemeinen KEIN Geschäftsmodell!

Als Weizenbaum 1972 von einer *schweren geistigen Krise* sprach bezog er sich auf die zukünftigen Einsatzmöglichkeiten von Computern und die Naivität von Nutzern und Entscheidungsträgern mit dessen Umgang.[34]

Heute setzen wir Computerprogramme an den Börsen ein und überlassen es Maschinen (=Software) zu entscheiden ob Aktien gekauft oder verkauft werden. Der „kleine Börsencrash" im Mai 2010[35] hat die negativen Auswirkungen deutlich gezeigt.

Mit dem Einsatz von Computern in einer vernetzten Welt haben wir eine neue Büchse der Pandora[36] geöffnet. Technische Entwicklungen sind nicht umkehrbar.

Den technischen Bedrohungen können wir mit technischen und organisatorischen Massnahmen begegnen[37].

Darüber hinaus müssen wir einem globalen gesellschaftlichen Diskurs führen und einen Konsenz einer globalen Internetgesellschaft finden. Es geht nicht darum, was wir in Deutschland oder Europa gerne hätten – das Internet endet nicht an Landesgrenzen - es geht um die Frage, was weltweit erreichbar ist!

---

[31] http://de.wikipedia.org/wiki/Kritische_Infrastrukturen
[32] http://de.wikipedia.org/wiki/Denial_of_Service
[33] http://de.wikipedia.org/wiki/Kaukasuskrieg_2008
[34] Seinerzeit auch aufgund des Hypes um die Künstliche Intelligenz
[35] http://www.pressemitteilungen-online.de/index.php/boersencrash-an-wall-street-durch-tippfehler-verursacht/ http://www.pressemitteilungen-online.de/index.php/automatisierter-wertpapierhandel-birgt-erhebliche-risiken-fuer-die-finanzmaerkte/
[36] http://de.wikipedia.org/wiki/B%C3%BCchse_der_Pandora
[37] Technisch z.B. durch Virenschutz-Software, Firewalls, Softwareupdates, orgnisatorisch z.B. durch Vorschriften, Gesetzte, Prüfungen, Bestellung von IT-Scherheitsbeauftragen in Unternehmen.

Protektionismus und Macht garantieren nur beschränkt Einfluss. In der realen Welt sind politische Macht und persönliche Handlungen territorial begrenzt. Rechtssysteme und damit die Sicherheit für die Bürger waren und sind bis heute staatsspezifisch. Imperien konnten Ihre Einflusssphäre zwar ausweiten, aber Reisen, auch militärische Truppenbewegungen und Kommunizieren kosten Zeit. Mit den Möglichkeiten der Telekommunikation, gegen Ende des letzten Jahrhundert insbesondere durch die Mobilkommunikation, können wir zeitgleich kommunizieren.

Mit dem Internet ist aber darüber hinaus eine neue virtuelle Welt entstanden, in der es im Besonderen

1. keine nationalen Grenzen
2. kein einheitliches Rechtssystem
3. ein neues Zahlungsmittel: personenbezogene Daten

gibt. Insbesondere der Wert personenbezogener Daten (3.) ist leider nur den wenigsten Internetnutzern bewusst. Der Einsatz der Computer-Technologie (siehe These 1), die neuen Internet-Geschäftsmodelle (siehe These 2), die fehlende Internet-Sozialisierung (siehe These 3) und die fehlenden monitären Anreizsysteme für IT-Sicherheit (siehe These 4) führen zu den wesentlichen Schlussfolgerungen:

A. Wir müssen die sozialen Regeln und geignete Rechtsnormen in der virtuellen Welt definieren, um- und durchsetzen
   Umkehrschluss: Sonst erreichenen wir keine Sicherheit im Internet.
B. Wir benötigen ein ROSI[38]-Modell
   Umkehrschluss: sonst investieren Unternehmen nicht in IT Sicherheit.

Den technischen Bedrohungen können wir mit technischen und organisatorischen Maßnahmen begegnen. Um den beschriebenen soziologischen Herausforderungen zu begegnen, bedarf es mehr.Daher richtet sich mein Appell

an die Hochschule: IT-Sicherheit in die Kurrikula aufnehmen!
an die Industrie: IT-Sicherheit als Designkriterium spezifizieren!
an die Gesellschaft: Soziales Verhalten im Internet lehren und lernen!

Dank

Bevor ich nun meinen Vortrag schliesse, möchte ich mich für die herzliche Aufnahme am *Institut für technische Informatik* bedanken. Mein Dank geht an Herr Eyermann, Herr Stelte und Herr Kretzschmar. Sie haben mich bei meinen Vorlesungen und Seminaren vorzüglich unterstützt. Mein Dank gilt Frau Prof. Dreo und Herr Prof. Teege nun darf ich sagen, Kollegen, die für meine Fragen immer Zeit hatten. Und auch Herrn Prof. Lehmann danke ich, mit dem ich gemeinsam eine Reihe öffentlicher Veranstaltungen organisiert habe.

Vielen Dank.

[38] ROSI = Return of IT-Security Investment