Kompaktkurs IT und Internet.
Elementares Wissen von Experten für Entscheider

Wie gefährlich ist das Internet?

Ulrich Wolf

Microsoft

Kompaktkurs IT und Internet.
Elementares Wissen von Experten für Entscheider

Wie gefährlich ist das Internet?

Ulrich Wolf

Microsoft

Inhaltsübersicht

Vorwort

Wir leben im digitalen Zeitalter – das bestreitet niemand mehr. Doch was heißt das eigentlich genau? Begriffe wie E-Mail, Cloud Computing und Online-Strategien nehmen wir wie selbstverständlich in den Mund – aber wissen wir auch wirklich, welche komplexen Funktionen und Strukturen sich dahinter verbergen? Bahnbrechende Innovationen, an deren Spitze die Erfindung des Computers und des Internets im 20. Jahrhundert stehen, haben ungeahnte Möglichkeiten, die Revolution von Arbeit und Alltag und zugleich Desorientierung und Unsicherheit hervorgebracht.

Wer heute in Politik, Wirtschaft und Verwaltung Entscheidungsträger ist und verantwortlich handeln und mit Weitblick führen will, muss die Konsequenzen des eigenen Tuns genau abschätzen können. Das setzt voraus, die Zusammenhänge der modernen Informations- und Kommunikationstechnologien zu kennen und zu wissen, wie sie effizient und passgenau für die jeweiligen Anforderungen einsetzbar sind. Nur so schöpfen wir die Potenziale, die die drahtlose Wissensvermittlung und digitale Datenverarbeitung für Institutionen bietet, voll aus.

Man muss kein Digital Native, kein digitaler Eingeborener sein, um sich die Welt des Online-Wissens zu erschließen. Dennoch hat Microsoft die Erfahrung gemacht, dass Entscheider mit den grundlegenden Fragen zu Internet und IT-Sicherheit oft alleingelassen werden.

Der neue „Kompaktkurs IT und Internet. Elementares Wissen von Experten für Entscheider“ – die erste Folge halten Sie in Händen – soll diese Lücke schließen.

Die in der neuen Microsoft-Reihe erscheinenden Handbücher erklären in einzelnen Bänden die wichtigsten Begriffe und Funktionsweisen der Online-Technologie, von Datenschutz bis Transparenz, von Piraterie bis Start-up. Der Grundkurs stellt ein Bildungsangebot für Sie als Entscheider dar, damit Sie sich sicher im Online-Dschungel bewegen können. Er erläutert konkret und kompakt, was Sie in Ihrer täglichen Arbeit an den Schlüsselstellen von Politik, Wirtschaft oder Verwaltung wissen sollten, und zeigt anschaulich, was die einzelnen Aspekte der IT für Sie konkret bedeuten.

Unsere Autoren sind namhafte Persönlichkeiten und ausgewiesene Experten auf ihrem Gebiet. Die Sammelreihe eröffnet der ehemalige NATO-General Ulrich Wolf. Er widmet sich in diesem Band der Frage: „Wie gefährlich ist das Internet?“ und erläutert, was „Kriminalität, Terror und Führung im digitalen Zeitalter“ bedeuten. Generalleutnant Wolf hat als Direktor der NATO-Agentur für Informationssysteme (NCSA) den Übergang des transatlantischen Bündnisses vom Industrie- zum Informationszeitalter entscheidend mitgestaltet und die digitale Kultur der Organisation geprägt. Er ist ein bekannter und respektierter Experte auf diesem Gebiet, aber er kennt auch die vielen Fragen zum Thema digitale Kriminalität und weiß sie ohne den komplizierten Jargon, der mit Expertentum üblicherweise einhergeht, zu beantworten.

Ulrich Wolf, Jahrgang 1947, trat 1967 in die Bundeswehr als Wehrpflichtiger ein. Seine Laufbahn als Berufsoffizier war geprägt vom Wechsel zwischen Truppe, Stäben und dem Bundesministerium der Verteidigung. Er war Kommandeur auf Bataillons-, Brigade- und Divisionsebene. Er hatte mehrere Verwendungen im Atlantischen Bündnis, zuletzt fünf Jahre als Generalleutnant und Direktor der NATO-Agentur NCSA, verantwortlich für den Betrieb des weltweiten IT- und Informationsnetzes und die Cyber-Verteidigung der Allianz. Wolf ist Diplom-Betriebswirt und Absolvent der deutschen und der US-amerikanischen Generalstabsausbildung. Er ist verheiratet, hat eine Tochter, lebt in Münster, Westfalen, und arbeitet als freier Berater und Autor auf dem Gebiet der IT-Sicherheit und Cyber Defense.

Wolf ist überzeugt, dass Informations- und Entscheidungsmacht auf einem zuverlässigen Kommunikationsnetzwerk basieren – nicht nur im militärischen Bereich, sondern auch in politischen Institutionen, in Wirtschaft und Verwaltung. Dabei berge die wachsende Vernetzung zahlreiche neue Herausforderungen. Terror ist nicht allein eine neue Art des Krieges in verschiedenen Brennpunkten der Welt, sondern auch ein Phänomen im Internet, Cyber-Kriminalität eine nicht zu unterschätzende Gefahr, die zerstörerische Wirkungen entfalten und ganze Unternehmen vernichten kann. Eine der wichtigsten Aufgaben für jede Institution ist deshalb, funktionsfähige Sicherheitsstrukturen zu implementieren, die Würmer, Trojaner und andere Viren abwehren und die Informationsinfrastruktur gegen Hacker-Angriffe schützen. Cyber Defense hat mehr als eine militärische Komponente und ist eine gesamtgesellschaftliche Aufgabe.

Diesem zentralen Thema der Gefahrenpotenziale des Internets und der Kriminalitäts- und Terrorabwehr widmet sich das erste Handbuch des Microsoft „Kompaktkurs IT und Internet. Elementares Wissen von Experten für Entscheider“. Ulrich Wolf erläutert in sechs Kapiteln, welche Bedrohungen im Netz lauern, was Cyber War bedeutet und wie man seine Institution, das Unternehmen und die Verwaltung effektiv schützen kann. Denn wer heute erfolgreich sein will, muss Bescheid wissen, verstehen und mitreden können.

Viel Spaß beim Lesen wünscht Ihnen

Henrik Tesch
Direktor Politik und gesellschaftliches Engagement
Microsoft Deutschland
Berlin, im Dezember 2012

Cyber War – neue Formen der Kriegsführung im Netz

Wird heute bei öffentlichen oder privaten Diskussionen oder in den Medien über die Gefahren des Internets gesprochen, ist zu beobachten, dass häufig die entsprechenden Begriffe unterschiedlich gebraucht werden: Internet-Kriminalität, Spionage, Datendiebstahl, Manipulation von Soft- und Hardware, Zerstörungen und Sabotage und der schlimmste Fall eines groß angelegten Angriffs im Rahmen eines Internet-Krieges werden häufig durcheinandergebracht.

Cyber-Krieg

Versuchen wir zunächst, uns dieser relativ neuen Form der Fortsetzung der Politik mit anderen Mitteln mit der traditionellen Definition eines Kriegszustandes zu nähern. Hier helfen vier Fragen:

1. **Der Verursacher:** Ist die Aggression von einem Staat ausgelöst oder unterstützt?
2. **Die Wirkung:** Verursachte der Angriff einen erheblichen Schaden?
3. **Das Motiv:** Liegt dem Angriff eine politische Absicht und Zielsetzung zugrunde?
4. **Die Komplexität:** Ist der Angriff technisch und planerisch so anspruchsvoll, dass er nicht von Laien ohne Weiteres hätte organisiert werden können?

Auch wenn alle vier Fragen positiv beantwortet werden, bleibt das Erkennen der Grenze zwischen Kriminalität und Krieg im Internet schwierig, unter anderem deshalb, weil die Mehrzahl der verwendeten Angriffsmethoden in beiden Fällen gleich ist. Dazu kann oft die Frage nach den am Krieg beteiligten Kombattanten oder Nicht-Kombattanten nicht eindeutig beantwortet werden, weil der Cyber-Anteil einer Aggression auch von Zivilisten und sogar Privatpersonen getragen sein kann.

Entscheidender Schlüssel ist wohl die Qualität der Auswirkungen und ob sie existenzgefährdend für die gesamte oder wesentliche Teile der lebenswichtigen Infrastruktur einer Gesellschaft oder eines Staates sind und ob die Gefahr von menschlichen Opfern besteht.

Kalter Internet-Krieg

Ist der Cyber-Krieg eine reale Gefahr oder nur eine Marketingkampagne der IT-Sicherheitsindustrie? Für uns in entwickelten Industriegesellschaften ist die Antwort eindeutig: Es ist eine rapide wachsende Gefahr. Nahezu jeder Bereich unserer hochentwickelten technischen Infrastruktur ist wesentlich, oft sogar total, von einer funktionierenden, leistungsfähigen IT-Unterstützung abhängig. Auch wenn manche, insbesondere sicherheitsempfindliche Bereiche, nicht mit dem Internet verbunden sind, bedeutet das nicht, dass sie nicht angegriffen werden können.

Leben wir bereits in der Situation eines kalten Cyber-Krieges? Zieht man ein wesentliches Element des Kalten

Krieges zwischen Ost und West vor 1990 in Betracht, nämlich die ständigen Versuche der Opponenten, durch Spionage und Aufklärung die Schwachstellen des anderen in Vorbereitung eines eigenen Angriffs herauszufinden, dann kann man durchaus Parallelen feststellen. In einer Sicherheitsanalyse der NATO wurde bereits 2006 eine Vielzahl von Versuchen aufgedeckt, die Schwachstellen und Eindringmöglichkeiten in die Netzwerke der Allianz herauszufinden. Dabei ist es in den meisten Fällen nicht zum Datendiebstahl gekommen, allerdings wurden teilweise schlafende Schadprogramme hinterlegt, die bei Bedarf aktiviert werden können. Im Militärjargon wird so etwas die Vorbereitung des zukünftigen Schlachtfeldes genannt.

Nun sind elektronische Angriffe im weltweit vielfach vernetzten Internet nicht so einfach auf den angestrebten Zweck hin zu begrenzen. Vor dem Irak-Krieg 2003 erwogen die USA einen Cyber-Angriff auf das irakische Finanzsystem, Saddams Konten, die Gehaltskassen der Streitkräfte und Ähnliches. Man hat jedoch davon abgesehen, weil man nicht beherrschbare negative Auswirkungen auf das Banken- und Finanzsystem der übrigen Welt befürchtete. Heute sind wir fast zehn Jahre weiter. Die Techno-Waffensysteme sind verfeinert und die Gefahr von Kollateralschäden verringert. Das erhöht die Gefährdung des Angegriffenen.

Internet-Bürgerkrieg

Eine Grauzone ist die Rolle des Internets in bürgerkriegsähnlichen Situationen wie jüngst in Nordafrika.

Soziale Netzwerke haben hier wohl eine wichtige Rolle im Kampf um die Informationshoheit gespielt. Ohne Twitter und Facebook hätte die aufständische Bevölkerung weder ihre Sicht der Vorgänge im Land weltweit verbreiten noch sich wirksam und rasch organisieren können. Interessant ist hierbei, dass es sich um IT-Firmen des Westens handelt, die diese Netzwerke betreiben. Twitter wollte 2011 aus technischen Gründen weltweit die Zahl der Beiträge je Nutzer und Tag einschränken. Die US-Regierung hat ihren Einfluss geltend gemacht, während der Krise in Libyen davon abzusehen. Ein eher mediokrer Aspekt des Propagandakrieges in solchen Konflikten. Auch die diktatorischen Regierungen versuchen, mit Netzabschaltungen, Desinformationen und physischer Gewalt den Informationskrieg für sich zu entscheiden. Es bleibt jedoch festzuhalten, dass das Internet, dank seiner komplexen technischen Struktur, der Seite der Freiheitlichen Vorteile bietet.

Datendiebstahl, Erpressung und Sabotage

Die Dimension und Variantenvielfalt dieser rasant zunehmenden Gefahr aus dem Internet wird am besten an ein paar Beispielen deutlich.

Der wohl erste Fall von Cyber-Kriminalität ereignete sich 1970 in New York, als ein Angestellter der Unions Dim Savings Bank über längere Zeit Kundenbelege im Zentralrechner des Geldinstitutes nach unten korrigierte und das so entstandene virtuelle Geld über mehrere weitere und verschleiernde Transaktionen für sich selbst nutzbar machte. Leider litt er unter

Spielsucht, und es fiel bei der Routineüberprüfung eines Wettbüros auf, dass er bis zu 30 000 Dollar am Tag bei einem Jahreseinkommen von nur 11 000 Dollar gesetzt hatte.

Im Jahr 2000 schaffte es ein gerade mal 15 Jahre alter kanadischer Schüler aus Montreal, Rechner amerikanischer Universitäten zu kapern und so zusammenzuschalten, dass er die Web-Seiten großer Firmen, darunter Dell, Amazon, CNN und andere mit einer solchen Masse an sinnlosen Anfragen überschwemmen konnte, dass sie zeitweise für Kunden nicht mehr erreichbar waren. Der Schaden betrug etwa 1,2 Milliarden Dollar. Auch ihm wurde menschliche Schwäche zum Verhängnis. Seine Prahlerei im Internet unter dem Pseudonym „Mafia Boy" führte die Polizei auf seine Spur.

Ebenfalls im Jahr 2000 ereignete sich ein eher kurioser Fall: Ein russischer Hacker mit dem Decknamen „Maxim" stahl dem CD-Verkäufer cdUniverse 300 000 Kunden-Datensätze einschließlich der Kreditkartennummern. Sein Versuch, die Firma damit um 100 000 Dollar zu erpressen, lief jedoch ins Leere, weil der Internet-Händler sich weigerte zu reagieren. Den Kunden sicherte er zu, für etwaige Schäden aufzukommen. Auch die Veröffentlichung von 25 000 Kreditkartennummern auf der Web-Seite des Hackers konnte cdUniverse zu keiner Reaktion bewegen. „Maxim" stellte daraufhin keine weiteren Forderungen mehr.

Erheblich folgenschwerer für das Ansehen eines großen japanischen Elektronikkonzerns war der Diebstahl der ungeheuerlichen Zahl von 100 Millionen Kundendaten

im April 2011. Und es kam noch schlimmer: Ein halbes Jahr später gelangte eine andere Hacker-Gruppe nochmals an mehr als eine Million Datensätze. Der Schaden hat sich bisher auf 1,2 Milliarden Euro summiert.

Industriespionage

Sie ist eine der am schnellsten wachsenden Arten der Internet-Kriminalität. Hier geht es weniger um den direkten finanziellen Gewinn als vielmehr um den Zugriff auf Informationen, die einem Konkurrenten am Markt Vorteile gegenüber dem eigenen Unternehmen oder einer ganzen Branche, vielleicht sogar der Wirtschaft eines Staates bringen können. Sie ist durch die zunehmende Abhängigkeit von der IT-Unterstützung, insbesondere der technologisch anspruchsvollen Unternehmen und deren oft weltweiter Vernetzung nicht nur des Vertriebs, sondern auch der Forschung und Entwicklung, besonders lohnend. Bevorzugte Ziele sind auf der Ebene von Branchen und Staat die Grundlagenforschung, nicht nur in der Industrie, sondern vor allem in Universitäten und wissenschaftlichen Instituten. Auf der Unternehmensebene sind es die Produktentwicklung, die Herstellungsverfahren, die Investitionsplanung und alle Bereiche, in denen Innovationen kreiert werden.

Industriespionage ist kein neues Phänomen. Die Natur der IT-Unterstützung bietet jedoch eine Fülle von neuen, zum Teil recht einfachen Eindringmöglichkeiten. Darüber hinaus sind der Ertrag und die Qualität der erbeuteten Daten oft wesentlich höher als bei den überkommenen Spionagemethoden. Die mühsam von

einem bestochenen Angestellten mit einer MINOX-Kamera illegal abfotografierten Konstruktionsunterlagen waren meist um ein Vielfaches teurer für den Auftraggeber, aber in ihrem Nutzen überhaupt nicht vergleichbar mit dem über das Netz abgegriffenen kompletten Datenbestand der Entwicklungsabteilung.

Es ist schwer, den Schaden durch Industriespionage zu beziffern, weil er sich meist nur indirekt durch Verlust an Marktanteilen oder Erstarken der Konkurrenz manifestiert. Deswegen sind die in den Medien von Experten genannten Zahlen, die allein für Deutschland bis zu mehreren Milliarden pro Jahr reichen, zwar sicherlich nicht unrealistisch, aber für die Beurteilung der Gefahr durch die Führung eines Unternehmens eher wenig relevant. Diese sollte sich jedoch darüber im Klaren sein, dass die Daten, die das Alleinstellungsmerkmal einer Firma darstellen, über Nacht verloren gehen können, wenn sie nicht für ausreichende Sicherheit im IT-Bereich gesorgt hat.

Diebstahl, Betrug und Abzocke von Privatpersonen

Banken reden verständlicherweise nicht gern darüber. Anwälte verdienen gut daran. Es passiert tausendfach jeden Tag, und schuld daran sind wir selbst.

Wenn Kreditkartendaten gestohlen und Bankkonten abgeräumt werden, überteuerte Verträge abgeschlossen, Fantasie-Lotterien ohne reale Preise, aber zu überhöhten Gebühren Absatz finden, dann liegt das an einer weitverbreiteten Haltung, die uns das Internet in den vergangenen zwei Jahrzehnten beigebracht hat:

Wir haben uns daran gewöhnt, alles immer überall und sofort zu bekommen, was uns das Internet bieten kann. Gepaart mit Sorglosigkeit und Neugierde, veranlasst uns das dazu, die Frage vor einem Kaufabschluss, ob man die Geschäftsbedingungen gelesen habe, bereits nach spätestens drei Zeilen wegzuklicken. 75 Prozent der User öffnen eine ungewöhnliche, aber interessant formulierte E-Mail und klicken auf einen darin enthaltenen Link, obwohl die meisten wissen, dass man damit Gefahr läuft, Opfer von Datendieben zu werden. Bei Internet-Auktionshäusern werden immer noch leere Verpackungen zum Preis des nicht vorhandenen Inhalts ersteigert, weil man die Beschreibung im Angebot nicht sorgfältig gelesen hat.

Was macht eigentlich das Paket mit den persönlichen Daten, die wir bei der Nutzung des Internets kontinuierlich preisgeben, so interessant? Ganz einfach: Man kann es verkaufen. Ein häufig von einer bestimmten Person genutzter Dienst im Internet generiert einen „Power-User-Datensatz", der der Werbewirtschaft bis zu 50 Euro wert sein kann.

Angriffstechniken

Wie funktioniert eigentlich so ein Internet-Angriff? Das hängt von der Zielsetzung ab. Nehmen wir an, es soll eine bestimmte Internet-Seite für einen bestimmten Zeitraum unerreichbar gemacht werden. Oft steht dahinter eine politische oder ideologisch untermauerte Absicht. Ein Beispiel war der Angriff der Hacker-Organisation Anonymous auf eine Web-Seite der katholischen Kirche, die eigens zur Vorbereitung des Papstbesuchs in Spanien im August 2011 eingerichtet war. Anonymous war der Ansicht, dass angesichts der Wirtschaftskrise in Spanien 50 Millionen Euro für den Papstbesuch Verschwendung seien und der Papst die sexuellen Verbrechen in der katholischen Kirche gedeckt habe.

Die Netzkampagne dauerte etwa einen Monat. In einer ersten Phase wurden über soziale Netzwerke wie YouTube und Facebook Unterstützer rekrutiert. Mit deren Hilfe wurde dann das Netzwerk der katholischen Kirche in Spanien auf Schwachstellen untersucht, um ein Eindringen und Abgreifen von Daten zu ermöglichen. Wäre das gelungen, hätte man brisante Informationen veröffentlichen und vielleicht einen Skandal kreieren können. Da das in unserem Beispiel nicht gelang, hat man in einer dritten Phase Mitstreiter für den Aufbau einer Rechnerarmee angeworben, die die betreffende Web-Seite durch die Bombardierung mit einer Unzahl von Anfragen zum Einsturz bringen sollte.

In der Fachsprache heißt das Distributed Denial of Service Attack (DDoS)[1]. Dies gelang auch für einige Zeit; die Papstbesuchseite war für mehrere Stunden nicht erreichbar.

In ein fremdes Netz einzudringen, um an Informationen zu gelangen, die aus geschäftlichen, finanziellen, politischen, medialen oder anderen Gründen interessant sind – für dieses Ziel gibt es vielfältige Wege.

Sogenannte Würmer, Viren oder Schadprogramme können auf unterschiedlichste Weise platziert werden. Jeder Zugang aus dem Internet zu einem mit dem internen Netzwerk einer Firma, Behörde oder anderen Organisation verbundenen Computer ist ein potenzielles Tor für den Zugriff von außen. Einmal erfolgreich eingedrungen, nistet sich das Schadprogramm in Speicherbereiche in den Tiefen des Betriebssystems ein und sendet die für den Eindringling interessanten Informationen nach draußen. Einfache Beispiele für kriminell genutzte Schadsoftware sind sogenannte Keylogger (Tastenaufzeichner), die die Tastatur überwachen und die damit eingegebenen Passwörter oder Bankkontoinformationen mitlesen und verschicken.

1 Denial of Service Attacks, auch Botnet Attacks (von: Roboter-Netz) genannt, werden typisch organisiert mit bis zu Hunderttausenden weltweit gekaperten (highjacked) Computern, die unbemerkt von ihren Besitzern für die massenhafte Versendung von Daten zu bestimmten Servern zusammengeschaltet werden, um diese durch Überlastung zum Erliegen zu bringen. So etwas kann man mieten. Mit rapide fallenden Preisen. Was vor fünf Jahren noch 20 000 $ kostete, ist jetzt für unter 1000 $ zu haben.

Der konventionelle und in überraschend häufigen Fällen erfolgreiche Weg ist das sogenannte „Social Engineering“, bei dem Mitarbeiter der angegriffenen Organisation wissentlich oder unwissentlich dazu gebracht werden, den illegalen Zugang zu geschützten Daten zu ermöglichen. Dies kann über gefälschte E-Mails, persönliche Ansprache, Bestechung, Nachlässigkeit bei der Aufbewahrung oder beobachtbare Eingabe von Passwörtern, geschenkte Datenträger mit versteckten Spionageprogrammen und Ähnliches geschehen. Dieser Weg ist auch für Netzwerke, die nicht mit dem Internet verbunden sind, gefährlich. Der sogenannte Wikileaks-Skandal, also der Diebstahl und die Veröffentlichung Tausender zum Teil brisanter Informationen aus dem weltweiten geheimen Diplomatie- und Militärnetzwerk der USA, geschah durch einen Unteroffizier mittels Kopien auf DVD.

Eine weitere Kategorie von Schadsoftware sind Viren und Würmer, die Computer zur Steuerung von technischen Anlagen manipulieren. Das bisher raffinierteste war im Jahr 2010 das sogenannte STUXNET-Virus, mit dem die Drehzahl von Zentrifugen zur Anreicherung von Uran im Iran längere Zeit unbemerkt so verändert wurde, dass sie ihre Funktion nicht mehr erfüllen konnten. Der Wurm wurde von Menschenhand mittels eines USB-Sticks eingeschleust.

Bei einem Kongress einer der großen IT-Sicherheitsfirmen im September 2011 in Las Vegas wurde die ferngesteuerte Manipulation der elektronisch gelenkten Insulinpumpe eines Zuckerkranken demonstriert, die vom Hersteller und von unabhängigen Prüfern als

sicher zertifiziert war. Auf gleiche Weise lassen sich z. B. die elektronisch geleiteten Ölkühler von Transformatoren der Elektrizitätswerke so manipulieren, dass sie überhitzen, wie es bereits vor Jahren bei einem Test in den USA nachgewiesen wurde.

Schaut man sich die Geschichte und Entwicklung der Internet-Angriffe an, dann überrascht zunächst, dass sie nicht weiter als dreißig Jahre zurückreicht. 1983 wurde der Begriff „Computervirus" zum ersten Mal gebraucht. Die ersten weiter verbreiteten Viren wurden 1986 in Pakistan programmiert. Bekannt wurden in den Folgejahren eher relativ harmlose, aber zum Teil weltweit verbreitete Würmer mit so ironisch klingenden Namen wie „Good Times", „Melissa" und „I love you". Das Jahr 2000 erlebte eine erste groß angelegte Denial-of-Service-Attacke auf Yahoo, eBay, Amazon und andere große Internet-Firmen in den USA, die Schaden in Millionenhöhe verursachte. Ab etwa 2001 wurde es Ernst mit wahrscheinlich zum Teil auch von Regierungen veranlassten groß angelegten Angriffen auf Verwaltung, Militär, Wirtschaft und Industrie. In Deutschland wurden die Ausspähversuche in Ministerien und insbesondere im Bundeskanzleramt bekannt, und selbst die NATO meldete erste Fälle, dass Hacker von außen erfolgreich in Netze eingedrungen waren, die mit dem Internet verbunden sind.

Der erste in seiner Dimension und Auswirkung zu Recht als Cyber-Krieg bezeichnete Großangriff auf einen Staat geschah 2007 in Estland. Er war in dreifacher Hinsicht bemerkenswert: Erstens, weil Estland die wohl am weitesten entwickelte Nutzung des

Internets in allen Teilen des Staates, der Wirtschaft und der Gesellschaft in Europa aufweist. Schon lange nutzen dort über 80 Prozent der Bürger Online-Banking, nahezu alle staatlichen Dienste werden über das Internet abgewickelt; selbst wählen kann man über das Netz von zu Hause aus. Zweitens verfügt Estland über vergleichsweise weit vorangetriebene Vorkehrungen zur Sicherung der IT-Infrastruktur, die alle relevanten Bereiche erfassen: Staat, Gesellschaft, Verwaltung, IT-Dienstleister, Wissenschaft, Finanzwelt, Wirtschaft, Industrie, Polizei, Militär und Geheimdienste. Drittens brach, als ein Kriegerdenkmal gegen den Willen der russischen Minderheit aus dem Zentrum der Hauptstadt Tallinn in einen Außenbezirk verlegt wurde, ein Sturm von Internet-Angriffen der verschiedensten Art über das kleine Land herein, den es so vorher noch nicht gegeben hatte. Das Bankensystem war mehrere Tage nahezu lahmgelegt, offizielle Internet-Dienste waren nicht mehr erreichbar, das nationale Internet brach stundenweise zusammen. Einzig der Flugverkehr und die Energieversorgung waren glücklicherweise nicht betroffen.

Estland hat diesen Angriff in bemerkenswert kurzer Zeit in den Griff bekommen. Unter anderem auch mit Unterstützung von IT-Experten der NATO und insbesondere der nationalen und internationalen IT-Industrie.

Wer hinter dem Cyber-Krieg stand, ist umstritten. Russland leugnete eine offizielle Beteiligung, obwohl viele Faktoren zumindest auf eine Koordination von russischem Territorium aus hinwiesen. Es ist jedoch

charakteristisch für den IT-Krieg, dass die Geografie keine entscheidende Rolle mehr spielt. Die für die DDoS-Attacken zusammengeschalteten Tausende von Computern wurden in nahezu allen Teilen der Welt lokalisiert. Eine zweifelsfreie Zuordnung zu bestimmten Tätergruppen ist in solchen Fällen äußerst schwierig.

Heute entstehen durch Internet-Kriminalität und Wirtschaftsspionage Schäden in Milliardenhöhe, die sich seit etwa einer Dekade jährlich verdoppeln. Der Großteil der sicherheitsrelevanten Vorkommnisse wird jedoch nicht publik. Manche bleiben auch in großen Organisationen jahrelang unentdeckt. Niemand möchte in den Verdacht geraten, dass seine Sicherheitssysteme Lücken aufweisen.

Datenschutz und Privatsphäre

Das Internet verändert grundsätzlich unsere überkommene Auffassung von Privatsphäre. Alles, wirklich alles, was wir im Netz tun, bleibt nicht mehr unser persönliches Eigentum. Sobald wir uns einloggen, wird jeder Mausklick, jede Eingabe von Daten, jede Auswahl einer Web-Seite, jede Suchmaschinenanfrage, jeder Kommentar oder jede Meinungsäußerung, jede Bestellung, jede Zahlung, jeder Kontakt registriert und nie mehr vergessen. Davon profitieren diejenigen, die vom Internet leben und damit Geld verdienen. Aber davon profitieren auch die Nutzer, die aufgrund der gespeicherten Daten ganz neue und innovative Dienste im Internet nutzen können. Nun kann man sagen, man hat nichts zu verbergen, deswegen ist es eigentlich egal, was irgendwo gespeichert wird. Anders jedoch könnte das Urteil ausfallen, wenn man weiß, dass der Datensatz eines sogenannten Powerusers des Internets bis zu 50 Euro wert sein kann und damit reger Handel getrieben wird. Das heißt Handel mit individuellen persönlichen Daten.

Eine Umfrage unter mehr als 1000 Internet-Nutzern in Deutschland Anfang 2012 ergab, dass zwar etwa 80 Prozent der Befragten sich als zurückhaltend im Umgang mit sensiblen Daten einstufen, dass bei den über 50-Jährigen fast 90 Prozent vorsichtig bei deren Veröffentlichung sind, bei den 16- bis 29-Jährigen hingegen nur 60 Prozent.[2] Mehr als die Hälfte der befragten Schüler gibt ihre Daten bedenkenlos preis.

2 Innofact AG 7. Februar 2012

Deutschland ist mit 60 Gesetzen, die wesentliche Datenschutzelemente enthalten, Weltmeister auf diesem Gebiet. Der Föderalismus hat noch dazu 16 verschiedene Datenschutzbeauftragte und einen Bundesbeauftragten in Position gebracht. Die Mutter aller Datenschutzregelungen in der Bundesrepublik ist das Volkszählungsurteil des Bundesverfassungsgerichts von 1983[3]. Liest man die gerichtlichen Leitsätze des Urteils, wird deutlich, warum wir uns heute so schwertun, die Rechte des Bürgers auf informationelle Selbstbestimmung den veränderten Bedingungen des Internets anzupassen:

1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung“ sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen

3 BVerfG, Urteil v. 15.12.1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83 (gekürzte Version der gerichtlichen Leitsätze)

Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

3. Bei den verfassungsrechtlichen Anforderungen an derartige Einschränkungen ist zu unterscheiden zwischen personenbezogenen Daten, die in individualisierter, nicht anonymer Form erhoben und verarbeitet werden, und solchen, die für statistische Zwecke bestimmt sind.

1983 gab es noch kein weltweites Internet. Computer waren schrankgroße Ungetüme, die mit Lochkarten gefüttert werden mussten. Apple hatte gerade begonnen, die Welt der Kreativen zu erobern, Bill Gates legte den Grundstein für sein weltweites Software-Unternehmen. Bis die ersten Desktop-Computer mit grünem Bildschirm in größerer Zahl in die Betriebe kamen, dauerte es noch ein paar Jahre.

Die Richtlinien des Volkszählungsurteils waren Regelungen für das Verhältnis zwischen Bürger und Staat. Sie können nicht einfach auf das Verhältnis Nutzer und Dienstanbieter im Internet und nur bedingt auf die digital zunehmend global vernetzte Wirtschaft übertragen werden. Wenn unsere Wirtschaft im weltweiten Wettbewerb bestehen soll, darf sie nicht durch nationale und regionale komplizierte Schutzbestimmungen behindert werden. Was wir brauchen, ist ein möglichst

international gültiger Datenschutzrahmen. Deshalb sollten wir die Europäische Union nutzen, um das nötige Gewicht zur Einflussnahme auf globale Entwicklungen aufzubauen.

Im Artikel 8 der Grundrechte-Charta der EU ist bereits das Recht auf informationelle Selbstbestimmung verankert. Leider hat jedoch die EU-Datenschutzrichtlinie von 1995 zu 27 verschiedenen Umsetzungen in den Mitgliedsstaaten geführt. Das kostet die europäische Wirtschaft etwa 2,3 Milliarden Euro pro Jahr.

Neue Ansätze, wie sie im Entwurfsstadium auf europäischer Ebene gegenwärtig diskutiert werden, sollten jedoch die technische Realität nicht außer Acht lassen. Die Forderung nach einem Recht auf Löschen und Vergessen persönlicher Daten kann im Internet nur unvollkommen erfüllt werden, weil die Spuren eines intensiven Nutzers der digitalen Welt kaum mehr vollständig rekonstruiert und restlos gelöscht werden können. Die Übersetzung dieser Forderung in gesetzliche Datenschutzregeln verursacht immense Kosten für die Dienstanbieter. Die Großen können sich das vielleicht noch leisten. Für kleinere Unternehmen kann das jedoch das Aus bedeuten.

Es muss also um eine neue kreative Balance zwischen Schutz des Individuums und innovationsfördernden Rahmenbedingungen für unsere Wirtschaft gehen, um das Internet als Wachstumstreiber optimal zu nutzen.

Abwehrstrategien

Die Frage, wie man sich gegen die Gefahren des Internets wappnen kann, sollte man differenziert nach Ebenen der Nutzung beantworten. Für einen Überblick mag es genügen, drei Bereiche zu unterscheiden: Nutzer, Organisationen sowie Staat und Gesellschaft.

1. Nutzer

In der Verkehrserziehung gab es bereits in den Sechzigerjahren den Spruch: „Gefahr erkannt, Gefahr gebannt!“ Als erster Schritt zur Gefahrenabwehr in der digitalen Welt ist diese simple Regel immer noch aktuell. Nur wer in etwa weiß, was die negativen Auswirkungen des Internets sein können und wie sie entstehen, versteht auch die Methoden und Instrumente der Abwehr und ist bereit, diese anzuwenden. Das Internet ist zwar technisch wesentlich komplexer als der Straßenverkehr, die Regeln für den individuellen Nutzer zum sicheren Bewegen auf der Datenautobahn sind jedoch weit weniger zahlreich und eigentlich sehr einfach zu befolgen.

Das ist wie Autofahren ohne Gurt. Den Account eines aktiven Nutzers, z.B. im Hotel, zu kapern, ist kinderleicht. Der verantwortungs- und selbstbewusste Nutzer sollte sich die geringen technischen Kenntnisse zur Anwendung dieser Regeln aneignen.

Die Regeln der Datenautobahn:

Das Betriebssystem und die Programme auf den eigenen Computern aktuell halten.

Eine Sicherheitssoftware installieren, die sich automatisch updatet.

Passwörter ernst nehmen, auch wenn es unbequem ist.

Persönliche Daten restriktiv ins Netz geben, insbesondere in sozialen Netzwerken.

Misstrauisch sein gegenüber allen nicht bestellten E-Mails, SMS und Eingabeaufforderungen in Web-Seiten.

Keine Online-Umfragen mit persönlichen Daten ausfüllen.

Mobile Geräte nicht im Auto, Hotelzimmer, Restaurant, zu Hause, wenn Fremde anwesend sind oder sonstwo unbeaufsichtigt lassen.

Das private WLAN verschlüsseln und öffentliche WLAN-Netze nur im Notfall nutzen.

Vor jedem Mausklick, der zu etwas verpflichtet, dreimal durchatmen und dabei nachdenken.

Muss alles immer überall sofort sein?

2. Organisationen

Unternehmen, Verwaltungen, militärische Stäbe und Hauptquartiere ebenso wie Vereine, Krankenkassen und Universitäten arbeiten heute überwiegend teamorientiert. Waren noch 1985 nur 20 Prozent des Beitrags eines Mitarbeiters zum Organisationsziel abhängig von der Zusammenarbeit mit anderen, hat sich dieser Anteil bis 2010 bereits auf 70 Prozent erhöht, mit weiterhin steigender Tendenz. Teamarbeit ist der Schlüssel zum Erfolg moderner Organisationen.

Der überwiegende Teil dieser Teamarbeit vollzieht sich heute IT-unterstützt, und das sowohl organisationsintern als auch in teilweise globalen Netzwerken. Hier liegt die Herausforderung für die Organisationsführung. Auf der einen Seite muss der Informationsaustausch der Mitarbeiter untereinander und mit der Welt außerhalb der Organisation so frei von Einschränkungen wie möglich gefördert werden, auf der anderen Seite muss der Schutz sensibler Informationen und Daten gewährleistet bleiben.

Man kann sich die Informationssicherheit in einem Unternehmen oder einer Organisation auch als eine Pyramide vorstellen. An der Basis herrscht keine, an der Spitze der Pyramide höchste Informationssicherheit. Betrachtet man die nötigen Investitionen, die getätigt werden müssen, um die Informationssicherheit in der Organisation zu verbessern, dann lässt sich feststellen, dass mit jeder Stufe, die man hin zur optimalen Informationssicherheit geht, die notwendige Investition größer wird.

Mit anderen Worten: Ein Zuwachs an Sicherheit ist an der Basis am billigsten und in der Spitze am teuersten.

Betrachtet man die Pyramide unter organisatorischen Gesichtspunkten, sieht man, dass die breite Basis der Pyramide durch die Mitarbeiter gebildet wird, der Mittelbau durch die Administration des internen IT-Netzwerkes und die Spitze durch die technischen Vorkehrungen, die das interne Netzwerk gegen Angriffe von außen abschirmen.

Daraus folgt, dass Investitionen in eine Verbesserung der Informationssicherheit auf der Ebene der Mitarbeiter schon bei relativ geringem Aufwand einen erheblichen Zuwachs an Informationssicherheit bringen.

Wenn wir die Mitarbeiter einer Organisation dazu bringen können, aktiv während ihrer täglichen Arbeit darauf zu achten, dass die Informationen, die sie z.B. in Form von E-Mails und Dokumenten erstellen, nicht in falsche Hände geraten, wäre bereits ein gutes Stück zusätzlicher Sicherheit erreicht.

Gelingt dies nicht, bleibt die Belegschaft einer Organisation die gefährlichste Quelle für Sicherheitsverstöße mit schwerwiegenden Folgen.

Mitarbeiter bedrohen die Informationssicherheit einer Organisation aus verschiedenen Gründen, abhängig davon, um welchen Typ von Gefährder es sich handelt:

Der Gestresste, der unter Druck Fehler macht.

Der Ignorant, der die Regeln aus Unbekümmertheit verletzt.

Der Chaot, der sensitive Informationen in seiner Unordnung liegen lässt.

Der Saboteur, der sich an Vorgesetzten oder unliebsamen Mitarbeitern rächen will.

Der Spion, der Informationen für einen Konkurrenten sammelt.

Der Fleißige, der Sicherheitsregeln umgeht, um Zeit zu sparen.

Der Faule, dem Sicherheit egal ist.

Der Unerfahrene, der es nicht besser weiß.

Der Neue, der die Regeln noch nicht kennt.

Der Übervorsichtige, der alles als sensitiv einstuft.

Der Heimarbeiter, der geheime Projekte am Computer zu Hause bearbeitet.

Auch wenn der Großteil der Mitarbeiter kein Sicherheitsrisiko darstellt, muss die Gefahr durch die gefährlichen Ausnahmen wirksam bekämpft werden. Dies kann durch Aufklärung, Ausbildung und technische Hilfen erreicht werden. Letztere, zum Beispiel automatische

Warnhinweise bei Fehlern in der Erstellung und dem Versand von Dokumenten und E-Mails, dürfen jedoch nicht die flüssige Arbeit behindern, sonst werden sie umgangen. Werden die Auswirkungen von Sicherheitsverstößen als existenzbedrohend für die Organisation beurteilt, darf man vor drastischen Sanktionen nicht zurückschrecken. Dies sollte in den Anstellungsverträgen eindeutig festgeschrieben sein. Es gibt Unternehmen, die z.B. den Verlust eines Laptops im Hotel mit der Entlassung des betreffenden Mitarbeiters bedrohen.

Die Auswirkungen von Sicherheitslücken sollten nicht erst dann erkannt werden, wenn es zu einem ernsten Sicherheitsvorkommnis gekommen ist. Ihre Beurteilung ist auch keine Aufgabe für die IT-Sicherheitsmanager und Computerspezialisten des Unternehmens. Sie ist vielmehr eine Frage der betriebswirtschaftlichen Analyse und Bewertung, also eine Aufgabe für den Vorstand.

Diese Analyse sollte fünf Fragen beantworten:

- Welche Daten sind wichtig für die Alleinstellungsmerkmale im Wettbewerb?
- Welche finanziellen Auswirkungen hätte ein Verlust dieser Daten?
- Wie hoch ist das aktuelle Risiko für einen Verlust dieser Daten?
- Welche Maßnahmen sind notwendig zur Minimierung des Risikos?
- Welche Lösungen bringen den besten Gegenwert für die damit verbundenen Kosten?

In vielen Unternehmen und Organisationen ist zwar ein allgemeines Gefühl für die Gefährdung der Informationssicherheit vorhanden, aber es bleibt häufig dem IT-Bereich überlassen, für die notwendigen Maßnahmen auf diesem eher technisch komplizierten Gebiet zu sorgen. Das IT-Sicherheitssystem ist daher oft lückenhaft, technokratisch bestimmt und nicht betriebswirtschaftlich bewertet.

Die Organisationsführung muss Informationssicherheit als eines ihrer Verantwortungsfelder begreifen.

3. Staat und Gesellschaft

Das Streben nach Sicherheit ist wesentliches, wenn nicht gar bestimmendes Element im Leben der Europäer heute. Ein angemessenes Maß an Sicherheit ist die Voraussetzung für das Funktionieren aller Bereiche, die für unsere demokratisch verfassten Gemeinwesen von elementarer Bedeutung sind: Gesundheit, Soziales, Wirtschaft, Finanzen, Verkehr, Verteidigung, Politik, Bildung, Kultur, Medien; selbst Religion braucht einen sicheren Rahmen, der ihre Ausübung erst möglich macht. Voraussetzung für das Zusammenwirken dieser Elementarbausteine unserer Gesellschaften ist der intensive Austausch von Informationen, der heute im Wesentlichen auf der Nutzung computergestützter Netzwerke basiert. Unser aller Sicherheit hängt daher von der Funktionsfähigkeit dieser Netzwerke ab.

Unsere Informationsinfrastruktur ist bereits seit Jahren zunehmend bedroht. Die Angriffe reichen von

spielerischen Versuchen jugendlicher Hacker über kriminelle Manipulationen, Spionage, Veröffentlichung geheimer Daten bis hin zu massiven elektronischen Angriffen mit politischem Hintergrund.

Die Verteidigung unserer Informationsnetzwerke gegen Angriffe von außen und innen muss ganzheitlich und global gedacht werden. Ganzheitlich, weil jeder Bereich unserer Gesellschaften, ja jeder einzelne Bürger, von einem Angriff betroffen sein kann und deshalb jeder dieser Bereiche einen Beitrag zur Abwehr leisten muss. Global, weil die moderne Informationstechnologie in weltweiten Netzen arbeitet.

Im Unterschied zur konventionellen Verteidigung eines bestimmten Territoriums oder einer Region sind im IT-Krieg die Faktoren Zeit und Geografie auf dramatische Weise verändert. Die Basis möglicher Angriffe auf unsere Computernetzwerke ist nicht von geografischer Nähe zum Angriffsziel bestimmt, sondern nur vom geeigneten Element des weltweiten Cyberspace. Kalkulierten die Großmächte im Kalten Krieg noch mit Stunden, Tagen und Wochen der Reaktionszeit auf einen Angriff, reduziert sich diese im IT-Konflikt auf Minuten und Sekunden.

Die mögliche Art eines Angriffs auf unsere Informationssicherheit ist vorhersehbar. Der Zeitpunkt jedoch kaum. Auf eine improvisierte Abwehr zu zählen wäre daher unverantwortlich.

Daraus folgern vier Konsequenzen: Erstens müssen wir vorbereitet sein. Zweitens müssen wir alle gemeinsam

vorbereitet sein. Drittens muss die Abwehr detailliert geplant und viertens gut geführt werden.

Erfolgreiche Abwehr kann in der vernetzten Welt nur entwickelt werden, wenn alle Betroffenen und Akteure zusammenarbeiten. Estlands Gesellschaft hat den ersten großangelegten Angriff auf die IT-Infrastruktur eines Landes 2007 nur deshalb überstanden, weil sowohl Regierung als auch Verwaltung, Finanzsystem, IT-Service-Provider, Wirtschaft, Militär und Nutzer in einem vorbereiteten System der Abwehr verbunden waren, das reaktionsschnell geführt wurde.

Je kürzer die Reaktionszeit, desto sorgfältiger und detaillierter muss die Verteidigung vorbereitet sein. Wir brauchen umfassende, also organisationsübergreifend besetzte Stäbe für die Beurteilung der Lage und die Planung, Operationszentralen für die Einübung und Durchführung, Dienste für die Aufklärung sowie Wissenschaft und Industrie für die Entwicklung wirksamer Schutzmaßnahmen. Das alles muss in einen rechtlichen Rahmen gestellt und demokratisch kontrolliert werden.

Da die Bedrohung global ist, sollte eine Cyber-Verteidigung so weit wie möglich in Bündnissen organisiert werden. Für Europa bieten sich dazu die NATO und die EU an.

Das Atlantische Bündnis hat bereits relativ weit entwickelte technische Fähigkeiten und den Vorteil der Einbeziehung der fortgeschrittensten Cyber-Macht, der USA. Darüber hinaus verfügt es über eingespielte

Verfahren der Konsultation, Entscheidungsfindung und des gemeinsamen Einsatzes, allerdings längst noch nicht mit der erforderlichen schnellen Reaktionsfähigkeit.

Die EU mit ihrer stärker politischen Ausrichtung könnte sich hier ein Gebiet erschließen, auf dem sie gemeinsame Verteidigung organisiert, die nicht zuvorderst militärisch, sondern eher zivil, wirtschaftlich, technisch bestimmt ist und darüber hinaus weniger dem Einfluss traditionell rüstungswirtschaftlicher Interessen unterliegt.

Die größte Herausforderung bleibt jedoch der immense Zeitdruck, der durch die rasante Entwicklung der Bedrohung entsteht. Ein Virus kostet nur einen Bruchteil des Preises eines Kampfflugzeugs und lässt sich in wesentlich weniger Zeit entwickeln, kann aber eine weit höhere Zerstörungskraft besitzen.

Was wir brauchen, ist eine große gemeinsame Kraftanstrengung, vergleichbar mit der Vision des ersten Menschen auf dem Mond. Was auf dem Spiel steht, ist unsere Art zu leben, denn ohne eine intakte Informationsinfrastruktur funktionieren weder Energieversorgung noch Gesundheitswesen, Verkehr, innere und äußere Sicherheit, Bildung, Klimaschutz, Finanzwesen und Kultur.

Handlungsfelder der Politik

Zukunftsinnovationen können nicht allein den Unternehmen und Wissenschaftlern überlassen werden. Neben Investitionen in die Internet-Infrastruktur und moderne zukunftsorientierte und international abgestimmte Regulierungsregelungen ist vor allem eine optimistische Einstellung von Politik und Gesellschaft zu neuen technischen Entwicklungen gefragt. Übertriebene Skepsis und überzogene Angst vor Gefahren dürfen uns nicht den Blick auf unsere Zukunftschancen verstellen. Hier liegt vor allem eine Verantwortung bei der Politik, die die richtigen Weichen stellen und Anreize schaffen kann, besonders in den Bereichen der Bildung, Energieversorgung und des Gesundheitswesens.

1. Schule

„Jedem Schüler sein Laptop!" Bereits seit Jahren ein bildungspolitischer Schlager. Dabei ist der Zugang zum Internet gar nicht die entscheidende Herausforderung. Den hat der durchschnittliche Jugendliche auch ohne den Computer der Schule bereits.

Viel wichtiger ist: „Jeder Lehrer einen Computer und einen Breitbandanschluss zum Internet!" Dazu bereits im Studium eine solide Ausbildung im Umgang mit der Technik und die Lehrberechtigung zum sicheren, verantwortungsbewussten und kreativen Umgang mit der digitalen Welt. Jugendliche von heute sind es gewohnt, Informationen und Unterhaltung in kurzen, schrillen, farbigen Videosequenzen aufzunehmen.

Das Leben eines jungen Menschen von heute ereignet sich zum nicht geringen Teil in der digitalen Welt des Internets. Lehrer, die sich hier nicht auskennen, können dort auch keine Orientierung vermitteln. Ein Bildungssystem, das dies zulässt, versagt.

Der Zugang zum Internet ist selbst Kindern nur sehr schwer zu verwehren. Wenn Eltern und Lehrer nicht die grundlegenden Kenntnisse haben, um wenigstens die verfügbaren technischen Möglichkeiten zur Regulierung anzuwenden, bleibt dieser Zugang völlig unkontrolliert.

Besser ist es, aufgrund eigener Erfahrung mit dem Internet und persönlicher Freude an dessen Nutzung mit Kindern und Jugendlichen zusammen die digitale Welt zu erschließen und dabei auch die Gefahren und die Methoden zu ihrer Vermeidung zu vermitteln. Geschieht das nicht, oder nur im Rahmen von freiwilligen Zusatzkursen in der Schule, wird unserer jungen Generation ein Großteil der Segnungen des Internets vorenthalten, und wir überlassen sie dem Risiko des Absturzes in seine zweifelhaften Abgründe.

Die Situation in der Praxis ist sehr unterschiedlich. Es gibt Schulen, die die digitale Welt als Teil ihres Erziehungs- und Bildungskosmos vollkommen integriert haben, und andere, die IT und Computer den wenigen Internet-Nerds im Lehrerkollegium überlassen. Das Gleiche gilt für die Nutzung der überwiegend positiven Möglichkeiten des Internets. Wenn wir unsere Kinder nicht fit machen im selbstverständlichen, verantwortungsbewussten und kreativen Gebrauch der

Bildungs-, Forschungs-, Kultur-, Kommunikations- und Unterhaltungsangebote des Internets, nehmen wir ihnen nicht nur ein Stück Lebensqualität, sondern benachteiligen sie auch im globalen Wettbewerb.

Wenn es um Orientierung, Bewertung von gut und schlecht, moralische und ethische Einordnung, Wirkungsbeurteilung, Auswahlentscheidung, Normenerläuterung und Effektivitätsberatung geht, ist Mut zur Erziehung, Begleitung und wenn nötig auch Sanktion gefragt. Dieser Aufgabe müssen sich Bildungspolitiker stellen.

2. Energie

Deutschland hat 1590 Stromlieferanten. Jeder hat seine eigene Organisation, Preispolitik, Kundenstruktur und Lieferquellen, aber alle sind mehr oder weniger von IT-Unterstützung abhängig. Ohne diese gäbe es z.B. keine Liberalisierung des Strommarktes.

Die Stromnetze, die die Lieferanten und Kunden miteinander verbinden, werden mit Hard- und Software gesteuert, die den Anforderungen der traditionellen Struktur der Stromversorger und Verbraucher genügen.

Jetzt kommt die Energiewende, und die Netzstruktur ändert sich rapide. Die Zahl der atomaren Kraftwerke nimmt ab, alternative Energie, vor allem die Windkraft, konzentriert sich in Gegenden, in denen es keine entsprechende Nachfrage gibt. Die Solarenergie verteilt sich auf Millionen Haus- und Scheunendächer

in der gesamten Republik. Das Stromaufkommen schwankt an den Entstehungsorten zum Teil extrem. Unter diesen Umständen muss aber unverändert Strom für die Kunden in der Industrie und bei den Privatabnehmern zuverlässig kontinuierlich, in gleichbleibender Stärke und zu international konkurrenzfähigen Preisen bereitgestellt werden.

Dies ist nur mit einem hochleistungsfähigen, weitgehend zentral gesteuerten und gegen Gefährdung von außen sicheren IT-System zu erreichen. Das Stromnetz muss zum Smart Grid und die Verbraucher müssen zu Smart Costumern und unsere Gebäude zu Smart Homes werden[4].

Die Überwachung des Stromverbrauchs, die aktuelle Verfügbarkeit bei den Lieferanten, das Abrufen und Einlagern von Energie in Speichern und das Vorhalten von Reserven sind in Zukunft voneinander abhängige Stellgrößen, verteilt auf Millionen von Standorten. Die Herausforderung an das digitale Netz, das dies alles in Echtzeit miteinander verbinden muss, und die Verarbeitung der ungeheuren Menge an Daten sind weit jenseits dessen, was zur Zeit in anderen Bereichen bereits verwirklicht ist.

---

4 grid (englisch) = Energieverteilernetz. Smart Grid = intelligentes Netz, das digital gesteuert die Energie verteilt. Smart Customer = digitalisierter industrieller Verbraucher, der seinen Energiebedarf intern digital steuert. Smart Home = Haushalt, in dem Heizung, Wasser und Strom digital gesteuert und der Verbrauch per Smart-Meter (digitaler Verbrauchszähler) kontinuierlich an das Smart Grid gemeldet wird. All das verbunden über das Internet. Spart im Privathaushalt bis zu 10 Prozent, in der Industrie bis zu 20 Prozent Energie.

Technisch ist das machbar. Dazu müssen allerdings die Zuständigkeiten und die Verteilung der immensen Investitionslasten neu geordnet werden. Vor allem erfordert das einen umfassenden planerischen und regulatorischen Rahmen, einen Masterplan, der verhindert, dass es zu Fehlinvestitionen und technischen Sackgassen kommt.

Wichtig ist dabei vor allem die Akzeptanz bei den Entscheidern in der Wirtschaft und bei den Konsumenten in den Haushalten. Ein solches Jahrhundertprojekt erfordert eine auch von den Medien getragene nachhaltige und gegen Rückschläge resistente Aufbruchsstimmung. Nach der Entscheidung zum Ausstieg aus der Kernenergie bleibt uns kein anderer Weg, als zu zeigen, dass man auch als hochentwickelte Industrienation die Wende zur bedarfsgerechten Energieversorgung weitestgehend unabhängig von fossilen Brennstoffen und Atomkraft schaffen kann.

Die Politik wird sich hier mehr einfallen lassen müssen als bloße Vorgaben zur Energieeinsparung und CO_2-Vermeidung.

3. Gesundheitswesen

Das Internet könnte unser Gesundheitswesen von einer ganzen Reihe von Krankheiten kurieren. Könnte, wenn nicht eine andere, typisch deutsche, Krankheit dagegenstünde: übertriebener Datenschutz, Angstmache, Gruppeninteressen und Fortschrittsskepsis. Prägnantes Beispiel ist die Gesundheitskarte. Eine Art Scheckkarte, auf der alle medizinischen und

verwaltungstechnischen Daten eines Patienten gespeichert sind. Im Krankheitsfall stehen dadurch dem behandelnden Arzt alle relevanten Informationen unmittelbar zur Verfügung: Vorerkrankungen, aktuelle und frühere Untersuchungsergebnisse, Röntgenbilder, Medikation, Blutwerte. Es hat quälend lange Jahre gedauert, bis in Deutschland endlich ein mit erheblichen Einschränkungen befrachtetes Pilotprojekt angelaufen ist.

Die Vorteile der Karte beschreiben gleichzeitig die Gründe für die ständigen Verzögerungen der Einführung: Doppelte und unnötige Untersuchungen werden vermieden, Anamnese und Diagnose erheblich beschleunigt, Allergien und Unverträglichkeiten nicht übersehen, der Medikamentenverbrauch dokumentiert, die Kosten transparent gemacht, kurz, der Patient wird gläsern, aber auch der Arzt, die Kasse und das Krankenhaus.

Um das Gesamtsystem technisch zu realisieren, gibt es zwei grundsätzliche Möglichkeiten: die Daten zentral oder dezentral verwalten. Zentrale Speicherung bedeutet sehr hohe Investitionen, langdauernde Infrastrukturmaßnahmen und hohe Konzentration sensitiver Informationen.

Besser geeignet scheinen bereits verfügbare Software-Lösungen zu sein, die die Daten dort belassen, wo sie bereits jetzt gespeichert werden, im Krankenhaus, in der Praxis, bei der Krankenkasse oder im Labor, und die deren Abruf und Zusammenführung im Behandlungsfall unter Berücksichtigung des Datenschutzes und der

Informationssicherheit verzugslos ermöglichen. Die jüngste EU-Richtlinie zur Speicherung und Verarbeitung von Gesundheitsdaten weist diesen Weg. Damit könnte auch sichergestellt werden, dass Reisende in ganz Europa unkompliziert kompetente Behandlung im Krankheitsfall und bei Unfällen erhalten.

Die Forderung der Zeit für die Politik sollte nicht zuvorderst der Datenschutz sein, sondern die Forschung auf diesem Gebiet zu fördern und die notwendige IT-Infrastruktur und sicheren Übertragungswege auszubauen. Die Industrie muss dafür Sorge tragen, die breite Basis an technischen und Verfahrensstandards zu schaffen, die möglichst rasche Fortschritte ermöglicht.

Handlungsempfehlungen für Führungskräfte

Beginnen wir mit einem Exkurs in die Welt des Militärs, das zwar eine Organisation mit besonderen Anforderungen an Führung ist, aber dennoch Rückschlüsse auf andere Unternehmen zulässt. Angesichts neuer Technologien ist Führung vor neue, komplexe Aufgaben gestellt. Die technisch vernetzte Operation der Zukunft zielt auf ein vollständiges und aktuelles Lagebild in Echtzeit, verfügbar an jedem Punkt des Operationsgebietes. Der für die jeweilige Entscheidungsebene optimale Informationsstand wird automatisch generiert, kann aber sowohl nach oben als auch nach unten erweitert werden.

Ein Beispiel aus den Einsätzen unsere Tage: Der Kommandeur einer multinationalen Stabilisierungsmission hat das aktuelle Gesamtlagebild, kann aber auch Echtzeit-Videobilder von einer Situation auf Patrouillenebene in einer politisch brisanten lokalen Situation abrufen.

Unter diesen Bedingungen muss Führen mit Auftrag in neuem Rahmen gedacht werden: Der Feldherrenhügel kann elektronisch generiert werden. Die virtuelle Präsenz jedes Kommandeurs im Brennpunkt ist ohne Zeitverzug möglich. Seine Verfügbarkeit für Entscheidungen auf seiner Ebene ist unabhängig von seinem Standort.

Eine solche Informationsumgebung ermöglicht auch neue Dimensionen der Kontrolle: Wird der Auftrag

vollständig und im Sinne der übergeordneten Führung ausgeführt? Hat die Formation, die den Entschluss eines unterstellten Kommandeurs ausführen soll, die nötigen Ressourcen? Ist ihre Aktion mit den anderen Truppen des unterstellten Bereiches kompatibel? Welches sind die politischen und strategischen Konsequenzen einer taktischen Maßnahme? Diese und ähnliche Fragen lassen sich auf Knopfdruck beantworten.

Ein vollständig vernetztes Führungssystem schafft kontinuierlich weitestgehende Transparenz der gemeinsamen Operation für alle Kommandeure und deren Stäbe. Das gemeinsame Handeln im Sinne der übergeordneten Führung kann jederzeit von jedem Entscheider geprüft werden.

Die höhere Qualität des Lagebildes wird zu schnelleren Entschlüssen und drastisch kürzeren Befehlslaufzeiten führen. Auch große und komplizierte Truppenkörper werden erheblich schneller auf Lageänderungen reagieren können. Die Entwicklung eines Operationsplans wird wesentlich mehr im Dialog zwischen den Führungsebenen geschehen. Die Dimension Führung wird sich in beiden Richtungen verändern: mehr Zentralisierung nach oben und mehr Entscheidungsbreite nach unten. Führungsunterstützung und Kommunikationstechnik werden sich in Armeen und Unternehmen, weit mehr noch als bereits heute, zu einem entscheidenden Führungsfaktor entwickeln.

Das stellt besondere Anforderungen an die Cyber-Sicherheit, die nicht allein den IT-Unternehmen überlassen werden kann, sondern maßgeblich politisch zu steuern ist. Für Sicherheit zu sorgen, liegt auch in der Verantwortung der politischen Entscheider, denn Staat, kritische Infrastrukturen, Wirtschaft und Bevölkerung sind auf ein verlässliches Netz angewiesen. Fast 60 000 Internetstraftaten wurden 2011 verübt. Sie haben einen Schaden von mehr als 71 Millionen Euro verursacht.

Je mehr hochkomplexe Bereiche und Strukturen ins Internet verlagert werden, umso mehr wächst auch hier das Schadenspotenzial. Neue Straftatbestände, von denen wir heute noch nicht einmal alle kennen, erfordern gesetzgeberisches Handeln. Und trotz zahlreicher Gesetzesinitiativen sowie nationaler und internationaler Bündnisse bleibt für politische Entscheider im Bereich Cyber-Sicherheit noch Vieles zu tun. Wichtige Handlungsfelder sind Datenhehlerei, Telekommunikationsüberwachung und Vorratsspeicherung.

So fehlerfrei oder fehleranfällig Systeme auch sind und bei allen Vorteilen, die moderne Kommunikationstechnik bieten kann, darf eines nicht vergessen werden: Auch ein vollkommen vernetztes Führungssystem, ob in der Wirtschaft oder beim Militär besteht aus Entscheidern aus Fleisch und Blut, nicht aus Operationsrobotern. Bei IT-Sicherheit im eigenen Arbeitsumfeld sind alle, auch die höheren Führungsebenen gefordert, denen häufig noch die nötige Bereitschaft fehlt, sich intensiv mit modernster Technik zu beschäftigen.

Sollten Sie feststellen, dass Sie sich bisher zu wenig um die IT-Unterstützung Ihrer Organisation und vor allem um deren Sicherheit gekümmert haben, hier ein paar Vorschläge, damit zu beginnen:

Lassen Sie sich vom Leiter der EDV vortragen, wie die IT Ihres Unternehmens organisiert ist. Machen Sie von Beginn an klar, dass Sie Fachausdrücke beim ersten Gebrauch erläutert haben wollen. Das erspart ständiges Nachfragen und vermeidet die unnötige Aufdeckung Ihrer lückenhaften Kenntnisse. Falls wesentliche IT-Dienste an Dritte vergeben sind, vereinbaren Sie ein Gespräch mit deren Vorständen, damit diesen klar wird, dass sie für Sie arbeiten, nicht für Ihre IT-Abteilung.

Zu Beginn des Themas Sicherheit fragen Sie nach den zu schützenden Informationen Ihrer Organisation, um festzustellen, ob nicht unnötig in die Sicherheit von Bereichen investiert wird, in denen keine sensitiven Daten bearbeitet werden.

Lassen Sie sich die physische Sicherheit der IT-Technik, insbesondere die der zentralen Datenspeicher, beschreiben und ruhig einmal vor Ort zeigen. Das gilt auch, wenn sie bei Dritten ausgelagert sind. Stichworte sind hier: Zugangskontrolle, Einbruchssicherungen, Schutz vor Brand- und Wasserschäden, Redundanzen, Stromausfall, regelmäßige Sicherung der Daten physisch ausreichend getrennt von den Speichern für den laufenden Betrieb. Bestehen Sie darauf, Schwächen rasch abzustellen, auch wenn es Geld kostet.

Lassen Sie sich erklären, wie festgestellt wird, ob in das IT-Netz Ihrer Organisation eingebrochen wurde und ob Datenverluste entstanden sind.

Fragen Sie nach der Auslastung der IT-Kapazität. Gibt es starke Schwankungen? Sollte man besser eine Cloud-Lösung suchen? Das heißt, dass die gesamte IT aus Ihrer Organisation über das Netzwerk ausgelagert und von einem externen Dienstleister dynamisch an Ihren jeweiligen Bedarf angepasst übernommen wird.

Falls am Ende Zweifel an der IT-Sicherheit der Unternehmung bleiben, sollte man nicht die Kosten für eine neutrale Bewertung von außen scheuen, auch wenn die finanzielle Beurteilung eines Verlustes wichtiger Informationen manchmal nicht einfach ist. Das Ergebnis sollte ein vom Vorstand genehmigtes IT-Konzept Ihrer Organisation sein, das in regelmäßigen Abständen überprüft und aktuell gehalten wird.

Nach diesen Schritten sind Sie besser abgesichert als 80 Prozent aller Firmen, Unternehmen und Organisationen in Deutschland und der EU.

Die Herausforderung für die Entscheider von heute liegt in der Rasanz, mit der sich die digitale Welt in den nächsten Jahren entwickeln wird. Wir brauchen eine Politik, die rechtzeitig die richtigen Rahmenbedingungen schafft, und Unternehmen, die Trendsetter und nicht bloße Follower sein wollen. Dazu gehören eine kontinuierliche Beobachtung und die

sorgfältige Beurteilung der technischen Trends und deren Auswirkungen auf unser soziales Umfeld, die zukünftigen Lebensbedingungen und die globalen Märkte. Wir haben die maschinelle Revolution des 20. Jahrhunderts erfolgreich gemeistert, die weltweite Konkurrenz um Erfolg im laufenden Jahrhundert des Internets ist jedoch ungleich härter.

Das Internet birgt Chancen, wie sie die Menschheit seit ihrer Existenz nicht hatte, aber auch Gefahren. Wer in unserer Gesellschaft Verantwortung tragen und entscheiden will, darf die digitale Welt nicht nur nutzen, sondern muss sie mitgestalten.

Herausgeber
Microsoft Deutschland GmbH
Konrad-Zuse-Str. 1, 85716 Unterschleißheim
www.microsoft.de/politik ©2012

Foto Autor
Microsoft/Alex Schelbert

Ulrich Wolf

Der ehemalige Kommandeur auf Bataillons-, Brigade- und Divisionsebene trat 1967 seine Wehrpflicht in der Bundeswehr an. Er absolvierte seinen Dienst im Wechsel zwischen Truppe, Stäben und Bundesministerium der Verteidigung und war für das Atlantische Bündnis tätig, zuletzt als Generalleutnant und Direktor der NATO-Agentur NCSA. In dieser Funktion verantwortete er den Betrieb des weltweiten IT- und Informationsnetzes und der Cyber-Verteidigung der Allianz. Er ist Absolvent der deutschen und der US-amerikanischen Generalstabsausbildung. Heute lebt der Diplom-Betriebswirt in Münster, Westfalen, und arbeitet als freier Berater und Autor auf dem Gebiet der IT-Sicherheit und Cyber Defense. Ulrich Wolf ist verheiratet und hat eine Tochter.

Microsoft