GovNet-Debatte in den USA

Wegweiser für ein sichereres Internet?

Stefan Krempl

Alcatel SEL Stiftung für Kommunikations-Forschung

GovNet ideas don't come cheaply - [Diese Seite übersetzen] ...34 **GovNet** ideas don't come cheaply By William Jackson GCN staff President adviser Richard A. Clarke's October request for information for a... www gcn.com/20-_34/news/17620-1.html - 37 - Im Archiv - Ähnliche Seiten - [Weitere Resultate von www.gcn.com] **GovNet:** What Is It Good For? - [Diese Seite übersetzen] „Michelle Delio">. **GovNet:** What Is It Good For? **...GovNet** is the pet projekt of Richard Marke, special assistent to the president for cyberspace security **...** www.wired.com/news/print/0,1294,49858,00.html - 19k - Im Archiv - Ähnliche

53
Stiftungsreihe

GovNet-Debatte in den USA
Wegweiser für ein sichereres Internet?

Übersicht

Impressum

Stiftungs-Reihe

Redaktion
Dr. Dieter Klumpp
Petra Bonnet M.A.
Renate Förstner

Druck der Broschüre
Alcatel SEL AG

Postadresse
Alcatel SEL Stiftung
Postfach 40 07 49
70407 Stuttgart
Telefon (0711) 821-45002
Telefax (0711) 821-42253
E-mail sel.stiftung@alcatel.de
ISSN 0932-156x

Autor

1990-1995: Studium der Gesellschafts- und Wirtschaftskommunikation an der Hochschule der Künste Berlin, Abschluss als Diplom-Kommunikationswirt (Diplomarbeit "Das Phänomen Berlusconi", Peter Lang Verlag), 1995-1996 freie journalistische Arbeit, Pressearbeit in einer Berliner PR-Agentur für die Deutsche Post und den Berliner Senat (Verwaltungsreform), Vorbereitung und Betreuung des Symposiums "Förderpreis Software Qualität" 1995. 1996-2001 Wissenschaftlicher Mitarbeiter am Lehrstuhl für Sprachwissenschaft der kulturwissenschaftlichen Fakultät bei Prof. Dr. Hartmut Schröder an der Europa-Universität Viadrina Frankfurt (Oder). 1997/1998 Gastforscher am Center for Cultural Studies der University of California in Santa Cruz. Seit 2001: Dozent am Südosteuropäischen Medienzentrum in Sofia. Autor für Online-Publikationen wie heise online und Telepolis sowie für Printmedien wie c't, Financial Times Deutschland, Neue Zürcher Zeitung, vdi nachrichten, Die Zeit. Schwerpunkt: das Netz zwischen Wirtschaft, Politik und Kultur. Siehe auch: www.stefan-krempl.de

Vorwort

Mit der zunehmenden Durchdringung alle gesellschaftlichen Lebensbereiche mit elektronischen Informations- und Kommunikationstechnologien (IuK) rückt auch die Frage nach der Sicherheit und Verlässlichkeit der technischen Infrastrukturen in den Mittelpunkt. Dies gilt insbesondere, wenn in wachsendem Maße auch sensible, vertrauliche und/oder extrem folgenreiche Daten, Informationen oder Kommunikationen in und mit elektronischer IuK-Infrastrukturen ausgetauscht oder abgewickelt werden. Hier sind neben dem zunehmenden Rechts- und Geschäftsverkehr oder dem hochsensiblen Datenaustausch im medizinischen Bereich vor allem elektronische Dienstleistungen und Kommunikationsangebote öffentlicher Einrichtungen für die Bürgerinnen und Bürger zu nennen. Insbesondere der moderne Staat muss darüber hinaus für den internen Datenaustausch bzw. die interne Kommunikation von öffentlichen Organen und Behörden, sicherheitsrelevanten Einrichtungen und auch der klassischen sicherheitsrelevanten, sogenannten ‚kritischen' Infrastrukturen (wie z.B. Energie, Wasser, Verkehr) die Funktionsfähigkeit und auch verlässliche Verfügbarkeit sicherer IuK-Infrastrukturen gewährleisten. Dies ist der Kontext, indem verschiedene IT-Sicherheitsstrategien insbesondere für öffentliche Einrichtungen, wie eben beispielsweise vollkommen isolierte Regierungsnetze, diskutiert werden.

Denn mit der internationalen Vernetzung sowie der hohen technischen Komplexität und Dynamik der IuK-Infrastrukturen gehen ebenfalls neue Gefährdungen und Sicherheitsrisiken einher, wie nicht zuletzt die Anschläge vom 11. September 2001 in den USA deutlich gemacht haben. Kriminelle oder gar terroristische Angriffe auf sensible elektronische IuK-Infrastrukturen oder gar gezielte, mit Computernetzen lediglich durchgeführte Angriffe auf die klassischen lebenswichtigen Infrastrukturen sind ein zunehmend reales Gefährdungs-Szenario. Auch die Gefährdung der Vertraulichkeit oder der Integrität elektronischer Kommunikation bzw. die Manipulation sensibler Daten bedeutet gerade für sicherheitsrelevante öffentliche Einrichtungen und Behörden ein enormes Risiko. Ebenso können Funktionsbeeinträchtigung infolge technischer Ausfälle oder menschlicher Fehlbedienungen beträchtliche Folgeschäden verursachen.

Die Gewährleistung sicherer Netze ist für eine moderne Gesellschaft unverzichtbar und verlangt auch im Rahmen der staatlichen Daseinsvorsorge nach spezifischen Präventions- und Risikominimierungsmaßnahmen. Allerdings streiten sich die Politiker wie Experten durchaus über das ‚Wie'. In dieser Debatte ist die vorliegende Broschüre des ausgewiesenen Netzexperten Stefan Krempl ein wichtiger Beitrag. Er erlaubt nicht nur eine Orientierung in der Diskussion um ein isoliertes Regierungsnetz, darüber hinaus problematisiert der Autor zielgenau die bisher diskutierten Ansätze und nennt mögliche Alternativen. Aufgrund seiner journalistisch geschulten literarischen Qualitäten ist der Beitrag zudem sehr gut lesbar, was man sicherlich nicht von allen IT-Fachbeiträgen zu diesem Thema behaupten kann.

Jörg Tauss, MdB
Vorsitzender des Unterausschusses Neue Medien
des Deutschen Bundestages

1. Ein Konzept für ein besseres Netz

Am 11. Oktober 2001, genau einen Monat nach den Terroranschlägen auf das World Trade Center in New York und das Pentagon in Washington, überraschte der neu ernannte Berater des US-Präsidenten George W. Bush für "Sicherheit im Cyberspace", Richard Clarke, die Fachwelt mit einem ungewöhnlichen Diskussionspapier: In einem "Request for Information" (RfI)[1], einer Art inoffiziellen Regierungsausschreibung mit der Bitte um Stellungnahme durch mögliche Projektträger in der freien Wirtschaft, skizzierte der auch unter Bill Clinton bereits als Chefkoordinator für Infrastruktursicherheit und Antiterrorfragen dienende Kämpe seinen Traum von einem "besseren" Internet, dem GOVNET. Kurz gefasst soll es sich bei diesem Projekt dem RfI zufolge, den die General Services Administration (GSA) der US-Regierung auf Geheiß von Clarke offiziell veröffentlichte, um ein "Government Network designed to provide protected services for critical Government functions" handeln.

Clarke hatte als alter Hase im National Security Council des Weißen Hauses bereits seit Jahren vor den Auswirkungen eines bevorstehenden "digital Pearl Harbor"[2] gewarnt[3]. Er wirkte mit an der Ausarbeitung eines ersten Weißbuchs zum Schutz kritischer Infrastruk turen wie den Telekommunikationsnetzen, der Energieversorgung oder dem Bankensektor, das die Clinton-Administration im Mai 1998 vorlegte[4], und versuchte zwischen den damals aus den Boden sprießenden Regierungsbehörden wie dem ans Wirtschaftsministerium angehängten Critical Infrastructure Assurance Office (CIAO) oder dem National Infrastructure Protection Center (NIPC) des FBI zu vermitteln. Nach dem 11. September spürte Clarke endlich den erwünschten politischen Rückhalt, den Kampf gegen Cyberwarriors und insbesondere Cyberterroristen zu verstärken – obwohl die Selbstmordattentäter von New York und Washington auf Flugzeuge und angeblich auf Papiermesser statt auf das Internet als Terrormittel setzten.

Zuvor habe es an dem echten Glauben gefehlt, dass Angriffe aus dem Cyberspace eine "wahre Bedrohung" darstellen könnten, sagte Clarke in einem Interview im November 2001[5]. Jetzt sei das Ziel, eine einheitliche Linie für eine nationale Sicherheitsstrategie für das digitale Zeitalter aufzubauen. In diesem Zusammenhang wurde auch die GOVNET-Idee geboren, die Clarke im selben Interview als "ein Konzept" bezeichnete, das zusammen mit der Privatwirtschaft ausgearbeitet werden solle: 'The concept is a series of intranets for federal departments so that people in a particular department could talk securely to other people in that department. The agencies would be walled off from each other."

2. Die Anforderungen an GOVNET (Sicherheitsziele)

Die Sicherheitsziele, die der RfI für ein GOVNET aufstellt, sind weit gehend allgemein gehalten und weisen kaum konkrete technische Vorgaben auf. Das gesamte Papier ist zwar in der Zukunftsform ("wird sein")

[1] Request for Information for a Government Network Designed to Serve Critical Government Functions (GOVNET), http://www.fts.gsa.gov/govnet/govnet.doc (Link vom 18.06.2002).

[2] Der inzwischen gängige Begriff verschmilzt die mögliche Bedrohung der Informationsadern digitaler Gesellschaften mit dem historischen US-Trauma eines Angriffs "aus heiterem Himmel" und wurde vor allem vom Infowar-Propheten Winn Schwartau spätestens seit 1991 bekannt gemacht.

[3] Vgl. z.B. eine Reuters-Meldung von Scott Hillis vom 08.12.2000: U.S. Could Face 'Pearl Harbor' in Cyberspace, http://dailynews.yahoo.com/h/nm/20001208/tc/security_dc_3.html (Link vom 09.12.2000).

[4] http://www.epic.org/security/infowar/cip_white_paper.html (Link vom 19.06.2002).

[5] San Jose Mercury News, 02.11.01, http://www.siliconvalley.com/docs/news/svfront/clrkqa110301.htm (Link vom 06.11.2001).

statt im Konjunktiv ("sollte, könnte so aussehen") gehalten, bittet gleichzeitig aber immer wieder um Alternativvorschläge. Den Anforderungen/Vorstellungen der GSA entsprechend soll GOVNET:

- ein privat betriebenes, auf dem Internet-Protokoll (IP) basierendes Netzwerk sein, an das nur Regierungsabteilungen und "andere autorisierte Nutzer" über eine bestimmte Zahl von Zugangspunkten angeschlossen sind;
- keine Verbindungen oder Gateways zum Internet oder anderen privaten Netzen aufweisen, also ein reines Intranet innerhalb der 48 Festland-Staaten der USA darstellen;
- Telekommunikationsmöglichkeiten im Bereich Sprache und möglichst auch Bild (Video) auf Basis des aktuell verfügbaren kommerziellen Standards bieten und auch Konferenzschaltungen sowie IP-Multi- und Broadcast (Streaming von AV-Inhalten) ermöglichen;
- ausfall- und krisenfest sein. Gedacht ist dabei vor allem an eine "Immunität" vor Schädlingssoftware (wie Viren oder Trojanern) oder so genannten "Cyber-Attacken" auf die Infrastruktur. Erwähnt werden vor allem die seit den Angriffen auf kommerzielle Server von Firmen wie Amazon, eBay oder Yahoo Anfang 2000 hinlänglich bekannten "Denial of Service"-Attacken (DOS)[6];

    - die "höchsten Level an Zuverlässigkeit und Verfügbarkeit" bieten;
    - Kommunikation mit Hilfe von Techniken verschlüsseln, die von der National Security Agency (NSA), dem technischen Supergeheimdienst der USA, gebilligt wurden. Unverschlüsselt sollen dabei Routing- und Adressinformationen bleiben;
    - innerhalb von sechs Monaten eine schlüsselfertige Lösung mit der Abrechnung aller Dienste aus einer Hand darstellen und "24/7" betreut werden. Video- und Sprachkommunikation sollen innerhalb eines Jahres implementiert sein;
    - im Bereich Bandbreite der Nachfrage immer entsprechen;
    - auf Technologien und Dienstleistungen zurückgreifen, die dem besten erdenklichen Stand der wirtschaftlichen Entwicklung entsprechen.

Der RfI setzt ausdrücklich keine Vorgaben zu spezifischen Sicherheitspraktiken oder Kontrollmechanismen und ermuntert zu "kreativem Denken outside the box". Er zeigt auch keine Präferenz für die Nutzung einer dedizierten physikalischen Infrastruktur für GOVNET bestehend auf Glasfaserleitungen und eigener Hard- und Softwareausrüstung auf der einen und "anderen Ansätzen" auf der anderen Seite, bei denen die funktionalen Anforderungen auf der Basis geteilter Netzleitungen billiger erreicht werden. Die Kosten sollen für einen Fünf- und einen Zehn-Jahres-Vertrag ausgewiesen werden. Einreichungen konnten bis zum 21. November 2001 erfolgen.

3. GOVNET in der Kritik

Der Request for Information wurde in der kritischen Netzgemeinde sehr schnell ablehnend – teilweise mit einer gehörigen Portion Hohn und Spott – aufgenommen. Andy Oram etwa, Redakteur beim Internet-Auftritt des kalifornischen Computer-Fachverlags O-Reilly, machte in dem "grandiose scheme for a self-contained government network" mehre-

[6] Eine ausführliche Übersicht über Angriffsmöglichkeiten auf Netzwerke findet sich im Anhang.

re "naïve errors" aus[7], die gerne von Leuten gemacht würden, die sich mit Fragen der Sicherheit der Informationstechnologie (IT) nicht näher beschäftigt haben. So vermisst er die Skizzierung einer praktischen Sicherheitsrichtlinie für GOVNET, die viel entscheidender sei als alle weitmaschigen Vorgaben, etwa Verschlüsselungstechniken zu nutzen. Als besondere Ironie bezeichnet es Oram, dass der ein sicheres Netz einklagende RfI in Microsoft Word veröffentlicht wurde und sogar Antworten im selben Format verlangte. Dabei bietet das zur Erstellung von Word-Dokumenten nötige Microsoft Office "bekanntlich eine hervorragende Ablaufumgebung für Computer-Viren und anderen schädlichen Programmcode"[8], der die GOVNET-Theoretiker doch gerade einen Riegel vorschieben wollen. Unerklärlich erscheint es Oram gleichzeitig, warum in dem RfI nicht der Einsatz transparenter Software mit offenem, von mehreren Augen leichter zu überprüfendem Quellcode gefordert wird.

Das Netzmagazin Telepolis spöttelte wenig später über den geplanten "Auszug" der Amerikaner aus dem zunächst doch von ihnen selbst groß gezogenen Internet und erinnerte an die Mär von einem geplanten "Cyberschutz-Schild", den die USA einem NSA-Berater zufolge angeblich schon einmal auf die Agenda gesetzt hätten[9]. Wenige Tage nach der Veröffentlichung des RfI forderten zudem Analysten der Gartner Group die US-Regierung auf, lieber ihren Fokus auf das Verbessern der "Leistung, Sicherheit und Überlebensfähigkeit" des Internet zu legen statt ein separates Regierungsnetzwerk zu entwickeln. Große Hoffnungen auf Aufträge machten die Berater der Telekommunikations- und IT-Branche nicht. Falls GOVNET wider Erwarten doch staatlich gewollt und vor allem bezahlt würde, sollten "defense contractors, network providers and security vendors" das Projekt als eine "short-term opportunity to sell products and services" sehen. Die besseren Umsatzmöglichkeiten macht Gartner aber im normalen Internet-Bereich aus: "Enterprises and government agencies should assume that a long-term solution to Internet security will arise elsewhere and should proceed to buy denial-of-service protection and other managed security services from commercial providers"[10]. Das Marktforschungsunternehmen Forrester Research stimmte noch im Oktober in den aufklingenden Schwanengesang ein und verriss in einem Report den Vorschlag: GOVNET sei ein "pipe dream" und könne angesichts der vorgesehenen Komplexität gar nicht funktionieren.

Auch der Security- und Kryptografie-Guru Bruce Schneier, Chef der Sicherheitsfirma Counterpane, knöpfte sich neben vielen anderen Experten in der Folgezeit den GOVNET-Vorschlag vor. In der Novemberausgabe seines monatlichen Newsletters Crypto-Gram[11] begrüßte er den RfI zunächst als eine "gute Idee", auch wenn das Ganze wohl "sehr teuer" kommen, schwierig umzusetzen und ziemlich sicher mit einigen Unsicherheiten befrachtet sein würde. Aber selbst eine "mittelmäßige Implementierung" des Projekts sei besser als alles, was die Regierungsabteilungen bisher an Sicherheitsaufwand im IT-Bereich betrei-

[7] Oram, Andy: Many Devils in GOVNET Details. The O'Reilly Network, 15.10.2001, http://www.oreillynet.com/lpt/wlg/766 (Link vom 17.06.2002).
[8] Münch, Isabel (Hg.) (2002): IT-Sicherheitsstrukturen in der deutschen Kreditwirtschaft. Ingelheim (SecuMedia-Verlag/Bundesamt für Sicherheit in der Informationstechnik), 76f.
[9] Rötzer, Florian: Auszug aus dem Internet. Telepolis ,17.11.2001, http://www.heise.de/tp/deutsch/special/info/9989/1.html (Link vom 03.07.2002).
[10] Pescatore, John/Jay Pultz: Kommentar zu GOVNET (o.Titel), 16.10.2001, http://www3.gartner.com/DisplayDocument?doc_cd=101741 (Link vom 17.10.2001).
[11] Schneier, Bruce: Crypto-gram, November 2001. Email-Newsletter. Webarchiv unter http://www.counterpane.com/crypto-gram.html

ben würden. Sodann folgt eine lange Liste voller Wenn und Aber, nach deren Studium selbst der größte GOVNET-Protagonist von dem Vorhaben wohl Abstand nehmen dürfte. Wie schön wäre es, schwärmt Schneier etwa, wenn man GOVNET wirklich 'from scratch" neu designen, starke Authentifizierungstechniken einbauen, alle Verknüpfungen verschlüsseln und Anonymität innerhalb des Netzwerks ausschließen könnte. "There can be better accountability", träumt der Experte. "There can be an approved list of permitted software." Insider-Attacken seien man zwar nicht ganz ausschließen. Aber es dürfte schwerer werden, in einem derart kontrollierbaren Netz dabei unerkannt davon zu kommen. Die Sache mit dem Hochsicherheitsnetz habe jedoch vor allem einen Haken: "Unfortunately, the security of something like GOVNET is likely to be inversely proportional to its utility." Da hätte man also ein schönes abgeschlossenes Netzwerk, doch die Kommunikations- und Anwendungsmöglichkeiten wären dann eben sehr begrenzt.

4. Einwände gegen GOVNET im Detail

Die vielfach von allen Seiten geäußerte Kritik an dem klassifizierten, von der Außen-Internetwelt abgeschlossenen Regierungsnetz lässt sich in mehrere Kategorien unterteilen. An der generellen technischen Machbarkeit werden dabei so gut wie keine Zweifel geäußert, aber an dem (nicht nur finanziellen) Preis für die durch Isolation erzwungene Sicherheit.

a) Das ist nichts Neues, das haben wir schon, das brauchen wir nicht.

Selbst Richard Clarke, der geistige Vater des GOVNET, erkannte es einige Monate nach seinem formalen Aufruf: 'What we discovered is that the idea of having a separate air-gapped network ... is in fact an old idea," sagte der Sicherheitszar des US-Präsidenten im Februar 2002 auf dem Stelldichein der amerikanischen IT-Security-Branche, der RSA-Konferenz in San Francisco. "There are already such networks out there"[12].

Die meiste Presse hat im Umfeld der GOVNET-Berichterstattung das INTELINK-Netzwerk der US-Regierung bekommen[13]. Es ging 1994 online, erfreute sich allerdings erst nach dem 11. September einer verstärkten Nutzung. Es dient nach seinem Dornröschenschlaf, während dem es allein zum Spielplatz für militärische Computerfreaks avancierte, inzwischen vor allem den amerikanischen Sicherheitsbehörden zum Austausch von Nachrichten über das Vorgehen im Krieg gegen den Terror beziehungsweise gegen die "Achse des Bösen". Betrieben wird INTELINK über gesonderte Server[14] des US-Verteidigungsministeriums[15].

Immer wieder Erwähnung finden zudem die geschlossenen und teilweise vollständig verschlüsselten Netzwerke SIPRNET (Secret Internet Protocol Router Network) und NIPRNET (Naval Internet Protocol Router Network) der US-Regierung. Dean berichtet außerdem von einem weiteren "Joint Worldwide Intelligence Communications System"

[12] Poulsen, Kevin: Terror talk stalks RSA Conference. The Register, 21.02.2002, http://www.theregister.co.uk/content/55/24164.html (Link vom 19.06.2002).

[13] Vgl. am ausführlichsten: Delio, Michelle: GovNet: What is it good for? Wired News, 21.01.2002, http://www.wired.com/news/print/0,1294,49858,00.html (Link vom 21.01.2002).

[14] Ein "totes" Verzeichnis der Intelink-Server ist unter http://www.topsecretnet.com/intelink/index.html abzurufen.

[15] Vgl. Delio, a.a.O.

(JWICS), einem "classified network with no links at all to the public Internet that is used by intelligence agencies"[16]. Wozu die Vereinigten Staaten da auch noch ein GOVNET brauchen, konnte Clarke bisher nicht hinreichend erklären.

b) Das bringt‘s doch eh nicht

Schneier berichtet süffisant in seinem Newsletter, dass die INTELINKs, SIPRNETs und NIPRNETs dieser Welt zwar "deutlich sicherer seien als das Internet." Trotzdem habe es nur 24 Stunden gedauert, bis der Melissa-Virus seinen Weg vom öffentlichen Netz in eines der abgetrennten Paralleluniversen genommen hatte. "And the LoveLetter virus infected several of these computers." Irgendein Zugangsberechtigter wird also wohl doch seinen heimischen Laptop angeschlossen und die Netzwerksicherheit damit kompromittiert haben. GOVNET müsste daher physikalisch absolut vom Internet getrennt sein, so Schneier. Das hieße beispielsweise, dass ein Datenaustausch nicht einmal per Diskette stattfinden dürfte. "GOVNET can't have firewall-protected gateways to the Internet. … GOVNET has to use its own routers, its own servers, and its own clients. If a GOVNET user wants to use the Internet, he needs two computers on his desk. … And he can't share files between them, not even by floppy disk". Die Sicherheitsvorkehrungen würden es auch nötig machen, vollständig eigene Datenleitungen für GOVNET zu nutzen, deren Bandbreite nie mit einem anderen Netz geteilt werden dürften.

Ähnlich sieht die Sache Anthony D’Agata, Chef der Regierungsabteilung der Telekommunikationsfirma Sprint. Möglich sei es schon, ein Hochsicherheitsnetz aufzuziehen, das unerwünschte Eingriffe sehr schwierig mache. Damit setze man der Skalierbarkeit und der Interoperabilität dieses Netzwerks aber gleichzeitig deutliche Grenzen[17].

c) Das ist zu teuer und zu zeitaufwändig

Einig sind sich Sicherheitsexperten aus der Branche rund um die Informations- und Kommunikationstechnologien (IuK), dass ein Projekt wie GOVNET nicht billig zu haben ist. Vor allem, wenn die Regierung ihr eigenes Glasfasernetz beanspruchen würde, erklärt Tony Cira, Leiter der Abteilung Verteidigung bei AT&T. Dann würde GOVNET nicht nur eine sehr abgeschottete Sache darstellen, sondern auch "sehr teuer", da auch die letzte Meile zwischen den lokalen Telefondienst und den nationalen Backbone gesondert betrieben werden müsste. Für den Aufbau eines solchen Netzwerks müssten Leitungsrechte aufgekauft und eine "beträchtliche Menge Zeit" investiert werden[18].

d) Das schafft ein falsches Sicherheitsgefühl

Ein sicheres Übertragungsnetz kann paradoxerweise gerade der Sicherheit des gesamten Systems an der Schnittstelle zum Menschen abträglich sein. Nutzer klassifizierter Netzwerke, sagt zumindest Amit Yoran, vormaliger Leiter der Schwachstellenanalyse des Computernotfall-Teams im Pentagon. "Sie glauben, dass sie schon allein deswegen sicher genug sind, weil sie abgeschottet sind." In der Realität könne aber aufgrund eines

[16] Dean, Joshua: Secure network proposal stirs debate among telecom companies, Gov Exec 15.10.2001, http://www.govexec.com/dailyfed/1001/101501j1.htm (Link vom 17.10.2001).

[17] Jackson, William: GovNet ideas don't come cheaply, Government Computer News, 10.12.2001, http://www.gcn.com/20_34/news/17620-1.html (Link vom 17.06.2002).

[18] Dean, a.a.O.

kleinen Sprungs in der virtuellen Rüstung die gesamte Infrastruktur auseinander brechen, da es für solche Netzwerke dann keine eingespielten Sicherheitspraktiken gebe[19].

e) Das ist ein Rückschritt gegenüber dem Internet

Bevor es das eigentliche Internet gab, existierten in den 1970ern bereits eine ganze Reihe allein stehender Netzwerke wie das ARPANET – das meist als eigentlicher Vorläufer des Internet gehandelt wird –, das MILNET, das BITNET oder das JANET. Daraus entwickelte sich schließlich das "Netzwerk der Netzwerke" als Verbundsystem, wie wir es heute kennen, weil die Abgeschlossenheit der Inseln die Verwendbarkeit und Nützlichkeit dieser Kommunikationsnetze schmälerte. Der Zusammenschluss war daher eine bewusste Entscheidung. Die Absplitterung vom Internet würde die gewonnenen Kommunikationsvorteile und Netzwerkeffekte[20] wieder rückgängig machen[21].

f) Heimatverteidigung gegen Terrorismus braucht offenere, nicht stärker abgedichtete Netzwerke

Im Umfeld von Militärpraktikern, denen ein GOVNET zusammen mit den Sicherheitsbehörden ja zunächst am meisten Nutzen zu versprechen schien, stießen Details des Aufrufs Clarkes interessanterweise zum Teil auf wenig Gegenliebe. Aufgrund der im RfI gestellten Anforderungen würden just die Behörden, die bei der Sicherung der Heimatfront zusammenarbeiten, isoliert und die Kommunikation zur Organisation der Ersten Hilfe im Katastrophenfall mit der Außenwelt blockiert, kritisierte etwa Grant Holcomb, Chef der Softwarefirma TeraGlobal und Golfkriegsveteran. "Eigentlich erforderlich wäre es, den Informationsfluss zu öffnen." Schließlich gehe es um die Rettung von Menschenleben[22].

5. Potenzielle Folgen von GOVNET

Das Center for Democracy and Technology (CDT), eine umtriebige amerikanische Bürgerrechtsorganisation, hat die möglichen Konsequenzen der Inbetriebnahme eines GOVNET an zwei Szenarien einmal durchgespielt[23]. So sieht Ari Schwartz, stellvertretender Leiter des Center, auf der einen Seite die Gefahr, dass der Online-Hochsicherheitstrakt der US-Regierung zu wenig genutzt und sich dadurch nicht rentieren würde. Das sei die wahrscheinlichere Variante, da das Projekt bereits mehrfach durch die oben beschriebenen anderen Subnetze in der US-Administration an mehreren Stellen angegangen worden sei. Die Versuche seien aber immer nur auf beschränkte Akzeptanz bei den anvisierten Nutzern gestoßen. Allein Behörden mit einem hohen Anteil an vertraulichen Informationen hätten die geschlossenen Netze angenommen. In diesem Fall "werden gewaltige öffentliche Mittel, die in die Forschung und in

[19] Mills Abreu, Elinor : 'Govnet' Would Be Costly, Prone to Failure-Experts, Reuters-Meldung, 15.10.2001, http://www.reuters.com/printerfriendly.jhtml?type=internetnews&StoryID=291987 (Link vom 16.10.2002).

[20] Die – nicht gänzlich unumstrittene – Theorie von den Netzwerkeffekten (network effects) besagt, dass mit jedem neu an ein Kommunikationsnetz angeschlossenem Nutzer dessen Wert für die Gesamtheit der Anwender exponentiell steigt.

[21] Vgl. a. Schneier, a.a.O.

[22] Porteus, Liza: Plan for government-only computer network called 'colossal mistake', Gov Exec, 20.11.2001, http://www.govexec.com/dailyfed/1101/112001td3.htm (Link vom 22.11.2001).

[23] Ari Schwartz: In the Matter of 'Request for Information for a Government Network Designed to Serve Critical Government Functions (GOVNET)' Comments of the Center For Democracy and Technology, 19.11.2001, http://www.cdt.org/righttoknow/011119govnet.shtml (Link vom 29.6.2002).

Dienste zur Verbesserung der Sicherheit im Internet hätten einfließen können, verschwendet."

Auf der anderen Seite könnte GOVNET sehr stark in Anspruch genommen, spinnt Schwartz die Sache weiter. Auch das hätte seiner Meinung nach fatale Folgen und würde die Geheimniskrämerei unterstützen: "Wichtige öffentliche Informationen und Verabredungen, die im Internet stattfinden sollten, werden geheim gehalten", fürchtet der Bürgerrechtler für diesen Fall. Die Bush-Administration habe zwar versichert, dass auch nach der vollen Implementierung des GOVNET das Internet informationstechnisch nicht vergessen würde. Clarke selbst habe aber klar gemacht, dass Dokumente mit dem Status "Mission Critical" in das neue System fließen würden. Das Problem, das das CDT darin sieht, sind intransparente Entscheidungsmechanismen über das hier oder dort zu publizierende Material sowie mögliche Datenschutzverletzungen. "What protections are in place to assure the public that agencies do not put public information online? How will the general public be able to monitor that new services that should be public are not put directly on to a system that is secretive by design?" Da ein Netzwerk seine Stärke aus den Eingaben einer möglichst unterschiedlichen Nutzerschar ziehe, könne auch die "Allmende Internet" vertrocknen: "While this may not create the extreme of a second Internet, it could lead to a very real 'tragedy of the commons'".

Die Regierung hätte so insgesamt bei der Realisierung von GOVNET "sehr ernste Bedenken auszuräumen" und müsste zeigen, dass die "gut gemeinte Idee" tatsächlich stärker zum Vorteil als zur Last für die amerikanische Öffentlichkeit und vor allem die Internet-Nutzer gerate. Die Ansicht des CDT, dass das Geld für GOVNET besser und sicherer in anderen Bereichen angelegt sei, teilen viele Experten. So gab Richard Forno, Chef der US-Sicherheitsfirma Shadowlogic, Clarke im Januar folgenden Rat: "He should take the GovNet money and fix the existing problems; put in newer, more secure software and operating systems; train the IT staffs and agency managers on how to work in an information-based society and enterprise; and develop a government-wide IT infrastructure that can truly be called 'assured,' 'secured' and 'trusted'"[24].

6. Stand der Diskussion in den USA

Schon aus dem "Kreativität" fordernden RfI leiteten Skeptiker ab, dass es der US-Regierung eventuell um eine rein intellektuelle Herausforderung gehen könnte. Dennoch hat die Anforderung mit über 170 Projektskizzen[25] aus der Wirtschaft eine weit über dem Durchschnitt liegende Antwortrate erzielt. Was allerdings nicht unbedingt etwas über die Durchführbarkeit des Planspiels aussagen muss, sondern zunächst nur Zeugnis für die Misere der IuK-Branche ablegt: Jede Firma kann in den schlechten Konjunktur- und Börsenzeiten einen Großauftrag gut gebrauchen, über dessen Volumen bereits Zahlen von bis zu 45 Milliarden US-Dollar kursierten[26].

Derlei Summen sowie das ganze Projekt sind nach wie vor Gedankenspielereien. Schon kurz nach der Veröffentlichung des RfI stellte Clarke klar, dass die US-Regierung GOVNET nicht unter jeden Umständen realisieren würde: "Wenn sich herausstellt, dass es sehr teuer wird, dann werden wir dies ver-

[24] Zitiert nach: Delio, a.a.O.
[25] Vgl. Delio, a.a.O.
[26] Harris, Shane: Securing the cyber front, Gov Exec, 02.04.02, http://www.govexec.com/dailyfed/0402/040202ti.htm (Link vom 19.06.2002).

mutlich nicht machen"[27]. Aber die Wirtschaft fragen koste die Regierung ja zunächst nichts. Weitere Selbstzweifel plagten den Sicherheitszaren im Dezember auf dem "Global Tech Summit" der Business Software Alliance in Washington. Dort verlieh er nach wie vor der Hoffnung Ausdruck, dass GOVNET Realität werden würde. Gleichzeitig ließ er jedoch durchblicken, dass es auch niemals abheben könnte[28].

Mit einer unabhängigen Untersuchung des vorgeschlagenen Netzwerks sowie der eingereichten Unternehmensideen wurde das Software Engineering Institute der Carnegie Mellon University beauftragt. Bisher liegen allerdings keine offiziellen Ergebnisse vor. Bezeichnend ist auch, dass die Bush-Regierung zwar das Budget für Sicherheit in der Informationstechnik für 2002 um satte 64 Prozent auf vier Milliarden US-Dollar aufstocken will – das wären acht Prozent des gesamten IT-Haushalts. Kein Cent ist dabei bislang jedoch für GOVNET reserviert[29]. Ferner gibt es keine feste Deadline für das weitere Vorgehen im Rahmen des in den Nachwehen des 11. September geborenen Projektentwurfs[30].

In der Wirtschaft hat sich daher Unmut über die schlechte Informationspolitik der Regierung über das weitere Vorgehen breit gemacht: Die meisten involvierten Manager sähen sich im Dunkel gelassen über die eigentlichen Wünsche der Regierung, schrieb der Fachdienst Gov Exec im April. "The consensus among industry officials appears to be that the government hasn't really made a request for anything, but rather that it's gone on an intellectual fishing trip, throwing the prospect of a huge Govnet contract into the technology shark tank and watching the players go to work on it"[31].

Insgesamt ist es mehr als fraglich, ob die Idee weiter verfolgt wird. Anfang Juni hat US-Präsident Bush entgegen früherer Bezeugungen erklärt, ein Ministerium für Homeland Security ins Leben rufen zu wollen. Formell soll es durch diesen Strategiewechsel auf Kabinettsebene in Bezug aufs Clarkes Position wenig Änderungen geben. Dessen Stellvertreter, Paul Kurtz, erklärte jüngst, dass der Cybersicherheits-Chef weiter hauptsächlich an das von der nationalen Sicherheitsberaterin Condoleezza Rice geleitete National Security Council (NSC) angebunden bleibe, in Zukunft aber auch dem Chef des neuen Ressorts berichten würde[32]. Der Vorstoß Bushs belegt, dass der Schutz der Cybersicherheit der Nation in den USA höchste Priorität auf Bundesebene erlangt hat.

Vom GOVNET selbst ist in der aktuellen Diskussion um Cybersecurity in den USA allerdings nicht mehr die Rede. Stattdessen wird – wie von zahlreichen Experten gefordert – der Schutz der bestehenden Netzwerke in den Vordergrund gerückt. "Die Infrastruktur ist das Angriffsziel", gab Kurtz im Juni als warnende Leitparole aus[33]. Zukünftige Terroranschläge würden die Informations-, Finanz- und Transportnetzwerke höchstwahrscheinlich mit einbeziehen. Das auch vom Präsidenten abgesegnete Ziel sei es, Netzunterbrechungen weit gehend zu verhindern und sie andernfalls kurz und handhabbar zu halten.

---

[27] Zitiert nach Rötzer, a.a.O.

[28] Vgl. Delio, a.a.O.

[29] Harris, Shane: White House cyber czar describes next phase of Internet plan. Gov Exec, 17.04.2002, http://www.govexec.com/dailyfed/0402/041702h1.htm (Link vom 18.04.2002).

[30] McGuire, David: Plans For Secure Federal Intranet Moving Forward, Newsbytes, 19.04.2002, http://www.newsbytes.com/news/02/176029.html (Link vom 20.04.2002).

[31] Harris, Securing the cyber front, a.a.O.

[32] New, William: Homeland department likely to house cybersecurity office, Gov Exec, 13.6.2002, http://www.govexec.com/dailyfed/0602/061302td1.htm (Link vom 14.06.2002).

[33] Leopold, George: Homeland defense shifts focus to secure nets, EE Times, 14.06.2002, http://www.eet.com/sys/news/OEG20020614S0093 (Link vom 03.07.2002).

"Wir sind jetzt schwer damit beschäftigt, die Löcher [in den bestehenden Telekommunikationsinfrastrukturen] zu stopfen"[34]. Eine nationale Strategie zur Verbesserung der Sicherheit und Verlässlichkeit von Netzwerken schließe den Einbau von entsprechenden Funktionen in zukünftige Netze sowie das "Härten" des Internet durch die Verwendung sichererer Netzwerkprotokolle ein. Auf der Prioritätsliste des Weißen Hauses weit oben steht laut Kurtz neben dem Ausbau der fortschreitenden Überwachung der Surfer auch, ein schärferes Bewusstsein für die Gefahren und Sicherheitsregeln im Internet bei allen Nutzern über die Site "staysafeonline.info" zu schaffen. Ein Pendant dazu hat die deutsche Bundesregierung bereits seit mehreren Jahren mit dem Angebot "sicherheit-im-internet.de" in Betrieb.

Mit der "National Strategy to Secure Cyberspace" hat die Bush-Regierung ihre Bemühungen inzwischen in eine neue Sicherheitsinitiative gefasst, die zusammen mit der Wirtschaft bis September ausgearbeitet werden soll. "Die Initiative basiert auf zwei Grundideen", erklärte Clarke. "Nummer eins: Nicht nur die Regierung ist verantwortlich für die Sicherheit im Internet. Jeder Einzelne muss jetzt dazu beitragen, seinen Teil des Cyberspace vor Angriffen zu schützen. Nummer zwei: Wir müssen weg vom derzeitigen Akut-Bedrohungs-Konzept hin zu einer Langzeitstrategie, bei der die Gefahren einer möglichen Cyberspace-Verwundbarkeit im Vordergrund stehen"[35]. Gleichzeitig wird er informationstechnologischen Architektur des neuen Homeland Security Department Modellcharakter zuerkannt: Sie soll vom Reißbrett her von einer übergeordneten Sicherheitsleitlinie geplant werden, die sich auf den unteren Ebenen der Pyramide fortsetzt in Business-Abläufen, übergeordneten "Informationsprodukten" wie Terroristen-Suchlisten bis hinunter zu den eingesetzten Technologien im Bereich Hardware und Software-Applikationen, wozu etwa die verwendeten Datenbanksysteme gehören sollen[36].

7. Überschwappen der GOVNET-Debatte nach Deutschland

Mit dem üblichen transatlantischen Time-Lag entdeckte die CDU/CSU-Bundestagsfraktion das GOVNET-Papier Clarkes im Frühjahr 2002 als frühreifes Wahlkampfthema[37]. In einem Antrag[38] (Bundestagsdrucksache 14/8592) forderte die Union die Bundesregierung Ende März auf, "ein Computer- und Datennetzwerk ... zu entwickeln, das von den bisherigen Netzwerken getrennt funktioniert und im Falle einer Störung der vorhandenen Netzwerke unabhängig betrieben werden kann." Zu diesem Netz sollen "sämtliche Bundes- und Landesministerien" sowie "wichtige, für die Aufrechterhaltung der öffentlichen Sicherheit und Ordnung relevante Behörden" Zugang erhalten. Es sollte "dem innovativen Stand an Flexibilität, Integrität und Datensicherheit" entsprechen – beispielsweise wie bei einem Sicherheits-UMTS-Netz für geschlossene Nutzergruppen. Ein solches Computersystem könnte den Behörden bei einer elektronischen Attacke oder ei-

[34] Ebd.
[35] US-Regierung startet Netzwerk-Sicherheitsinitiative, heise online, 11.06.2002, http://www.heise.de/newsticker/data/pmz-11.06.02-000 (Link vom 03.07.2002).

[36] Harris, Shane: White House crafting homeland security technology plan. Gov Exec, 01.02.2002, http://www.govexec.com/dailyfed/0702/070102h1.htm (Link vom 02.07.2002).
[37] Das Magazin Telepolis kritisiert in diesem Zusammenhang u.a. "das Schielen auf das konservativ regierte Vorbild USA" sowie die "pauschale Kritik gegenüber den bisherigen Initiativen in Deutschland". Vgl. Bendrath, Ralf: CDU/CSU will sicheres Regierungsnetz schaffen, 30.03.2002, http://www.heise.de/tp/deutsch/special/info/12202/1.html (Link vom 03.07.2002).
[38] http://www.cducsu.de/aktuelles/initiativen/zx6njv852111348-m16f10tg.pdf

nem Katastrophenfall zur Verfügung stehen, wenn die normalen Systeme ausgefallen sein sollten, heißt es in der Begründung des Antrags. Dies sei auch für den Schutz der Zivilbevölkerung von größter Bedeutung. Besonderen Wert legt die Unionsfraktion ferner auf eine "strenge Trennung" bereits bestehender und neuer Systeme, um ein Übergreifen von Hackerangriffen und Viren auf das neue Netzwerk zu verhindern. Die Task-Force "Sicheres Internet" der Bundesregierung sei damit zu beauftragen, den Netzaufbau zu überwachen und zu begleiten.

Internet- und Medienexperten der rot-grünen Fraktionen erarbeiteten daraufhin eine Art "Gegenantrag" unter dem Titel "Sichere Informations- und Kommunikationsinfrastrukturen gewährleisten"[39]. Darin weisen sie vor allem darauf hin, "dass anders als der US-Administration der Bundesregierung mit dem Informationsverbund Berlin-Bonn (IVBB) bereits ein eigenes, breitbandiges und logisch vom Internet getrenntes eigenständiges Netzwerk zur Verfügung steht. Dieses ist vor äußeren Hackerangriffen oder Viren ebenso besonders geschützt, wie die Benutzer gegenseitig voreinander vor internen Angriffen. Die wenigen Übergänge zum offenen Netzwerken sind sehr gut abgesichert und werden ständig kontrolliert (Firewall, Intrusion Detection, Virenscanner usw.)." Angeschlossen an den IVBB seien neben den Bundesministerien, dem Deutschen Bundestag und dem Bundesrat alle Sicherheitsbehörden, die obersten Gerichte und das Robert-Koch-Institut. Ferner hätten sich auch die Bundesländer für ihren Datenverkehr in einem eigenen Verbund – TESTA Deutschland – zusammengeschlossen, der über Querverbindungen zum IVBB verfüge.

Dezidiert Abstand nehmen die Verfasser des Antrags von der GOVNET-Idee aus den USA – auch wenn der direkte namentliche Bezug nicht erfolgt – sowie den Wünschen der Unionskollegen: "Nicht förderlich ist es aus Perspektive der informationstechnischen Sicherheit, alle elektronischen IuK-Netze der bestehenden kritischen Infrastrukturen in einem gesonderten, einheitlichen und zentralen Netz zusammenfassen zu wollen. Zentralisierte Lösungen bergen allein aufgrund ihrer hohen technischen und organisatorischen Komplexität besondere Risiken (Vielfalt der Gefährdungsdimensionen, Anzahl der Nutzungsberechtigten usw.) und erhöhen sogar die Gefährdung, da Funktionsbeeinträchtigungen infolge von technischen Störungen oder von Angriffen sich innerhalb homogener Netzstrukturen kaum lokal begrenzen lassen." Zu den konkreten Forderungen an die Bundesregierung gehört stattdessen, den IVBB "weiterzuentwickeln und zu prüfen, inwieweit weitere sensible Einrichtungen und Institutionen ebenfalls angeschlossen werden können". Sicherheitsvorteile verspricht sich Rot-Grün außerdem von der weiteren "Entwicklung und Implementierung von Open Source Software".

Gelobt wird die Bundesregierung in dem Antrag auch für die Einrichtung der interministeriellen Arbeitsgruppe KRITIS, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) koordiniert wird. Sie habe die Aufgabe, eine Gefährdungsanalyse zu erstellen und mögliche Bedrohungsszenarien zu bestimmen. Dabei würden neben der Verfügbarkeit elektronischer IuK-Infrastrukturen auch weitere "kritische Infrastrukturen" wie beispielsweise die Wasser- und Energieversorgung oder das Verkehrssystem auf mögliche Schutzlücken hin überprüft. Die Effektivität der Arbeitsgruppe leidet seit ihrem Start 1997 allerdings an den Befindlichkeiten einzelner Ressorts, die sich nur ungern in ihre Sicherheitsvorkehrungen schauen lassen

[39] Der Antrag ist allerdings anscheinend im vorwahlkampfbestimmten Abstimmungsprozess stecken geblieben und bislang nicht in den Bundestag eingebracht worden.

wollen. So hatte die Leiterin von KRITIS, Marit Blattner-Zimmermann, bereits 1999 befürchtet, dass man als "Tiger" gestartet sei und als "Bettvorleger" enden werde[40]. Bis auf rein mündlich vorgestellte Ergebnisse eines ersten "Sensibilisierungsberichts"[41] hat das zuständige Bundesinnenministerium denn auch alle Reports der Gruppe bisher unter Verschluss gehalten. "Die Öffentlichkeit kann also in keiner Weise von den gewonnenen Erkenntnissen profitieren", kritisiert das Computermagazin c't[42].

Weniger Rücksichten auf verwaltungstechnische Diplomatie muss der "Arbeitskreis Schutz von Infrastrukturen" (AKSIS) nehmen, zu dem sich hauptsächlich Unternehmen wie die Deutsche Bahn oder die Lufthansa, Energieversorger sowie Großbanken unter Einbeziehung von Ministerialexperten zusammengeschlossen haben. Durch AKSIS sollen kritische Abhängigkeiten zwischen einzelnen Branchen unter direkten Einwirkungen von "Informationsoperationen" sowie Auswirkungen auf das öffentliche Leben, Wirtschaft und Verwaltung untersucht werden. Ziel ist es, Maßnahmen zur Prävention und Minderung der potenziellen Folgen zu entwickeln. Dazu wurde unter anderem im November 2001 ein erstes computergestütztes Planspiel unter dem Titel 'Cytex 2001" durchgeführt. Ein in Berlin kursierendes, allerdings nicht offiziell veröffentlichtes Kurzgutachten, das von der Ottobrunner IABG im Auftrag des Bundeswirtschaftsministeriums erstellt wurde, fordert interessanterweise unter anderem den "Aufbau eines über Notstrom betreibbaren lokalen Intranetzes in den für Krisenreaktion zuständigen Behörden"[43] – womit der Kreis zu einer Art GOVNET-lite wieder geschlossen wäre.

8. Internationale Initiativen zur Sicherung von Netzwerken

Auch in internationalen Gremien wie einzelnen Beratungsgruppen der G8-Staaten[44], der Organisation for Economic Co-Operation and Development (OECD), dem Europarat[45] sowie der Europäischen Union wird seit einigen Jahren intensiv an der Stärkung der Sicherheit im Bereich Internet und IuK-Technologien allgemein auf der einen sowie an der Bekämpfung der Cyberkriminalität auf der anderen Seite laboriert. Da es in dieser Abhandlung nicht um den Beitrag gehen soll, denn eine effektive Strafverfolgung zur Absicherung von Netzwerken leisten könnte, werden im Folgenden kurz die Initiativen der Europäischen Kommission sowie der OECD im Bereich Netzsicherheit vorgestellt.

[40] Vgl. Drösser, Christoph/Stefan Krempl: Krieg im Computer. Die Zeit 2/2000, 24.
[41] Vgl. Krempl, Stefan: "Der Dialog mit der Wirtschaft muss intensiver werden", VDI nachrichten, 05.05.2000.
[42] Bleich, Holger/Jürgen Kuri: Bedrohtes Netz. Was tun gegen den elektronischen Terrorismus? c't 25/2001, 106-108, hier: 108.

[43] Vgl. Krempl, Stefan: Cytex 200x – die Bedrohung kommt aus dem Cyberspace, Telepolis, 03.02.2002, http://www.heise.de/tp/deutsch/special/info/11746/1.html (Link vom 01.07.2002).
[44] Vgl. Krempl, Stefan: Heiße Luft in bunten Tüten. G8-Staaten tun sich schwer mit der Bekämpfung der Cyberkriminalität, Telepolis, 26.10.2000, http://www.heise.de/tp/deutsch/inhalt/te/4134/1.html (Link vom 30.06.2002).
[45] Die Mitgliedsstaaten des Europarats haben nach jahrelangen Verhandlungen im Herbst 2001 eine "Cybercrime-Konvention" verabschiedet, die Datenschützern und Sicherheitsexperten zufolge über das Ziel weit hinaus schießt und beispielsweise auch "gutwillige Hacker" das Aufspüren von Sicherheitslücken erschweren könnte. Zu den Kritikpunkten im Detail vgl. Krempl, Stefan: Fette Bugs im Cybercrime-Abkommen. Eine Arbeitsgruppe von europäischen Datenschützern findet in der Europarats-Konvention gegen Computerkriminalität schwerwiegende Designfehler, Telepolis, 28.03.2001, http://www.heise.de/tp/deutsch/inhalt/te/7239/1.html (Link vom 30.06.2002).

8.1. Der Aktionsplan für ein sicheres Internet der EU

Die Europäische Kommission hat bereits 1996 einen Aktionsplan[46] zur Förderung einer sicheren Nutzung des Internet aufgelegt[47], der im März 2002 um eine zweite Phase bis 2004 verlängert wurde. Der Finanzrahmen für den ursprünglichen Aktionsplan (1999-2003) betrug 25 Millionen Euro. Für die Neuauflage wurden 13,3 Millionen Euro an zusätzlichen Mitteln bereitgestellt. Der Titel des finanziell gut gepolsterten Programms ist allerdings leicht irreführend: Geht es doch nicht etwa um den Schutz der Netzwerkinfrastrukturen vor unerwünschten Angriffen oder die Abschottung der Nutzer vor Viren. Vielmehr stehen Belange des Jugendschutzes im Vordergrund. So soll der Aktionsplan hauptsächlich "durch den Aufbau eines Netzes von Meldestellen in Europa und die Förderung der Selbstkontrolle ein sichereres Umfeld schaffen", "zur Entwicklung von Filter- und Bewertungssystemen für Inhalte beitragen" sowie grenzübergreifende europäische Sensibilisierungsmaßnahmen fördern".

8.2. Der OECD-Vorstoß zur Begründung einer "Kultur der Netzwerk-Sicherheit"

Um das Internet verlässlicher zu machen, will die OECD eine groß angelegte Kampagne für mehr IT-Sicherheit starten. In einem zehnseitigen Richtlinienpapier hat die "Arbeitsgruppe zu Informationssicherheit und Datenschutz" des Wirtschaftsverbunds der 30 wichtigsten Industrienationen nach dem 11. September Prinzipien zur Begründung einer "Kultur der Sicherheit" im Netzwerkbereich aufgestellt[48]. Sicherheitsfragen sollen demnach auf allen Regierungs- und Industrieebenen Top-Priorität erhalten. Nur so könne der notwendige Schutz der kritischen Infrastrukturen ins Bewusstsein aller Beteiligten gelangen und der Informationsfluss über Schutzmethoden und ihre Implementierung verbessert werden. Mit dem Papier will die OECD einen Ansatz fördern, in dem die Sicherheit zum integralen Bestandteil im Design und in der Anwendung aller Netzwerke und informationstechnischen Systeme wird. Die Mitgliedsstaaten werden aufgefordert, die Richtlinien unter Regierungsstellen, Unternehmen, Organisationen und individuellen Nutzern bekannt zu machen.

Das sich schnell wandelnde Umfeld der Informationstechnologien und des Internets erfordert den Experten zufolge ein neues Denken im Sicherheitsbereich. Die Prinzipien selbst sind allgemein gehalten und beziehen sich auf Punkte wie Sensibilisierung, die Festlegung von Verantwortlichkeiten, rasche Reaktion auf Sicherheitsvorfälle oder die Verbreitung einer gemeinsamen Sicherheitsethik. Die Adressaten der Resolution werden angehalten, ihre internen und externen Arbeitsumgebungen einer permanenten Risikoanalyse zu unterziehen, um Hackereinbrüchen vorzubeugen. Dabei sollen Schlüsselfaktoren wie Technologie, das physikalische und menschliche Umfeld sowie Verhaltensregeln angesichts der sich ständig wandelnden Bedrohungen aus dem Cyberspace immer wieder aufs Neue überprüft werden. Die Fähigkeit zum Aufspüren von Risiken sieht die OECD als Teil eines übergeordneten Sicherheitsmanagements, dank dem alle Beteiligten ent-

46 http://europa.eu.int/information_society/programmes/iap/index_en.htm

47 Vgl. Krempl, Stefan: Sicher, sauber und geschäftsfreundlich, Telepolis, 26.06.1998, http://www.heise.de/tp/deutsch/inhalt/te/1472/1.html (Link vom 30.06.2002).

48 Vgl. Krempl, Stefan: OECD will 'Kultur der Netzwerk-Sicherheit' begründen, heise online, 09.05.2002, http://www.heise.de/newsticker/data/anw-09.05.02-001 (Link vom 30.06.2002).

sprechend ihrer Positionen auf potenzielle Gefahren variabel reagieren können.

Auch die Endanwender sollen ihren Teil zur Sicherheitskultur beitragen. Sie werden aufgefordert, stärker als bisher bei der Auswahl und der Konfiguration von Produkten auf Sicherheitsfaktoren zu achten. Nur so könne Druck auf die Hersteller ausgeübt werden, bei ihrer Soft- und Hardware sowie ihren Dienstleistungen Fragen der Verlässlichkeit in den Vordergrund zu stellen und als essenzielle Elemente bei der Fertigung zu beachten. Die OECD zäumt das Pferd damit von einer anderen Seite als der sonst üblichen Drohung mit der Strafrechtskeule her auf und will die Systeme weniger angreifbar machen. Konkret verlangt eine der Richtlinien, dass die Sicherheitsvorkehrungen mit demokratischen Werten wie "dem freien Informationsfluss, der Vertraulichkeit der Kommunikation, Offenheit und Transparenz" in Einklang zu bringen seien.

9. Was bleibt von GOVNET?

Etwas wie 'völlige Sicherheit' gibt es in einem benutzbaren System schlicht und einfach nicht. Deshalb ist es sinnvoller, sich auf die Verminderung des Risikos zu konzentrieren, als Ressourcen bei dem Versuch zu verschwenden, Risiken vollständig auszuschließen.

Heike Faller, Symantec Schweiz

Die Idee, ein sicheres und vertrauenswürdiges Netz zu schaffen, steht seit langem im Vordergrund des Interesses von Politik sowie Wirtschaft. Das wird auch vor und nach der GOVNET-Debatte "mit Sicherheit" noch eine Weile so bleiben. Der Aufbau verlässlicher informationstechnologischer Infrastrukturen ist eine langwierige Angelegenheit. Zumal, wenn dabei nicht vorschnell Bürger- und Freiheitsrechte wie der Datenschutz oder die freie Meinungsäußerung auf dem Altar der Sicherheit geopfert werden sollen[49].

Der Ist-Zustand im Bereich Netzwerksicherheit wird allgemein als unbefriedigend erachtet[50] – während gleichzeitig tagtäglich die Abhängigkeit der Gesellschaft von den vernetzten Infrastrukturen wächst. So heißt es im bereits erwähnten rot-grünen Antrag "Sichere Informations- und Kommunikationsinfrastrukturen gewährleisten": "Der unerlaubte Zugriff auf vertrauliche Daten und Kommunikation, das unerlaubte Eindringen in geschlossene Netzwerke (Hacking), die Funktionsbeeinträchtigung der technischen Systeme (Denial of Service Attacks) bis hin zu Terrorakten oder der regelrechten Kriegsführung im Netz (Cyber Terror oder Cyber War) machen deutlich, dass eine umfassende informationstechnische Sicherheit (IT-Sicherheit) zunehmend zur Voraussetzung für eine positive Entwicklung der Informationsgesellschaft wird." Die hinreichende Sicherheit und Verfügbarkeit der IuK-Infrastrukturen sei nicht allein eine Frage von E-Commerce oder E-Government. "Sie ist vor allem auch für den modernen Staat eine zentrale Aufgabe einer zukunftsfähigen Vorsorge- und Infrastrukturpolitik."

---

[49] Zu den Konflikten zwischen dem Schutz kritischer Infrastrukturen und den Bürgerrechten s. Madsen, Wayne: Der Schutz kritischer Infrastrukturen, Information Warfare und Bürgerrechte, Telepolis, 07.06.2000, http://www.heise.de/tp/deutsch/special/info/6837/1.html (Link vom 01.07.2002).

[50] In den USA überschlagen sich inzwischen Think Tanks, Regierungsstellen und Wirtschaftsinitiativen schier täglich mit ihren Warnungen vor Angriffen auf die Netzinfrastrukturen des Landes mit terroristischem Hintergrund beziehungsweise in Koppelung mit einem konventionellen Terrorschlag. Zu nennen sind etwa Reports der National Academy of Sciences sowie der Business Software Alliance oder ein Bericht der Washington Post über die Ausforschung von Cyberschwachstellen durch Al-Qaida-Kämpfer, der auch in Deutschland für Schlagzeilen sorgte (vgl. Al Qaida testet angeblich Internet als Terrorwerkzeug, heise online 27.06.2002, http://www.heise.de/newsticker/data/anw-27.06.02-004 (Link vom 03.07.2002).

Die Maximalforderungen des GOVNET-Aufrufs sind allerdings – wie hier dargelegt – kaum zu halten, würden bei einer Umsetzung zu kostspieligen, wenig nutzbaren Separationslösungen führen und könnten sich im schlimmsten Fall als kontraproduktiv erweisen. Unmöglich zu erreichen sind sie allerdings nicht.

9.1 SWIFT – ein Beispiel für ein funktionierendes Eremiten-Net im Finanzsektor

Noch nicht zusammengebracht wurde das in den USA gewünschte Regierungsnetz – zumindest in der öffentlichen Debatte – mit den Erfahrungen aus dem Finanzsektor. Dort betreibt die Society for Worldwide Interbank Financial Telecommunication (SWIFT) weitab vom Internet seit 1973 ein gemeinsames Datenverbundsystem auf Basis internationaler Standards. Es hat inzwischen über 7000 Teilnehmer in 192 Ländern und wickelt über sein 24 Stunden pro Tag erreichbares Nachrichtennetz 90 Prozent des internationalen Finanzverkehrs ab. Im Jahr 2000 wurden bereits 1,2 Milliarden Botschaften übermittelt und so Zahlungsnachrichten von über 5000 Milliarden US-Dollar verarbeitet. Noch in 2002 soll der Dienst auch über eine Variante des Internet-Protokolls, das so genannte Secure IP Network (SIPN), laufen.

Durch das entsprechende SWIFTNet sollen folgende Sicherheitsziele durchgesetzt werden[51]:

- Nur registrierte Endkunden haben Zugang zum Netz;
- die Integrität der Daten beim Transport; nur der Adressat kann die empfangenen Daten lesen;
- die Daten werden rechtzeitig zugestellt (Quality of Service garantiert);
- die Identifizierung aller Teilnehmer wird durch Registrierungsprozesse sichergestellt;
- die Authentizität des Absenders wird gewährleistet und ist überprüfbar;
- die Unabstreitbarkeit (Non-Repudiation) von abgesandten Botschaften wird sichergestellt.

Technologische Basis von SWIFTNet ist ein so genanntes Virtual Private Network (VPN). Über diese Technik lassen sich auch durch das normale Internet "Tunnel" schlagen, die zumindest auf dem Übertragungsweg weit gehend sichere Verbindungsbrücken zwischen den angeschlossenen Kommunikationsteilnehmern bilden. Bei SWIFT kommt zusätzlich ein eigenes IP-Netz zum Einsatz, das vor allem über eigene, geleaste Leitungen sowie über ISDN- und Modem-Einwahlknoten angebunden ist. Zugangs- und Benutzerauthentisierung erfolgen mit Hilfe von Smartcards und einer eigenen Public Key Infrastruktur (PKI), der Basis für den Einsatz von Verschlüsselungssoftware und "Online-Ausweisen" in Form von elektronischen Zertifikaten beziehungsweise Signaturen. Alle übertragenen Nachrichten werden mit einem Zeitstempel versehen. Ein IP-Paketfilter an den Zugangspunkten sorgt dafür, dass Daten nur zwischen autorisierten Kommunikationspartnern vermittelt durch SWIFT transportiert werden können.

Zumindest für sehr beschränkte Einsatzgebiete – das SWIFTNet dient allein dem Nachrichtenaustausch für die Übermittlung von Zahlungsaufträgen und schon die gängigen Büro-PCs der Banken sind nicht an dieses Hochsicherheitsnetz angeschlossen und damit "normal" verwundbar – lässt sich mit dem entsprechenden finanziellen Aufwand also

[51] Vgl. zu den weiteren SWIFT-Ausführungen: Münch, a.a.O., 116ff.

durchaus ein größtenteils abgeschottetes Netz realisieren. Trotzdem bleiben – rein theoretisch – mehrere Risiken in Sicherheitsfragen erhalten. So ist auch das SWIFTNet wie jede Netzwerklösung vom Funktionieren der zugrunde liegenden Telekommunikationsinfrastruktur abhängig, von der es durch gezielte, massive verteilte Denial-of-Service-Angriffe abgeschnitten werden könnte. Auch Attacken auf die übertragenen Daten und damit die Unterwanderung ihrer Vertraulichkeit und ihrer Integrität ist an den Endpunkten einer jeden Verbindung weiterhin prinzipiell möglich[52].

9.2 Kompromisslösung IVBB?

Der bereits erwähnte Informationsverbund Berlin-Bonn (IVBB) ist ein weiteres Beispiel für ein separates Netzwerk auf VPN-Basis. Die Sicherheitsanforderungen sind hier allerdings nicht so hoch wie beim SWIFTNet oder beim vorgeschlagenen GOVNET. So ist im IVBB bislang keine durchgehende Nutzerauthentisierung auf Basis von Signaturkarten implementiert und die PKI dadurch schwächer als im Bankennetz. Der durchgeleitete Verkehr wird jedoch durchgängig verschlüsselt. Wenn technisch möglich und wirtschaftlich vertretbar, soll Ende-zu-Ende-Sicherheit auf Anwendungsebene erreicht werden, z.B. für den elektronischen Dokumentenaustausch.

Wenn auch in der Öffentlichkeit kaum bekannt, hat der IVBB doch bereits einige Jährchen auf dem Buckel[53]: Zwischen den Bonner Ministerien existierte ein Behördennetz bereits vor dem neuen "Hauptstadtbeschluss". 1994 erfolgte dann eine Ausschreibung zur Erweiterung dieses Netzes nach Berlin. Als Ergebnis realisierte die Deutsche Bundespost Telekom (die heutige Deutsche Telekom) die so genannte IVBB-Einstiegslösung ("IVBB-Minimalkonzept"). 1995 wurde das Konzept zur mittel- und langfristigen Realisierung des breitbandigen IVBB fertiggestellt. Parallel dazu erarbeitete das BSI das IT-Sicherheitskonzept für den Verbund. Das Bundeskabinett entschied im März 1996, den Ausbau und Betrieb des dauerhaften, breitbandigen IVBB gemeinsam mit der Telekom weiterzuentwickeln. Ein unabhängiges Ingenieurbüro sollte den Aufbau begleiten. Im Oktober 1996 erhielt das Beratungsunternehmen Gora, Hecken & Partner (GHP) mit seiner Partnerfirma TEKO Ingenieurbüro den Auftrag zur Erarbeitung des Realisierungskonzepts und zur Überwachung und Betreuung der Arbeiten zu dessen Umsetzung. Das Konzept wurde im Juni 1997 vorgelegt und mit den obersten Bundesbehörden abgestimmt. Anfang Januar 1998 unterzeichneten das Bundesinnenministerium und die Firma DeTeSystem Deutsche Telekom Systemlösungen, die heutige T-Systems, den IVBB-Vertrag. Im Januar 1999 begann der Wirkbetrieb auf Basis des breitbandigen Sondernetzes. Der Vertrag hat eine Laufzeit von mindestens 10 Jahren (bis Ende 2008).

Zu den schon in Bonn angebotenen ISDN-Services (Telefonie, Telefax) kamen im Laufe der Zeit Internetdienste hinzu, insbesondere Email. 1997 wurden ein gemeinsames Intranet und ein zentraler Internetzugang für alle Nutzer auf Basis eines IP-Backbone eingerichtet. Eine zentrale Firewall schützt den Übergang zwischen den Netzen der Nutzer, dem IVBB-Intranet und dem Internet. Den hohen Anforderungen an die Verfügbarkeit, Vertraulichkeit und Integrität der Kommunikation ist das Netz bisher gerecht geworden. Im rot-grünen Antrag zu sicheren Informationsinfrastrukturen heißt es zumindest, dass

[52] Vgl. ebd., 130ff.

[53] Vgl. Informationsverbund Berlin-Bonn. Publikation der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) vom Dezember 1999, www.ivbb.de/ aktuell/infopapier/pdf/ivbb5de.pdf (Link vom 02.07.2002).

"bisher kein erfolgreicher Fall eines unerlaubten Eindringens in das bzw. Schädigens des IVBB bekannt ist". Die Infrastruktur unterliegt ständigen Sicherheits- und Funktionsüberprüfungen durch das BSI und muss simulierte Angriffsversuche durch Sicherheitsfachleute bestehen. Der Informationsverbund ist ferner so ausgelegt, dass der Ausfall wesentlicher Komponenten aufgefangen werden kann. "Dies wird unter anderem durch die ringförmige Anbindung (Zweiwegeführung) sowie die doppelte Auslegung (Redundanz) wesentlicher Komponenten erreicht. Die Auslegung als exklusives, separates Netz mit eigenen Übergängen zum Telefonnetz und dem Internet in Berlin und Bonn sorgt für zusätzliche Sicherheit. Damit steht im Krisenfall neben der gesicherten Telefonversorgung auch eine unabhängige Informationsplattform mit IVBB-Intranet zur Verfügung"[54].

Auch wenn der IVBB ausschließlich Nutzern in den angeschlossenen Ressorts und Behörden offen steht, wird über seinen Rücken auch bereits so manche Bürgerdienstleistung mit abgewickelt. Wie der Präsident des Bundesverwaltungsamtes, Jürgen Hensen, in einem Interview[55] erklärte, realisiert sein Haus mit Hilfe des Verwaltungsnetz E-Governmentlösungen, beispielsweise für alle Nutzer neben BaföG-Online auch das Angebot Bildungskredit-Online. Explizit für die Bundesressorts bietet sein Amt das Kabinett-Informationssystem an, für Auslandsschulen sowie Lehrerbewerber eine gesonderte Informations- und Akkreditierungsseite oder für die Mitarbeiter des Bundesverwaltungsamtes ein Informations- und Wissensmanagement. Geplant ist zudem die Einführung eines Travel-Managementsystem mit Workflow- und Internetelementen, mit dem die Reisekosten des Bundes bei Dienststellen und Reisebüros reduziert werden könnten. Daneben baut das Amt mit dem Deutschen Notfallvorsorge Informationssystem (deNIS) im Zivilschutz ein Angebot auf, das neben allgemeinen Informationen für Bürger erstmalig den Handlungsträgern des Zivil- und Katastrophenschutzes die bisher an unterschiedlichsten Stellen in Bund, Ländern, Kommunen, Hilfsorganisationen, Feuerwehren vorgehaltenen Fachinformationen über ein Portal gebündelt zugänglich machen soll.

9.3 Lösung „E-Govnet“?

Wie müsste nun ein verlässliches Netz aussehen, über das Firmen und Behörden elektronische Geschäfts- und Amtsvorgänge ohne tägliche Gewissensbisse anbieten könnten? Ein Netz, in dem die Bürger ohne schlaflose Nächte und Angst vor Hackern dem E-Commerce frönen und das virtuelle Rathaus besuchen könnten?

Ein Netz fürs E-Government, das bei alltäglicher Benutzbarkeit ausreichende Sicherheit bringt, dabei aber die Vision eines unbenutzbaren Hochsicherheitstrakts des ursprünglichen GOVNET-Vorschlags und das Entgleiten in eine Orwellsche "Sicherungszwangsgesellschaft"[56] vermeidet?

Welche Bauteile eines solchen "E-Govnet"[57] sind in Deutschland mit dem IVBB sowie dem Signaturgesetz bereits gelegt und wie könnten diese die internationale Debatte um Cybersecurity befruchten?

Die Schutzziele, die ein E-Govnet berücksichtigen müsste, sind in der Literatur bereits ausführlich beschrieben und werden hier in einer Übersicht noch einmal in ihrer System-

[54] Kruschel, Carsten: Aktuelle Fragen zum IVBB, http://www.ivbb.de/betrieb/f_index.html (Link vom 03.07.2002).
[55] E-Government im IVBB. Interview mit Dr. Jürgen Hensen, http://www.ivbb.de/interview/f_index.html (Link vom 02.07.2002).

[56] Das Thema E-Signaturen als Kontrolltechnik beleuchtet: Krempl, Stefan: Weitersurfen nur gegen Autogramm, Die Woche, 14.04.2000, 34.
[57] Vgl. „E-Gov-Netz“ bei Klumpp (Alcatel Stiftung)

verknüpftheit dargestellt[58]. In der Regel fassen Experten die einzelnen Punkte zu den übergeordneten Gruppen der Vertraulichkeits-, Integritäts- und Verfügbarkeitsziele zusammen.

- *Vertraulichkeit* sichert die Geheimhaltung von Daten während der Übertragung. Niemand außer den Kommunikationspartnern kann den Inhalt der Kommunikation erkennen.
- *Verdecktheit* versteckt bereits den Übertragungsprozess vertraulicher Daten. Niemand außer den Kommunikationspartnern kann die Existenz einer solchen Kommunikation erkennen.
- *Anonymität* sichert, dass ein Nutzer Ressourcen und Dienste benutzen kann, ohne seine Identität zu offenbaren. Selbst der Kommunikationspartner erfährt nicht die Identität des Nutzers.
- *Pseudonymität* sichert, dass ein Nutzer eine Ressource oder einen Dienst benutzen kann, ohne seine Identität preiszugeben, ihm aber trotzdem diese Nutzung zurechenbar ist.
- *Unbeobachtbarkeit* sichert, dass ein Nutzer Ressourcen und Dienste nutzen kann, ohne dass andere beobachten können, dass die Ressource oder der Dienst genutzt wird. Dritte können weder das Senden noch den Erhalt von Nachrichten beobachten.
- *Integrität* sichert, dass Modifikationen der kommunizierten Inhalte – einschließlich des Namen des Senders – durch den Empfänger erkannt werden.
- *Zurechenbarkeit* sichert, dass Sendern beziehungsweise Empfängern von Informationen das Senden beziehungsweise der Empfang der Informationen gegenüber Dritten bewiesen werden kann.
- *Verfügbarkeit* sichert die Nutzbarkeit von Ressourcen und Diensten, wenn ein Teilnehmer sie benutzen will.
- *Erreichbarkeit* sichert, dass zu einer Ressource (Nutzer oder Maschine) Kontakt aufgenommen werden kann, wenn gewünscht.
- *Verbindlichkeit* sichert, dass ein Nutzer belangt werden kann, um seine Zusagen innerhalb einer angemessenen Zeit zu erfüllen.

Wie aus der Übersicht (vorige Seite) unschwer zu erkennen ist, kann es zu "Zielkonflikten" zwischen den einzelnen Gruppen kommen. Das wird noch deutlicher, wenn man die Schutzziele allgemein nach den Kriterien "Privatheit" und "Korrektheit" unterteilt. Dabei kollidiert vor allem das Interesse des Nutzers, kein virtuelles Doppeldasein in unzähligen Datenbanken von Unternehmen und Behörden zu führen oder sich unerkannt im Cyberspace zu bewegen, mit dem Anspruch des Kommunikations- oder Geschäftspartners, es mit einer "ausgewiesenen", ihre Verpflichtungen erfüllenden Persönlichkeit zu tun zu haben. Hier sind Kompromisslösungen ins Auge zu ziehen, die technisch in der Regel möglich sind. So lässt sich der Konflikt zwischen Anonymität und Zurechenbarkeit etwa durch das freie Spiel mit Pseudonymen mildern.

Konkret auf das E-Govnet bezogen: Bei den handelnden Instanzen ist dabei – vor allem auf der Verwaltungsseite – sehr häufig die Identifikation der handelnden Personen erforderlich. In einzelnen Fällen soll jedoch beispielsweise nur die Rolle einer Person festgestellt und ihr etwa ein Gruppenrecht zugewie-

[58] Als konkrete Vorlage verweise ich auf: Wolf, Gritta/Andreas Pfitzmann (2000): Charakteristika von Schutzzielen und Konsequenzen für Benutzungsschnittstellen. In: Informatik Spektrum, 23.06.2000, 173-191, hier: 175. Vergleichbare Definitionen finden sich in: Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements. Version 15408-2 FDIS, ISO/IEC SC27 N2162, 15.11.1998.

sen werden. Die Person selbst kann dabei pseudonym bleiben.

Generell muss ferner zwischen dem Schutz gegen unbeteiligte Dritte und dem Schutz gegenüber den Kommunikationspartnern untereinander unterschieden werden, auch wenn beide Gruppen als "Angreifer" gesehen werden können. Doch die "Schutzziele unterscheiden sich in ihrem Wirkungsbereich gegenüber Angreifern. Manche Schutzziele bieten Schutz vor nicht an der Kommunikation beteiligten Dritten, andere dagegen sogar vor Kommunikationspartnern. Anonymität und Unbeobachtbarkeit sowie Zurechenbarkeit und Erreichbarkeit bieten Schutz gegen den Kommunikationspartner. Diese Schutzziele schließen einen Schutz vor Dritten mit ein. Schutz gegen Dritte (und nur diese) kann weiterhin erreicht werden durch Vertraulichkeit und Verdecktheit, sowie Integrität und Verfügbarkeit"[59].

Für die Umsetzung der meisten Schutzziele stehen heute Wald- und Wiesentechnolgien zur Verfügung. Unterschiedlichste Hersteller bieten Firewalls, Virtual Private Networks oder Public-Key-Infrastrukturen mit Verschlüsselung und elektronischen Signaturen an, wie sie etwa beim IVBB gemeinsam zum Tragen kommen[60]. Es gibt komplette Lösungen "von der Stange", die durchgehende „End-to-End“-Sicherheit zumindest versprechen, auch wenn der Erfolg letztlich stark von den angewandten Sicherheitskonzepten, den Verhaltensregeln und ihrer Befolgung durch die Nutzer abhängt. Mit Hilfe von Mechanismen wie AAA (Authentication, Authorization und Accounting beziehungsweise Identifikation, Berechtigungsprüfung und Abrechnung) lassen sich Zugriffsrechte – auch über das drahtlose Netz – gestalten und verwalten. Die technische Umsetzung einzelner Schutzziele – insbesondere die der Unbeobachtbarkeit und Verfügbarkeit – kann allerdings sehr aufwändig oder teuer sein sowie mit Performance-Einbußen einhergehen. Für manche kann eine schwächere Form des Schutzes durch andere einzelne Schutzziele oder Kombinationen von Schutzzielen erreicht werden[61].

Für die Gewährleistung von Zielen wie Verfügbarkeit und Erreichbarkeit ist zudem das Angebot redundanter Kommunikationswege und die Erarbeitung so genannter Fallback-Strategien entscheidend, die bis zur Duplizierung von Infrastrukturen reichen. Ein wichtiger Faktor ist dabei auch die Vermeidung von Strukturen, die es mit der Standardisierung übertreiben und immer nach dem gleichen Schema mit denselben Komponenten aufgebaut sind.

In diesem Bereich hat Deutschland auf der Softwareseite bereits entscheidende Weichenstellungen vorgenommen und könnte sich damit zum Vorbild beziehungsweise zumindest zum Testfall für andere Nationen entwickeln: Anfang Juni unterzeichnete Bundesinnenminister Otto Schily mit IBM Deutschland einen Rahmenvertrag, dank dem Behördencomputer in Zukunft auch mit Support versehen sind, wenn sie mit Programmen ausgerüstet sind, die im offenen, frei verfügbaren Quellcode vorliegen. Den Zuschlag begründete der SPD-Politiker vor allem mit dem Argument, auf diesem Weg "die IT-Sicherheit durch die Vermeidung von Monokulturen" zu erhöhen. "Wir verringern die Abhängigkeit von einzelnen Anbietern, und wir sparen bei Kauf der Software"[62]. Wenn alle dasselbe E-Mail-Programm verwendeten, führte Schily weiter aus, habe es ein Angreifer sehr viel leichter, einen Computervirus oder ein ande-

[59] Wolf/Pfitzmann, a.a.O., 176.

[60] Für eine Übersicht der Sicherheitstechnologien sowie Beispiele für ihre Implementierung in Firmen siehe: Krempl, Stefan: Der globale Albtraum. Schwerpunkt Internetkriminalität, Connectis 10/2001 (Beilage der Financial Times Deutschland), 15-24.

[61] Vgl. Wolf/Pfitzmann, a.a.O., 181.

[62] Wihofszki, Oliver/Martin Virtel: Schily kickt Microsoft aus Behörden. Financial Times Deutschland, 04.06.2002.

res Angriffswerkzeug zu erstellen. "Linux und andere freie Software bieten die Chance für mehr Vielfalt und damit die Chance zu mehr Sicherheit"[63].

Als Vorreiter präsentiert sich Deutschland auch seit langem bei den E-Signaturen, die im wahrsten Sinne des Wortes eine "Schlüsseltechnologie" für ein sicheres E-Govnet darstellen. Seit der Verabschiedung des Signaturgesetzes 1997 und der Gleichsetzung der elektronischen Signatur mit der eigenhändigen Unterschrift im Sommer 2001 ist der rechtliche Rahmen tatsächlich weit gehend abgesteckt. Doch noch mangelt es am Ausschlag gebenden Erfolgsfaktor: an Anwendungen. Praktisch spielt die Technik, die auf asymmetrischen Verschlüsselungsverfahren beruht, die Authentizität von Dokumenten belegt und als eine Art "Pass" für den Cyberspace fungieren kann[64], im Alltag der Verbraucher und etlicher Unternehmen nach wie vor eine geringe Rolle. Vor allem die unterschriftsersetzende, qualifizierte elektronische Signatur wird vom Rechtsverkehr bislang so gut wie nicht angenommen.

Falls Deutschland seinen Standortvorteil aufgrund der Gesetzgebung und fertiger Wurzelzertifizierstelle nicht verspielen will, müssen Staat und Wirtschaft hier weitere Standardisierungen und Anwendungsszenarien gemeinsam vorantreiben. Die Arbeit am E-Govnet könnte hier entscheidende Anstöße liefern, zumal, wenn dabei auch Aspekte wie die Pseudonymisierung von Nutzern und die Lösung anderer angesprochener Zielkonflikte konzeptionell und technisch mitbedacht würden.

[63] Ewert, Burkard: Schily ärgert Gates. Handelsblatt Netzwert, 01.07.2002.

[64] Bei der elektronischen Signatur wird mittels eines Hash-Algorithmus ein vom Dokument abgeleiteter Prüfwert (der so genannte elektronische Fingerabdruck) mit einem asymmetrischen Verschlüsselungsverfahren verschlüsselt. Jede Veränderung am Dokument kann erkannt werden. Darüber hinaus kann jeder die Urheberschaft des Unterzeichners prüfen, da die akkreditierte Signatur mittels des öffentlichen Schlüssels des Unterzeichners, den man etwa aus einem Verzeichnis laden kann, zeitlich unbegrenzt auf ihre Gültigkeit hin kontrolliert werden kann.

Anhang

Übersicht der Angriffsvarianten auf Netzwerke

Die Palette der möglichen Angriffsziele im Internet, die gute wie böse Hacker ins Visier nehmen können, entspricht der gesamten Netzwerktechnik. Webserver, Hosts oder Applikationen können genauso in ihrem Visier liegen wie Router und Switches, mit deren Hilfe der Datenverkehr durchs Inter- beziehungsweise Intranet geschaufelt wird. Die in der Regel auch von Webadministratoren zur Überwachung ihrer Server verwendete Angriffssoftware ist häufig frei im Netz verfügbar, und per Mausklick lassen sich automatische Suchroutinen starten. Entdecken die Programme Sicherheitslücken, können die Angreifer häufig aus der Ferne bedienbare Software-Applikationen in Form von Trojanern in ein Netzwerk einnisten.

Spionage, Sabotage und Betrug sind einfach im Netz, das von seinen Erfindern als Kommunikationsmedium – und eben nicht als Hochsicherheitstrakt – konzipiert wurde. Die dem Internet eigene Methode, Datenpakete in einzelnen Teilen mit Hilfe des Internet-Protokolls (IP) durch die Leitungen zu schleusen, muss daher fürs E-Business nachgebessert werden. Zahlreiche Schlupflöcher bietet das fundamentale Netz-Design bis heute. Aber viele lassen sich mit marktüblichen Sicherheitslösungen stopfen. Da auch die andere Seite am Ball bleibt und ständig neue Lücken entdeckt oder Angriffstools entwirft, müssen die virtuellen Bollwerke regelmäßig gewartet werden. Tipps für Patches – Pflaster fürs Netzwerk – werden in Newsgruppen oder Mailinglisten wie NTBugtraq (www. ntbugtraq.com) oder Security Focus (www. securityfocus.com) ausgetauscht. Bei täglich rund 200 Nachrichten geht dabei aber manchem Zerberus der Überblick verloren, sodass die Hacker mal wieder die Nase vorn haben. "Da findet ein Wettrüsten statt", sagt Peter Dorrington, Business Solutions Marketing Manager beim Softwarehaus SAS in London.

Paket-Schnüffler

Mit Hilfe eines Packet-Sniffers lassen sich alle Netzwerkpäckchen abfangen, die über eine bestimmte Domain gesendet werden. Administratoren dienen Sniffer zum Aufspüren von Fehlern im Datenverkehr. Da Dienste wie Telnet, FTP oder das gern verwendete E-Mail-Protokoll SMTP aber Daten unverschlüsselt versenden, können Hacker damit auch vertrauliche Informationen wie Benutzernamen oder Passwörter ins Netz gehen. Da diese Kennungen häufig für verschiedene Applikationen verwendet werden, stehen den Datenspionen mit diesen Angaben Tür und Tor zu zahlreichen Ressourcen in einem Netzwerk offen. Im Trüben fischen Paket-Schnüffler allerdings, wenn für die Authentifizierung von Benutzern Einmalkennwörter verwendet werden. Dazu benötigt der User eine PIN sowie eine "Token-Card". Das ist eine Hard- oder Softwarekomponente, die in festgelegten Intervallen Zufallspasswörter generiert. Versucht ein Hacker, sich mit einer abgehörten Kennziffer ins Netz einzuloggen, ist diese dann bereits wieder ungültig. Anti-Sniffer können zudem anhand von Antwortzeiten einzelner Server erkennen, ob diese mehr als den eigenen Datenverkehr bearbeiten. Den besten Schutz gegen die Schnüffler bietet die durchgängige Verschlüsselung der Kommunikationskanäle über Standardprotokolle wie IPSec, Secure Shell (SSH) oder Secure Sockets Layer (SSL). Zudem empfiehlt sich der Aufbau eines verschlüsselten "Tunnels" durch das Netz in Form eines Virtual Private Network (VPN).

IP-Spoofing

Im Internet ist eine durchgehende Authentifizierung von Nutzern anhand einer festen Kennung wie etwa einer unveränderlichen IP-Adresse nicht vorgesehen. Angreifer können sich daher hinter Adressen verbergen, die in einem Netzwerk als vertrauenswürdig gelten, und sich so erweiterte Zugriffsrechte verschaffen beziehungsweise alle an die "getürkte" IP-Adresse gehenden Datenpakete abfangen. Derartige Attacken lassen sich nur durch eine verbesserte Konfiguration der Zugangskontrolle mit Hilfe von Filtern oder einer kryptografischen Authentifizierung durch den Aufbau von Vertrauensinfrastrukturen (Public-Key-Infrastructures) verhindern.

Denial-of-Service-Attacken (DoS)

Derlei Überflutungen von Serverkapazitäten gehören zu den bekanntesten Angriffsformen. Mit Hilfe von Programmen wie Tribe Flood Network, Trinoo oder Stacheldraht werden die betroffenen Server mit sinnlosen Anfragen und Datenpaketen unter Beschuss genommen und lahmgelegt. Oft werden die Attacken von mehreren Rechnern aus gleichzeitig durch vorher dort eingelagerte "Zombies" oder "Agenten" gestartet ("Distributed DoS"). Diese in Hackerkreisen aufgrund ihrer Trivialität verpönte Angriffsform lässt sich nur abschwächen, nicht ganz verhindern. So können Internet Service Provider beispielsweise Begrenzungen von Datenraten einstellen.

Brute-Force-Angriffe

Bei dieser Form des Kennwortangriffs versucht der Hacker durch wiederholte Eingabe von Login-Informationen die richtigen Daten zu erraten. Dazu ist oft nicht viel Einfallsreichtum erforderlich: Britische Psychologen haben anhand einer Befragung von 1200 Internet-Nutzern herausgefunden, dass 80 Prozent als ihr Passwort den Namen oder das Geburtsdatum eines nahe stehenden Familienmitglieds oder den Namen von Stars wie Madonna oder George Clooney wählten. Nur 9 Prozent wählten "kryptische" Kennwörter, die aus unkenntlichen Codes bestanden. Als Hilfe für den Brute-Force-Angriff stehen dem faulen Hacker auch Programme zur Verfügung, die automatisch Passwörter abfragen. Derartige Versuche zum unberechtigten Zugriff auf Netzwerkressourcen lassen sich durch Begrenzungen von Diensten wie Telnet unterbinden. Auch die Hauptfunktion von Firewalls, den virtuellen Türstehern im Internet, besteht in der Abwehr von einfachen, nicht autorisierten Zugriffen.

Social Engineering

Noch leichter gestaltet sich die Ausnutzung menschlicher Schwächen. Mit psychologischen Tricks erfahren Hacker etwa über einen Anruf bei einer Firma oft mehr vertrauliche Informationen, als durch "rohe Gewalt". Im schlimmsten Fall kann ein Angreifer sich mit diesen Sozialtechniken Zugang zu einem Benutzerkonto auf Systemebene verschaffen.

Angriffe auf der Applikations-Ebene

Für Attacken in der Anwendungsschicht werden in der Regel allgemein bekannte Schwachstellen von Software und Protokollen wie Sendmail oder HTTP ausgenutzt. Damit erlangen Hacker Zugriff auf Server mit häufig weit reichenden Berechtigungen. Gegen derlei Angriffe hilft neben einer effizienten, die Security-Diskussion verfolgenden Systemadministration die Verwendung von Intrusion-Detection-Systemen (IDS), die auffällige Abläufe im Netzwerk aufdecken.

Viren, Würmer und Trojaner

Schädliche Software macht Endnutzern genauso wie Firmen zu schaffen. Ein Computervirus löscht Dateien und kann sogar das gesamte Betriebssystem infizieren. Verbreitet sich ein Virus automatisch – etwa über die Adressliste des E-Mail-Programms – weiter, spricht man von einem Wurm. Trojanische Pferde tarnen sich hinter unscheinbaren Dateianhängen, nisten sich beim Anklicken auf dem befallenen Rechner ein und übermitteln wie ein Spion im Netz Informationen an den Absender. Trojaner wie Nebus oder Back Orifice erlauben es Hackern, die eroberten Rechner fernzusteuern. Einen rudimentären Schutz gegen die PC-Ungetüme bieten Anti-Virenprogramme zahlreicher Hersteller wie F-Secure, Network Associates, Sophos, Symantec oder Trend Micro.

Angriffe durch Insider

Viel größer als die Gefahr, die von Hackern außerhalb des Netzwerks droht, ist die von Insidern ausgehende Bedrohung. Die berüchtigten verärgerten Angestellten, Spione, oder Besucher können – oft mit enormem Wissen und als "Man in the Middle" mit vollen Zugriffsrechten ausgestattet – Angriffe von innen heraus ohne große Anstrengungen starten und wichtige Informationen abziehen oder zerstören. In Frage kommen auch Auftragnehmer bis hin zur "Reinigungsfirma oder zum Gebäudemanagement", weiß Klaus Gerd Hartmann, Geschäftsführer des Aktionskreis Sichere Wirtschaft (www.asw-online.de) in Berlin. Abhilfe bietet auch die Verschlüsselung sensibler Firmenkommunikation. Seriöse Studien schätzen den Anteil der von Innentätern begangenen Cyber-Straftaten auf 60 bis 80 Prozent.

Alcatel SEL Stiftung

Alcatel SEL Stiftung

Hauptanliegen und Themenschwerpunkt der Alcatel SEL Stiftung für Kommunikationsforschung ist seit ihrem Bestehen die Förderung von herausragenden Forschungsarbeiten, die zum besseren Zusammenwirken von Mensch und Technik in Kommunikationssystemen beitragen. Damit ist eine übergreifende Schnittmenge der verschiedensten Disziplinen und Gruppen in Wissenschaft und Praxis angesprochen.

Leistungsteile sind neben dem jährlichen „Forschungspreis Technische Kommunikation“ für die besten wirtschaftswissenschaftlichen Arbeiten zum Themengebiet der Kommunikationstechnik derzeit mit jährlichen Zuschüssen vier eigenständige Stiftungskollegs an deutschen Hochschulen. An der Universität Stuttgart ist es das „Stiftungskolleg zur Förderung von Forschung und Lehre über Theorie und Anwendung der Kommunikation“, an der TU Dresden das „Stiftungskolleg für interdisziplinäre Verkehrsforschung“, an der TU Darmstadt die „Stiftungsgastprofessur für interdisziplinäre Studien“ sowie das Stiftungs-Verbundkolleg Berlin zum Thema „Informationsgesellschaft“.

Die 1979 eingerichtete Stiftung, die als gemeinnützige Wissenschaftsstiftung vom Stifterverband für die Deutsche Wissenschaft als Treuhänder verwaltet wird, unterstützt mit Veranstaltungen, Publikationen und Expertisen ein eng mit der Praxis verbundenes multidisziplinäres wissenschaftliches Netzwerk, in dem wichtige Fragestellungen der Informations- und Wissensgesellschaft frühzeitig aufgenommen und behandelt werden.

Alcatel SEL Stiftungskolleg an der Universität Stuttgart

Die Alcatel SEL Stiftung gründete 1986 gemeinsam mit der Universität Stuttgart das interdisziplinäre „Stiftungskolleg zur Förderung von Forschung und Lehre über Theorie und Anwendung der Kommunikation“. Impulse für eine verstärkte Forschung, Lehre und andere Wissensvermittlung zwischen den einzelnen Disziplinen durch Gastwissenschaftler, Symposien und sonstige Lehrveranstaltungen sollen helfen, eine menschengerechte Technik zu entwickeln. Im Vordergrund steht das Zusammenwirken von Mensch und Technik in Kommunikationssystemen. Neben der Vorlesung des jeweiligen Kollegiaten finden diverse (internationale) Kolloquien, Tagungen sowie Workshops statt.

Stiftungskollegiaten an der Universität Stuttgart waren im Sommersemester 2001 Professor Peter deBois, Institut für Städtebau und Entwerfen an der Technischen Universität Delft, sowie Professor Elizabeth Deakin, Department of City and Regional Planning, University of California, Berkeley. Die Vorlesung und der Workshop von Professor deBois befassten sich mit „Städtebauliche Analyse- und Entwurfsmethodik im Kontext der europäischen Kulturen“, Professor Deakin las zum Thema „Bedeutungswandel der Zentren“.

Vom 15. bis 17. November 2001 fand der Kongress „Wirtschaftsethische Fragen der E-Economy“ statt, den das Stiftungskolleg gemeinsam mit dem Ausschuss Wirtschaftsethik der allgemeinen Gesellschaft für Philosophie in Deutschland veranstaltete. Am 23. November fand die Tagung „E-Commerce (b2b) und seine Folgen für Stadt und Verkehr“ statt. Darüber hinaus wurde im Wintersemester 2001/ 2002, gemeinsam mit Gastdozenten, die Vorlesung „Methoden der Modellierung und der ereignisorientierten Simulation der Logistik“ durchgeführt.

Kontakt

Alcatel SEL Stiftung
Lorenzstraße 10, 70435 Stuttgart
Telefon 0711-821-45002
Telefax 0711-821-42253
E-mail sel.stiftung@alcatel.de
URL: http://www.alcatel.de/stiftung