TeleTrusT Deutschland e.V.
Der IT-Sicherheitsverband.

IT-Sicherheit als politische Aufgabe

TeleTrusT-Publikation – Mit freundlicher Genehmigung der Deutschen Gesellschaft für Auswärtige Politik e.V.

Impressum

Herausgeber:

TeleTrusT Deutschland e.V.
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 306
Fax: +49 30 400 54 311
E-Mail: info@teletrust.de
http://www.teletrust.de

Herstellung:

DATEV eG, Nürnberg

1. Auflage

Die Zusammenstellung der Beiträge in dieser TeleTrusT-Publikation beruht auf Veröffentlichungen in 'IP – Internationale Politik' (2009-09/10), herausgegeben von der Deutschen Gesellschaft für Internationale Politik e.V. (DGAP), Rauchstraße 17/18, 10787 Berlin.

Zu den Autoren:

HENNING WEGENER, Botschafter a.D., ist Chairman des Permanent Monitoring Panel on Information Security der World Federation of Scientists, Genf.

JODY WESTBY ist Direktorin der Firma Global Cyber Risks in Washingon D.C. und Fellow des Carnegie Mellow CyLab.

Dr. UDO HELMBRECHT war Präsident des Bundesamtes für Sicherheit in der Informationstechnik und ist nunmehr geschäftsführender Direktor bei der Europäischen Agentur für Netz- und Informationssicherheit ENISA.

Die Beiträge behandeln das Thema IT-Sicherheit in einem weit gesteckten außen- und innenpolitischen Rahmen. TeleTrusT dankt der IP-Redaktion, namentlich Frau Dr. Sylke Tempel, Chefredakteurin, für die freundliche Unterstützung.

Dr. Holger Mühlbauer
TeleTrusT Deutschland e.V.

HENNING WEGENER

Der unsichtbare Feind - Die neuen Gefahrenlagen im digitalen Raum

Krankenhäuser, Unternehmen, Banken, nationale Verteidigung – unsere gesamte Infrastruktur wird von Computertechnik gesteuert. Wir stehen vor einem Quantensprung: Die Vorteile der digitalen Technik sind immens, die Gefahren noch größer. Denn die Angreifer auf die digitale Infrastruktur sind den Verteidigern immer einen Schritt voraus.

Digitale Techniken schaffen neue Paradigmen für Struktur und Betrieb unserer Gesellschaft. Immer mehr Lebensbereiche werden mit digitalen Techniken gesteuert, vernetzt und sind von ihnen abhängig. Je mehr diese Abhängigkeit wächst, desto mehr werden die Stabilität, Sicherheit und Verlässlichkeit der Systeme, das Vertrauen in ihre Funktionsfähigkeit und der Schutz der Privatsphäre auch zur Funktionsvoraussetzung unserer Gesellschaft.

Informationssicherheit wird damit zu einer Schlüsselaufgabe politischen Handelns, zu einer Herausforderung, die allerdings noch der universellen Analyse und strategischen Antwort harrt. Die Verwundbarkeit der digitalen Endgeräte und der sie verbindenden Netze wird unterschätzt – obwohl die Gefahren und Schäden mit zunehmender Beschleunigung und höherer technischer Raffinesse alarmierend und exponentiell wachsen. Die Dynamik dieses Wachstums, das unkontrollierte Wuchern der Angriffe im Cyberspace und die enorme Potenzierung der Gefahren zeigen: Wir stehen vor einem Quantensprung im Bereich der digitalen Bedrohungen.

Die Segnungen der neuen Informations- und Kommunikationstechniken (IKT) sind evident. Doch hat der digitale Planet auch eine ausgesprochen sinistre Seite. Wie bei allen modernen Technologien stehen den Chancen auch Verwundbarkeiten gegen-über. Die digitalen Technologien jedoch weisen ein besonderes Merkmal auf: Sie vergrößern die Ausschläge; mit den Gewinnen steigern sich meist überproportional auch die Risiken. Der digitale Raum wird ein immer gefährlicheres Ambiente.

Es ist das System moderner Kommunikationstechnologie selbst, das auch die Möglichkeit für Missbrauch und Attacken bietet. Dabei geht es nicht nur um das Internet, sondern um alle digitalen Datenträgerdispositive und die sie verbindenden Netze. Sie sind leicht und von überall zugänglich und damit auch überall angreifbar. Die Manipulation von Daten und Systemen ist Individuen ebenso wie Gruppen mit krimineller Absicht oder Staaten möglich.

Angriffe sind grundsätzlich anonym oder anonymisierbar. Sie können von jedem Punkt der Welt aus auf jedes vernetzte System erfolgen: Informationssicherheit ist eine Herausforderung universaler Dimension. Angriffe wirken in Bruchteilen von Sekunden. Sie sind unsichtbar, „virtuell“ und unmittelbar, aber ihre Folgen können oft auch lange unerkannt bleiben. Die Zuordnung und Verfolgung der Verur-

sacher sind ein Problem, das sich in anderen Bereichen in diesem Ausmaß nicht stellt. Angriffe im Internet und auf andere Netzwerke sind gratis oder extrem kosteneffizient; es gibt keine ökonomische Relation zwischen einem Cyberangriff und dem angerichteten Schaden.

Erste Abwehr

Je besser die nationale digitale Infrastruktur, umso höher sind die Gefährdung und der Bedarf an Gegenmaßnahmen. Selbstverständlich wurden schon einige Grundlagen geschaffen, um diesen Herausforderungen zu begegnen. Die USA investieren seit Jahren hunderte Millionen Dollar in den Schutz ihrer nationalen Infrastrukturen. Beispielhaft für das gestiegene Bewusstsein und eine entschlossene nationale Sicherheitspolitik ist die Erklärung Präsident Obamas vom 29. Mai 2009,[1] in der er zu mehr Sicherheitsinvestitionen und nationaler Koordination aufruft und einen Chefkoordinator im Weißen Haus bestellt.

In anderen Staaten bleiben die Vorkehrungen lückenhaft und es fehlt an ausreichender Reaktionsfähigkeit und Koordination. International ist eine Sicherheitsindustrie hohen technischen Niveaus mit zweistelligen jährlichen Wachstumsraten entstanden. Die Wirtschaft schützt sich mit hohen Investitionen kollektiv und auf Unternehmensebene. Durch teils öffentliche, teils private Initiativen ist ein Netz von technischen Eingriffskommandos (Computer Emergency Response Teams/CERT) eingerichtet worden, das heute bereits in den meisten Ländern tätig ist und sich koordiniert.

Auch die übernationalen und internationalen Organisationen reagieren. Die EU-Kommission hat, wie in der ganzen Digitaltechnik, umfassende regulatorische Intiativen ergriffen und eine eigene Netzsicherheitsagentur (ENISA) eingerichtet. Die NATO betreibt ein Schwerpunktprogramm Cyberdefence.[2] Der Europarat hat mit der Aushandlung der Convention on Cybercrime rechtliche Basisarbeit geleistet. Bei den UN-Gipfeln zur Informationsgesellschaft 2003 und 2005 wurde das Thema Vertrauen und Sicherheit in den IKT ganz prominent behandelt. Die Internationale Fernmeldeunion (ITU) wurde zum Koordinator dieses Aufgabenbereichs bestellt und hat seither hervorragende Arbeit geleistet, die ihr eine internationale Führungsrolle[3] sichert. Die UN-Generalversammlung hat seit den neunziger Jahren die Auswirkungen von Cyberangriffen auf die internationale Sicherheit problematisiert. Immer wieder haben die Vereinten Nationen die Schafffung einer Global Culture of Cybersecurity gefordert. Nichts zu wünschen übrig lässt die wissenschaftliche Befassung mit den Cybergefahren.

Es ist also Bemerkenswertes geleistet worden. Doch bleiben die Verteidigungs- und Vorsorgemaßnahmen immer wieder hinter den wachsenden Gefahren zurück. Die Cyberverteidigung hält mit den frenetischen Veränderungen im digitalen Raum und den neuen Gefährdungen einfach nicht Schritt. Im digitalen Kampf kann der Angreifer eine Attacke mit fast unbegrenzter technischer Freiheit wählen, während die Verteidigung reagieren und Schwachstellen abdichten muss. International stellt sich deshalb oft die Frage, ob der Kampf gegen die Cyberkriminalität angesichts der Allgegenwart digitaler Systeme überhaupt noch zu gewinnen ist.

Im öffentlichen Bewusstsein hingegen werden das Ausmaß der Bedrohung, die Dringlichkeit wirksamer Gegenstrategien und die Abwehr- und Beteiligungsmöglichkeit der Einzelnen noch nicht ausreichend wahrgenommen. Auch Beurteilungsmaßstäbe fehlen, eher machen sich die Ängste an meist irrational überhöhten Gefahren im Bereich der Atomenergie, des Klimas, der Umweltverschmutzung, an eventuellen Pandemien oder der Wirtschaftskrise fest.

Digitale Delikte

Kern der Computerdelikte (Cybercrimes) ist der direkte Zugriff auf Datenverarbeitungs- und –speicherapparate durch illegalen Zugang. Datenraub oder Datenmanipulation sowie durch Störung bzw. Zerstörung oder Missbrauch des Datenträgersysteme. Es handelt sich also um Delikte gegen die Integrität, Authentizität, Verfügbarkeit oder Vertraulichkeit von digitalen Systemen und ihren Daten, wie sie auch die wegweisende Convention on Cybercrime des Europarates definiert.[4]

Davon zu unterscheiden, wenn auch nicht weniger bedeutend, ist die Nutzung der enormen Kommunikations- und Multiplikatorfähigkeiten des Internets und anderer digitaler Mittel für illegale Inhalte: Pornographie mit Minderjährigen, Verletzung von Urheberrechten, Propagierung von Rassenhass, Anstiftung zu Krieg und Verbrechen, Werbung für Terrorismus oder betrügerische Offerten aller Art. Die Konvention des Europarats stellt Kinderpornographie und die Verletzung von Urheberrechten, in einem Zusatzprotokoll auch Fremdenhass und Rassismus, unter Strafe. Da für die große Zahl der sonstigen inhaltsbezogenen Internetdelikte „normale“ nationale und internationale Sanktionen greifen, konzentrieren sich diese Ausführungen auf den Kernbereich der Cyberdelikte: die technische Manipulation von digitalen Systemen und ihrer Daten.

Die neue Dimension der Bedrohung beeindruckt zunächst durch das schiere Ausmaß: Zurzeit dürfte es weltweit mehr als 1,5 Milliarden -konventionelle internetfähige Computer geben. Immer mehr verfügen über einen Breitbandzugang; in manchen Ländern liegt diese Quote sogar bei über 80 Prozent. Breitbandkapazität ist für alle großen digitalen Steuerungsaufgaben und für Datentransport unabdinglich. Computer sind ein wichtiger Teil der Bedrohungslandschaft, aber potenzielle Opfer von Computerdelikten sind auch alle anderen Gerätschaften, in denen Mikroprozessoren digitale Daten verarbeiten. Dazu gehören Mikroprozessoren in eingebetteten Systemen, mobile Systeme von Mobiltelefonen zu Taschencomputern und die schon heute omnipräsenten Sensoren wie Radio Frequency Identification/RFID.

Hier befinden wir uns bereits im zweistelligen Milliardenbereich. Die jüngsten technologischen Entwicklungen zeigen, welche Dimensionen sich hier eröffnen: Ultraminiaturisierung von digitalen Schaltkreisen, massiver Einsatz von Prozessoren mit Mehrfachkernen, vermehrter Einsatz von Glasfaser, rapide Zunahme des mobilen Datentransports, Entwicklung neuer potenter „smarter“ Geräte, Reifwerden des Quantum Computing, Ubiquität von neuen miniaturisierten Computing-Elementen, die auch zu ganz neuen, andersartigen Strukturen und Verarbeitungsmechanismen digitaler Netze konfiguriert werden. Dazu kommen eingebettete Systeme, Biometrie, die Entwicklung zum „Internet

of Things“ mit in Kleidung eingenähten oder in Brillengestellen untergebrachten Miniaturcomputern, die Konstruktion von autonom operierenden und sich selbst organisierenden Zwergcomputern, die automatisch mit anderen digitalen Geräten kommunizieren. Alle diese Entwicklungen tragen zum explosiven Wachstum der digitalen Akteure, zu einer enormen Vernetzung und damit zu einer neuen Größenordnung der Verwundbarkeiten bei.

Zu diesen quantitativen Fakten treten die Phänomene von Migration und Konvergenz. Es kann immer weniger zwischen verschiedenen digitalen Handlungsebenen unterschieden werden. Die Festnetztelefonie wandert immer mehr in den Bereich drahtloser Kommunikation und ins Internet, und die Computing-Vorgänge und die Speicherung großer Datenmengen werden aus den individuellen und Geschäftscomputersystemen in riesige externe Datenzentren (Server-Farmen oder auch Grid Computing) mit tausenden von Servern und Speicherkapazität im Petabyte-Bereich verlegt. Die Rechen- und Speichervorgänge sind dabei für den einzelnen Nutzer völlig intransparent und machen im Übrigen die traditionellen Zugangsschleusen (Firewalls) funktionslos. Festnetze und drahtlose Netze konvergieren bis zur Ununterscheidbarkeit, zumal sich zunehmend Ad-hoc-Netze für bestimmte Anwendungen bilden lassen.

So entsteht eine riesige integrierte Netzwerkstruktur mit einem kaum noch fassbaren Universum von Konnektivitäten – und Verwundbarkeiten – , in dem wichtige Komponenten wie mobile Systeme, RFID und eingebettete Mikroprozessoren mit wichtigen Steuerungsfunktionen digitalen Angriffen völlig schutzlos ausgeliefert sind.

Ende der romantischen Ära

Seit dem Beginn des Computerzeitalters hat es Virusattacken, teilweise auch massiver Art, gegeben, für die leicht Antivirus-Software entwickelt werden konnte. Aber diese „romantische Ära“ ist endgültig vorbei. An die Stelle von Einzeltätern, meist jugendlichen Hackern mit spielerischem Motiv, sind riesige kriminelle Konsortien mit hoher Professionalität und unbegrenzten technischen und finanziellen Mitteln getreten.

Diese organisierte Kriminalität konzentriert sich auf wenige Länder, kanalisiert aber ihre Attacken zwecks Anonymisierung über andere Staaten (Schwerpunkt: USA) und benutzt weltweit auch Individuen im Netz, zum Beispiel zur Geldwäsche. Diese Konsortien verfügen über riesige Karteien von Emailadressen, mit denen massiv Spamnachrichten abgesetzt werden können, die für entsprechende Auftraggeber ein lukratives Geschäft sind. Heute sind bis zu 90 Prozent des weltweiten Emailverkehrs Spammails, die der Einzelnutzer nur deshalb nicht in vollem Umfang bemerkt, weil die Netzbetreiber relativ wirksame Filter einsetzen. Spamnachrichten belästigen die Nutzer nicht nur, sie dienen auch als Träger von Viren und anderer Schadens-Software (malware).

Vor zehn Jahren wurden 40 000 Virusvarianten gezählt; 2008 hat die Sicherheitsfirma Panda deren Zahl auf 13 Millionen geschätzt. Bei allen Formen von Malware wirken die Schutzprogramme nur ge-

gen bekannte Versionen. Die mit häufig überlegenen Techniken arbeitenden und erstaunlich schnellen neuen Angreifer entwickeln jedoch ständig neue Varianten, so dass die Verteidiger ohne Pause neue Schwachstellen beseitigen müssen. Ein gutes Antivirusprogramm muss mehrfach täglich seine Datenbasis aktualisieren.

Versklavte Rechner

Die vielleicht gefährlichste neue Entwicklung ist das Entstehen von Botnets. Der Begriff bezeichnet das für den Computernutzer nicht erkennbare Einpflanzen von Viren, die ruhen, aber vom Angreifer jederzeit „geweckt" werden können („Trojaner"). Sie machen die Computer zu Zombies und erlauben, wenn in großer Zahl vernetzt, dem kriminellen Manager (bot herder oder bot master) jederzeit umfassende Operationen. Große Botnets sind hierarchisch, ja geradezu militärisch organisiert. Schätzungen zufolge sind in manchen Ländern 60 Prozent der Computer von Trojanern befallen. Einige Varianten der Botnet-Software sind in der Lage, selbsttätig weitere Computer für das net zu rekrutieren.

Zu den aktuellen Schadensformen gehört insbesondere das Ausspähen persönlicher Daten aus allen Lebensbereichen, einschließlich privater Passworte. Damit können Bankkonten geplündert, Geschäftszahlen, Kundenkarteien, Produktionsplanungen und -entwürfe geraubt und die entsprechenden Dateien sogar gefälscht werden. Datenspionage führt immer häufiger zu einem „Identitätsdiebstahl", mit dessen Hilfe der kriminelle Urheber die Identität des Ausgespähten zu Lasten des Ausgespähten nutzen kann. Über die Botnets können auch die Prozessfunktionen von Computern (Logikbomben) oder deren Daten zerstört oder verändert werden. Nicht weniger gravierend ist, dass Botnets durch gleichzeitiges Aufrufen einer großen Zahl von Computern beispielsweise die Webserver oder die Emailadressen der Zielempfänger saturieren, lahmlegen und sogar dauerhaft beschädigen können (Distributed Denial of Service/DDoS). Damit können nicht nur Unternehmen oder ganze Geschäftszweige, sondern auch essentielle Infrastrukturen – Regierung, Elektrizitätsversorgung, Steuerungscomputer im Bankwesen, Luft- und Eisenbahnverkehr, bei Talsperren, die technische IKT-Infrastruktur selbst – mit hoher Schadenswirkung funktionsunfähig gesetzt werden. Das gleiche gilt, noch gravierender, für Einrichtungen im Verteidigungssektor. Die dreifache Nutzungsmöglichkeit der Botnets für Datenspionage, insbesondere Industriespionage, Logikbomben und DDoS ist in der Tat ominös.

Die von kriminellen Konsortien aufgebauten Botnets nehmen immer größere Ausmaße an. Das bisher größte erkannte Botnet hatte laut Schätzung 1,5 Millionen Computer versklavt. Das neueste Botnet Conficker, gegen das noch keine Gegenstrategie entwickelt werden konnte, wäre in der Lage, fünf Millionen Computer in 122 Ländern zu steuern.

Andere gängige Methoden der Netzkriminalität mittels Botnets oder auch außerhalb sind die Umleitung von Computern auf gefälschte Internetseiten von Banken, um Passwörter oder Kreditkartennummern und damit Zugang zu Konten zu erlangen (phishing) oder das Pharming, das ebenfalls betrügerisch auf andere Seiten umlenkt. Verlässlichen Schätzungen zufolge belaufen sich die durch

Internetkriminalität entstehenden Schäden für die Wirtschaft auf etwa 180 Milliarden Euro jährlich. Genaue Quantifizierungen sind allerdings nicht möglich, da Unternehmen, vornehmlich Banken, die Schäden im Interesse des Kundenvertrauens oft stillschweigend decken.

Digitales Pearl Harbour

Die riesigen Gewinne, die vor allem das organisierte Verbrechen durch digitale Wirtschaftskriminalität abschöpft, sind nur ein Teil des Bedrohungszenarios. Wichtiger sind die neuen Möglichkeiten im Bereich der Cyberkonflikte. Botnets erlauben es, mit koordinierten gleichzeitigen Angriffen gegen das Wirtschaftssystem zentrale nationale Infrastrukturen und das Verteidigungsdispositiv eines Landes in Sekundenschnelle faktisch alle bedeutsamen Lebensbereiche durch massives DDoS lahmzulegen.
Die Cyberattacken auf Estland und Georgien vom Frühjahr 2007, bei denen die Server von Banken, Unternehmen, Regierungen und Parteien lahmgelegt wurden, geben einen Vorgeschmack auf das, was inzwischen technisch möglich ist. Die technischen Voraussetzungen für ein digitales Pearl Harbour sind eindeutig gegeben. Da alle Verteidungsministerien neben den geschützten, aber ebenfalls verletzbaren Infranetzen auch die zivilen Netze nutzen, sind nicht nur massive DDoS-Blockaden möglich. Darüber hinaus kann Verteidigungsplanung ausspioniert, Gefechtsfeldinformation verfälscht, in Befehlsstränge interveniert und das Funktionieren von Waffensystemen beeinflusst werden.

Die direkten gewinnträchtigen Aktivitäten der kriminellen Manager sind nur ein Teil ihres „Geschäftsmodells“. Im Internet sind ganz aktuelle Malware oder Hinweise auf die Schwachstellen kommerzieller Software und Instruktionen für den Diebstahl von Passworten oder Kreditkartennummern erhältlich. Listen mit bis zu Millionen Emailadressen stehen zum Verkauf. Konsortien können auch Cyberangriffsdienste kaufen oder stundenweise mieten, so dass andere kriminelle Akteure wie Terroristen oder feindliche Regierungen, ohne identifiziert zu werden, hinter derart unheiligen Allianzen agieren können. Angesichts solcher Aktivitäten verschwimmen die Grenzen zwischen den Kategorien Cybercrime, Cyberterrorism und Cyberwar.

Fast alle Regierungen sehen diese Entwicklungen mit Sorge und versuchen, größtmögliche Vorsorge zu treffen. Über die legitimen defensiven Vorkehrungen hinaus ist jedoch problematisch, dass sich heute bis zu 140 Länder – darunter vor allem die großen Mächte – mit offensiver Informatik ausrüsten und Cyberangriffsoptionen in ihre Planungen einbauen. Zugegeben, eine klare Unterscheidung zwischen Angriffs- und Abwehrtechnologie ist schwer möglich; „Information Weapon“ ist noch nicht definiert. Eine Unterscheidung ist aber bei Absichten und strategischer Planung möglich: Cyberangriffe, die sich im zivilen und militärischen Bereich der gleichen Techniken bedienen, sind klar definiert.

Weltweite Verbotsnormen

Welche wirksamen Gegenstrategien stehen zur Verfügung? Welche Aufgaben haben nationale Regierungen, internationale Organisationen, Wirtschaft und Industrie sowie einzelne Nutzer? Da die Bedrohung global ist, muss auch das Netz der Verbots- und Sanktionsnormen weltweit komplettiert werden. Es darf keine rechtsfreien Räume geben, die straffreie Angriffe erlauben. Die im Europarat ausgehan-

delte 'Convention on Cybercrime' hat hier den Boden bereitet. Sie ist von 26 Staaten ratifiziert, von weiteren 20 gezeichnet worden. Die Vorschriften haben aber über den Kreis der Vertragsparteien hinaus Modellcharakter. Die Konvention muss Standard für eine universelle, harmonisierte Strafverfolgung von Cyberdelikten werden.

Dringend gefordert ist auch eine universelle Möglichkeit der Rechtsverfolgung. Hier bietet die Konvention Regeln für die internationale polizeiliche und gerichtliche Zusammenarbeit. Zentrale Elemente sind die permanente Kontakt- und Informationsmöglichkeit der Rechtsverfolgungsbehörden sowie eine stärkere Rolle von Interpol und Europol. Zur effektiveren Rechtsverfolgung sollte möglichst schnell und einheitlich das Internetprotokoll IPv6 eingeführt werden, um Identifikation, Zuordnung und Transparenz von digitalen Nachrichten zu erleichtern.

Das Netz von technischen Eingriffskommandos muss komplettiert und zu einem Netz international operierender, multidisziplinärer Cyber Reponse Centers mit umfassenden Überwachungs- und Koordinierungsaufgaben ausgebaut werden.

Auch die Industrie muss sich verantwortlich dafür fühlen, in die Designs ihrer Geräte und Software von Anfang an mehr Sicherheit einzubauen. Heute sind neue Anwendungen viel zu anfällig gegen Angriffe. Das gilt gerade auch für mobile Systeme, deren enorm gestiegene Verbreitung die integrierten Netze zunehmend gefährdet, und für die neuen Techniken im Grid Computing und Cloud Computing.

Die Regierungen müssen sich den neuen Bedrohungen noch umfassender stellen und Vorkehrungen für Vorsorge und -Abwehr treffen, wobei einer raschen und effektiven nationalen Koordination große Bedeutung zukommt. Das Bewusstsein und die Kenntnis von den Gefahren im digitalen Raum und verantwortungsvolle Nutzung müssen integrale Teile der Erziehung besonders der jungen Generation für das Internetzeitalter werden. Ihr muss früh eine Kultur der Informations-sicherheit vermittelt werden.

Die Nutzer der IKT – Wirtschaft, Manager von Infrastrukturanlagen und der individuelle Benutzer – müssen mehr Wachsamkeit und Selbstschutzinstinkt entwickeln. Dazu gehören unter anderem aktualisierter Virusschutz, Verschlüsselung, Sorgfalt mit Passworten, Zugangskontrolle bei Computern mit Nutzeridentifizierung und Authentifizierung der benutzten Software. In den Unternehmen muss den mit Informationssicherheit betrauten Mitarbeitern ein höherer organisatorischer Stellenwert zugeordnet werden. Sie müssen ein quantitatives Risikomanagement für ihre Anlagen einführen. Die Sicherheitstechniken mittels Kryptographie, Zertifikationen, elektronischen Unterschriften oder Trustworthy Computing müssen weiterentwickelt werden, und zwar so, dass sie auch künftigen Herausforderungen wie Quantum Computing standhalten.

Im internationalen Bereich sollte die technische und politische Leitung der ITU als internationale Führungsbehörde in der Informationssicherheit gestärkt werden. Notwendig ist auch die Erarbeitung von Standards mit internationaler Gültigkeit für den Schutz der Privatsphäre und von Geschäftsdaten, wobei die zunehmende Eindringfähigkeit von Spionagetechniken, Suchmaschinen und Data mining mit den öffentlichen Sicherheitsinteressen abgeglichen werden müssen.

Anpassung des Völkerrechts

Von vielleicht noch größerer Bedeutung ist die Erarbeitung eines modernen völkerrechtlichen Rahmens für die Beurteilung der militärischen Nutzung von IKT (Cyberwar und Cyberdefence). Zwar lassen sich aus dem Vertragsvölkerrecht und aus den umfassenden Prinzipienerklärungen der UN-Generalversammlung zu den -Themen Agression und Intervention einige allgemeine Standards ableiten, die Aufgabe einer Anpassung des Völkerrechts an die Erfordernisse des Digitalzeitalters ist aber ungelöst. Hier braucht man eine autoritative Neuinterpretation der UN-Charta (und des NATO-Vertrags) zu Begriffen wie bewaffneter Angriff, territoriale Integrität und nationale Souveränität. Die rechtlichen Grenzen von Information Operations auf der einen, Selbstverteidigung unter Artikel 51 der Charta auf der anderen Seite, müssen anhand von realistischen Cyberwar-Szenarien aufgezeigt werden. Es bedarf einer Definition der Information Weapons und ihres offensiven Einsatzes ebenso wie der Entwicklung operativer Standards für die Anwendung von Kapitel VII der Charta bzw. kollektiver Gegenmaßnahmen unter dem NATO-Vertrag. In diesem Zusammenhang ist zu prüfen, ob der offensive Einsatz von Cyberweapons nicht grundsätzlich geächtet werden sollte, ungeachtet der schwierigen Abgrenzung zwischen offensiver und defensiver Anwendung von IKT und den Problemen etwaiger Sanktionen. Darüber hinaus stellt sich eine übergreifende ordnungspolitische Aufgabe. Ebenso wie die Weltmeere und der Weltraum bedarf auch die neue Domäne des Cyberspace, des digitalen Raumes, einer konzeptionellen Gesamterfassung. Für die Meere ist eine umfassende Kodifikation in der Seerechtskonvention gelungen, für den Weltraum zeichnet sich ein Regime mit wesentlichen Regeln ab. Auch für die digitale Sphäre ist bereits ein internationales „Law of Cyberspace“ als Ordnungsrahmen gefordert worden. Er würde eine schlüssigere Bearbeitung der Probleme des Cyberconflict und die Erarbeitung eines allgemeingültigen Cyber-Verhaltenskodexes ermöglichen und uns vielleicht einem Zustand näherbringen, bei dem an die Stelle einer Konfliktperspektive mit hohem Destabilisierungspotenzial die Normalität eines Cyberpeace tritt.

[1] The White House, Office of the Press Secretary

[2] NATO-Erklärung von Bukarest, 4.4.2008, Absatz 47

[3] Vgl. Henning Wegener: Harnessing the Perils in Cyberspace: Who is in Charge? Disarmament Forum, UNIDIR, Nr. 3, 2007

[4] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Jody Westby

Stabilität statt Cyberkrieg -
Was für den Frieden im digitalen Raum notwendig wäre

Staaten entwickeln nationale Strategien zur Sicherung des digitalen Raumes und führen mit alarmierender Häufigkeit Angriffe im Cyberspace durch. Im Augenblick fließt mehr Geld, um Cyberkriege zu führen, als für deren Abwehr. Es wird Zeit, dass sich Regierungen auf ein durch Kooperation und Regulierung erreichbares Maß an Sicherheit einigen.

Hinter dem Begriff „Geo-Cyber-Stabilität“ steckt die Fähigkeit von Staaten, das Internet sowohl für ihre nationalen Sicherheitsbelange als auch zu ihrem wirtschaftlichen, sozialen und politischen Vorteil zu nutzen, ohne unnötig Schaden und Zerstörung zu verursachen. Mit 1,6 Milliarden Usern in 266 Staaten oder Gebieten mit Zugang zum Internet sind Cyberattacken zum Normalzustand geworden. Die Missbrauchsmöglichkeiten von Informations- und Kommunikationstechnologien (IKT) sind mittlerweile so groß, dass sich Regierungsserver, Militärnetzwerke und Wirtschaftstransaktionen in einem permanenten Bedrohungszustand befinden.

Auch in der Vergangenheit gab es regelmäßige Cyberattacken. Aber die Häufigkeit und Qualität der Angriffe hat enorm zugenommen. Angesichts der veränderten Sicherheitslage scheint es fraglich, ob Staaten ihre Infrastruktur und Informationssysteme angemessen schützen können.

Der Angriff auf staatliche und private Server in Estland im Frühjahr 2007 markierte einen Wendepunkt: Die Attacken eskalierten schnell und legten Netzwerke und Websites von Regierung, Medien und Finanzinstitutionen lahm. Bei den Angriffen zeigte sich deutlich, wie schnell Cyberattacken zu einer Angelegenheit der nationalen Sicherheit werden können, die auch andere Staaten betrifft und die die Frage nach kollektiver Verteidigung aufwirft.

Die Angriffe waren auch deshalb so bedeutsam, weil Estland zwar zu den „vernetztesten“ Staaten der Welt gehört, aber die estnische Regierung beim Tracking and Blocking verdächtiger Vorgänge im Internet um Unterstützung aus dem Ausland bitten musste. Noch vor dem Ende der Angriffe halfen IT-Experten aus den USA, Israel sowie der EU und NATO aus – und hatten Gelegenheit, einiges zu lernen. Estland sah sich gezwungen, große Teile des nationalen Netzes für den Auslandsverkehr zu schließen, um die Situation wieder unter Kontrolle zu bringen. Estland behauptete, es habe verdächtige Vorgänge bis zu einer Internetadresse im Kreml zurückverfolgen können. Russland stritt jegliche Verantwortung ab, weigerte sich aber, an der Aufklärung mitzuwirken.

Chaos und Unsicherheit

Die Angriffe auf Estland offenbarten die „Grenzlosigkeit“ der Cyberkriminalität und die Schwierigkeit, derartige Attacken aufzudecken und zurückzuverfolgen. Der mit den Angriffen im Zusammenhang stehende Internetverkehr führte jedenfalls bis in so unterschiedliche Staaten wie die USA, China, Vietnam, Ägypten und Peru. Möglich, aber nicht beweisbar ist auch, dass es sich bei den Angreifern um eine Koalition von organisierter Cyberkriminalität und Staaten handelte, die ihre Angriffe koordinierten.

Wenige Monate nach den Attacken auf estnische Server drangen vermutlich chinesische Militärangehörige in amerikanische Pentagon-Computer ein. Der Vorfall wurde als „erfolgreichster Cyberangriff auf eine US-Verteidigungsbehörde“ bezeichnet und legte für mehr als eine Woche Teile des Pentagon-Systems lahm. Chinesische Hacker wurden auch beschuldigt, Cyberspionageangriffe gegen britische Regierungsserver durchgeführt und deutsche Regierungsserver beschädigt zu haben.

Der Generaldirektor der britischen Gegenspionage- und Sicherheitsbehörde MI5 warnte in einem Schreiben an 300 Geschäftsführer und Sicherheitschefs, dass ihre Einrichtungen und Firmen von „chinesischen Staatsorganisationen“ bedroht würden; diese Angriffe seien dazu angelegt, bisherige Best Practices im Sicherheitsbereich zu zerstören. Ebenso wie die estnischen Cyberattacken warfen auch diese Angriffe Fragen grundsätzlicher Art auf, zum Beispiel zum Einsatz staatlicher Cybersöldner zur Gegenspionage im Netz.

Bei den russischen Angriffen auf georgische Server während des russisch-georgischen Krieges in Südossetien 2008 wurde noch deutlicher, in welchem Maße Staaten von Computern und Kommunikationssystemen abhängig sind – insbesondere in Krisenzeiten. Eine Reihe von DDoS-Angriffen (Distributed Denial of Service) auf georgische Regierungswebsites legte das staatliche Kommunikationssystem weitgehend lahm. Während die Angriffe in Estland Artikel 5 des NATO-Vertrags (kollektive Verteidigung) auf den Prüfstand stellten, warfen die Ereignisse in Georgien ganz andere völkerrechtliche Fragen auf. Die Juristen Stephen Korn und Joshua Kastenberg zum Beispiel fragten sich in ihrer Analyse der Vorfälle, ob Georgien die amerikanische Neutralitätspflicht unter dem Haager Abkommen verletzt habe, als es den „unorthodoxen Schritt“ unternahm, ohne vorherige Erlaubnis in den USA „virtuell Zuflucht“ zu suchen.

Die Cyberattacken auf Estland und Georgien sind ausgezeichnete Beispiele für die Folgen solcher Angriffe, nämlich Chaos und Unsicherheit hinsichtlich des rechtlichen Rahmens der Gegenmaßnahmen. In Krisenzeiten hinkt die Theorie der Realität hinterher: Weder NATO noch die Staaten, die Estland zur Hilfe eilten, waren rechtlich zu Abwehrmaßnahmen befugt.

Jüngere Cyberattacken werfen ein Schlaglicht auf die vernetzte Verwundbarkeit im Internet und zeigen, wie dringend ein gewisses Maß an „Geo-Cyber-Stabilität“ benötigt wird. „Tracking GhostNet“, so der im März 2009 veröffentlichte Titel eines Berichts des Information Warfare Monitor am Munk Center der University of Toronto über chinesische Hackerangriffe gegen Tibeter, berichtet von einem 1295

Computer in über 100 Staaten umfassenden Netzwerk, das von kommerziellen Internetadressen in China ferngesteuert wurde. Das GhostNet-System, so der Bericht, brachte Computer von Ministerien, Botschaften, Organisationen und der NATO in ganz Europa und Asien dazu, Schadprogramme aus dem Internet herunterzuladen. Mit Hilfe dieser Malware konnten die Angreifer umfassende Kontrolle über diese Computer erlangen, einschließlich der Dateien und Bedienelemente wie Mikrophone und Webcams.

1996 schätzten US-Regierungsvertreter, dass zwischen 120 und 140 Staaten entweder bereits über Mittel für Cyberkrieg verfügten oder im Begriff seien, solche herzustellen. Staaten müssen in der Lage sein, ihre Infrastruktur und Informationssysteme vor Angriffen, Spionage, Sabotage, unerlaubtem Zugang, widerrechtlicher Veröffentlichung und anderen Formen von Cyberkriminalität zu schützen, die ihre nationale und wirtschaftliche Sicherheit unterwandern könnten. Ebenso brauchen Staaten aber Rechtssicherheit hinsichtlich alltäglicher Operationen im Netz und hinsichtlich der Entscheidungen, die ihre nationale und Wirtschaftssicherheit und den Schutz ihrer Bevölkerung betreffen. Bislang fehlt ein solcher rechtlicher Rahmen.

Traditionelle Vorstellungen von nationaler Sicherheit – zum Beispiel geopolitische Sicherheit, Einflusssphären, Machtkorrelationen – sind überholt. Im virtuellen Raum gibt es keine Grenzen, und die Paragraphen zur kollektiven Verteidigung waren für traditionelle Konflikte gedacht, nicht für Cyberkriege. Auch wenn geopolitische Überlegungen weiterhin Bedeutung haben, muss die Gefährdung sensibler Infrastrukturen auch vor dem Hintergrund globaler Cyberstabilität bewertet werden.
Alle Staaten sind auf ein Minimum an Cyberstabilität angewiesen, das durch internationale Abkommen garantiert wird. Die lebenswichtige Infrastruktur eines Staates kann auf eine Weise zerstört werden, die den einschlägigen Abkommen widerspricht – wie der Genfer Konvention oder dem Haager Abkommen, das Nationen auch im Kriegsfall zur Wahrung der Neutralität gegenüber anderen Ländern verpflichtet.

Rechtliche und politische Fragen

Die Gesetze für bewaffnete Konflikte regulieren die Durchführung von bewaffneten Auseinandersetzungen und haben den Zweck, Leid und Zerstörung möglichst zu vermeiden. Nach diesen Gesetzen können Kampftruppen angreifen, wenn die Maßnahme notwendig ist, um ein berechtigtes militärisches Ziel zu erreichen (Prinzip der Notwendigkeit). Dabei müssen sie zwischen rechtmäßigen und unrechtmäßigen Zielen, wie -Zivilisten, ziviles Eigentum, Verwundete und Kranke, differenzieren (Prinzip der Unterscheidung). Der Umfang der Truppen darf nicht größer sein als zur Erreichung der militärischen Ziele erforderlich wäre (Prinzip der Verhältnismäßigkeit). Reguläre Kriegsteilnehmer müssen von der Regierung für die Teilnahme an Kampfhandlungen ermächtigt worden sein; sie müssen unverkennbare Abzeichen tragen und aus der Ferne erkennbar sein. Unrechtmäßige Kriegsteilnehmer sind solche, die ohne Befehl einer Regierung oder völkerrechtlich abgesichertes Mandat an Kampfhandlungen teilnehmen.

Die erste offensichtliche Frage, die sich im Zusammenhang mit dem Internet stellt, lautet: Was begründet einen Akt des Cyberkriegs? Andere Fragen betreffen den Angriff auf Kommunikationssysteme und andere entscheidende Infrastruktur, die der Privatwirtschaft gehören und das zivile Leben aufrechterhalten wie beispielsweise Krankenhäuser (und damit die Versorgung von Kranken, Verletzten, Alten und Minderjährigen). Sollten diese und die Angriffsziele, die von der Genfer Konvention geschützt werden, tabu sein? Sind Angriffe auf diese Einrichtungen wirklich notwendig, um militärische Ziele zu erreichen? Steht der Schaden an den Netzwerken im Verhältnis zum militärischen Ziel? Wenn ein Angriff erfolgt, weiß niemand, wer der Aggressor ist, bis der Angriff zurückverfolgt wird und eine Zuordnung erfolgen kann. Reguläre Internetsoldaten sind nicht von jugendlichen Hackern oder irgendwelchen Cyberschurken zu unterscheiden. Wie kann man feststellen, ob ein Angreifer ein militärischer Gegner ist? Welche internationale Zusammenarbeit ist erforderlich? Desgleichen stellt sich die Frage: Wie kann man wissen, ob ein Dritter auf Geheiß eines Nationalstaats handelt? Gewiss tragen die Angreifer keine „erkennbaren Zeichen" – oder sollten Internetsoldaten oder Cybersöldner eine Internetuniform tragen? Was bedeutet unverhältnismäßige Gewalt im Internet?

Hoffnungslos veraltet

Die beiden wesentlichen rechtlichen Instrumente zur Regelung von Konflikten zwischen Nationalstaaten sind der NATO-Vertrag und die UN-Charta. Beide Dokumente sind schon älter als 50 Jahre und dem Zeitalter des Internet nicht mehr angemessen. Die Termini des NATO-Vertrags sind „bewaffneter Angriff", „territoriale Unversehrtheit und politische Unabhängigkeit". Die Begriffe Selbsthilfe, gegenseitige Unterstützung und kollektiver Beistand werden nur im Zusammenhang eines „bewaffneten Angriffs" verwendet. Estlands Verteidigungsminister Jaak Aaviksoo hat die Mängel des NATO-Vertrags bei Cyberattacken auf den Punkt gebracht: „Kein einziger NATO-Verteidigungsminister würde zurzeit einen Internetangriff als militärischen Angriff definieren."

Artikel 12 des Vertrags erlaubt es den Mitgliedern, den Vertrag hinsichtlich „Faktoren, die Frieden und Sicherheit betreffen" zu bewerten. Demnach könnte dieser Artikel den NATO-Mitgliedern dazu dienen, -Internetangriffe, kollektive Verteidigung und Geo-Internetsicherheit zu berücksichtigen.
Die UN-Charta wiederum dient als Grundlage des internationalen Rechts in Fragen der Staatsführung, einschließlich der Frage bewaffneter Konflikte. Die Sprache der UN-Charta ist eng abgestimmt mit der des NATO-Vertrags. Auch sie spricht von „territorialer Unversehrtheit und politischer Unabhängigkeit" oder dem „Einsatz bewaffneter Truppen". Die Bestimmungen über Selbstverteidigung verwirren mehr als sie Klarheit schaffen. Artikel 51 besagt, dass nichts eine Nation oder eine Gruppe von Nationen davon abhalten kann, in kollektiver Selbstverteidigung anzugreifen, falls ein bewaffneter Angriff erfolgt – was die Frage aufwirft, ob ein Internetangriff einen „bewaffneten Angriff" darstellt. Sogar, wenn der Angriff von regulären Streitkräfte, käme, spricht Artikel 41 gegen diese Interpretation, der speziell die Handlungen auflistet, die nicht als bewaffnete Gewalt erachtet werden können. Zu den erlaubten Maßnahmen zählen die gesamte oder teilweise Unterbrechung des Kommunikationsbereichs, was auf das Szenario eines Internetangriffs zutreffen könnte.

UN-Charta und NATO-Vertrag erfassen die elektronischen Möglichkeiten des 21. Jahrhunderts also nicht. Nie zuvor war die Notwendigkeit so groß wie heute, diese rechtlichen Instrumente zu aktualisieren, um die Maßnahmen der Nationalstaaten im Hinblick auf Cyberkrieg und Angriffsmöglichkeiten zu regeln. Die Bekämpfung des globalen Terrorismus hat ohnehin schon die Fundamente des Rechtsstaats bedenklich erodiert. Die verhängnisvolle Bedrohung durch Internetangriffe von Nationalstaaten und Cyberschurken ist inzwischen Realität geworden. Staaten können es sich nicht länger leisten, einander an die Gurgel zu gehen anstatt sich die Hand zu reichen, wie Winston Churchill einmal bemerkte. Regierungen, die Privatwirtschaft und multinationale Organisationen müssen einen internationalen Dialog über neue militärische Einsatzmöglichkeiten, gemeinsame Maßnahmen und eine „Geo-Cyber-Politik“ führen. Werden diese Fragen vernachlässigt, dann wachsen sich die Gefahren des Cyberspace in den nächsten fünf Jahren zu einer immensen Bedrohung für die nationalen und wirtschaftlichen Sicherheitsinteressen aller Länder aus.

Vorreiterrolle Russlands

Der Dialog über eine globale Cyberstabilität muss mit der Frage internationaler Kooperation beginnen. Sie ist fast immer erforderlich, wenn man Internetkommunikationen verfolgen will, schon weil das Internetprotokoll eine Mitteilung in Datenpakete zerlegt und durch viele Netzwerke – und Länder – leitet, bevor die Datenteile an ihrem Bestimmungsort wieder zusammengesetzt werden. Auch bei der Verteidigung gegen Internetangriffe ist die Hilfe anderer Nationalstaaten erforderlich.

Ursprünglich hatte man geglaubt, dass das Abkommen des Europarats über Internetkriminalität, das ausgezeichnete Bestimmungen hinsichtlich gegenseitiger Unterstützung und Zusammenarbeit enthält, das beste Vehikel wäre, um eine entsprechende Übereinkunft zu erzielen. Jedoch haben das Abkommen seit 2001 nur 46 Staaten unterzeichnet und 26 ratifiziert. Allerdings gibt es in mehr als 200 Ländern Zugang zum Internet. Das Abkommen des Europarats scheint also kaum die richtige Lösung zu sein.

Ganz eindeutig müssen die Vereinten Nationen die Führung übernehmen, um ein internationales Abkommen über Zusammenarbeit und Beherrschung von Internetkonflikten zu erarbeiten. Auf die USA scheint man dabei nicht zählen zu können. Sie haben zwar das Internet erfunden, stehen aber bei der Vergabe des Postens als Vorreiter in dieser Frage bei den UN nicht in erster Reihe.

Ironischerweise hat Russland – eines der aktivsten Länder beim Engagement in der Internetkriegsführung – die größte Führerschaft an den Tag gelegt. Seit 1998 hat Russland jedes Jahr eine UN-Resolution zu „Entwicklungen auf dem Gebiet der Information und Telekommunikation im Zusammenhang mit internationaler Sicherheit“ eingebracht. So forderte es zu einer multilateralen Abwägung der Bedrohungen auf, die im Bereich er Internetsicherheit auftauchen und verlangte eine Definition der grundlegenden Absichten der internationalen Prinzipien zur Bekämpfung von Internetkriminalität und Terrorismus. Die Resolution aus dem Jahr 1999 beinhaltet das militärische Potenzial der Informations- und Kommunikationstechnik. Diese Resolutionen wurden von der Generalversammlung regelmäßig

verabschiedet. Die USA haben regelmäßig dagegen gestimmt. Russlands Resolution aus dem Jahr 2008 wurde sowohl vom First Committee der UN als auch von der Generalversammlung angenommen – allein die USA legten Einspruch ein.

Die internationale Gemeinschaft muss kooperieren und erkennen, dass die enormen Vorteile des Internet in Gefahr sind, wenn es als Werkzeug benutzt wird, um jenseits der gesetzlichen Regelungen Schaden zu verursachen. Regierungen haben die Verpflichtung, bei der Verteidigung des Internet und der Systeme zu helfen, die ihre Wirtschaft fördern, das Leben ihrer Bürger bereichern und die Regierung sowie militärische Operationen unterstützen. Sie haben auch eine Verpflichtung, bei der Verfolgung und Ahndung von Cyberaktivitäten zu helfen. Notwendig ist die Entwicklung eines rechtlichen Systems, das auf Internetkonflikte Anwendung findet und ein Mindestmaß an Geo-Cyberstabilität garantiert, damit das Wild Wild Web nicht die völkerrechtlichen Regeln im Krieg, die Menschenrechte und die freundschaftlichen Beziehungen der Staaten zerstört und damit zum Werkzeug der Verwüstung im 21. Jahrhundert wird.

UDO HELMBRECHT

Haltet den Wurm!
Wie Deutschland die sichere IT-Nutzung verbessern will

Zum Funktionieren unseres Gemeinwesens sind wir auf sichere Informations- und Kommunikationstechnik angewiesen. Hierbei spielt das Bundesamt für Sicherheit in der Informationstechnik eine zentrale Rolle: Es will die Bedrohungen für Verwaltung, Wirtschaft und Menschen begrenzen und neu aufkommende Gefahren frühzeitig erkennen.

Ob man es wie einige Medien Cyberwar nennt oder von Sabotageakten spricht – Vorkommnisse wie die Angriffe auf amerikanische und südkoreanische Internetseiten im Juli dieses Jahres verfügen über eine weitreichende Wirkung. Allein in Korea sind hunderttausende Internetnutzer daran gehindert worden, Finanztransaktionen, Einkäufe und andere Geschäfte durchzuführen.[1] In den USA und Südkorea waren einige Dutzend Websites von Regierungsstellen lahmgelegt. In den USA zählten das Heimatschutz-, das Finanz- und das Verteidigungsministerium zu den Angriffszielen, in Südkorea die Websites des Präsidenten, der Nationalversammlung und einer Suchmaschine. Ähnliche Vorfällen ereigneten sich in der Vergangenheit in Estland und Georgien.

Weitaus gravierendere Folgen für Unternehmen, Verwaltungen und die Bevölkerung können Angriffe auf Computer haben, die Versorgungsinfrastrukturen steuern. Kleinere Vorfälle dieser Art mit regional begrenzten Auswirkungen hat es bereits gegeben, größere scheinen nur eine Frage der Zeit zu sein. Der Präsident der Internet Security Advisors Group, Ira Winkler, warnt seit einiger Zeit vor möglichen Angriffspunkten im US-Stromnetz. „Breaking into a power station in three easy steps“ lautete die Schlagzeile eines IT-Newsdiensts[2] dazu.

Neben der Sabotage von Websites oder Infrastrukturen ist ein weiteres Einsatzfeld für elektronische Angriffe die Spionage. Dass es einem technisch gut gemachten Schädling möglich ist, in die verschiedensten Computernetzwerke einzudringen, hat der Conficker-Wurm in diesem Jahr eindrucksvoll bewiesen. Ist eine Schadsoftware erst einmal in das Innere eines Unternehmens- oder Behördennetzwerks vorgedrungen, ist ihr Schadenspotenzial enorm. Sie kann nicht nur wichtige Daten manipulieren oder zerstören, sie kann Geschäftsgeheimnisse auch so nach außen senden, dass der Empfänger unerkannt bleibt.

Professionelle Untergrundwirtschaft

Mit dem Schädling Conficker ist eine neue Qualitätsstufe bei Schadsoftware erreicht. Das zeigt sich schon daran, dass sich die Computerexperten immer noch mit diesem Wurm auseinandersetzen.[3] Letztendlich ist Conficker aber nur ein weiterer Schritt in einer schon länger andauernden Entwicklung. Schadprogramme und die Untergrundwirtschaft, aus der sie entstehen, werden zusehends professio-

neller. Die Erstellung und Verbreitung von Computerschädlingen erfolgen inzwischen arbeitsteilig und international vernetzt. Diese Entwicklung verwundert nicht: „Durch die zunehmende Verlagerung alltäglicher Aktivitäten – wie Bankgeschäfte tätigen oder einkaufen – ins World Wide Web ist IT-Kriminalität für die Angreifer ein lohnenswertes Geschäft bei vergleichsweise niedrigem Risiko“, heißt es im aktuellen Lagebericht zur IT-Sicherheit in Deutschland,[4] den das Bundesamt für Sicherheit in der Informationstechnik (BSI) zweijährlich herausgibt.

Der Bericht zeigt auch auf, dass die Zahl der gefährlichen Sicherheitslücken weiterhin steigt: Über drei Viertel der im Jahr 2008 neu entdeckten Schwachstellen können von einem entfernten Angreifer ausgenutzt werden. Zum Einsatz kommen meist modular aufgebaute Schadprogramme, die über mehrere Schadfunktionen verfügen. So kann beispielsweise ein Trojanisches Pferd über Backdoor- und Spywarefunktionen verfügen, einen Keylogger verwenden und den befallenen Rechner zusätzlich an ein Bot-Netz anschließen. Zudem verfügen die meisten Schadprogramme über Updatefunktionen, so dass neue Programme oder Tarnmechanismen jederzeit nachgeladen werden können. Bot-Rechner, die mehrfach am Tag mit Updates versorgt werden, sind daher Standard.

In Bezug auf Spionage und Sabotage ist vor allem interessant, dass einzelne Schadprogramme heute gezielter eingesetzt werden als früher und nicht mehr wahllos an möglichst viele Opfer verteilt werden. Die Einsatzdauer eines Schadprogramms lässt sich so verlängern. Zudem schützen sich die meisten Schadprogramme inzwischen mit kryptografischen Verfahren und passen ihr Verhalten an – je nachdem, ob sie in einer typischen Analyseumgebung oder auf einem echten Opferrechner ausgeführt werden. Die Tarnmechanismen werden beständig verbessert. Beispielsweise ist zukünftig mit Schadprogrammen zu rechnen, die das Betriebssystem in eine virtuelle Umgebung verschieben, so dass sie von herkömmlichen Schutzprogrammen nicht mehr entdeckt werden können.

Steigende IT-Durchdringung

Dies trägt dazu bei, dass die Gewinn-erwartung der Angreifer steigt, während das Risiko abnimmt. Gleichzeitig eröffnen sich immer mehr Möglichkeiten für Angriffe. In einem Interview mit der Zeitschrift *Technology Review*[5] erläutert Ira Winkler, warum Infrastrukturen wie das US-amerikanische Stromnetz Schnittstellen nach außen haben: „Die Firmen begannen damit, die Funktionalitäten von Business- und Kontroll-PCs zu kombinieren – in dem Glauben, dass man ja keine Verbindung nach außen entstehen lassen wird. Dann begannen die Unternehmen schließlich damit, auch das Internet in ihren geschäftlichen Netzwerken verfügbar zu machen.“ Dies habe große Angriffsflächen entstehen lassen.

In nahezu allen Bereichen steigt die Durchdringung mit Informationstechnik unaufhaltsam. In besonderem Maße gilt dies für Dienstleister und Behörden, aber auch im produzierenden Gewerbe und in der Landwirtschaft werden Prozesse automatisiert und mit IT unterstützt. Generell profitieren Bürger, Staat und Wirtschaft von dieser zunehmenden Verbreitung der Informationstechnik. Für Unternehmen, die sich immer stärker einem globalen Wettbewerb stellen müssen, ist sie gar essentiell, denn sie sind auf eine internationale Vernetzung angewiesen. Gleiches gilt mehr und mehr für Wirtschaftsregionen

und ganze Staaten. Diese geopolitischen Entwicklungen bringen es aber mit sich, dass sich nicht nur die Geschäfte, sondern auch die Verteilungskämpfe um Marktanteile und Ressourcen vermehrt elektronisch abspielen.

Alle Beteiligten müssen sich deshalb für ihren Verantwortungsbereich der Herausforderung stellen, die die Bedrohungen in der virtuellen Welt mit sich bringen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) befindet sich hierbei in Deutschland an einer Schnittstellenposition. Es ist zuständig für die Netze von Behörden und Verwaltungen, fördert aber auch den Schutz von Unternehmen und informiert und sensibilisiert Privatanwender.[6] BSI-Verantwortliche sind in deutschen und internationalen Gremien vertreten, um weitreichende Maßnahmen zum Schutz der Informationstechnik anzustoßen und durchzusetzen.

Ziel der Maßnahmen des BSI ist es, die Bedrohungen für die Bundesverwaltung, Wirtschaft und Bürgerinnen und Bürger zu begrenzen und neu aufkommende Gefahren frühzeitig zu erkennen, um entsprechende Gegenmaßnahmen einleiten zu können. Diese Arbeit gewinnt mit den weiter wachsenden Schadenspotenzialen an Bedeutung.

Schutz Kritischer Infrastrukturen

Die neuralgischen Punkte sind in der Informations- und Kommunikationstechnik (IKT) so genannter Kritischer Infrastrukturen zu suchen. Dies sind Einrichtungen, bei deren Ausfall erhebliche Schäden für das Gemeinwesen entstehen können. Das Gemeinwesen ist von Kritischen Infrastrukturen wie Transport und Verkehr, Energie- und Wasserversorgung sowie Justiz und Behörden abhängig. Diese Infrastrukturen sind wiederum auf eine zuverlässige Informations- und Kommunikationstechnik angewiesen. Um das Funktionieren einer Gesellschaft zu gewährleisten, ist somit die Sicherung der eingesetzten Informations- und Kommunikationstechnik unbedingt erforderlich.

Der Bund realisiert diese umfangreiche Aufgabe mit dem Nationalen Plan zum Schutz der Informations-infrastrukturen (NPSI),[7] der drei strategische Ziele vorgibt: Prävention, Reaktion, Nachhaltigkeit. Das BSI ist als nationale IT-Sicherheitsbehörde und zentraler IT-Sicherheitsdienstleister des Bundes koordinierend für die Umsetzung des Nationalen Planes zuständig.

Durch Schutzvorkehrungen in Verwaltungen und Unternehmen soll das strategische Ziel Prävention erreicht werden. Dies wird durch die weitere Sensibilisierung und Aufklärung von Mitarbeitern über IT-Risiken sowie den Einsatz verlässlicher IT-Produkte realisiert. Weitere Maßnahmen bestehen in der Initiierung der Entwicklung vertrauenswürdiger Kryptoprodukte sowie in der Definition gemeinsamer Standards hinsichtlich der Schutzmaßnahmen.

Das strategische Ziel Reaktion umfasst das Sammeln, Analysieren und Bewerten von Informationen, die Alarmierung von Betroffenen und das Ergreifen von Maßnahmen zur Schadensminimierung. Die Bundesregierung etabliert dazu ein nationales IT-Krisenmanagement. Dieses besteht aus dem Nati-

onalen Lage- und Analysezentrum, das jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland verfügt, sowie aus dem IT-Krisenreaktionszentrum, das die schnelle Reaktion auf schwerwiegende Vorfälle sicherstellt. Das Krisenreaktionszentrum gibt Analysen und Bewertungen zu Vorfällen an alle relevanten Stellen weiter und koordiniert die Zusammenarbeit mit anderen Krisenmanagementorganisationen, z.B. im Bereich der Bundesverwaltung oder mit den Betreibern Kritischer Infrastrukturen.

Durch die verstärkte Entwicklung vertrauenswürdiger und verlässlicher Informationstechnik soll das strategische Ziel Nachhaltigkeit erreicht werden. Um die nationalen Informationsinfrastrukturen langfristig zu schützen, benötigt Deutschland Fachkompetenz sowie vertrauenswürdige IT-Dienstleistungen und IT-Sicherheitsprodukte.

Sicherheit für gesellschaftsrelevante Unternehmen

Die Ziele Prävention, Reaktion und Nachhaltigkeit ergänzen die IT-Strategie des Bundes. Die Erreichung der Ziele wird durch einen Umsetzungsplan für die Bundesverwaltung (UP Bund), einen Umsetzungsplan für die Kritischen Infrastrukturen (UP KRITIS)[8] und gegebenenfalls weitere Umsetzungspläne sichergestellt. Der UP Bund legt die Richtlinien zur Umsetzung des NPSI in der Bundesverwaltung fest, im UP KRITIS werden die Aspekte der IT-Sicherheit in Kritischen Infrastrukturen adressiert. Mit dem UP KRITIS wird ein einheitlich hohes Sicherheitsniveau für die Unternehmen fokussiert, deren Funktionsfähigkeit besonders gesellschaftsrelevant ist. Die an der Erstellung des UP KRITIS Beteiligten – Bundesverwaltung und Betreiber Kritischer Infrastrukturen – wollen die Empfehlungen in den nächsten Jahren umsetzen.

Das Bundesamt für Sicherheit in der Informationstechnik ist an diesen Prozessen aktiv beteiligt. Das Nationale IT-Lagezentrum beobachtet und analysiert nicht nur die Bedrohungslage und bewertet die Erkenntnisse für eine politisch-strategische Zielgruppe, sondern dient auch als Anlaufstelle bezüglich KRITIS.

Die Herausforderung für die kommenden Jahrzehnte wird sein, Software, Hardware und IKT-Architekturen so weiterzuentwickeln, dass sie ein verlässliches Instrument zur Prozessunterstützung darstellen beziehungsweise bleiben. Gleichzeitig muss sichergestellt werden, dass IKT auch bei Störungen handlungsfähig bleibt. Hierzu sollten IT-Infrastrukturen verstärkt redundant ausgelegt sein. Gleichzeitig ist eine interdisziplinäre Zusammenarbeit beim Erkennen und Bewerten neuer IKT-Bedrohungen erforderlich. Insbesondere im Bereich der Kritischen Infrastrukturen ist außerdem der weitere Ausbau einer übergreifenden Zusammenarbeit für den Umgang mit Vorfällen notwendig, die zu IKT-bedingten Krisen führen können, wie er im Rahmen der Umsetzung des UP KRITIS begonnen wurde.

Internationale Kooperation

Der Schutz Kritischer Infrastrukturen ist eine wichtige politische Aufgabe, die auch für die Gewährleistung der Inneren Sicherheit Deutschlands von elementarer Bedeutung ist. Damit in Deutschland auch in Zukunft alle gesellschaftlichen Gruppen in ein verlässliches IKT-Umfeld vertrauen können, muss die Realisierung dieser Aufgabe in Abhängigkeit von der technologischen und wirtschaftlichen Entwicklung weiter vorangetrieben werden.

Schließlich muss festgehalten werden, dass isolierte nationale Bemühungen nur begrenzt erfolgreich sein können. Das BSI kooperiert deshalb international auf europäischer Ebene und darüber hinaus. Seitens der EU-Kommission und Einrichtungen wie der European Network and Information Security Agency (ENISA) gibt es hierzu eine Reihe von Aktivitäten, wie etwa das Europäische Programm für den Schutz Kritischer Infrastrukturen (EPSKI)[9].

Die Arbeit für sichere Nutzung der Informationstechnik in unserer Gesellschaft muss auf vielen Ebenen stattfinden. Auf politischer, wirtschaftlicher und gesellschaftlicher Ebene sowie national und international müssen die begonnenen Aktivitäten zur Informationssicherheit weiter voranschreiten und intensiviert werden, damit Fälle wie Estland und Südkorea Ausnahmen bleiben.

[1] http://www.heise.de/newsticker/meldung/141799

[2] http://news.cnet.com/8301-10784_3-9914896-7.html

[3] http://www.heise.de/newsticker/meldung/141663

[4] http://www.bsi.bund.de/literat/lagebericht/Lagebericht2009.pdf

[5] http://www.heise.de/tr/artikel/109126

[6] http://www.bsi-fuer-buerger.de/

[7] http://www.bmi.bund.de/cae/servlet/contentblob/121734/publicationFile/13312/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf

[8] http://www.bsi.bund.de/fachthem/kritis/veroeff_upkritis.htm

[9] http://www.bsi.bund.de/veranst/IT-SiKongress/pdfdownload/Keynote-Rudolf-Strohmeier.pdf

TeleTrusT Deutschland e.V.

Der IT-Sicherheitsverband TeleTrusT Deutschland wurde 1989 gegründet, um verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik zu schaffen. TeleTrusT entwickelte sich zu einem bekannten Kompetenznetzwerk für IT-Sicherheit, dessen Stimme in Deutschland und Europa gehört wird. Heute vertritt TeleTrusT rund 100 Mitglieder aus Industrie, Wissenschaft und Forschung sowie öffentlichen Institutionen. In Projektgruppen zu aktuellen Themen der IT-Sicherheit und des Sicherheitsmanagements tauschen die Mitglieder ihr Know-how aus. TeleTrusT äußert sich zu politischen und rechtlichen Fragen, organisiert Messen und Messebeteiligungen und ist Träger der "European Bridge CA" (Bereitstellung von Public-Key-Zertifikaten für sichere E-Mailkommunikation) sowie des Zertifikates "TeleTrusT Information Security Professional" (T.I.S.P.). Hauptsitz des Verbandes ist Berlin.

Kontakt:
Dr. Holger Mühlbauer
TeleTrusT Deutschland e.V.
Chausseestraße 17
10115 Berlin
Tel.: + 49 30 400 54 310
holger.muehlbauer@teletrust.de
www.teletrust.de