**Policy Brief | Dezember 2015**

stiftung | neue verantwortung

# IT-Sicherheitspolitik
# Aktuelle Themen, Entwicklungen und Handlungsfelder für Deutschland

von **Jan-Peter Kleinhans**

| www.stiftung-nv.de
| Twitter: @snv_berlin

## Executive Summary

2015 drangen Hacker in das interne Netzwerk des deutschen Bundestages ein und legten es lahm. Im gleichen Jahr stahlen Unbekannte persönliche Daten von 22 Millionen Mitarbeiterinnen und Mitarbeitern des öffentlichen Dienstes in den USA. 2014 richtete ein digitaler Angriff auf ein Stahlwerk der ThyssenKrupp AG massiven Schaden bei einem Hochofen an. IT-Sicherheit ist bereits heute von großer Bedeutung und wird mit der milliardenfachen Vernetzung von Geräten und Maschinen in privaten Haushalten, Industrieanlagen oder Behörden an Bedeutung gewinnen.

Obwohl bei Angriffen immer mehr auf dem Spiel steht, wird das Thema IT-Sicherheit in weiten Teilen der Politik nur langsam als Aufgabenfeld von Regierung und Parlament wahrgenommen. Der Grund: IT-Sicherheitspolitik erscheint durch die technische Komponente kompliziert – die Einflussmöglichkeiten für Politik sind oft unklar. Hinzu kommt, dass sich unser eingeübtes Verständnis von Sicherheit kaum in die Welt des Internets, einem globalen digitalen Netzwerk, übertragen lässt. Ein öffentliches Gelände lässt sich räumlich absichern. Eine mit dem Internet verwobene Wirtschaft und Gesellschaft dagegen nicht. Wirtschafts-, Innen- und Rechtspolitiker müssen dieses neue sicherheitspolitische Umfeld mit seinen Eigenarten verstehen, um wirkungsvolle Gesetze und Maßnahmen zu entwerfen.

Im Bereich der IT-Sicherheit sind vor allem fünf Aspekte von zentraler Bedeutung, die zur Unsicherheit von Hard- und Software grundsätzlich beitragen und die daher bei einer strategischen IT-Sicherheitspolitik adressiert werden müssen:

- **Die Komplexität heutiger Technologie:** IT-Systeme basieren auf mehreren hundert Millionen Zeilen geschriebenen Quellcodes und Milliarden von Transistoren. Sicherheitslücken und absichtlich eingebaute Hintertüren lassen sich nur schwer entdecken und sind nicht zu verhindern.

- **Abhängigkeit von internationalen Zulieferern:** Moderne IT-Systeme setzen sich aus vielen Einzelteilen unterschiedlicher Hersteller zusammen. Zwar wird ein Smartphone unter der Marke Apple, Samsung oder Motorola verkauft. In Wirklichkeit besteht es jedoch aus Komponenten von Broadcom, intel, Sanyo und Unzähligen mehr. Eine Schwachstelle in einer einzelnen Komponente kann das gesamte System gefährden.

- **Ein globales Netzwerk:** Wird ein Computer mit dem Internet verbunden, besteht zwangsläufig auch eine Verbindung mit allen anderen Computern weltweit. Ein Angriff ist damit von überall möglich.

- **Weltweit verbreitete Hard- und Software:** Menschen, Organisationen und Geräte nutzen weltweit häufig die gleichen IT-Produkte einiger weniger Hersteller. Cisco stellt etwa 60 Prozent der Internetrouter weltweit her. 80 Prozent der Smartphones verwenden Googles Android Betriebssystem. Einzelne Sicherheitslücken werden somit zu einer massenhaften Gefahr und Angriffe können leicht übertragen werden.

- **Wenig Marktanreize für sichere IT:** Sicherheit spielt bei der Kaufentscheidung nur eine geringe Rolle, weil gerade Verbraucher nur schwer die Sicherheit von Geräten und Software einschätzen können. Zudem sorgt die schnelle Entwicklung immer neuer Produkte dazu, dass die Behebung von Sicherheitslücken bei bestehenden Model-

len vernachlässigt wird. Hersteller können für Sicherheitsmängel nur schwer haftbar gemacht werden. So gibt es für sie kaum ökonomische Anreize auf Sicherheit bei der Entwicklung zu achten.

Bisher setzt die staatliche IT-Sicherheitspolitk vor allem auf eine Stärkung der Überwachungs- und Angriffsfähigkeiten von Bundeswehr, Bundesnachrichtendienst und Bundesverfassungsschutz. Die Konsequenz: Die IT-Sicherheitspolitik in Deutschland ist derzeit nur begrenzt wirksam, weil sie nur einen sehr kleinen Teil der bestehenden Sicherheitsprobleme adressiert. Eine umfassende IT-Sicherheitspolitik sollte unter anderem die folgenden Handlungsfelder abdecken:

- **Gleichgewicht zwischen offensiver und defensiver Politik:** Sicherheitsbehörden und Militär sollten Sicherheitslücken nicht horten, um sie selbst irgendwann zu benutzen. Dadurch wird die Sicherheit aller gefährdet. Stattdessen sollten gefundene Sicherheitslücken konsequent geschlossen werden.

- **Der Informationsaustausch über Sicherheitsrisiken:** Die deutsche IT-Sicherheitspolitik steht vor der Herausforderung Vertrauensnetzwerke in den unterschiedlichen Branchen zu fördern und hierfür der Position des IT-Sicherheitsbeauftragten mehr Relevanz zu geben. Gleichzeitig sollte das BSI vollständig unabhängig werden, um seiner Aufgabe gegenüber Zivilgesellschaft und Unternehmen gerecht werden zu können.

- **Marktanreize schaffen:** Verbesserung der Softwarequalität spielt eine zentrale Rolle in einer nachhaltigen Sicherheitspolitik. Aus ökonomischer Sicht haben IT-Hersteller bisher wenige Anreize von Anfang an bei der Entwicklung auf Sicherheit zu fokussieren. Die Politik sollte daher einerseits Open Source-Software fördern und andererseits Hersteller proprietärer Software stärker in die Haftung nehmen und gesetzliche Gewährleistungen ausweiten.

- **Internationale Kooperation:** Erfolgreiche Angriffe auf kritische Infrastrukturen oder auch Wirtschaftsspionage gehen selten von Kriminellen oder Terroristen aus, sondern werden maßgeblich von Geheimdiensten oder ihnen nahestehenden Hackergruppen durchgeführt. Wie bei klassischer Sicherheitspolitik ist daher die reine Abwehr wenig zielführend. Es braucht gleichzeitig internationale Kooperation und Abkommen.

## Einführung

1998. Das World Wide Web ist rund 7 Jahre alt. Im ersten Quartal werden auf ebay Waren für $100 Millionen versteigert.[1] Die Suchmaschine Google geht online aber es wird noch 3 Jahre dauern, bis die Wikipedia entsteht.[2] An YouTube, Facebook und Twitter ist nicht zu denken. Die US-Amerikanische Regierung erkennt langsam das Potenzial aber auch die Gefahren, die das Internet mit sich bringt.[3] So befragt der Regierungsausschuss des US Senats die Hackergruppe "LOpht" in einer einstündigen Anhörung, wie es um die Sicherheit im Internet bestellt ist.[4] Die Hackergruppe antwortet, "If you're looking for computer security, then the Internet is not the place to be." Die sieben Hacker verdeutlichen dies im Verlauf der Sitzung mit vielfältigen Beispielen zu immanenten Schwächen des Internets und damaliger IT-Systeme. Laut "LOpht" wurde das Internet entwickelt, um Daten schnell und ausfallsicher zu transportieren - Sicherheit spielte bei der Entwicklung jedoch nie eine Rolle. Als weiteren Grund identifizieren sie fehlende Anreize privater Unternehmen sichere Soft- und Hardware zu produzieren. Die Senatoren hören gespannt zu, stellen viele Fragen und sind sich am Ende einig, dass IT-Sicherheit künftig höchste Priorität haben sollte.

2015. Das Internet ist mittlerweile fester Bestandteil unseres privaten und beruflichen Alltags: Wirtschaftspolitisch wird unter dem Schlagwort "Industrie 4.0" die umfassende Vernetzung unserer Industrie vorangetrieben. Durch das Internet der Dinge werden in wenigen Jahren rund 25 Milliarden Geräte mit dem Internet verbunden sein.[5] Über Facebook kommunizieren etwa 1.5 Milliarden Menschen miteinander.[6] Hinsichtlich IT-Sicherheit hat sich in den letzten 17 Jahren jedoch scheinbar wenig getan und die Sicherheit unserer Daten stellt weiterhin ein ungelöstes Problem dar[7]: So sind Hacker erfolgreich in das interne Netzwerk des deutschen Bundestages eingedrungen[8] und auch Monate nach dem Angriff ist weiterhin unklar, von wem genau dieser ausging und wie viele sensible Informationen abflossen.[9] Etwa zeitgleich wurde in den Vereinigten Staaten das US Office of Personnel Management (OPM) gehackt. Das OPM ist unter anderem für die Überprüfung und Einstufung von Geheimnisträgern verantwortlich - es wird vermutet, dass Daten von mindestens 22 Millionen US Personen gestohlen wurden.[10] Bei privaten Unternehmen ist es um die Sicherheit keineswegs besser bestellt: Durch einen Angriff auf ein Stahlwerk der ThyssenKrupp AG[11] wurde ein Hochofen massiv beschädigt.[12] Hacker stahlen von Sony etwa 40GB an sensiblen E-Mails und Dokumente mit Gehalts- und Finanzinformationen.[13] Kaspersky Labs, selbst ein renommiertes IT-Sicherheitsunternehmen, wurde ebenso gehackt.[14] Die Gefahren sind besonders schwerwiegend beim Internet der Dinge: In heutigen Autos befinden sich mehrere Dutzend vernetzter Steuercomputer und immer mehr Hersteller verbinden ihre Autos mit dem Internet, um Multimediadienste anbieten zu können. Dadurch werden Autos jedoch direkt über das Internet angreifbar. So haben Hacker praktisch vollständige Kontrolle über einen Fiat Chrysler Jeep erhalten.[15] Die Liste ließe sich beliebig fortführen. Es scheint als sei keine Branche, kein Industriezweig vor solchen Angriffen gefeit.

Wie kann es sein, dass das Internet zwar massiv an Bedeutung gewonnen hat, die Sicherheit aber systematisch ignoriert wurde? Als "digitale Sorglosigkeit"[16] bezeichnet das BSI dieses Paradoxon unserer Informationsgesellschaft: Obwohl digitale Systeme unseren privaten und beruflichen Alltag fast vollständig durchdringen, ist das allgemeine Interesse an ihrer Sicherheit gering. Gerade die Politik darf sich dieser Sorglosigkeit nicht weiter hingeben: Die Potenziale von Industrie 4.0, dem Internet der Dinge und Big Data werden sich nur realisieren lassen, wenn sich strategisch mit der Frage nach der Sicherheit[17] unserer IT auseinandergesetzt wird. Um sich dieser Frage zu stellen werden im Folgenden fünf zentrale Gründe diskutiert, die zur Unsicherheit unserer IT-Systeme beitragen: (1) Komplexe Hard- und Software, (2) internationale Lieferketten, (3) ein globales Netzwerk, (4) Gemeinsame Hard- und

Software-Infrastruktur und (5) falsche Marktanreize. Basierend auf dem unterschiedlichen Zusammenspiel dieser fünf Aspekte werden im zweiten Teil strategische Handlungsoptionen für die Politik abgeleitet, um die Sicherheit unserer IT nachhaltig zu fördern, statt nur - wie bisher - punktuell zu reagieren.

## A. WARUM IT-SICHERHEIT SO SCHWIERIG IST

### 1. Komplexe Hard- und Software

"Complexity is the worst enemy of security" erklärt IT-Sicherheitsexperte Bruce Schneier.[18] Schon 1965 konstatierte Gordon Moore, Mitgründer des Chipherstellers Intel, dass sich die Komplexität integrierter Schaltkreise regelmäßig verdoppeln wird. Während die ersten kommerziellen Prozessoren für Computer noch aus wenigen Tausend Transistoren bestanden, besitzen aktuelle Prozessoren mehrere Milliarden Transistoren.[19] Bereits im Jahr 2002 verfügte ein durchschnittliches Mobiltelefon über mehr Rechenleistung als die Apollo-Spaceshuttles der 60er Jahren.[20] Bei Software verhält es sich ähnlich. Aktuelle Internet-Browser bestehen aus 15-20 Millionen Codezeilen. Heutige Betriebssysteme kommen schnell auf 50-100 Millionen Zeilen an Quellcode.[21] In jeder einzelnen Zeile kann ein Programmierfehler stecken, der die Sicherheit des ganzen Systems kompromittieren könnte. Je höher die Komplexität von Hard- und Software, desto schwieriger lassen sich Fehler finden und beheben - geschweige denn ausschließen. Außerdem lassen sich in Millionen Codezeilen oder Milliarden von Transistoren viel leichter Hintertüren verstecken, die Unbefugten unbemerkt Zugriff zum gesamten System ermöglichen können. Gerade bei Software steigt die Komplexität nochmals durch das Zusammenspiel und die Abhängigkeiten unterschiedlicher Softwarekomponenten signifikant an.

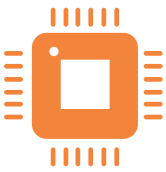
### 2. Internationale Lieferketten

Heutige IT-Systeme sind in der Regel aus Komponenten vieler verschiedener Hersteller zusammengebaut. Die 40-50 Steuercomputer in einem modernen Auto können aufgrund der starken Spezialisierung der Zulieferer von Dutzenden unterschiedlichen Herstellern kommen. Diese Hersteller wiederum beziehen bestimmte Einzelteile von anderen Unternehmen. Gleiches gilt für Laptops und Smartphones: Zwar steht Apple, Samsung oder Dell auf dem Gerät - in Wirklichkeit besteht es jedoch aus Komponenten von Broadcom, intel, Sanyo und unzähligen mehr. Diese Modularisierung und Spezialisierung führt zu Kosteneffizienz und ermöglicht erst die fortlaufenden Innovationen im IT-Sektor. Gleichzeitig stellt es eine Gefahr für die IT-Sicherheit dar. Fahrlässigkeit oder mangelndes Bewusstsein für IT-Sicherheit bei einem einzelnen Hersteller in der Lieferkette kann die Sicherheit des gesamten Systems kompromittieren.[22] Zusätzlich kann ein einziger Hersteller in der Lieferkette durch gezieltes Implementieren von Schwachstellen und Sicherheitslücken das gleiche Resultat erzielen.[23] Aufgrund der hohen Komplexität, die entsteht wenn viele unterschiedliche Systemkomponenten ineinandergreifen, ist es unmöglich geworden, die Sicherheit des Gesamtsystems zu verifizieren. Dieser Verlust über die Kontrolle der Integrität des gesamten Systems hat Russland 2014 als Anlass genommen, Behörden-Computer zukünftig nicht mehr mit (ausländischen) Intel- oder AMD-Prozessoren auszustatten, sondern Prozessor und Betriebssystem selbst in Russland herzustellen.[24] Auch wenn bezweifelt werden darf, dass die russischen Computer nun sicherer vor fremden Zugriff sind, verdeutlicht das Beispiel das Bedürfnis, Hoheit über die Lieferkette zurückzugewinnen.

### 3. Ein globales Netzwerk

Laut IT-Sicherheitsexperte Ross Anderson ist jeder Computer ist ein potenzieller Angreifer, da alle über das Internet miteinander verbunden sind: “In a world in which the ‘black hats’ can attack anywhere but the ‘white hats’ have to defend everywhere, the black hats have a huge economic advantage”.[25] Das Internet besteht zurzeit aus rund 52.000 einzelnen, selbst organisierten und ständig wachsenden Netzwerken - den sogenannten Autonomen Systemen (AS).[26] Durch einheitliche, technische Protokolle ist sichergestellt, dass alle AS untereinander kommunizieren können und dadurch potenziell jeder Computer innerhalb eines AS eine Verbindung zu jedem anderen Computer in jedem anderen AS herstellen kann. AS können von den unterschiedlichsten Organisationen, wie z.B. Universitäten, privaten Unternehmen oder Behörden betrieben werden. Diese potenzielle Konnektivität zu jedem anderen Endpunkt des Netzwerkes ist Grund für das enorme Wachstum des Internets - dem Netzwerk aus Netzwerken. Und zukünftig soll immer mehr mit dem Internet verbunden werden. Gleichzeitig ist diese physische Verbindung zu jedem anderen Computer ein Sicherheitsrisiko. So hatte der NSA-Untersuchungsausschuss kurzfristig erwogen Sitzungen fortan per Schreibmaschine zu protokollieren - um sich so dem Sicherheitsrisiko des Netzwerkes zu entziehen.[27]

### 4. Gemeinsame Hardware- und Software-Infrastruktur



Immer mehr Technologien migrieren aus vorrangig ökonomischen Gründen zum Internet - vom Telefon, über Fernsehen bis hin zu SCADA-Systemen[28] der Industrie. Weiterhin bilden sich bei Hard- und Software dominante Plattformen, Monopole und Quasi-Standards heraus. So will die Deutsche Telekom bis 2018 die vollständige Umstellung von Analog- und ISDN-Telefonie auf Internet-Telefonie abgeschlossen haben.[29] Cisco stellt etwa 60% der Internetrouter weltweit her.[30] Rund 80% der Computer nutzen Microsoft Windows als Betriebssystem[31] - bis hin zu Geldautomaten.[32] Ebenso basieren etwa 80% der Smartphones auf Googles Android Betriebssystem.[33] Um die Verbindung zwischen Server und Endgerät zu verschlüsseln setzen 70% der Websites weltweit die Softwarebibliothek OpenSSL ein.[34] Systeme, die über das Internet kommunizieren, basieren also vorrangig auf (entsprechend angepasster) standardisierter Hard- und Software. Dies ermöglicht erst die kurzen Produktzyklen und hohe Innovationskraft, an die man sich im IT-Sektor gewöhnt hat. Gleichzeitig gehen hiervon jedoch viele Gefahren für die Sicherheit aus: Wenn Büro-Computer, Geldautomaten und medizinische Geräte das gleiche Betriebssystem nutzen, sind sie durch Schwachstellen in selbigem auch alle gleich angreifbar - mit verheerenden Konsequenzen. Medizinische Geräte in Krankenhäusern nutzen z.B. oft noch Windows XP, ein veraltetes Desktop-Betriebssystem mit vielen Sicherheitsschwächen, und sind dadurch sehr leicht angreifbar.[35] Der hohe Grad an Standardisierung führt aber auch dazu, dass sich erfolgreiche Angriffe sehr leicht übertragen lassen. Dadurch lassen sich die Folgen einer bestimmten Schwachstelle nur sehr schwer abschätzen, da man nicht weiß in welchen Domänen und Branchen diese Software oder dieses spezielle Hardwaremodul noch eingesetzt wird.[36]

## 5. Falsche Marktanreize

Insbesondere drei wirtschaftliche Faktoren, die auf den ersten Blick nichts miteinander zu tun haben, wirken sich direkt negativ auf die IT-Sicherheit aus: Fehlendes Wissen über die tatsächliche Qualität proprietärer Software (Informationsasymmetrie), fehlende Haftung für Softwarefehler und ein Markt der vor allem Innovation und neue Features honoriert.

**Proprietäre Software** gilt als Geschäftsgeheimnis und Dritten ist es daher nicht gestattet, den Quellcode einzusehen. Dies ist zunächst kein Problem, da z.B. die Leistungsfähigkeit neuer Software durch Benchmarks objektiv gemessen werden kann und neue Feature vorgeführt und ausführlich getestet werden können. Gesteigerte Leistung und innovative Feature werden daher vom Markt honoriert. In Bezug auf Sicherheit besteht jedoch eine Informationsasymmetrie zwischen Herstellern proprietärer Software und den Kunden: Kunden können die Softwarequalität von außen nicht einschätzen - dafür müsste man den Quellcode analysieren dürfen - daher fließt dieser Aspekt kaum in die Kaufentscheidung mit ein. Diese Art von Marktversagen ist in anderen Bereichen seit Jahrzehnten bekannt.[37]

In Kombination mit **unzureichender Softwarehaftung** entstand so in den letzten Jahrzehnten ein Markt, der Sicherheitsaspekte bei Software weitgehend ignoriert, da sie weder überprüft noch eingefordert bzw. eingeklagt werden können: Softwarehersteller können kaum für Fehler oder Schwachstellen in ihrer Software haftbar gemacht werden. Dies fördert zwar die Innovationsfreudigkeit sowie die schnelle Entwicklung und Vermarktung neuer Ideen und Produkte. Die fehlende Haftung begünstigt jedoch auch, dass Sicherheit bei der Softwareentwicklung nur eine untergeordnete Rolle spielt: Wenn IT-Unternehmen vom Markt vorrangig für neue Feature und Innovationen belohnt werden und die Haftung für Softwarefehler gleichzeitig ausgeschlossen ist, macht es aus Unternehmenssicht wirtschaftlich wenig Sinn auf Sicherheit zu fokussieren. Aufgrund der kurzen Produkt- und Entwicklungszyklen wird daher oft erst im Nachhinein an Sicherheit gedacht. Jedoch ist es im Nachhinein wesentlich schwieriger, kostenintensiver und teils gar nicht mehr möglich ein Produkt überhaupt abzusichern.[38]

Die fehlenden Marktanreize bei der Entwicklung von Anfang an auf Sicherheit zu achten, haben gerade beim Internet der Dinge und bei mobilen Endgeräten potenziell verheerende Folgen. So werden Smartphones vergleichsweise kurze Zeit nach ihrer Veröffentlichung durch den Hersteller nicht mehr mit Software- und Sicherheitsupdates versorgt. Hersteller stehen unter großem Druck neue Modelle der nächsten Generation zu verkaufen, statt Softwarepflege bei der alten Generation zu betreiben.[39] Es fehlt nicht nur an Bewusstsein sondern auch an Zeit und Ressourcen, um Sicherheit in der Produktentwicklung ausreichend zu berücksichtigen. Ähnlich sieht es beim Internet der Dinge aus - “intelligente” Endgeräte besitzen oft unzureichende Möglichkeiten zur Softwareaktualisierung und desolate Sicherheitskonzepte.[40]

## Schlussfolgerungen

Diese fünf, hier aufgeführten Gründe tragen in unterschiedlichem Maße dazu bei, dass IT-Sicherheit ein zentrales Problem unserer heutigen Informationsgesellschaft ist. Das rasante Voranschreiten des Internets der Dinge wird dieses Problem noch weiter verschärfen. In den nächsten Jahren werden Milliarden autonomer Geräte mit dem Internet vernetzt werden. Dadurch werden diese Maschinen von außen angreifbar. Auch wenn die Herausforderungen groß sind, kann sich die Politik dem Problem produktiv annehmen. Es gibt zahlreiche politische Handlungsmöglichkeiten, um die Sicherheit unserer Informationstechnologien zu erhöhen. Wenn man allerdings tragfähige und nachhaltige Verbesserungen erreichen will, muss man

die hier aufgelisteten strukturellen Ursachen für IT-Sicherheit adressieren. Zusätzlich sollte man bedenken, welche Problemfelder wirklich wirkungsvoll im gegebenen politischen Handlungsspielraum und angesichts begrenzter Ressourcen bearbeitet werden können. Im Folgenden werden einige Überlegungen zu politische Handlungsoptionen angestellt und zentrale Bausteine einer politischen Strategie für mehr IT Sicherheit identifiziert.

## B. HANDLUNGSOPTIONEN FÜR DIE POLITIK

IT-Sicherheit ist im Sinne eines anzustrebenden Idealzustands nie erreichbar: Unsere IT-Systeme bestehen aus unzähligen Einzelteilen unterschiedlichster Hersteller, basieren auf komplexer Hard- und Software und sind über das Internet von überall angreifbar. Und selbst wenn die Technik "sicher" ist, bleibt immer noch der Faktor Mensch.[41] IT-Sicherheit ist daher vielmehr als ein Prozess zu begreifen, den es stetig zu verbessern gilt. So wird IT-Sicherheit und Schutz kritischer Infrastrukturen gerne als Grund angeführt, Präsenz und Rechte von Sicherheitsbehörden[42] und Bundeswehr[43] im Internet auszuweiten. Jedoch liegen diesen Maßnahmen Maxime klassischer Sicherheitspolitik zugrunde, die zentrale Funktionsweisen und Eigenheiten des Internets ignorieren.

In Abgrenzung zum gängigen Begriffs des "Cyberraums" hat die Europäische Agentur für Netz- und Informationssicherheit (ENISA) schon vor einigen Jahren den Begriff[44] des Internet Interconnection Ecosystems geprägt und versucht so die Komplexität des Internets auszudrücken: Einen einzelnen Raum kann man absichern, aber nicht ein Netzwerk aus Zehntausenden von Netzwerken. Diese Unterscheidung ist besonders bei staatlichem Handeln wichtig: Ein "unsicherer" öffentlicher Raum - z.B. ein öffentlicher Park oder ein Platz - kann durch erhöhte Präsenz von Sicherheitsbehörden durchaus "abgesichert" werden. Diese Logik funktioniert jedoch nicht bei einem Netzwerk aus Netzwerken. Dennoch verfolgen viele staatliche Maßnahmen der jüngsten Vergangenheit genau diese Logik - indem Bundeswehr, Bundesnachrichtendienst und Bundesverfassungschutz mit immer mehr Ressourcen zur "Cyber-Abwehr" ausgestattet werden. Zur IT-Sicherheit trägt dies jedoch nur bedingt bei, da Cyber-Abwehr eben nur ein Teilaspekt von Cyber-Sicherheit ist. So wird sich einem trügerischen Sicherheitsgefühl hingegeben, ohne effektiv etwas an der Lage verbessert zu haben und tatsächlich wirkungsvolle Maßnahmen werden ignoriert oder nicht mit den nötigen Ressourcen ausgestattet.

### 1. Defensive vs Offensive

Offensive Maßnahmen von Sicherheitsbehörden und Bundeswehr stärken zwar die Überwachungs- und Angriffsfähigkeiten des Staates, sie gefährden jedoch die allgemeine IT-Sicherheit und schädigen ebenso das Vertrauen zwischen Staat, Unternehmen und Bürgern: So wurde dem Bundesnachrichtendienst (BND) im Zuge der "Strategischen Initiative Technik"[45] bis 2020 ein Budget von 4,5 Mio Euro zugesagt, um Software-Sicherheitslücken auf dem internationalen grauen Markt einzukaufen.[46] Diese Sicherheitslücken nutzt der BND dann aus, um in fremde IT-Systeme einzudringen. Ähnliche Pläne verfolgt Verteidigungsministerin Ursula von der Leyen. Sie will die Bundeswehr mit "offensiven Cyber-Fähigkeiten" ausstatten und sie mit der "gesamtstaatlichen Sicherheitsvorsorge" betrauen.[47] Auch die Entwicklung und der Einsatz von Remote Forensic Software (umgangssprachlich "Bundestrojaner" genannt) durch deutsche Strafverfolgungsbehörden zur Quellen-Telekommunikationsüberwachung stellen eine offensive Maßnahme dar.[48]

Das Problem offensiver Maßnahmen im Internet liegt in der Ungewissheit darüber, wer diese Schwachstellen noch kennt und ausnutzt.[49] Da immer mehr IT-Systeme auf der gleichen Hard- und Software basieren (4) und diese über das Internet direkt miteinander verbunden sind (3) stellt eine einzige Sicherheitslücke unter Umständen eine Gefahr für unzählige IT-Systeme in den verschiedensten Bereichen dar: Eine bestimmte Sicherheitslücke in einem Internetbrowser kann durch Sicherheitsbehörden genutzt werden, um einen Terroristen zu überwachen. Da die Sicherheitsbehörden die Schwachstelle geheimhalten und sie nicht an den Hersteller melden, kann dieselbe Schwachstelle jedoch auch durch einen Hacker für Industriespionage genutzt werden.[50] Dies gefährdet aktiv die Sicherheit aller deutscher Unternehmen und Privatpersonen.[51] Sicherheitslücken geheim zu halten, um sie möglicherweise selbst zu nutzen, ist daher reines Glücksspiel, da man - gerade wenn diese auf dem grauen Markt eingekauft wurden - nicht weiß, wer noch Kenntnis von ihnen hat bzw. an wen sie noch verkauft wurden.[52]

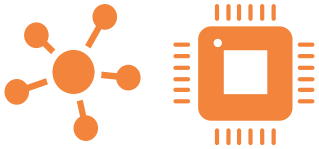
Diese Ungewissheit schädigt nachhaltig das Vertrauensverhältnis zwischen Staat, Unternehmen und Zivilgesellschaft: Unternehmen werden es sich genau überlegen, ob sie Informationen über Schwachstellen mit staatlichen Akteuren teilen (wie vom IT-Sicherheitsgesetz gefordert), wenn sie nicht sicher sein können, ob die Information für eigene offensive Maßnahmen benutzt wird, anstatt die Schwachstelle zu beheben. Als Beispiel sei hier die Meldepflicht gegenüber dem BSI genannt, die viele Unternehmen aufgrund der Nähe des BSI zum BND kritisch betrachten. Wie ein zu starker Fokus auf offensive Maßnahmen die eigene Wirtschaft schädigen kann, sieht man in den Vereinigten Staaten: Die Enthüllungen der NSA-Überwachungsmaßnahmen haben bei US-amerikanischen Cloudanbietern, wie IBM und Microsoft, zu drastischen Umsatzeinbußen im Ausland geführt.[53] Sicherheitslücken sollten daher durch deutsche Sicherheitsbehörden und Bundeswehr weder auf dem grauen Markt gekauft noch ausgenutzt werden.

Stattdessen sollte der Fokus stärker auf defensive Maßnahmen gelegt werden. Defensive Maßnahmen zielen darauf ab, IT-Sicherheit grundsätzlich zu stärken und so erfolgreiche Angriffe durch fremde Staaten oder organisiertes Verbrechen zu erschweren. Dies kann zum Beispiel durch Forschungsförderung, der Entwicklung und Implementierung von Sicherheitsstandards oder der Verbesserung des Informationsaustausches zwischen betroffenen Akteuren geschehen. Das 1999 vorgestellte Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik[54] wäre dieser Unterscheidung zufolge eine defensive Maßnahme. Des weiteren zählen das kürzlich in Kraft getretene IT-Sicherheitsgesetz[55] zum besseren Schutz kritischer Infrastrukturen, das Forschungsrahmenprogramm der Bundesregierung zu IT-Sicherheit[56] mit einem Volumen von 180 Mio. Euro bis 2020 und die auf Initiative des BSI ins Leben gerufene Allianz für Cyber-Sicherheit zu den defensiven Maßnahmen der Bundesregierung.

***#1 – Statt Sicherheitslücken auf dem grauen Markt einzukaufen sollten Behörden dabei helfen diese zu schließen.***

Die konsequente, politische Unterstützung von IT-Sicherheit stärkt außerdem die deutsche Industrie. Vertrauen in die Sicherheit technischer Lösungen und rechtlicher Rahmenbedingungen ist für Deutschland als Exportnation essenzielle Grundlage, um international wettbewerbsfähig zu bleiben. Gleichzeitig ist Deutschland - im Gegensatz zu den USA oder China - auf ausländische IT-Lösungen angewiesen. Daher liegt es in unserem Interesse, international die Entwicklung von möglichst hohen IT-Sicherheitsstandards zu unterstützen.

## 2. Gefährdungslage und Vertrauensnetzwerke



Zur Steigerung der IT-Sicherheit im Internet-Zeitalter ist ein umfassendes Bild über die aktuelle Gefährdungslage essenziell. Welche neuen Schwachstellen gibt es und durch wen werden sie ausgenutzt? Welche Netzwerke und Systeme sind gefährdet oder gar kompromittiert? Da der Austausch von Informationen nicht dem Selbstzweck dient, sondern das Ziel verfolgt, die (eigenen) IT-Systeme besser schützen zu können, ist die Qualität und Aussagekraft der geteilten Informationen daher von entscheidender Bedeutung. Diese sensiblen Informationen über die eigenen Systeme werden nur geteilt, wenn dem Gegenüber vertraut wird. In den vergangenen Jahren sind so in Deutschland verschiedene solcher losen Vertrauensnetzwerke entstanden: Das Krisenreaktionszentrum für IT-Sicherheit der deutschen Versicherungswirtschaft (LKRZV)[57], das Cyber Security Sharing and Analytics (CSSA)[58] oder das German Competence Centre against Cyber Crime (G4C) sind als Beispiele zu nennen.[59] Diese Initiativen basieren auf einem gemeinsamen Problembewusstsein, freiwilliger Mitgliedschaft und Vertrauen unter den Mitgliedern - teils auch mit staatlichen Behörden als externe Partner.

Die durch das IT-Sicherheitsgesetz verordnete Meldepflicht an das BSI für Betreiber kritischer Infrastruktur ignoriert viele dieser Aspekte - vor allem wird die Relevanz von Vertrauen unterschätzt: Wenn dem Gegenüber nicht vertraut wird und Ungewissheit besteht, was mit den anvertrauten Informationen passiert, verringert dies die Bereitschaft zum Informationsaustausch. Das nötige Vertrauen kann man regulatorisch nicht erzwingen. Ob sich Unternehmen an eine Meldepflicht halten und wie wertvoll die Informationen sind, die sie weiterreichen hängt daher von drei Fragen ab: 1) Wie sehr vertraut man der Stelle, an die gemeldet werden muss? 2) Wie hoch sind die Sanktionen, falls ein Angriff nicht gemeldet wird? 3) Wie wahrscheinlich ist es, dass das Verschweigen eines Angriffs oder einer Schwachstelle aufgedeckt wird? Um zeitnah qualitativ hochwertige Informationen zu erhalten, die tatsächlich dabei helfen kritische Infrastrukturen besser zu schützen ist neben dem Vertrauen in das BSI auch dessen Kompetenz relevant. Bei mangelndem Vertrauen in das BSI oder in dessen Kompetenz werden die beteiligten Organisationen lediglich ein Minimum an Informationen weiterleiten oder gar in Erwägung ziehen, ob das Risiko einer Sanktion nicht geringer ist.

Zukünftig wird es daher von zentraler Bedeutung sein, wie man politisch die Bildung und Stärkung von Vertrauensnetzwerken sinnvoll und nachhaltig fördern kann. Die Politik sollte daher Anreize schaffen, dass die verschiedenen Branchen solche freiwilligen Austauschplattformen schaffen, statt nur auf die Meldepflicht gegenüber dem BSI zu setzen. Das BSI sollte hier trotzdem eine stärkere und vor allem unabhängige Position, ähnlich der der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), erhalten.[60] Die zivilen Bereiche des BSI sollten in eine eigene, unabhängige Behörde ausgegliedert werden. Erst ein solches unabhängiges, ziviles BSI ohne Unterabteilungen für Sicherheitsbehörden kann uneingeschränktes Vertrauen der Zivilgesellschaft und Wirtschaft genießen und seinen zukünftigen Aufgaben nachkommen. Dies wäre außerdem ein Gegengewicht zu den gesteigerten Ressourcen von Polizei, Geheimdiensten und Bundeswehr, die unsere Informationsnetzwerke zwar stärker überwachen aber dadurch unsere IT nicht zwingend sicherer machen.

***#2 – Das BSI sollte unabhängig werden.***

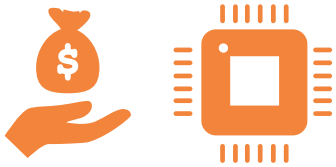
Weiterhin spielt die Stärkung der Position des IT-Sicherheitsbeauftragten in Organisationen eine wichtige Rolle. Im Vergleich zum Datenschutzbeauftragten ist diese Position noch kaum entwickelt, jedoch dringend benötigt. Eine Stärkung würde den Informationsaustausch be-

***#3 – Die Position des IT-Sicherheitsbeauftragten muss gestärkt werden.***

günstigen, IT-Sicherheit in Unternehmen strategisch etablieren[61] und der IT-Sicherheitsbeauftragte wäre außerdem Kontaktperson im Ernstfall.

Ebenso sollte ein stärkerer Fokus auf die Etablierung und Förderung von Computer Emergency Response Teams (CERT) gelegt werden. Aufgabe dieser Teams von IT-Sicherheitsexperten ist es, (kritische) IT-Infrastrukturen zu schützen und Cyberangriffe abzuwehren.[62] Ähnlich, wie bei den zuvor erwähnten Krisenreaktionszentren sind CERTs entweder privatwirtschaftlich oder staatlich organisiert. So betreibt das BSI das CERT-Bund für Bundesbehörden.[63] Gerade in der Privatwirtschaft zeichnen sich CERTs meist durch hohe Kompetenz, schnelle Reaktionszeiten, sehr gute Vernetzung und Austausch auf Vertrauensbasis aus. Diese Organisationsform und ihre unbürokratische Arbeitsweise sind entscheidend für den Erfolg. CERTs sind operative Einheiten und daher auf effektiven und guten Informationsaustausch angewiesen. Um Infrastrukturen effektiv vor Cyberangriffen zu schützen sind CERTs daher unerlässlich.

### 3. Marktanreize schaffen



Will man die Sicherheit von Informations- und Kommunikationstechnologie verbessern, muss man Asymmetrien zwischen dem Wissen von Hersteller und Kunde abbauen. Der Staat kann und sollte hier auf verschiedene Art und Weise regulierend eingreifen, um IT-Sicherheit langfristig zu fördern.

**Förderung von Open Source-Software.** Die Informationsasymmetrie ist bei Open Source-Software naturgemäß weniger problematisch, da der Quellcode der Allgemeinheit offen zur Verfügung steht. Somit kann jeder eine Überprüfung des Quellcodes auf Sicherheitslücken oder Fehler vornehmen bzw. beauftragen. Man muss den Aussagen des Softwareherstellers daher nicht einfach vertrauen, sondern kann sie auch überprüfen. Die Bundesregierung könnte daher sicherheitsrelevante und weitverbreitete Open Source-Software, z.B. zur verschlüsselten Kommunikation, regelmäßig durch unabhängige Auditoren überprüfen lassen.[64] Durch das kontinuierliche Aufspüren von Sicherheitslücken in kritischen Open Source-Anwendungen würde so direkt die Sicherheit dieser Anwendungen verbessert werden.

Die staatliche Förderung von Audits wäre vor allem bei sicherheitsrelevanten Open Source-Softwarebibliotheken (“Bausteine”, die durch jede Anwendung benutzt werden können) wichtig. GNU Privacy Guard, die am weitesten verbreitete Software zur Verschlüsselung von E-Mails, wird von einem Deutschen seit 1997 ehrenamtlich entwickelt.[65] OpenSSL, Verschlüsselungssoftware mit der die meisten Websites abgesichert werden, beruht größtenteils auf der Arbeit von vier Programmierern.[66] Ohne OpenSSL wäre Onlinehandel oder gar Onlinebanking nicht möglich. Sehr viele Unternehmen nutzen diese freie Softwarebibliothek allerdings ohne sie weiterzuentwickeln: das klassische Trittbrettfahrer (Free Rider) Dilemma. Anstatt selbst OpenSSL zu auditieren, warten alle lieber (vergeblich) darauf, dass ein Anderer diese Aufgabe übernimmt. Ganz ähnlich sieht es bei vielen anderen, sicherheitsrelevanten, freien Softwarebibliotheken aus. Abhilfe könnten staatlich finanzierte Audits schaffen. Sie würden direkt zur Verbesserung der Sicherheit aller Internetnutzer beitragen.

***#4 – Sicherheitsrelevante Open Source-Software sollte durch unabhängige Sicherheitsaudits staatlich gefördert werden.***

Um dem in der Digitalen Agenda der Bundesregierung formulierten Ziel, Deutschland zum "Verschlüsselungsstandort Nr. 1"[67] zu machen, näher zu kommen, wäre die finanzielle Unterstützung für Sicherheitsüberprüfungen etablierter Open Source-Software und Protokolle ein wichtiger erster Schritt. Ebenso könnte sich durch die Behörden direkt an der Weiterentwicklung von Open Source-Software beteiligt werden: So hat das französische Militär aktiv das offene Mailprogramm Thunderbird weiterentwickelt, um es mit besserer Verschlüsselung auszustatten. Die Weiterentwicklungen wurden der Allgemeinheit wieder unter der offenen Lizenz zur Verfügung gestellt.[68] All dies sind keine neuen Ansätze. Schon 1999 förderte das BMWi erwähntes GNU Privacy Guard Projekt mit 250.000€.[69] Die Förderung sicherheitsrelevanter Open Source Software muss jedoch ausgebaut und verstetigt werden.

**Softwarehaftung.** Schon 1997 monierte die Hackergruppe "LOpht" gegenüber dem US Senat die fehlende Haftung von Softwareherstellern für Sicherheitslücken in ihren Produkten. Ähnliches hört man seitdem fast jedes Jahr auf diversen Sicherheitskonferenzen weltweit.[70] Die wichtigsten Gegenargumente lauten, dass Software zu komplex sei und meist auf unzähligen unterschiedlichen Modulen von verschiedenen Anbietern basiere, sodass Fehler niemals ausgeschlossen werden könnten. Zudem würde Haftung sich vor allem negativ auf Innovation auswirken. Beide Argumente sind richtig. Jedoch ist Software integraler Bestandteil so vieler Aspekte unseres Alltags geworden, dass beide Argumente - Komplexität und weniger Innovation - im Kontext der hohen Kosten von fehlender Sicherheit betrachtet werden müssen. Vor allem die Kombination aus geschlossener, proprietärer Software (eine Blackbox) und Haftungsausschluss für Softwarefehler führt dazu, dass Sicherheit nur eine untergeordnete Rolle bei der Entwicklung spielt. Ziel ist es nicht, Softwarehersteller zur Offenlegung des Quellcodes zu bringen. Es geht vielmehr darum, ihnen Verantwortung für Fehler in ihrer Software zu übertragen. Letzteres kann man durch Haftung erreichen.

***#5 – Hersteller sollten für Sicherheitslücken in proprietärer Software leichter haftbar gemacht werden können.***

Wenn der Nutzer durch einen Programmierfehler in proprietärer Software physischen oder finanziellen Schaden erleidet, sollte der Softwarehersteller dafür haftbar gemacht werden können. Der Effekt wäre, dass sich Softwarehersteller gegen solche Schadensfälle versichern müssten. Die Versicherungen wiederum werden prüfen, wie sorgfältig das Softwareunternehmen bei der Entwicklung ist und wie sehr auf Sicherheit geachtet wird. Laxe Softwareentwicklung für sicherheitsrelevante Anwendungen würde so zu hohen Versicherungspolicen führen. Dies stellt wiederum einen Anreiz für das Unternehmen dar, durch sorgfältigere Entwicklung Versicherungskosten einzusparen.

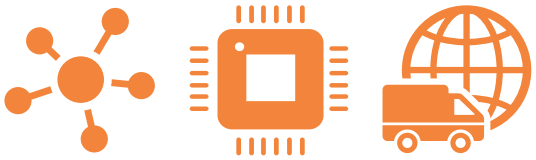
Natürlich wird in den seltensten Fällen die Schuld eindeutig und allein beim Softwarehersteller liegen. Auch beim zuvor erwähnten Fiat Chrysler Hack, der es ermöglichte, bestimmte Jeep Modelle über das Internet fernzusteuern, lag die Schuld nicht nur bei Fiat Chrysler. Harman ist Lieferant der Internetfähigen Mittelkonsole, die den Hack erst ermöglichte. Gleichzeitig tragen Fiat Chrysler und auch Sprint (Mobilfunkanbieter) eine Teilschuld.[71] Es wird Zeit und Aufwand bedeuten, Verantwortlichkeiten klar und fair abbilden zu können. Nur wenn wir uns dieser Herausforderung stellen, werden wir Marktanreize erfolgreich zur Stärkung von IT-Sicherheit nutzen können. Die Ratio der Softwarehaftung ist letztlich denkbar einfach: Entweder veröffentlicht der Hersteller seinen Quellcode, damit man seine Aussagen überprüfen kann und entzieht sich so der Haftung (Open Source Software unterläge daher nicht der Haftung). Oder der Hersteller steht im Ernstfall zu seinen Aussagen und muss unter Umständen dafür haften.
Eine weitere Option, gerade mit Blick auf das Internet der Dinge, ist die Ausweitung der

gesetzlichen Gewährleistung auf Software-Schwachstellen. Dies würde u.a. die Sicherheit privater Internetrouter verbessern: Internetrouter sind zwar die zentraler Schnittstelle, um Endgeräte wie Laptops oder Smartphones mit dem Internet zu verbinden, sie werden durch die Hersteller jedoch nur unzureichend abgesichert[72] und nur schlecht mit Updates versorgt.[73] Dadurch werden sie zunehmend zum lukrativen Ziel für Hacker.[74] Würde man Router-Hersteller dazu verpflichten ihre Geräte mit Sicherheitsupdates zu versorgen, zumindest während der zweijährigen gesetzlichen Gewährleistung, könnten Router zukünftig sicherer werden. Durch das verabschiedete IT-Sicherheitsgesetz werden Websitebetreibern schon heute ähnliche Sorgfaltspflichten auferlegt. Die Ratio: wer eine Website betreibt sollte zumindest dafür sorgen, die eingesetzte Software auf dem aktuellen Stand zu halten.[75] Was der Gesetzgeber daher von Websitebetreibern verlangt, sollte er ebenso von Routerherstellern verlangen.

***#6 – Ausweitung der gesetzlichen Gewährleistung auf die Firmware eines Gerätes.***

Öffentliche Beschaffung. In seiner Cyber-Sicherheitsstrategie für Deutschland schreibt das Bundesinnenministerium 2011, dass staatliche Stellen mit gutem Beispiel in Bezug auf Datensicherheit vorangehen müssten.[76] Gerade mit Blick auf die beschlossene IT-Konsolidierung[77] und die geplante "Bundes-Cloud" sollte hier nicht nur auf sichere Hard- und Software gesetzt werden sondern auch die entsprechenden Prozesse etabliert werden, um diese langfristig abzusichern. Die öffentliche Hand sollte sich hier stärker ihrer Rolle bewusst werden und konsequent auf Sicherheit fokussieren.

### 4. Internationale Kooperation



Für die Bevölkerung stellt das organisierte Verbrechen im Internet (Kreditkartenmissbrauch, Erpressung, Spam, etc.) die größte direkte Gefahr dar. Zum Zeitpunkt des Schreibens dieses Artikels verbreitet sich gerade wieder ein neues Schadprogramm und infiziert über 5000 Websites jeden Tag.[78] International sind die stärksten Akteure jedoch Staaten: Stuxnet, ein Cyberangriff auf das iranische Atomprogramm, wurde den USA zugeschrieben.[79] Gleiches gilt für die "Equation Group" - eine Hackergruppe mit direkten Verbindungen zur NSA.[80] 2013 sorgte ein Bericht[81] über die chinesische Hackergruppe "APT-1" für viele Schlagzeilen - mit einem Fokus auf Wirtschaftsspionage hat sie mehrere Terabyte an Daten von rund 150 Organisationen weltweit geklaut. Ganz gleich ob es sich um feste Abteilungen staatlicher Geheimdienste oder um lose Hackergruppen handelt, die durch die Regierung unterstützt werden - staatlichen Akteuren stehen schier unerschöpfliche Ressourcen zur Verfügung. Warum brauchen wir dann trotzdem internationale Kooperation statt Abschottung?

Zum einen benutzen alle gemeinsam die gleiche Hardware, Software und Infrastruktur: Steuercomputer für Industrieanlagen auf der ganzen Welt kommen von Siemens, Internetrouter von Cisco und Prozesssteuerung von SAP. Wenn ein Angriff bei einem deutschen Wasserwerk erfolgreich war, ist die Wahrscheinlichkeit groß, dass ein ähnlicher Angriff ebenso in den Niederlanden, USA oder Großbritannien funktioniert. Aus technischer Sicht stehen viele Staaten vor denselben Problemen, die sie alleine nicht lösen können.

Zum anderen fällt im Internet die Attribution extrem schwer. Ein Angreifer kann Dritte (Computer in anderen Ländern) ausnutzen, um den Angriff für ihn durchzuführen. Nur weil ein Angriff physisch aus einem bestimmten Land kommt, heißt es nicht, dass dieses Land auch

wirklich angreift. Beim Sony Hack streitet man sich z.B. immer noch, ob die verantwortliche Hackergruppe "Guardians of Peace" tatsächlich Verbindungen zur nordkoreanischen Regierung hat und diese den Angriff als Vergeltung für den Film "The Interview" durchführte.[82] Bei Stuxnet dauerte es Jahre, bis die Software einigermaßen verlässlichen den US-amerikanischen Geheimdiensten zugeordnet werden konnte.

Beide Faktoren führen dazu, dass Staaten immer stärker miteinander kooperieren, um das Internet und die damit verbundene kritische Infrastruktur zu schützen. So verabschiedete die Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security der Vereinten Nationen dieses Jahr das erste Mal einen Bericht, der sich mit dem verantwortungsvollen Handeln im Internet beschäftigt.[83] Dort wird unter anderem die Relevanz vertrauensbildender Maßnahmen angesprochen - auf diese fokussiert seit einigen Jahren auch die Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE).[84] Zusätzlich sollen sich Staaten verpflichten, nicht gegenseitig kritische Infrastruktur anzugreifen. Völkerrechtliche Normenbildung ist langwierig und kompliziert. Und am Ende steht oftmals doch nur der kleinste gemeinsame Nenner, der viel Raum für Kritik und Interpretation lässt. Der Bericht ist allerdings ein erster wichtiger Schritt. Er verdeutlicht eindrucksvoll, dass Regierungen für die Sicherheit ihrer Infrastrukturen kooperieren müssen.[85]

***#7 – Erarbeitung vertrauensbildender Maßnahmen auf Ebene der OSZE und UN.***

Im Report werden außerdem Computer Emergency Response Teams (CERT) und die Bedeutung ihrer Arbeit hervorgehoben. Da mittlerweile lebenswichtige Infrastrukturen, wie Strom- und Wasserwerke oder Verkehrsleitsysteme mit dem Internet verbunden sind und deren Angriff verheerende Folgen haben könnte, gibt es auch Überlegungen basierend auf CERTs eine internationale, humanitäre Institution ähnlich dem Roten Kreuz zu schaffen.[86]

## C. ABSCHLUSSBEMERKUNGEN

IT-Sicherheit stellt Politik, Wirtschaft und Gesellschaft bereits seit Jahrzehnten vor große Herausforderungen. Das Thema wird in den nächsten Jahren weiter an Bedeutung gewinnen, wenn mit dem Internet der Dinge Milliarden von Alltagsgeräten mit dem Internet verbunden und somit auch potenziell angreifbar werden. IT-Sicherheitsvorfälle sorgen zwar regelmäßig für Schlagzeilen in den Medien und haben es seit den Snowden Enthüllungen nach weit oben auf der politischen Agenda geschafft. Trotz einiger positiver Initiativen bleibt die Verbesserung der IT-Sicherheit jedoch schwierig. Die wichtigsten Gründe, warum dies so ist, sind hier zusammengetragen worden. Dabei liegt der Schwerpunkt auf den strukturellen Ursachen mangelnder IT-Sicherheit. Des Weiteren müssen die Widersprüchen zwischen den Bestrebungen nach offensiven Cyberfähigkeiten und defensiven Schutzmaßnahmen endlich klar benannt werden. Hier wird man strategische Grundsatzentscheidungen treffen müssen. Neben einer klaren Positionierung zu einem defensiven Ansatz enthält dieser Policy Brief eine Reihe weiterer Handlungsempfehlungen, die großes Potenzial für die Verbesserung der Sicherheit unserer Soft- und Hardware besitzen. Diese Handlungsempfehlungen bedürfen weitere Analysen, Diskussionen und Entwicklung. Dieser Policy Brief soll daher nicht nur als ein Beitrag zur Debatte sondern auch als ein Angebot an alle Stakeholder, sich zu den Möglichkeiten der Verbesserung der IT-Sicherheit weiter mit uns auszutauschen, verstanden werden.

## D. DANKSAGUNG

Der Autor bedankt sich bei Stefan Heumann, Thorsten Wetzling und Julia Manske für konstruktive Kritik und Unterstützung. Dank gilt außerdem allen Teilnehmern des Workshops IT-Sicherheit und Verschlüsselung in Kooperation mit dem Hasso-Plattner-Institut. Besonderer Dank geht weiterhin an Rahel Dette, Bernhard Esslinger, Joerg Heidrich, Julia Hesse, Mirko Hohmann, Nemanja Malisevic, Staffan Persson, Kai Rannenberg, Volker Roth, Isabel Skierka und Falk Steiner.

## Endnoten

1 Ellen Wernick und Nelson Rhodes. 2005. “eBay Inc”. International Directory of Company Histories. http://www.encyclopedia.com/topic/eBay_Inc.aspx

2 Cameron Chapman. 2009. “The History of the Internet in a Nutshell”. http://sixrevisions.com/resources/the-history-of-the-internet-in-a-nutshell/

3 CNN. 1999. “Man charged with unleashing ‚Melissa‘ computer virus”. http://edition.cnn.com/TECH/computing/9904/02/melissa.arrest.03/index.html

4 US Senat. 1998. Hackers Testifying at the United States Senate. https://www.youtube.com/watch?v=VVJldn_MmMY

5 Cisco. 2015. “Visual Networking Index - VNI Forecast Highlights”. http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html

6 Statista. 2015. “Number of monthly active Facebook users worldwide as of 2nd quarter 2015 (in millions)”. http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

7 Benjamin Edwards et al. 2015. “Hype and Heavy Tails : A Closer Look at Data Breaches”. 14th Annual Workshop on the Economics of Information Security (WEIS). http://weis2015.econinfosec.org/papers/WEIS_2015_edwards.pdf

8 Maik Baumgärtner, et al. 2015. “Sicherheitsalarm im Parlament: Cyberangriff auf den Bundestag”. Der Spiegel. http://www.spiegel.de/netzwelt/netzpolitik/cyber-angriff-auf-den-deutschen-bundestag-a-1033984.html

9 Maik Baumgärtner, et al. 2015. “Cyberangriff auf den Bundestag: Hacker kopierten Abgeordneten-E-Mails”. Der Spiegel. http://www.spiegel.de/politik/deutschland/cyberangriff-auf-bundestag-abgeordneten-e-mails-erbeutet-a-1039388.html

10 Ellen Nakashima. 2015. “Hacks of OPM databases compromised 22.1 million people, federal authorities say”. The Washington Post. http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

11 Michael Riley und Jordan Robertson. 2015. “Cyberspace Becomes Second Front in Russia’s Clash With NATO”. Bloomberg. http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato

12 BSI. 2014. “Die Lage der IT-Sicherheit in Deutschland 2014”, Seite 31

13 Kim Zetter. 2014. “Sony Got Hacked Hard: What We Know and Don’t Know So Far”. Wired. http://www.wired.com/2014/12/sony-hack-what-we-know/

14 Eugene Kaspersky. 2015. “Kaspersky Lab investigates hacker attack on its own network”. Kaspersky Lab Daily. https://blog.kaspersky.com/kaspersky-statement-duqu-attack/

15 Andy Greenberg. 2015. “Hackers Remotely Kill a Jeep on the Highway—With Me in It”. Wired. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

16 Siehe Endnote 13, Seite 12

17 Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität

18 Bruce Schneier. 2012. "Complexity the Worst Enemy of Security". Schneier on Security. https://www.schneier.com/news/archives/2012/12/complexity_the_worst.html

19 Wikipedia. Transistor count. https://en.wikipedia.org/wiki/Transistor_count

20 Christoph Drösser. 2002. "Mit dem Handy zum Mond". Die Zeit. http://www.zeit.de/2002/02/200202_stimmts.xml

21 David McCandless, et al. 2015. "Million Lines of Code". Information is Beautiful. http://www.informationisbeautiful.net/visualizations/million-lines-of-code/

22 Lee, Sangho, et al. 2014. „Stealing webpages rendered on your browser by exploiting GPU vulnerabilities". IEEE Symposium on Security and Privacy. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6956554

23 Steven Levy. 1994. "Battle of the Clipper Chip". The New York Times. http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html

24 TASS. 2014. "Russia wants to replace US computer chips with local processors". http://tass.ru/en/economy/736804

25 Ross Anderson. 2001. "Why Information Security is Hard– An Economic Perspective". http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf

26 CIDR Report. 2015. http://www.cidr-report.org/as2.0/

27 Annett Meiritz. 2014. " NSA-Ausschuss: Ruf nach Schreibmaschine löst Spott und Kritik aus". Spiegel Online.http://www.spiegel.de/politik/deutschland/schreibmaschine-chef-von-nsa-ausschuss-wird-fuer-appell-geruegt-a-980969.html

28 Unter Supervisory Control and Data Acquisition (SCADA) versteht man das Überwachen und Steuern technischer Prozesse mit Hilfe von Computern.

29 Alexander Zollondz. 2015. "Telekom: Alles Wichtige zur Umstellung auf IP-Telefonie". Netzwelt.de. http://www.netzwelt.de/news/152851-ende-festnetzes-alles-wichtige-ip-umstellung-telekom.html

30 International Data Corporation. 2015. "IDC's Worldwide Quarterly Ethernet Switch and Router Trackers Show Ethernet Switch Market Flat to Slightly Positive, Growth Indicators for Router Market". http://www.idc.com/getdoc.jsp?containerId=prUS25642515

31 Statista. 2015. "Global market share held by computer operating systems 2012-2015, by month". http://www.statista.com/statistics/268237/global-market-share-held-by-operating-systems-since-2009/

32 Jose Pagliery. 2015. "95% of bank ATMs face end of security support". CNN Money. http://money.cnn.com/2014/03/04/technology/security/atm-windows-xp/

33 International Data Corporation. 2015. “Smartphone OS Market Share, 2015 Q2”. http://www.idc.com/prodserv/smartphone-os-market-share.jsp

34 The Heartbleed Bug. http://heartbleed.com/

35 Scott Erven and Mark Collao. 2015. “Medical Devices: Pwnage and Honeypots”. Derbycon 2015. http://www.irongeek.com/i.php?page=videos%2Fderbycon5%2Fbreak-me14-medical-devices-pwnage-and-honeypots-scott-erven-mark-collao

36 Michael Mimoso. 2015. “Valasek: Today’s Furby Bug is Tomorrow’s SCADA Vulnerability”. Threatpost. https://threatpost.com/valasek-todays-furby-bug-is-tomorrows-scada-vulnerability/114620/

37 George A. Akerlof. 1970. „The market for „lemons“: Quality uncertainty and the market mechanism.“ The quarterly journal of economics. 488-500.

38 Craig Timberg. 2015. “Net of Insecurity Part 1: A Flaw in the Design”. The Washington Post. http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/

39 Ron Amadeo. 2015. “First-ever monthly Android security updates start to roll out”. ars technica. http://arstechnica.com/gadgets/2015/09/first-ever-monthly-android-security-updates-start-to-roll-out/?mbid=synd_moz_technews

40 Sanjay Sarma. 2015. “I helped invent the Internet of Things. Here’s why I’m worried about how secure it is”. Politico. http://www.politico.com/agenda/story/2015/06/internet-of-things-privacy-risks-security-000096

41 Verizon. 2015. “Data Breach Investigations Report”. S. 46. http://www.verizonenterprise.com/DBIR/2015/

42 Andre Meister. 2015. “Verfassungsschutz-Gesetz: Die Stellungnahme der Bundesdatenschutzbeauftragten, die der Union zu kritisch war”. Netzpolitik.org. https://netzpolitik.org/2015/verfassungsschutz-gesetz-die-stellungnahme-der-datenschutzbeauftragten-die-der-union-zu-kritisch-war/

43 Matthias Gebauer. 2015. “ Verteidigungsministerin von der Leyen: Vercybert”. Spiegel Online. http://www.spiegel.de/politik/deutschland/ursula-von-der-leyen-die-gezaehmte-cyber-kriegerin-a-1053549.html

44 European Union Agency for Network and Information Security. 2011. “Resilience of the Internet Interconnection Ecosystem”. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/interx/report/interx-report

45 Andre Meister. 2015. “Strategische Initiative Technik: Wir enthüllen, wie der BND für 300 Millionen Euro seine Technik aufrüsten will”. netzpolitik.org. https://netzpolitik.org/2015/strategische-initiative-technik-wir-enthuellen-wie-der-bnd-fuer-300-millionen-euro-seine-technik-aufruesten-will/

46 Spiegel Online. 2014. “Online-Spionage: BND will Informationen über Software-Sicherheitslücken einkaufen”. http://www.spiegel.de/politik/deutschland/bnd-will-informationen-ueber-software-sicherheitsluecken-einkaufen-a-1001844.html

47 Matthias Gebauer. 2015. “ Geheime Bundeswehr-Strategie: Von der Leyen rüstet an der Cyberfront auf”. Spiegel Online. http://www.spiegel.de/politik/deutschland/bundeswehr-

ursula-von-der-leyen-ruestet-an-der-cyber-front-auf-a-1042985.html ; Andre Meister. 2015. "Geheime Cyber-Leitlinie: Verteidigungsministerium erlaubt Bundeswehr „Cyberwar" und offensive digitale Angriffe". netzpolitik.org. https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/

48 Ulf Buermeyer. 2011. "Quellen-TKÜ – ein kleines Einmaleins (nicht nur) für Ermittlungsrichter". http://ijure.org/wp/archives/756

49 Matthew Green. 2015. „A history of backdoors". A Few Thoughts on Cryptographic Engineering. http://blog.cryptographyengineering.com/2015/07/a-history-of-backdoors.html

50 Chaos Computer Club, Pressemitteilung. 10. November 2014. "CCC verurteilt den Ankauf von Odays durch den BND". http://www.ccc.de/de/updates/2014/0days-an-den-bnd

51 Gesellschaft für Informatik, 18. November 2014, "IT-Sicherheitsgesetz schafft Unsicherheit". http://www.gi.de/aktuelles/meldungen/detailansicht/article/it-sicherheitsgesetz-schafft-unsicherheit.html

52 Bruce Schneier. 2015. "Hacking Team, Security Vulnerabilities, and the NSA". Georgetown Journal of International Affairs, http://journal.georgetown.edu/hacking-team-and-the-nsa/

53 Claire Caine Miller. 2014. "Revelations of N.S.A. Spying Cost U.S. Tech Companies". The New York Times. http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0

54 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. 2000. "22. Tätigkeitsbericht" https://www.datenschutzzentrum.de/material/tb/tb22/kap7.htm

55 Deutscher Bundestag. 2015. "Bundestag beschließt das IT-Sicherheitsgesetz". https://www.bundestag.de/dokumente/textarchiv/2015/kw24_de_it_sicherheit/377026

56 Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit. 2014. "Selbstbestimmt und sicher in der digitalen Welt 2015-2020". http://www.bmbf.de/de/73.php

57 Gesamtverband der deutschen Versicherungswirtschaft e.V.2015. "Gut gerüstet gegen Angriffe aus dem Netz". http://www.gdv.de/2015/05/gut-geruestet-gegen-angriffe-aus-dem-netz/

58 Cyber Security Sharing and Analytics (CSSA). http://www.cssa.de/

59 German Competence Centre against Cyber Crime (G4C). http://g4c-ev.com/ueberuns.html

60 Christiane Schulzki-Haddouti. 2015. "Crypto Wars 3.0: Neuorganisation des BSI gefordert". http://www.heise.de/newsticker/meldung/Crypto-Wars-3-0-Neuorganisation-des-BSI-gefordert-2530552.html

61 Net Security. 2015. "Companies leave vulnerabilities unpatched for up to 120 days". http://www.net-security.org/secworld.php?id=18911

62 Isabel Skierka, et al. 2015. "CSIRT Basics for Policy-Makers". Global PublicPolicy Institute and New America Working Paper. http://www.gppi.net/fileadmin/user_upload/media/pub/2015/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf

63 Bundesamt für Sicherheit in der Informationstechnik."CERT-Bund: Aufgaben und Ziele". https://www.bsi.bund.de/DE/Themen/IT-Krisenmanagement/CERTBund/certbund_node.html

64 Neumann, Linus. "Effektive IT-Sicherheitfördern". Stellungnahme zur 7. Sitzung des Ausschusses Digitale Agenda des Deutschen Bundestages, 7. Mai 2014

65 Julia Angwin. 2015. "The World's Email Encryption Software Relies on One Guy, Who is Going Broke". Pro Publica. http://www.propublica.org/article/the-worlds-email-encryption-software-relies-on-one-guy-who-is-going-broke

66 Julia Angwin. 2015. "The U.S. Government: Paying to Undermine Internet Security, Not to Fix It". Pro Publica. http://www.propublica.org/article/the-u.s.-government-paying-to-undermine-internet-security-not-to-fix-it

67 Digitale Agenda der Bundesregierung 2014-2017, S. 31

68 Forge Adullact. Trusted Bird. https://adullact.net/plugins/mediawiki/wiki/milimail/index.php/Trustedbird_Project

69 Florian Rötzer. 1999. "Bundesregierung fördert Open Source". heise online. http://www.heise.de/newsticker/meldung/Bundesregierung-foerdert-Open-Source-24110.html

70 Dan Geer. 2014. "Cybersecurity as Realpolitik". Blackhat Conference 2014. http://geer.tinho.net/geer.blackhat.6viii14.txt ; Jennifer Granick, 2015. "The End of the Internet Dream". Blackhat Conference 2015. https://medium.com/backchannel/the-end-of-the-internet-dream-ba060b17da61

71 siehe Endnote 26

72 Hauke Gierow. 2015. "BSI will Router-Sicherheit verbessern". Golem. http://www.golem.de/news/security-bsi-will-router-sicherheit-verbessern-1510-117030.html

73 Brian Krebs. 2015. „The Lingering Mess from Default Insecurity". Krebs on Security. https://krebsonsecurity.com/2015/11/the-lingering-mess-from-default-insecurity/

74 Dan Goodin. 2014. "Hackers hijack 300,000-plus wireless routers, make malicious changes". arstechnica. http://arstechnica.com/security/2014/03/hackers-hijack-300000-plus-wireless-routers-make-malicious-changes/

75 Jens Ferner. 2015. "IT-Sicherheitsgesetz (2015): Auswirkungen des IT-Sicherheitsgesetzes". Anwaltskanzlei Ferner. http://www.ferner-alsdorf.de/rechtsanwalt/it-recht/bundestag-beschliesst-it-sicherheitsgesetz-2015/18178/

76 Bundesministerium des Innern. 2011. "Cyber-Sicherheitsstrategie für Deutschland". http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile

77 Tomas Rudl. 2015. "Bundesregierung beschließt IT-Konsolidierung der Bundesverwaltung und will „Bundes-Cloud"". netzpolitik.org. https://netzpolitik.org/2015/bundesregierung-beschliesst-it-konsolidierung-der-bundesverwaltung/

78 Dan Goodin. 2015. "Active malware campaign uses thousands of WordPress sites to infect visitors". ars technica. http://arstechnica.com/security/2015/09/active-malware-campaign-uses-thousands-of-wordpress-sites-to-infect-visitors/

79 Kim Zetter. 2011. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History". Wired. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

80 Dan Goodin. 2015. "How "omnipotent" hackers tied to NSA hid for 14 years—and were found at last". ars technica. http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/

81 Mandiant Intelligence Center Report, 2013, "APT-1: Exposing one of China's Espionage Units". http://intelreport.mandiant.com/

82 Kim Zetter. 2014. "Sony Got Hacked Hard: What We Know and Don't Know So Far". Wired. http://www.wired.com/2014/12/sony-hack-what-we-know/

83 United Nations, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

84 OSCE. 2014. "Confidence building measures to enhance cybersecurity in focus at OSCE meeting in Vienna". http://www.osce.org/cio/126475

85 Alex Grigsby. 2015. "The 2015 GGE Report: Breaking New Ground, Ever So Slowly". Council on Foreign Relations. http://blogs.cfr.org/cyber/2015/09/08/the-2015-gge-report-breaking-new-ground-ever-so-slowly/

86 Duncan Hollis und Tim Maurer. 2015. "A Red Cross for Cyberspace". Time. http://time.com/3713226/red-cross-cyberspace/

## Über die stiftung neue verantwortung

Die stiftung neue verantwortung (snv) ist eine gemeinnützige Denkfabrik in Berlin, die Expertise aus Politik, Forschungseinrichtungen, NGOs und Unternehmen zusammenbringt, um überparteiliche Vorschläge zu aktuellen politischen Fragen zu entwickeln, zu diskutieren und zu verbreiten. In den Schwerpunkt-Programmen Digitalisierung, Energie- und Ressourcen sowie Zukunft des Regierens erstellt die snv Analysen, veröffentlicht Handlungsempfehlungen und formt sektorenübergreifende Koalitionen. Twitter: @snv_berlin

## Impressum

stiftung neue verantwortung e. V.
Beisheim Center
Berliner Freiheit 2
10785 Berlin

T. +49 30 81 45 03 78 80
F. +49 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Layout:
Franziska Wiese

Kostenloser Download:
www.stiftung-nv.de