BIGS | Essenz

Brandenburgisches Institut für GESELLSCHAFT und SICHERHEIT

Zivile Cybersicherheit: Cybercrime zwischen Realität und Risiko

Abstract

Die Bedeutung der zivilen Cybersicherheit wird in der Cyber-Sicherheitsstrategie der Bundesregierung in den Fokus genommen. Das Interesse richtet sich hierbei u. a. auf die Bekämpfung der Cyberkriminalität und den Schutz des Internets als kritische Infrastruktur. Die Wichtigkeit der Bekämpfung von Cybercrime für eine resiliente Gesellschaft wird im folgenden Artikel herausgestellt. Es wird argumentiert, dass wirksame Schutzmaßnahmen eine fundierte Datengrundlage brauchen, um effektiv sein zu können. Dabei werden verschiedene gesellschaftliche Ebenen betrachtet, um der Komplexität des Themas gerecht zu werden.

Kristin Krüger

Nummer 14 · Mai 2014

Einleitung

Die Abhängigkeit vom Internet in unserer Gesellschaft betrifft alle gesellschaftlichen Ebenen, beginnend beim Individuum über Unternehmen bis hin zu Behörden. Die Einstufung des Internets als kritische Infrastruktur bedeutet, dass besondere Schutzmaßnahmen ergriffen werden, um die Funktionalität zu gewährleisten. Dieser Schutz muss auf allen Ebenen erfolgen: sowohl bei der Hard- als auch der Software und dies jeweils sowohl bei Privatpersonen (Mikro-Ebene) als auch bei den Organisationen und Institutionen (Meso-Ebene). Erst dann entsteht eine gesamtgesellschaftliche Resilienz auf der Makro-Ebene. Einige Aspekte der kritischen Infrastruktur IT (Informationstechnologie) werden in diesem Artikel betrachtet. Der Fokus liegt jedoch nicht auf der behördlichen Zusammenarbeit, sondern auf der Etablierung einer IT-Sicherheitskultur, welche die gesellschaftliche Resilienz in Deutschland erhöhen soll.

Während Behörden und Unternehmen die Notwendigkeit dessen mittlerweile zum Teil erkannt haben, besteht beim Endverbraucher noch Handlungsbedarf. Hier ist ein Umdenken erforderlich. Ein Indiz hierfür ist die steigende Anzahl an Cybercrime-Straftaten.[1] Cybersicherheit muss gesamtgesellschaftlich etabliert werden, um eine resiliente Gesellschaft zu bilden und dem Internet als kritischer Infrastruktur gerecht zu werden.

Voraussetzung für ein gesellschaftliches Umdenken ist jedoch zunächst einmal eine gemeinsame Diskussionsgrundlage – sowohl in definitorischer Hinsicht als auch bezüglich des eigentlichen Bedrohungspotentials. Probleme, die sich aus mangelnden Definitionen ergeben, werden in diesem Artikel angerissen. Der Fokus liegt auf der derzeitigen Datengrundlage, die anhand ausgewählter Beispiele aus verschiedenen gesellschaftlichen Dimensionen beleuchtet wird. Aufgrund der Globalität des Phänomens Cybercrime werden hierbei auch internationale Aspekte betrachtet, wenngleich der Schwerpunkt auf Deutschland liegt. Bedrohungspotentiale einzelner Beispiele aus dem Bereich der Cyberkriminalität werden aufgezeigt.

BIGS
BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

Nach dieser Darstellung der Ausgangslage wird für Deutschland der Handlungsbedarf in den unterschiedlichen gesellschaftlichen Bereichen herausgearbeitet. Neben notwendigen vernetzten Strategien werden auch konkrete Maßnahmen analysiert, bspw. das Einführen von Bildungsstandards für das Schulfach Informatik oder Gütesiegeln für in Deutschland hergestellte Hardware.

Diese umfassende Betrachtungsweise von Cybercrime ist aufgrund der der Thematik immanenten Struktur notwendig, zieht aber auch unumgängliche Reduktionen nach sich. Der vorliegende Aufsatz ist ein Beitrag zur aktuellen Diskussion über die Cybersicherheit.

1 Fakten oder Fiktionen? Probleme bei der Erfassung von Cybercrime

1.1 Die internationale Datengrundlage

Cyberkriminalität ist ein globales Phänomen. Die Struktur des World Wide Webs ermöglicht den Kriminellen einen technischen und rechtlichen Handlungsfreiraum, der eine globale Betrachtung des Problems erforderlich macht. In einer kürzlich veröffentlichten Studie des United Nations Office on Drugs and Crime (UNODC) zum Thema „Cybercrime",[2] an der die Autorin mitgewirkt hat, wurde eine solche umfassende Betrachtungsweise vorgenommen. Im Rahmen der Untersuchung für die UNODC hat die Autorin mehr als 300 Studien, Berichte und Analysen zum Thema ausgewertet und nach unterschiedlichen Aspekten analysiert. Dabei kristallisierte sich ein besonderes Problem heraus, welches häufig insbesondere in ‚jungen' Forschungsfeldern auftritt: das der Definitionen.

Das fängt bei dem Begriff „Cyber" vs. IT (Informationstechnologie) an und setzt sich über Cybercrime, Cyberwar und Cyberespionage fort bis hin zu einzelnen Angriffstypisierungen wie Malware. Es gibt keine übergreifende Definition für Cybercrime, da die Begrifflichkeit häufig dem Verwendungszweck angepasst wird.[3] Cybercrime, Cyberespionage und Cyberwar überschneiden sich in einigen Bereichen, doch ein Kernbereich für Cybercrime kann in den vorhandenen Definitionen identifiziert werden, anhand derer sich in diesem Text orientiert wird:

„A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime."[4]

Jede wissenschaftliche Arbeit ist auf Definitionen angewiesen. Insbesondere Vergleiche jeglicher Art beruhen auf Gemeinsamkeiten der einzelnen Fälle. Im Bereich der Cybersicherheit gibt es aber zum einen nur selten Definitionen, zum anderen sind diese nicht übergreifend. Mittlerweile haben einzelne Unternehmen die Problematik erkannt: Hewlett Packard stellt in einer aktuellen Studie folgendes für Android-Anwendungen fest:

„Inkonsistente und voneinander abweichende Definitionen des Begriffs ‚Malware' erschweren die Analyse von Compliance-Risiken."[5]

Die Auswertung der – aus wissenschaftlicher Sicht – ohnehin schon schwierig zu bewertenden Datengrundlage[6] wird dadurch weiter erschwert. Nur in Einzelfällen stehen Daten staatlicher Behörden oder von Wissenschaftlern zur Verfügung. Die dort vorhandenen Definitionen werden allerdings selten von anderen Untersuchungen übernommen. Somit ist zum Beispiel nicht immer klar was genau mit einer *security vulnerability* oder einem *data breach* gemeint ist.[7] Eine vergleichende Betrachtung des Phänomens Cybercrime ist daher nur eingeschränkt möglich. Dies soll im Folgenden anhand von zwei Beispielen dargestellt werden:

In den *Threat Reports* verschiedener Firmen wird häufig nach einer Verletzung der Datensicherheit (*data breach*) und der Art und Weise wie bzw. wodurch die Kompromittierung zustande gekommen ist, gefragt. Verizon[8] bspw. fasst die Aktionen, die ein Angreifer durchgeführt hat, um an die Daten zu gelangen, unter den Oberbegriffen *Malware*,[9] *Hacking*, *Social*, *Misuse*, *Physical*, *Error* und *Environmental* zusammen. *SQL Injections*[10] fallen hierbei unter die Kategorie *Hacking* und nehmen einen überraschend geringen Anteil von 4 % der Aktivitäten ein.[11] Trustwave hingegen führt die *SQL Injections* separat auf, ihr Anteil liegt bei 26 %.[12]

Symantec mischt bei der Unterscheidung für die Gründe von *data breaches* unterschiedliche Betrachtungsweisen und unterscheidet nach *Hackers*, *Accidentally made public*, *Theft or loss of computer or drive*, *Insider theft*, *Unknown* und *Fraud*.[13] IBM[14] wählt einen ähnlichen Methodenansatz wie Trustwave und unterscheidet gesondert zwischen *SQL Injections* und weiteren, nennt aber keine genauen Zahlen.[15] Mittels *SQL Injection* wird dabei – laut IBM – am häufigsten die Datensicherheit verletzt.

Die folgende Tabelle soll das begriffliche Durcheinander illustrieren. Dabei wurde die Kategorisierung von Verizon willkürlich als Ausgangsbasis gewählt, ohne dass sie nach Meinung der Autorin Richtigkeit oder Vollständigkeit widerspiegelt. In der Tabelle wird deutlich, dass bestimmte Kategorien nicht von allen Berichten abgedeckt werden oder sich nicht eindeutig zuordnen lassen und Angriffe unterschiedlich detailliert klassifiziert werden. Dies soll verdeutlichen, dass es nur eingeschränkt möglich ist, die Ursachen für die Kompromittierung von Daten zu analysieren. Bereits die Frage, mit welcher Wahrscheinlichkeit webbasierte Attacken wie bspw. *SQL Injections* den Ausgangspunkt für den *data breach* bilden, kann nicht zuverlässig beantwortet werden. Das hängt nicht nur mit der Komplexität solcher Angriffe (häufig werden mehrere Methoden gleichzeitig oder nacheinander benutzt) und der schwierigen, anschließenden Forensik zusammen, sondern auch mit unklaren und uneinheitlichen Definitionen.

Tabelle 1: Ursachen für die Verletzung der Datensicherheit (*data breach*)

Verizon	Trustwave	Symantec	IBM
Malware *(infections of spyware, botnets, backdoors etc.)*	*Remote Code Execution*		*Malware*
Hacking (*stolen credentials, backdoor exploits, SQL Injections*)	*SQL Injection* *Remote Access* *Remote File Inclusion*	*Hackers*	*SQL Injection* *DDoS* *XSS*
Social	*Client Side Attack*		*Spear Phishing* *Watering Hole*
Physical	*Physical theft*	*Theft or loss of computer drive*	*Physical Access*
Misuse *(malicious privilege abuse, use policy violations)*		*Insider theft*	
Error *(lost devices, publishing goof-ups, mis-delivered e-mails, faxes and documents)*	*Authorization Flaw*	*Fraud* *Accidentally made public*	
Environmental			
Keine Kategorisierung bei Verizon für „Unbekannt“	*Unknown*	*Unknown*	*Unknown*

Ähnlich schwierig verhält es sich mit dem Begriff der Schwachstelle (*vulnerability*). Während Microsoft sowohl eine Definition liefert, was dort unter einer Schwachstellen verstanden wird, als auch eine Klassifikation nach Schwere und Komplexität der Schwachstelle veröffentlicht,[16] verzichtet IBM darauf. In ihrem Report[17] unterscheidet IBM nach *Web Application Vulnerabilities*, *Exploits* und anderen. Verizon hingegen greift Microsofts Klassifizierung auf und unterscheidet auf dieser Grundlage zwischen *Social Engineered*, *User Interaction* und *„Classic" Vulnerabilities*.[18] Diese Form der Kooperation auf der Grundlage derselben Definitionen und Begriffe ist leider bisher nur selten.

Während – relativ gesehen – die Analyse einfach zu messender Phänomene, wie bspw. das globale SPAM-Volumen (siehe Kapitel 2), recht zuverlässige Ergebnisse liefern kann, muss bei komplexeren Cybercrime-Phänomenen eine Einzelfallanalyse vorgenommen werden. Dies wiederum erschwert die wissenschaftliche Untersuchung und die Verifizierung der Daten aufgrund von unterschiedlichen Quellen. Die globale Dimension des Phänomens Cybercrime zu erfassen, ist somit eine Herausforderung, bei der vor allem auch die Definitionen berücksichtigt werden müssen.

Die Dunkelziffer ist sehr hoch

1.2 Die Datengrundlage für Deutschland

Als einem der wenigen Länder[19] stehen Deutschland neben den gängigen Studien von Sicherheitsdienstleistern Daten zu Cyberkriminalität zur Verfügung, die durch eine staatliche Behörde aufgezeichnet werden. Das Bundeskriminalamt (BKA) erfasst in seinem ‚Bundeslagebild Cybercrime' allerdings nur einen Teil der Daten. Relevante Erscheinungsformen von Cybercrime wie bspw. Formen der digitalen Erpressung durch *Ransomware*[20] oder *DDoS*-Attacken[21] werden in der Polizeilichen Kriminalstatistik (PKS) unter dem Tatbestand der Erpressung erfasst, nicht unter Computerbetrug. Damit werden sie zum einen nicht als Delikt im Bereich Cybercrime erfasst, zum anderen werden auch die ökonomischen Schäden, die dadurch verursacht werden, nicht unter diesem Aspekt verortet.[22] Die ohnehin begrenzte Aussagekraft der PKS wird hierdurch weiter reduziert.

Auch wenn Deutschland mit der Erfassung der Daten zum Thema Cybercrime eine Vorreiterrolle einnimmt, ist der Handlungsbedarf hier noch immens. Die Dunkelzifferrelation[23] in diesem Bereich wird noch nicht einmal geschätzt, es heißt nur, sie sei „sehr hoch"[24]. Niels Diers vom Institut für Kriminologische Sozialforschung kommt zu folgender Einschätzung:

„Internetkriminalität wird durch die Benutzung eines spezifischen Tatmittels von anderen Bereichen abgegrenzt. Beim Versuch der quantitativen Erfassung des Dunkelfeldes kommt es daher bei vielen Delikten zu einer Doppelerfassung, deren Ausmaß kaum abschätzbar ist."[25]

Des Weiteren wird eine Einschätzung der Dunkelzifferrelation durch internationale Täter-Opfer-Strukturen und eine wachsende Anzahl von Internetnutzern erschwert.[26] Ein weiteres Phänomen, das ebenfalls in den Bereich Cybercrime fällt und dem bisher nur wenig Aufmerksamkeit gewidmet wird, ist das der wachsenden Kriminalität mittels Smartphones. Dieser Trend wurde ungefähr ab 2011 von verschiedenen Unternehmen der Sicherheitsbranche registriert und die Kriminalität in diesem Bereich steigt seitdem beständig an. Gründe hierfür sind die zunehmende Verbreitung von Smartphones sowie das gering ausgeprägte Bewusstsein (*Awareness*[27]) der Nutzer, dass hierfür ebenso *Malware*, Trojaner und Co existieren und die Endgeräte dementsprechend geschützt werden müssen.

Für die Erfassung der Straftaten sollte es keine Rolle spielen, mittels welcher Geräte sie begangen wurden, mit sinkender *Awareness* erhöht sich jedoch wiederum die Dunkelziffer. Eine grundlegende, realistische Einschätzung des Phänomens Cybercrime kann aber nur bei einer umfassenden Datengrundlage vorgenommen werden. Auch für Deutschland besteht hier noch Nachholbedarf. Die Daten sollten von mehreren Quellen stammen und teilweise explizit für Deutschland erhoben worden sein. Dann kann man eventuell auch die Dunkelzifferrelation schätzen und neben quantitativen auch qualitative Aspekte berücksichtigen. Bis dahin lassen sich nur Trends erfassen und analysieren.

2 Ausgewählte Datenbeispiele

Eine der gut zu ermittelnden Zahlen ist das täglich versendete SPAM-Volumen. Mehrere Unternehmen kommen hierbei zu ähnlichen Ergebnissen: Im Jahr 2012 wurden in etwa 30 Milliarden SPAM-E-Mails pro Tag verschickt.[28] Bei Symantec entspricht dies 69 % aller versendeten E-Mails. Kaspersky beziffert das SPAM-Volumen auf 72,1 % des gesamten E-Mail Aufkommens.[29] Ähnlich sieht es mit detaillierteren Analysen aus: Trustwave bspw. beziffert 65-75 % aller E-Mails, die in Unternehmen eingehen als SPAM.[30] Es ist ein eindeutiger Trend zu erkennen, dass das SPAM-Aufkommen in den letzten Jahren gesunken ist und wahrscheinlich weiter sinken wird. Dies wird auf verstärkte internationale Zusammenarbeit und die Abschaltung mehrerer Botnetze[31] zurückgeführt.

Die Anzahl und Größe der illegalen Botnetze – die die technische Infrastruktur für einen Großteil der Cyberkriminalität bereitstellen – ist nicht genau zu bestimmen. Dies hängt vor allem mit technischen Faktoren, wie z. B. wechselnden IP-Adressen, zusammen. Aufgrund dessen schwanken die Schätzungen der Größe einzelner Botnetze erheblich. Unterschiedliche Bezeichnungen für dieselben Botnetze erschweren die Analyse zusätzlich.[32] Ein etwas älterer Bericht legt allerdings nahe, dass ein Großteil (73 %) aller durch Botnetze verursachten Schäden von den 20 größten Botnetzen verursacht wird, über die Hälfte (56 %) sogar nur von den zehn größten Botnetzen.[33] Deshalb ist es auch nicht verwunderlich, dass die Anzahl der versendeten SPAM-E-Mails jeweils nach der Abschaltung eines Botnetzes kurzfristig einbricht. Da die Abschaltung bzw. Übernahme eines Botnetzes eine komplizierte Angelegenheit ist, die die internationale Zusammenarbeit vieler Behörden erfordert, erscheint es somit sinnvoll, sich auf die größten Botnetze zu konzentrieren. Die Botnetzbetreiber werden dabei allerdings nur in seltenen Fällen gefasst.

2.1 Gesellschaftliche Dimensionen von Cybercrime

Auf gesellschaftlicher Ebene kann man die Opfer von Cyberkriminalität in Privatpersonen und Unternehmen unterteilen. Selbstverständlich stehen auch staatliche IT-Infrastrukturen unter beachtlichem Angriffsdruck, sollen hier aber nicht näher betrachtet werden.

Berichte über Unternehmen sind am häufigsten, da diese wiederum meist von Sicherheitsunternehmen stammen, die ihre Produkte an von Cyberkriminalität (und/oder Cyberspionage) betroffene Unternehmen verkaufen wollen. Auf eine detaillierte Analyse wird in diesem Artikel verzichtet, da die Aussagekraft einer solchen durch die Heterogenität der Unternehmensstrukturen sehr beschränkt wäre, einige Aspekte werden jedoch im Folgenden heraus gegriffen und dargestellt.

2.1.1 Unternehmen

GROSSE UNTERNEHMEN SIND EHER BETROFFEN

Zu größeren Unternehmen gibt es mehr Untersuchungen als zu kleinen. Dies ist nicht nur in dem Umstand begründet, dass sie eher gefährdet sind, sondern auch darin, dass größere Unternehmen eher Sicherheitsdienstleister in Anspruch nehmen, die die Kapazitäten haben, Berichte zu veröffentlichen.

Des Weiteren liegt die Vermutung nahe, dass die Faktoren für die Wahrscheinlichkeit eines Angriffs auch zwischen den einzelnen Ländern variieren – ein Umstand, der bisher wenig Beachtung findet. Für Deutschland mit seinen vielen kleinen und mittelständischen Betrieben kann sich hier ein durchaus differenzierteres Bild ergeben als in anderen Ländern. Hierbei handelt es sich um einen Faktor, der insbesondere im Hinblick auf die Kosten, die durch Cyberkriminalität entstehen, noch genauer untersucht werden muss.

Allgemein kann ein Zusammenhang zwischen Unternehmensgröße und der Häufigkeit von Cyberkriminalität angenommen werden.[34] Symantec stellt fest, dass sich ca. 50 % aller registrierten Attacken auf große Unternehmen (>2500 Mitarbeiter) richten. Auch bei anderen Berichten ist der Anteil an betroffenen großen Unternehmen ähnlich hoch, zum Beispiel gibt PricewaterhouseCoopers (PwC) ihn mit 54 % (bei Unternehmen mit >1000 Mitarbeitern) an.[35] Auch wenn die genannten Daten aus unterschiedlichen Jahren stammen und PwC sich im Report auf Betrug konzentriert, ist der Anteil betroffener großer Unternehmen ähnlich hoch und das auch über mehrere Jahre hinweg. Dies lässt den Schluss zu, dass die Daten ein realitätsnahes Bild vermitteln. Bei kleineren Unternehmen ist die Datenlage schwieriger, da bspw. häufig keine Unterscheidung zwischen kleinen

und mittleren Unternehmen (KMU) stattfindet oder die Daten gar nicht erfasst werden.

Die wenigen Angaben, die zu finden sind, verwenden zudem unterschiedliche Größendefinitionen für kleine Unternehmen, wie im Folgenden zu erkennen ist: Der Anteil attackierter kleiner Unternehmen (Mitarbeiterzahl 1-250) ist laut Symantec von 18 % im Jahr 2011 auf 31 % in 2012 angestiegen.[36] Des Weiteren unterscheiden sich die Angriffsmethoden bei kleineren und größeren Unternehmen voneinander. Während kleine Unternehmen (Mitarbeiterzahl <1000) häufig von Attacken mittels *Malware* (54 %) und *Hacking* (72 %) betroffen sind, ist das größte Problem für Unternehmen mit 1000 oder mehr Mitarbeitern *Physical*-Attacken (50 %).[37] Unter diesen physischen Attacken versteht Verizon: „[…] *actions that involve proximity, possession, or force*."[38] Gestohlene Hardware fällt bspw. hierunter.

Ferner scheint es bedeutende Unterschiede zwischen einzelnen Branchen zu geben. Die Angaben hierzu sind allerdings mit Vorsicht zu betrachten. Der Kundenstamm der Sicherheitsunternehmen, die hierzu Berichte veröffentlichen, kann durchaus variieren und ist nicht repräsentativ. Überdies ist die Differenzierung der einzelnen Branchen nicht übereinstimmend. Diese Bedenken spiegeln sich auch in den einzelnen Zahlen wieder, wie in der folgenden Tabelle anhand von drei Beispielen illustriert werden soll. Verglichen werden hierbei die Branchen nach der Anzahl ihrer *data breaches* für das Jahr 2011.[39]

© J. F. Krüger

Tabelle 2: *Data breaches* 2011 nach Branchen klassifiziert

data breach	Anzahl bei Symantec[40]	Anzahl bei Verizon[41]
Gesundheitswesen	43 %	7 %[42]
Finanzwesen	8 %	10 %[43]
Informationsbranche	3 %	3 %
Einzelhandel	20 %	4 %

Es ist deutlich zu erkennen, dass bezüglich der Branchen keine allgemeingültigen Aussagen getroffen werden können, zumal die Bedrohungslage für Unternehmen durchaus von Land zu Land unterschiedlich sein kann. Es ist bspw. anzunehmen, dass ein Großteil der Angriffe auf KMUs in Deutschland nicht erfasst werden, weil sie nicht erkannt werden.

2.1.2 Individuen

Über die individuellen Opfer von Cybercrime gibt es weit weniger Daten. In den USA wertet das *Internet Crime Complaint Center* (IC3) die Angaben derjenigen aus, die eine Beschwerde einreichen. Im Gegensatz zu Deutschland werden so die Vorfälle gesondert von einer Institution erfasst, die diese ggf. an die zuständigen Ermittlungsbehörden weiterleitet. Die Auswertung des IC3s beinhaltet aufgrund dessen auch Vorfälle, bei denen kein direkter Schaden entstanden ist. Des Weiteren wird vom *Australian Institute of Criminology* seit kurzem ein jährlicher Bericht der *Consumer Fraud Taskforce* veröffentlicht.[44]

Die Schwierigkeiten der Erfassung von Cybercrime in Deutschland mittels der PKS wurden in Kapitel 1.2 bereits erläutert. Es ist anzunehmen, dass ein Großteil der polizeilich erfassten Fälle nur deshalb gemeldet wird, weil ein wirtschaftlicher Schaden entstanden ist. Des Weiteren lässt sich mittels der PKS nicht zwischen betroffenen Individuen und Unternehmen unterscheiden.

Im Folgenden wird deshalb die Umfrage der Europäischen Kommission zum Thema Cybersecurity[45] herangezogen. In der repräsentativen Umfrage wurden die deutschen Teilnehmer gefragt: „Internet-Kriminalität kann viele unterschiedliche Formen krimineller Handlungen beinhalten. Wie häufig haben Sie eine der folgenden Situationen erlebt oder sind Opfer davon geworden?"[46] Zehn Prozent der Befragten konnten aufgrund von Cyber-Attacken nicht auf Online-Dienste zugreifen und elf Prozent sind Opfer von Warenbetrug über das Internet geworden. Die E-Mail-Konten oder die Konten bei sozialen Medien wurden bereits bei sieben Prozent der Befragten einmal gehackt. Opfer von Kreditkarten- oder Online-Banking-Betrug sind drei Prozent geworden, von Identitätsdiebstahl fünf Prozent. Die größte Gruppe mit 29 % macht diejenigen aus, die mittels E-Mail oder Telefonanrufen nach Zugangsdaten für ihren Computer oder nach persönlichen Details gefragt wurden.

Die Anzahl der Befragten, die sich über die Risiken von Internet-Kriminalität gut informiert fühlen, ist mit 47 % fast gleich groß wie die Gruppe, die dies nicht tut (48 %).[47] Hier besteht demzufolge noch Entwicklungspotential, zumal insbesondere in diesem Bereich Wissen über die Gefahren nicht damit gleichzusetzen ist, dass Schutzmaßnahmen ergriffen werden.[48]

Wie gering das Bewusstsein für Cybersicherheit in der Bevölkerung ausgeprägt ist, lässt sich auch anhand des folgenden Beispiels verdeutlichen: In den über 300 Studien und Reports der Jahre 2010-2012 zum Thema Cybersicherheit, die die Autorin für die UNODC-Studie[49] analysiert hat, wird der Trend zum mobilen Endgerät – und damit auch zur Notwendigkeit mobiler Sicherheit – insgesamt 93 Mal genannt. Im Gegensatz dazu erwähnt der Norton Report[50] von Symantec für 2013, dass die Hälfte aller befragten Tablet- und Smartphonebenutzer nicht einmal die einfachsten Sicherheitsanforderungen erfüllen wie bspw. Passwortschutz, Antivirensoftware und Sicherungskopien. Mehr als ein Drittel der Befragten in dieser Studie sind bereits Opfer von Cyberkriminalität auf mobilen Endgeräten geworden. Auch wenn diese Daten international erfasst wurden, ist anzunehmen, dass dieser Trend für Deutschland gleichermaßen gilt. Die zunehmende Verbreitung von Smartphones und Tablets geht also derzeit mit einem Verlust an IT-Sicherheit einher.

Diese Beispiele verdeutlichen, dass die Opferstrukturen im Bereich Cyberkriminalität bisher nicht ausreichend analysiert werden können. Eine präzisere Unterscheidung nach sozioökonomischen Merkmalen, wie bspw. zwischen Unternehmen und Privatpersonen oder Alter und Geschlecht, ist bei der Erfassung von Cybercrime zwingend notwendig für die Analyse. Erst dann können Bedrohungspotentiale identifiziert und Schutzmaßnahmen entwickelt werden. Die Vermittlung von Schutzmaßnahmen sollte aber zielgruppenorientiert erfolgen, so können bspw. ‚Digital Outsiders'[51] auch mittels Printmedien angesprochen werden, die ‚Unbekümmerten Hedonisten'[52] hingegen wird man dadurch wohl nicht erreichen. Die Bedrohungszenarien für diese beiden Gruppen unterscheiden sich deutlich voneinander. Um die Sicherheit beim Endverbraucher zu erhöhen, muss die Gefährdung einzelner Milieus vorab analysiert werden und dies kann nur auf der Basis einer gesicherten Datengrundlage gelingen. Äquivalentes gilt selbstverständlich für Unternehmen, wie im vorangegangenen Kapitel erläutert wurde.

Im Übrigen werden bei der derzeitigen Erfassung von Cybercrime die gesellschaftlichen Kosten nicht berücksichtigt, bspw. für die Schulung von Polizeibeamten, die dem Staat durch die steigende Internetkriminalität entstehen. Es mangelt gegenwärtig an einer zuverlässigen und umfassenden Datengrundlage sowohl für den Unternehmensbereich als auch für die betroffenen Bürger. Einige Möglichkeiten, dies zu ändern, werden im nächsten Kapitel vorgestellt.

3 Handlungsbedarf und -optionen

3.1 Strategische Überlegungen auf gesellschaftlicher Ebene

Nicht erst seit den verhaltenden Reaktionen auf die Enthüllungen von Edward Snowden ist bekannt, dass der deutsche Staat auf die neuen Herausforderungen der Cybersicherheit viel zu träge reagiert.

„Diese Tatsache und das Verhalten der Bundesregierung im Zuge der Enthüllungen um die amerikanisch-britischen Abhörprogramme stehen sinnbildlich für das politische Desinteresse, das informationstechnischen Themen über Jahre hinweg entgegengebracht wurde. Auch bei Themen von höchster sicherheitspolitischer Relevanz, wie dem Schutz der nationalen kritischen Infrastrukturen (insbesondere IT-Infrastrukturen, Anm. d. A.), wurden weichenstellende Maßnahmen, trotz seit langem bekannter Expertenberichte, erst in den letzten Jahren eingeleitet."[53]

Die Bundesregierung hat in ihrer Cybersicherheitsstrategie postuliert, zivile Ansätze und Maßnahmen in den Vordergrund stellen zu wollen.[54] Der umfassende, gesamtgesellschaftliche Ansatz kann jedoch – wie bei den meisten kritischen Infrastrukturen – nur zusammen mit der Bevölkerung umgesetzt werden. *Awareness*-Konzepte für die Bevölkerung fehlen jedoch bisher völlig,[55] hier wird bisher den Medien das Feld überlassen. Die Sensibilisierung der Verwaltung für IT-Sicherheit wird gezielter angegangen, bspw. durch Maßnahmen wie ‚Sicher gewinnt!'[56] der Bundesakademie für öffentliche Verwaltung. Auch im Bereich der Strafverfolgungsbehörden scheinen sich langsam Cybersicherheitskompetenzen herauszubilden. Europäische und internationale Kooperationen sind angestrebt, mangels eines rechtlichen Rahmens jedoch noch in der Anfangsphase.

Auf der Ebene der Bevölkerung besteht am meisten Handlungsbedarf hinsichtlich einer Entwicklung hin zu einer IT-Sicherheitskultur. Die Einbindung des Bürgers in ein Cybersicherheitskonzept für Deutschland ist nach Meinung der Autorin bisher nicht erfolgt. Eine solche ist aber notwendig, um eine flächendeckende Resilienz herzustellen. Hierzu bedarf es der Mithilfe des Einzelnen. Diese kann bspw. durch *Awareness*-Kampagnen angeregt werden.[57] Der Erfolg einzelner Warnungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) spricht dabei für den Erfolg solcher Kampagnen.

Die Warnung, dass das BSI 16 Millionen gestohlene Identitäten entdeckt hat und jeder überprüfen kann, ob die eigene dazu gehört, führte dazu, dass der angebotene Sicherheitstest des BSI innerhalb kürzester Zeit 15 Millionen Mal aufgerufen wurde.[58] Die Wahrscheinlichkeit, dass ein Nutzer mehrere E-Mail-Adressen testet, ist dabei zwar hoch, die Zahlen sprechen jedoch trotzdem für die öffentliche Wirksamkeit der Warnung. Die Reichweite des BSI kann genutzt werden, um die IT-Kompetenz der Bürger zu erhöhen.

Des Weiteren erscheint es sinnvoll, Ressourcen und Kompetenzen bei der Bekämpfung von Cybercrime zu bündeln. IT-Know-how ist gegenwärtig relativ knapp in Deutschland und dementsprechend teuer. Die Polizei flächendeckend mit diesem Spezialwissen aufzurüsten, wäre nicht effizient. In Nordrhein-Westfahlen und Bayern erfolgt die Bündelung bereits mittels speziell ausgebildeter Polizisten und so genannten Cybercrime-Zentren, in denen die größeren Fälle bearbeitet werden sollen. Eine föderale Bündelung innerhalb aller Bundesländer ist jedoch ebenso notwendig wie eine bundesweite. Die Einrichtung eines deutschlandweiten Kompetenzzentrums, ähnlich dem Vorbild des amerikanischen IC3, ist empfehlenswert. Zum einen könnte dort eine Priorisierung vorgenommen werden und aufgrund des Überblicks könnten kritische Fälle schneller erkannt und an die entsprechenden Stellen weiter geleitet werden. Zum anderen hätten die Bürger eine zentrale Anlaufstelle, die auch Fälle aufnehmen könnte, bei denen kein unmittelbarer Schaden entstanden ist. Dies wiederum hätte eine deutlich validere Datengrundlage zur Folge. Die Kommunikation über und durch das bundesweite Kompetenzzentrum wäre vereinfacht. Ein Anschluss an das BSI liegt nahe, um Synergien zu nutzen.

Ebenso gilt es, mittel- und langfristig eine IT-Sicherheitskultur in der Bevölkerung zu etablieren. Um die verschiedenen Bevölkerungsgruppen zu erreichen, sollten dabei mehrere Strategien parallel verfolgt werden. Beispielsweise könnte die Kultusministerkonferenz Bildungsstandards für das Schulfach Informatik vorgeben, in denen IT-Sicherheit einen Schwerpunkt bildet. Life-Hacks auf Konferenzen begeistern nicht nur Erwachsene, auch Schülern können die Konsequenzen ihres Handelns an praktischen Beispielen bewusst gemacht werden. Dies sollte aber unabhängig von der Initiative Einzelner geschehen.

Diese Beispiele sollen verdeutlichen, dass es eine breite Palette von Möglichkeiten gibt, die gesamtgesellschaftliche Cyberresilienz zu erhöhen. Es erfordert aber den politischen Willen, sich dem Thema zu widmen.

3.2 Handlungsempfehlungen

Diese vorgeschlagenen strategischen Aspekte ließen sich mit einer Vielzahl von Maßnahmen umsetzen. Einige Ideen hierfür werden im Folgenden umrissen.

Eine Möglichkeit die IT-Resilienz in der Gesellschaft zu erhöhen, bestünde in der Einführung eines Gütesiegels für Soft- und Hardware aus Deutschland. Hierbei handelt es sich um eine bereits seit längerem diskutierte Idee. Durch die NSA-Affäre ist die Bevölkerung erstmals ‚vorsensibilisiert', so dass hierauf aufgebaut werden kann. Der Sicherheitsgewinn bei bundesweiter Verbreitung selbst einzelner Produkte wäre aufgrund von Netzwerkeffekten enorm. In Kooperation mit Telekommunikationsanbietern könnten bspw. in Deutschland hergestellte Router vertrieben werden.

In diesem Kontext erscheint auch der Ausbau der Förderung seitens der Bundesregierung für deutsche IT-Produkte sinnvoll. Dabei müssen es nicht immer ganze Forschungsprogramme sein – auch wenn diese insbesondere im zivilen Bereich der Cybersicherheit dringend notwendig sind und das laut Koalitionsvertrag geplante Forschungsprogramm IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt" hoffentlich einen Schwerpunkt darauf legen wird – eine App wie bspw. Textsecure[59] ist sowohl in der Herstellung als auch der Anwendung vergleichsweise unaufwendig. Für den Verbraucher muss jedoch eindeutig erkennbar sein, dass das Produkt aus Deutschland stammt und schon deshalb einen Sicherheitsgewinn darstellt. Hundertprozentige Sicherheit gibt es selbstverständlich auch bei deutscher Hard- und Software nicht, einige Risiken sind jedoch deutlich reduziert. Backdoors in Routern[60] bspw. kann so vorgebeugt werden, da die Produkte dann im Rahmen der deutschen Gesetzgebung hergestellt werden. Insbesondere bei in Deutschland entwickelter Software sind hier datenschutzrechtliche Aspekte hervorzuheben, die dann berücksichtigt werden. Die weite Verbreitung solcher Produkte würde den Sicherheitsgewinn auf gesamtgesellschaftlicher Ebene, der daraus entsteht, potenzieren. Ein Gütesiegel würde für Transparenz beim Endnutzer sorgen und das Vertrauen, das durch ‚Made in Germany' bereits besteht, nutzen.

Ferner ließe sich eine breite Bevölkerungsschicht erreichen, indem man Kooperationen anregt und fördert. Workshops zum Thema Verschlüsselung, so genannte Cryptopartys, erreichen erstaunlich viele Bevölkerungsgruppen.[61] Mit dem wachsenden Bewusstsein, dass ihre persönlichen Daten leicht zu kompromittieren sind, entwickelt sich vor allem bei der älteren, datenschutzaffinieren Bevölkerung Unsicherheit im Umgang mit dem Internet und aller damit verbundenen Dinge. Dieser Unsicherheit gilt es, mit Wissen zu begegnen. Der Markt dafür entsteht gerade, wie die Cryptopartys zeigen. Eine Kooperation zwischen Universitäten oder Institutionen wie dem Hasso-Plattner-Institut und den Volkshochschulen bspw. würde diese Lücke ausnutzen und hätte mehrere Vorteile: Cybersicherheit könnte in standardisierter Form vermittelt werden und würde ein breites Publikum erreichen. Kostengünstige Online-Seminare könnten angeboten werden, um auch die ländliche Bevölkerung zu erreichen.

Insbesondere im Hinblick auf die Cyberkriminalität als einem Kernproblem der Cybersicherheit ist die derzeitige Schwerpunktsetzung der Bundesregierung unzureichend. Um die kritische Infrastruktur Internet in Deutschland schützen zu können, muss die Bevölkerung stärker einbezogen werden. Hierzu sind langfristige Strategien und konkrete Maßnahmen seitens der Bundesregierung notwendig, die sowohl die Bevölkerung als auch die Unternehmen mit einbeziehen.

© Stuart Miles / freedigitalphotos.net

3.3 Unternehmen als Bindeglied

Unternehmen und andere Organisationen und Institutionen stellen innerhalb einer Gesellschaft das Bindeglied zwischen Mikro- und Makroebene dar. Viele Unternehmen sind heutzutage auf eine funktionstüchtige IT-Infrastruktur angewiesen. Die Entwicklung einer IT-Sicherheitskultur in der Gesellschaft würde den Unternehmen einerseits zugute kommen, da der eigene Schutz dann verbessert würde, andererseits können die Organisationen selbst einen Teil zur Entwicklung der Kultur beitragen.

Die Autorin ist der Meinung, dass eine Erfassung der Cybervorfälle bei deutschen Unternehmen notwendig und von gesamtgesellschaftlicher Bedeutung ist.[62] Wie in Kapitel 2 dargelegt wurde, bedarf es einer konkreteren Datengrundlage, um auf die Veränderungen im Bereich der Cyberkriminalität angemessen und effizient zu reagieren. Jedoch muss eine solche Meldepflicht gut durchdacht und ausdefiniert sein, um nicht kontraproduktiv zu wirken. Meldewege sollten effizient sein und bereits etablierte Strukturen zum BSI und BKA nutzen. Des Weiteren ist eine Präzisierung des Schlüsselbegriffs ‚erheblicher IT-Sicherheitsvorfall' notwendig, sodass er in der Praxis anwendbar ist, damit schnell reagiert werden kann. Der Nutzen, den die Unternehmen aus der Meldepflicht ziehen können, muss die Kosten übersteigen und vor allem müssen die Daten sicher gespeichert werden. Den Bedenken der Wirtschaftsverbände sollte bei der Änderung des Gesetzesentwurfs Rechnung getragen werden.[63] Insbesondere sollte die Verhältnismäßigkeit der Anforderungen auch für KMUs gewahrt werden.

Denn vornehmlich in kleinen Unternehmen muss sich erst einmal eine IT-Sicherheitskultur entwickeln. Kleine Unternehmen greifen häufig auf externe Dienstleister für die Pflege ihrer IT-Infrastruktur zurück. Der Fokus liegt dann aber oft nicht auf der Sicherheit, sondern auf den Kosten. Doch auch in größeren Unternehmen mit eigener IT-Abteilung ist die Wahrscheinlichkeit, dass relevante Sicherheitsvorfälle überhaupt bemerkt werden, gering, solange kein konkreter Schaden entstanden ist. Felix ‚FX' Lindner beschreibt dies wie folgt:

„Leider sind die meisten IT-Abteilungen derart unterbesetzt, dass schon der reguläre Betrieb eine Herausforderung für die dünne Personaldecke ist – ganz zu schweigen davon, dass mal jemand krank wird. Für Nachforschungen zu Ursachen von auffälligem Systemverhalten oder ungewöhnlichem Netzwerkverkehr ist einfach keine Zeit."[64]

Dies geht mit einer weiteren Problematik einher: In den Berichten von Trustwave[65] wird eine Zeitachse veröffentlicht, die die Dauer vom Eindringen eines Angreifers in das System bis zur Beherrschung des IT-Vorfalls angibt. In 56 % der Fälle wird die Kompromittierung innerhalb der ersten sechs Monate erkannt, davon in neun Prozent innerhalb des ersten Monats und in 27 % innerhalb des zweiten und dritten Monats. In 25 % der Fälle dauert es sechs bis zwölf Monate bis der Vorfall bekannt und auf ihn reagiert wurde und 19 % werden erst innerhalb des zweiten Jahres oder später entdeckt. Abgesehen vielleicht von den neun Prozent, die innerhalb des ersten Monats erkannt werden, bleibt in jedem Fall genug Zeit für die Angreifer, um alle gewünschten Daten zu exfiltrieren.

Je nachdem, welche Definition man sich zu eigen macht, sind Cyberkriminalität und Cyberspionage entweder zwei unterschiedliche Bereiche oder Teil desselben Phänomens. Für Unternehmen verschwimmen jedoch die Grenzen, denn häufig geht das eine mit dem anderen einher. Überdies ist die rechtliche Grundlage noch nicht eindeutig.[66] Ein grundlegender Schutz sowohl auf der technischen als auch der personellen Seite ist in jedem Fall notwendig. Auch in Unternehmen, die nicht zu den kritischen Infrastrukturen gehören, sollte sich eine IT-Sicherheitskultur entwickeln.

Vor allem das Anreizsystem für Unternehmen, Sicherheitsvorfälle zu melden, sollte erweitert werden. Neben konkreter Hilfestellung und sachkompetenter Unterstützung durch die Behörden, wäre es bspw. auch denkbar, eine anonymisierte Auswertung der Daten nach Branchen spezifiziert – möglichst durch unabhängige Wissenschaftler – anzubieten. Dies ist sicherlich insbesondere für größere Unternehmen von Interesse. Cybercrime-Trends innerhalb einzelner Branchen könnten somit erkannt und entgegengewirkt werden.

Diese Überlegungen setzen jedoch immer einen sehr sensiblen und kompetenten Umgang mit den Unternehmensdaten voraus. Das Vertrauen zwischen Unternehmen und Behörden, das hierfür notwendig ist, muss bereits bei der Entwicklung des Gesetzesvorhabens etabliert werden. Sollte dies erfolgreich sein, könnte Deutschland aufgrund einer validen Datengrundlage mittel- und langfristig seine Wirtschaft effektiver schützen und eine Voreiterrolle bei der Bekämpfung von Cyberkriminalität einnehmen.

4 Fazit

Um die zivile Cybersicherheit Deutschlands zu erhöhen, ist ein gesellschaftliches Umdenken hin zu einer IT-Sicherheitskultur erforderlich. Dieses Umdenken muss sowohl in Behörden und Unternehmen als auch beim einzelnen Bürger stattfinden, damit eine resiliente Gesellschaft entstehen kann, die einen Ausfall der kritischen Infrastruktur Internet verkraftet. Hierfür bedarf es u. a. einer kritischen Diskussion innerhalb der Gesellschaft und langfristiger Ziele.

Der Schutz vor Cybercrime ist ein Bereich der zivilen Cybersicherheit Deutschlands. Die Mithilfe des Bürgers ist dafür unerlässlich. Es wurde aufgezeigt, dass eine fundierte Datengrundlage die Voraussetzung für den Diskurs einerseits und für die Analyse des Bedrohungspotentials andererseits ist. Geeignete Maßnahmen können nur unternommen werden, wenn das jeweilige Phänomen mittels valider Daten analysiert werden kann. Dies gilt sowohl auf nationaler als auch auf internationaler Ebene. Doch in jedem Fall ist die bisherige Datenlage unzureichend.

Der Komplexität und der Vernetzung, die durch das Internet entstehen, sollte im Falle der Bekämpfung von Straftaten mittels nationaler Maßnahmen begegnet werden, die dann gegebenenfalls in internationale Kooperationen münden könnten und sollten.

Die Zusammenarbeit von und mit Unternehmen zur Bekämpfung von Cybercrime ist essentiell, bringt jedoch auch neue Herausforderungen mit sich. Eine Meldepflicht für IT-Sicherheitsvorfälle ist nur der Anfang, deshalb sollte gleich zu Beginn eine effektive und vertrauensvolle Kooperation zwischen Unternehmen und Behörden etabliert werden.

Es besteht eine einmalige Chance, den derzeit stattfindenden Generationenwechsel hin zu den ‚Digital Natives'[67] mit einer Hinwendung zu einer IT-Sicherheitskultur zu verbinden. Die Wahrnehmung des Rechts auf informationelle Selbstbestimmung ist dabei die Voraussetzung, um Sicherheit im Internet als erstrebenswert anzusehen. Zivile Cybersicherheit ist darauf angewiesen, die Zivilbevölkerung mit einzubeziehen. Gelingt hier ein Umdenken, zieht das ein Umdenken in allen gesellschaftlichen Bereichen und damit eine resiliente Gesellschaft nach sich. Der Schritt ins digitale Zeitalter wäre dann gleichzeitig ein Schritt hin zur Cybersicherheit.

Fußnoten

1. Bundeskriminalamt, Cybercrime – Bundeslagebild 2012, 2012, 3.
2. United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime - Draft February 2013, Februar 2013.
3. Ebd., 11.
4. Ebd., xvii.
5. Hewlett Packard, HP-Studie: Gut 80 Prozent aller Anwendungen mit Sicherheitslücken, 3. Februar 2014.
6. Die Datengrundlage im Bereich Cybercrime besteht in vielen Fällen aus Unternehmensberichten, mit denen auch unternehmenseigene Ziele verfolgt werden. Des Weiteren leiten sich die Daten aus dem Produktportfolio und dem Kundenstamm der Unternehmen her und sind daher nicht repräsentativ. Primärquellen gibt es nur vereinzelt und nicht zu jedem Cybercrime-Bereich.
7. Die Autorin verzichtet in diesem Artikel darauf, alle englischen Begriffe in die deutsche Sprache zu übersetzen, da diese größtenteils Fachbegriffe sind. Eine Erläuterung der wichtigsten Begrifflichkeiten wird vorgenommen. Die Erläuterungen erheben keinen Anspruch auf Vollständigkeit, sie sind vereinfachte Darstellungen komplexer technischer Zusammenhänge und konzentrieren sich auf die für das Textverständnis wesentlichen Aspekte.
8. Verizon Enterprise Solutions, 2013 Data Breach Investigations Report, 2013, 25.
9. *Malware* ist ein Oberbegriff für Schadprogramme unterschiedlichster Art wie bspw. Viren und Trojaner, die auf softwarebasierten Geräten vom Benutzer unerwünschte Wirkungen entfalten können.
10. Bei *SQL Injections* handelt es sich um Angriffe auf SQL-Datenbanken, die z. B. häufig hinter Webseiten stehen. In einem Eingabefeld, wie bspw. einer ‚Suchen-Funktion', wird ein Befehl eingegeben, durch den bei vorhandenen Sicherheitslücken Daten aus der Datenbank ausgelesen werden können. Diese Angriffe können automatisiert oder gezielt erfolgen.
11. Verizon Enterprise Solutions, 2013 Data Breach Investigations Report, 2013, 27.
12. Trustwave, 2013 Global Security Report, 2013, 13.
13. Symantec, Internet Security Threat Report 2013, 18, 2013, 19.
14. IBM, IBM X-Force 2013 – Mid-Year Trend and Risk Report, September 2013, 13.
15. Hierbei ist zu beachten, dass es sich um öffentlich verfügbare Daten handelt, die von IBM ausgewertet wurden.
16. Microsoft, Microsoft Security Intelligence Report Volume 13, 2012, 13ff.
17. IBM, IBM X-Force 2013 – Mid-Year Trend and Risk Report, 50ff.
18. Verizon Enterprise Solutions, 2013 Data Breach Investigations Report, 32f.
19. In den USA gibt es bspw. das *Internet Crime Complaint Center*, das Beschwerden von Individuen, die Opfer von Cyberkriminalität geworden sind, aufnimmt und u. a. an die jeweils zuständigen Behörden weiterleitet.
20. Bei *Ransomware* handelt es sich um Schadprogramme, die bei dem infizierten Computer den Zugriff auf den gesamten Computer oder einzelne Dateien verhindern. Nach der Zahlung eines Geldbetrags soll der Zugriff wieder freigeschaltet werden, was aber nicht gewährleistet ist.
21. Mit DDoS (*Distributed Denial of Service*)-Attacken sind (koordinierte) Angriffe auf Infrastruktursysteme (z. B. eine Webseite) gemeint, die von vielen verschiedenen Systemen durchgeführt werden und zur Überlastung der Infrastruktur und damit der Nichtverfügbarkeit des angegriffenen Systems führen können.
22. Vgl. Bundeskriminalamt, Cybercrime – Bundeslagebild 2012, 4.
23. Die Dunkelzifferrelation beschreibt die Größe des Dunkelfeldes. Sie „wird definiert als Verhältnis aus der Zahl der der Polizei bekannt gewordenen Delikte zu der Anzahl der nicht bekannt gewordenen Straftaten." Hans-Dieter Schwind, Kriminologie – Eine praxisorientierte Einführung mit Beispielen, 22. Aufl., 39.
24. Heise Online, BKA-Präsident: Cybercrime in fünf Jahren verdoppelt, 21. August 2013.
25. Nils Diers, Wie viel Kriminalität hat die Gesellschaft? Eine Grundlage für die Ermittlung der Zahl der jährlich in Deutschland begangenen Straftaten, IKS Working Paper Series 1, 2010, 22.
26. Vgl. Ebd.
27. Mit dem Begriff *Awareness* wird im Bereich der IT-Sicherheit ein Sicherheitsbewusstsein umschrieben, dass innerhalb eines Konzeptes entwickelt und gefördert werden kann. Dabei sollen zum einen einfache, aber besonders effektive Methoden zur Erhöhung der IT-Sicherheit (z. B. das Generieren sicherer Passwörter) und zum anderen ein allgemeines Problembewusstsein vermittelt werden.
28. Symantec, Internet Security Threat Report 2013, 11.
29. Darya Gudkova, Kaspersky Security Bulletin: Spam Evolution 2012, hg. von Kaspersky, Securelist.
30. Trustwave, Global Security Report 2013, 2013, 42.
31. Bei Botnetzen handelt es sich um verteilte Software, die meist ohne Wissen der Anwender auf vielen mit dem Internet verbundenen Computern (auch Smartphone, Tablet o. ä.) automatisch agiert. Die infizierten Systeme werden als *Bots* bezeichnet und von *Command-and-Control-Servern* (C&C-Servern) gesteuert. Die *Bots* stellen dem Botnetz lokale Ressourcen des Computers wie z. B. Rechenleistung zur Verfügung.
32. Weiter kommt erschwerend hinzu, dass einige Quellcodes für Botnetze offen liegen bzw. käuflich sind und somit eine Vielzahl ähnlich aufgebauter Botnetze existiert.
33. Damballa, Damballa Threat Report - First Half 2011" 2011, 4.

34. Symantec, Internet Security Threat Report 2013, 2013, 16.
35. PricewaterhouseCoopers, Cybercrime: Protecting against the growing threat, Bd. 256, 2012, 22.
36. Symantec, Internet Security Threat Report 2013, 2013, 16.
37. Verizon Enterprise Solutions, 2013 Data Breach Investigations Report, 2013, 12.
38. Ebd., 40.
39. Die Bezeichnung der Branchen ist dabei in beiden Berichten unterschiedlich und umfasst nicht notwendigerweise die gleiche Art von Unternehmen.
40. Symantec, Internet Security Threat Report - 2011 Trends, 17, 2012, 22.
41. Verizon Enterprise Solutions, 2012 Data Breach Investigations Report, 2012, 11.
42. Inklusive *Social Assistance*.
43. Inklusive Versicherungen, bei Symantec hingegen wird das Versicherungswesen gesondert mit 3 % aufgeführt.
44. Mehr Informationen unter: http://www.aic.gov.au/publications/current%20series/tbp/41-60/tbp056.html.
45. TNS Opinion & Social, Special Eurobarometer 404 – Cyber Security, hg. von Europäische Kommission, November 2013.
46. TNS Opinion & Social, Special Eurobarometer 404 – Cyber Security, Factsheet Deutschland, hg. von Europäische Kommission, November 2013. Die Frage wurde den Internetnutzern der Befragung gestellt. Die Kategorien ‚Häufig' und ‚Gelegentlich' wurden bei der Auswertung zusammengefasst.
47. Ebd., 3.
48. Siehe hierzu auch: Kristin Krüger, IT-Sicherheit in der öffentlichen Wahrnehmung, hg. von Magdeburger Institut für Sicherheitsforschung, Bd. 1, Magdeburger Journal zur Sicherheitsforschung, 2012, 159f.
49. United Nations Office on Drugs and Crime, „Comprehensive Study on Cybercrime - Draft February 2013.
50. Symantec, Hrsg., 2013 Norton Report, 2013, 4.
51. Bei den ‚Digital Outsiders' handelt es sich um Menschen, die entweder offline oder unsicher im Umgang mit dem Internet sind. Siehe SINUS-Institut, DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet, hg. von Deutsches Institut für Vertrauen und Sicherheit im Internet (Hamburg, 2012), 34.
52. Das Milieu der ‚Unbekümmerten Hedonisten' umfasst spaßorientierte Internetnutzer, deren Gefahrenbewusstsein gering ausgeprägt ist. Siehe ebd., 86f.
53. Jacob Kullik, Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik, hg. von Beate Neuss, Bd. 7, Chemnitzer Schriften zur europäischen und internationalen Politik, 86.
54. Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland, Februar 2011, 3.
55. Die BSI-Seite für Bürger wird hier außen vor gelassen, da sie eine aktive Beschäftigung mit der Thematik voraussetzt.
56. Siehe: http://www.bakoev.bund.de/DE/03_Unser_Fortbildungsangebot/01_Unser_Seminarangebot/01_Themen/05_Informationstechnik/01_sicher_gewinnt/sicher_gewinnt.html.
57. Das Brandenburgische Institut für Gesellschaft und Sicherheit (BIGS) beschäftigt sich intensiv mit dem Thema Risikokommunikation und hat hierzu mehrere Studien veröffentlicht, z. B. „Behördliche Risikokommunikation in Deutschland" von Constance Baban.
58. Golem.de, BSI-Sicherheitswarnung: Fast eine Million gehackter Nutzer informiert, 22. Januar 2014.
59. Textsecure ist eine open-source Applikation für Android-Telefone, die auf einer Ende-zu-Ende-Verschlüsselung basiert und mittels derer zwischen verschlüsselte Nachrichten ausgetauscht werden können. Die Telefone der Empfänger müssen sich dafür einmalig gegenseitig authentifizieren und einen kryptographischen Schlüssel austauschen.
60. Vgl. Heise Online, Router-Backdoor: Cisco, Netgear und Linksys versprechen Schutz, 14. Januar 2014.; vgl. Bruce Schneier, HEADWATER: NSA Exploit of the Day, Schneier on Security, 14. Januar 2014.
61. Jonas Rest, Mit Cryptopartys gegen Big Brother, Berliner Zeitung, 12. Juli 2013.
62. Das Für und Wider einer Meldepflicht von Cybervorfällen für Unternehmen ist erschöpfend diskutiert worden und soll hier nicht noch einmal wiedergegeben werden.
63. Vgl. bspw. Bundesverband der Deutschen Industrie e.V., Positionspapier – Erwartungen der deutschen Industrie an ein IT-Sicherheitsgesetz, Februar 2014. und BITKOM, BITKOM fordert Nachbesserungen am IT-Sicherheitsgesetz, 3. April 2013.
64. Felix „FX" Lindner, Licht aus! Sicherheit kritischer Infrastrukturen im Test, c't, Nr. 9, 7. April 2014: 152.
65. Trustwave, 2013 Global Security Report, 2013, 11.
66. Vgl. Laura Poitras, Marcel Rosenbach, und Holger Stark, GCHQ and NSA Targeted Private German Companies, Spiegel online, 29. März 2014.
67. ‚Digital Natives' bezeichnen ein Milieu, in dem die Personen mit digitalen Technologien wie dem Internet aufgewachsen sind und daher einen anderen Umgang mit ihnen pflegen, als Personen, die diese Technologien erst später in ihrem Leben kennengelernt haben. Für weitere Angaben und weitere Unterteilungen des Milieus siehe: SINUS-Institut, DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet.

Literaturverzeichnis

BITKOM: „BITKOM fordert Nachbesserungen am IT-Sicherheitsgesetz", 3. April 2013. http://www.bitkom.org/de/themen/54746_75692.aspx.

Bundeskriminalamt (Hrsg.): „Cybercrime – Bundeslagebild 2012", 2012. www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2012,templateId=raw,property=publicationFile.pdf/cybercrimeBundeslagebild2012.pdf.

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

Bundesverband der Deutschen Industrie e.V.: „Positionspapier – Erwartungen der deutschen Industrie an ein IT-Sicherheitsgesetz", Februar 2014. http://www.bdi.eu/download_content/SicherheitUndVerteidigung/Positionspapier_Sicherheitsgesetz_25_02.pdf.

Damballa (Hrsg.): „Damballa Threat Report – First Half 2011", 2011. https://www.damballa.com/downloads/r_pubs/Damballa_Threat_Report-First_Half_2011.pdf.

Diers, Nils: „Wie viel Kriminalität hat die Gesellschaft? Eine Grundlage für die Ermittlung der Zahl der jährlich in Deutschland begangenen Straftaten", IKS Working Paper Series 1, 2010. http://www.wiso.uni-hamburg.de/fileadmin/sowi/kriminologie/Workin_Paper_Series/IKS_WPS_001_Diers.pdf.

Golem.de: „BSI-Sicherheitswarnung: Fast eine Million gehackter Nutzer informiert", 22. Januar 2014. http://www.golem.de/news/bsi-sicherheitswarnung-fast-eine-million-gehackter-nutzer-informiert-1401-104089.html.

Gudkova, Darya: „Kaspersky Security Bulletin: Spam Evolution 2012", Herausgegeben von Kaspersky, Securelist. http://www.securelist.com/en/analysis/204792276/Kaspersky_Security_Bulletin_Spam_Evolution_2012.

Heise Online: „BKA-Präsident: Cybercrime in fünf Jahren verdoppelt", 21. August 2013. http://www.heise.de/newsticker/meldung/BKA-Praesident-Cybercrime-in-fuenf-Jahren-verdoppelt-1939915.html.

Heise Online: „Router-Backdoor: Cisco, Netgear und Linksys versprechen Schutz", 14. Januar 2014. http://www.heise.de/security/meldung/Router-Backdoor-Cisco-Netgear-und-Linksys-versprechen-Schutz-2084884.html.

Hewlett Packard (Hrsg.): „HP-Studie: Gut 80 Prozent aller Anwendungen mit Sicherheitslücken", 3. Februar 2014. http://www8.hp.com/de/de/hp-news/press-release.html?id=1571502&pageTitle=HP-Studie-gut-80-Prozent-aller-Anwendungen-mit-Sicherheitsluecken#.Uv_BK7TEHD_.

IBM (Hrsg.): „IBM X-Force 2013 – Mid-Year Trend and Risk Report", September 2013. http://www-03.ibm.com/security/xforce/downloads.html.

Krüger, Kristin: „IT-Sicherheit in der öffentlichen Wahrnehmung", Herausgegeben von Magdeburger Institut für Sicherheitsforschung, 2012, 1:153–167. http://www.wissens-werk.de/index.php/mjs/article/view/111.

Kullik, Jacob: „Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik", Herausgegeben von Beate Neuss. Bd. 7. Chemnitzer Schriften zur europäischen und internationalen Politik. Hamburg: Dr. Kovač, 2014.

Lindner, Felix „FX": „Licht aus! Sicherheit kritischer Infrastrukturen im Test". c't, Nr. 9 (7. April 2014): 150–155.

Microsoft (Hrsg.): „Microsoft Security Intelligence Report Volume 13", 2012. http://www.microsoft.com/de-de/download/details.aspx?id=34955.

Poitras, Laura, **Marcel Rosenbach**, und **Holger Stark**: „GCHQ and NSA Targeted Private German Companies", Spiegel online, 29. März 2014. http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html.

PricewaterhouseCoopers (Hrsg.): „Cybercrime: Protecting against the growing threat", Bd. 256, 2012. https://www.pwc.tw/en_TW/tw/publications/events-and-trends/assets/e256.pdf.

Rest, Jonas: „Mit Cryptopartys gegen Big Brother", Berliner Zeitung, 12. Juli 2013. http://www.berliner-zeitung.de/kultur/cryptopartys-mit-cryptopartys-gegen-big-brother,10809150,23700214.html.

Schneier, Bruce: „HEADWATER: NSA Exploit of the Day", Schneier on Security, 14. Januar 2014. https://www.schneier.com/blog/archives/2014/01/headwater_nsa_e.html.

Schwind, Hans-Dieter: „Kriminologie – Eine praxisorientierte Einführung mit Beispielen", 22. Aufl. Heidelberg, 2013.

SINUS-Institut: „DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet", Herausgegeben von Deutsches Institut für Vertrauen und Sicherheit im Internet. Hamburg, 2012. https://www.divsi.de/sites/default/files/presse/docs/DIVSI-Milieu-Studie_Gesamtfassung.pdf.

Symantec (Hrsg.): „2013 Norton Report", 2013. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013.

Symantec (Hrsg.): „Internet Security Threat Report – 2011 Trends", 17, 2012. http://www.symantec.com/security_response/publications/archives.jsp.

Symantec (Hrsg.): „Internet Security Threat Report 2013", 18, 2013. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

TNS Opinion & Social: „Special Eurobarometer 404 – Cyber Security". Herausgegeben von Europäische Kommission, November 2013. http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf.

TNS Opinion & Social: „Special Eurobarometer 404 – Cyber Security, Factsheet Deutschland". Herausgegeben von Europäische Kommission, November 2013. http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_fact_de_de.pdf.

Trustwave (Hrsg.): „2013 Global Security Report", 2013. http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf.

United Nations Office on Drugs and Crime (Hrsg.): „Comprehensive Study on Cybercrime – Draft February 2013", Februar 2013. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Verizon Enterprise Solutions (Hrsg.): „2012 Data Breach Investigations Report", 2012. http://www.verizonenterprise.com/DBIR/2012/download.xml.

Verizon Enterprise Solutions (Hrsg.) „2013 Data Breach Investigations Report", 2013. http://www.verizonenterprise.com/DBIR/2013/.

IMPRESSUM

Die Brandenburgische Institut für Gesellschaft und Sicherheit (BIGS) gGmbH ist ein unabhängiges, überparteiliches und nicht-gewinnorientiertes wissenschaftliches Institut, das zu gesellschaftswissenschaftlichen Fragen ziviler Sicherheit forscht. Das BIGS publiziert seine Forschungsergebnisse und vermittelt diese in Veranstaltungen an eine interessierte Öffentlichkeit. Es entstand im Frühjahr 2010 in Potsdam unter der Beteiligung der Universität Potsdam und ihrer UP Transfer GmbH sowie der Unternehmen EADS, IABG und Rolls-Royce. Es wird vom Land Brandenburg gefördert. Alle Aussagen und Meinungsäußerungen in diesem Papier liegen in der alleinigen Verantwortung des Autors bzw. der Autoren.

Autor:
Kristin Krüger

Titel:
Zivile Cybersicherheit: Cybercrime zwischen Realität und Risiko

Herausgeber:
Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH

Verantwortlicher im Sinne des Rundfunkstaatsvertrages:
Dr. Tim H. Stuchtey

ISSN 2191-6756

Weitere Informationen über die Veröffentlichungen des BIGS befinden sich auf der Webseite des Instituts:

www.bigs-potsdam.org

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT

Geschäftsführender Direktor: Dr. Tim H. Stuchtey
Rudolf-Breitscheid-Straße 178 · 14482 Potsdam
Tel.: +49-331-704406-0 · Fax: +49-331-704406-19 · info@bigs-potsdam.org · www.bigs-potsdam.org