Kurz-Auswertung der neuen Cyber-Sicherheitsstrategie Deutschlands 2016

Thomas Reinhold,
Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, reinhold@ifsh.de, http://cyber-peace.org

Anmerkung: Zitate sind, so nicht explizit gekennzeichnet, der “Cyber-Sicherheitsstrategie Deutschlands 2016”, herausgegegeben von Bundes-Innenministerium, entnommen

Zu Einleitung und Hintergrund des Strategiepapiers

Die neue Cyber-Sicherheitsstrategie 2016[1] der Bundesregierung ist das Nachfolge-Dokument zur Cyber-Sicherheitsstrategie von 2011[2], mit dessen Veröffentlichung seinerzeit der nationale Cyber-Sicherheitsrat als Schnittstelle zwischen Wirtschaft und Politik etabliert sowie das nationale Cyber-Abwehrzentrum als Koordinations- und Austausch-Stelle für Cybersicherheits-Aspekte zwischen verschiedenen staatlichen Institutionen gegründet wurde.

Das neue Strategiepapier basiert den einführenden Worten des Dokuments zufolge auf der Einschätzung, das Cyber-Sicherheit “*inzwischen zu einem wesentlichen Baustein einer Vielzahl strategischer Konzepte und ressortübergreifender Vorhaben der Bundesregierung geworden*” ist, dabei “*Innere und äußere Sicherheit im Cyber-Raum (..) nicht mehr trennscharf voneinander abzugrenzen*” sind und “*die Wahrung der Cyber-Sicherheit und die Verteidigung gegen Cyber-Angriffe (..) so zu einer gesamtstaatlichen Aufgabe geworden*” sind.

Ausgehend von den Beschlüssen und Strategien von 2011 bildet *“die Cyber-Sicherheitsstrategie 2016 (..) den ressortübergreifenden strategischen Rahmen für die Aktivitäten der Bundesregierung mit Bezügen zur Cyber-Sicherheit und schreibt die Cyber-Sicherheitsstrategie aus dem Jahr 2011 fort."*

Zur attestierten Bedrohungslage

Hinsichtlich der adressierten Bedrohungslage umfasst die neue Cyber-Sicherheitsstrategie neben Gefahren, wie sie bereits 2011 aufgezählt wurden[3], nun auch das aktuell stark diskutierte Thema der gezielt verbreiteten Falschmeldung als Mittel der Desinformation und Meinungsmanipulation und bewerten diese als langfristige Gefahr für die freiheitliche Gesellschaft und die Demokratie. Darüber hinaus sieht das Strategiepapier die Gefahr, dass politisch-militärische Konflikte zunehmend von “Cyber-Kampagnen” begleitet oder “*unterhalb der Schwelle zum bewaffneten Konflikt*

[1] http://www.bmi.bund.de/cybersicherheitsstrategie/

[2] https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile

[3] Dazu zählen Vorfälle mit kriminellen, extremitischen/terroristischen, militärischen oder nachrichtendienstlichen Hintergrund

auch im Cyber-Raum ausgetragen" werden. "*Dies erschwert die politische Bewertung von Cyber-Angriffen und die Entscheidung über die gebotenen Gegenmaßnahmen*".

Darüber hinaus geht das Strategiepapier hinsichtlich der Bedrohungslage davon aus, dass "*Zahl und Qualität der Cyber-Angriffe (..) dabei kontinuierlich*" zunehmen und "*Angriffswerkzeuge (..) mittlerweile sowohl für staatliche Akteure als auch für kriminelle Gruppen oder Individuen verfügbar [sind]. Insbesondere gegenüber technologisch hoch entwickelten Schadprogrammen reichen die klassischen Abwehrwerkzeuge häufig nicht mehr aus.*" Ein solche Einschätzung, die eine Proliferation hoch-qualitativer Hacking-Werkzeugen impliziert ist aus einem technischen Blickwinkel nicht korrekt. Zum einen zeigen die sehr umfangreichen jährlichen Analysen des renommierten und von vielen internationalen IT-Sicherheitsunternehmen und Strafverfolgern unterstützten Verizon Data Breach Reports, dass die absoluten Zahlen von gemeldeten Vorfällen zwar steigen, dass diese aber kein eindeutiges Bild zeichnen. Setzt man die absoluten Zahlen von Vorfällen ins Verhältnis zur zunehmenden Bereitschaft von Unternehmen Vorfälle zu melden und der Anzahl der meldenden Organisationen dann bleibt das Gesamtverhältnis der Vorfälle mit konkretem Datenabfluß in den vergangenen Jahren etwa stabil. Im Anhang ist dazu eine kurze statistische Gegenüberstellung beigefügt. Darüber hinaus verweisen die Analysten dieser Berichte immer wieder darauf hin, dass sich die Vorfälle in der Gesamtheit nur schwer erfassen oder über Jahre hinweg konsistent bewerten lassen, da die absolute Menge der betroffenen Daten keine sinnvolle Aussagegröße bildet[4] und sich insbesondere in den vergangenen Jahren die Arten von Computern vom Desktop und Server hin zu mobilen Geräten massiv verändert und damit auch die Landschaft der IT-Sicherheitsvorfälle stark verändert hat.

Aus technischer Sicht ist es darüber hinaus so, dass Hacking-Werkzeuge seit sehr vielen Jahren Individuen und kriminellen Organisationen zur Verfügung stehen. Exemplarisch ist bspw. eines der sogenannten Exploit-Kits namens "MPack[5]", also ein "Baukästen" für die einfache und ohne komplexe IT-Erfahrungen zusammenstellbare Konfiguration von Schadsoftware in einer ersten Version schon 2006 erschienen. Bereits davor war die Programmierung von Computerviren und das Hacking von IT-System weit verbreitet. Vielmehr ist es so, dass in diesem Bereich eher Staaten mit ihren militärischen und nachrichtendienstlichen Institutionen die Nachzügler bilden, wie die zunehmende Aufrüstung in diesem Sektor in den vergangenen Jahren verdeutlicht[6]. Eine Proliferation von "Angriffswerkzeugen" aus Richtung einiger weniger staatlicher Akteure in Richtung krimineller, terroristischer oder individueller Hände - wie dies bspw. im Bereich der nuklearen Technologie anhand einer Proliferationskontrolle verhindert werden soll - kann für den Bereich der Hacking-Werkzeuge im allgemeinen nicht attestiert werden. Ebenso

---

[4] Dies liegt unter anderem daran, dass in vielen bis sehr vielen Fällen (> 85%) der gemeldeten Incidents die absolute Zahl der betroffenen Datensätze nicht empirisch sicher festgestellt werden konnte. Darüber hinaus ist es kaum zu bewerten, in welchem Verhältnis bspw. ein besonders schwerer Fall bei einem Unternehmen mit 10 Million betroffenen Datensätzen zu Vorfällen bei 10 Unternehmen mit jeweils einer Million betroffener Datensätze steht.

[5] https://en.wikipedia.org/wiki/MPack_(software)

[6] Vgl. dazu bspw. die UNIDIR Analyse: "The Cyber Index - International Security Trends and Realities", Genf, 2013

gibt es für die Annahme einer Proliferation von hochklassiger Schadsoftware kaum verlässliche öffentliche Daten die eine solche Interpretation für dieses Segment von Schadsoftware zulassen. Exemplarisch kann das Beispiel des Quellcodes der Schadsoftware Stuxnet herangezogen werden, dessen teilweise Veröffentlichung entgegen den Vermutung nicht zu weiteren derartigen Angriffen auf Basis dieser Software geführt hat[7]. Einer der Gründe für diesen Effekt könnte sein, dass Schadsoftware die für den Angriff von “Hochwertzielen” eingesetzt werden, mit dem Zeitpunkt ihrer Entdeckung für andere Hochwertziele wertlos werden, da mit ihrem Bekanntwerden und ihrer Analyse die verwendeten Sicherheitslücken und Angriffsvektoren bekannt werden und die für die - in aller Regel für die Sicherheit von Hochwertzielen ausreichend sensibilisierten - Verantwortlichen diese umgehend schließen.

Über die Leitlinien

Die Cyber-Sicherheitsstrategie definiert für die kommenden Jahre die folgenden Leitlinien für vier Kernbereiche:

1. Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung
2. Gemeinsamer Auftrag Cyber-Sicherheit von Staat und Wirtschaft
3. Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur
4. Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik

Die Strategie konkretisiert jede dieser einzelnen Punkte. Diese sollen nachfolgend im Detail betrachtet werden. Im Fokus steht dabei die Bedeutung der identifizierten Aufgaben und Problemfelder für die Friedens- und Sicherheitsforschung sowie die Implikationen und Fragen die sich mit Blick der Informatik allgemein und der IT-Sicherheitsforschung im speziellen daraus ergeben.

Zu Leitlinie 1. Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung

Mit dieser Leitlinie verbindet die Cyber-Sicherheitsstrategie die folgenden Handlungsfelder:

> Digitale Kompetenz bei allen Anwendern fördern
> Digitaler Sorglosigkeit entgegenwirken
> Voraussetzungen für sichere elektronische Kommunikation und sichere Webangebote schaffen
> Sichere elektronische Identitäten Zertifizierung und Zulassung stärken / Einführung eines Gütesiegels für IT-Sicherheit
> Digitalisierung sicher gestalten IT-Sicherheitsforschung vorantreiben

[7] Natürlich rückten nach Stuxnet vermehrt SCADA-Systeme in den Fokus von Cyberattacken, da mit Stuxnet deren hoher Grad an Angreifbarkeit deutlich wurde. Dies entspricht aber allenfalls der Proliferation einer Angriffs-Idee, nicht eines konkreten Werkzeugs.

Der Großteil dieser Aufgaben aus Leitlinie 1 berührt nicht unmittelbar die Friedens- und Sicherheitsforschung, da diese sich auf die Sicherung kommerzieller Angebot im Cyberspace sowie Fragen der individuellen privaten Sicherheit von Internet-fähigen Geräten sowie des E-Governments beziehen. Ausgenommen davon ist die "*Einführung eines Gütesiegels für IT-Sicherheit*". Dies ist - wenn auch im Strategiepapier vor allem auf den individuellen Anwender bezogen - eine entscheidende Maßnahme um internet-fähige Geräte und IT-Produkte in der Breite nachweislich sicherer und weniger anfällig für ungewollten und gewollten Missbrauch abzusichern. Neben dem unmittelbaren verbesserten Schutz durch den Einsatz derart kontrollierter Geräte und Produkte wird damit Angreifern und IT-Kriminellen der Boden entzogen. Insbesondere bei sogenannten Distributed denial of service (DDoS)[8]-Attacken werden zu tausenden private IT-Geräte wie PCs und Laptops, DSL-Router sowie Geräte des Internet of Things (IoT)[9] für massenhafte Zugriffe gegen große IT-Systeme ausgenutzt und damit unter Umständen zum Werkzeug für schwerwiegende Cyberangriffe. Der zeitweilige Ausfall von bis zu 900.000 Internetanschlüssen der deutschen Telekom[10] durch einen unbeabsichtigten Nebeneffekt einer Cyber-Attacke gegen Kunden eines irischen IT-Anbieters verdeutlicht darüber hinaus, wie unsichere, in der Breite verteilte IT-Geräte schnell zu einem komplexen Problem heranwachsen können. Vergleichbare "digitale Monokulturen" existieren beispielsweise auch im Bereich der Smartphone-Betriebssysteme (Android und IOS[11], bei PC-Betriebssystemen (Windows) oder Verwaltungs- und Büro-Software (Microsoft Office Produkte). In Analogie zum medizinischen Konzept der sogenannten "Herdenimmunität"[12] bei der Flächendurchimpfung gegen typische Infektionskrankheiten kann eine Verbesserung der IT-Sicherheit vieler Geräte und Produkte die allgemeine IT-Sicherheit der Gesellschaft daher deutlich verbessern. Mit Blick auf die kostenintensive Durchsetzung von entwickelten IT-Zertifikaten bei IT-Dienstleistern und Herstellern von IT-Geräten verharrt die Cyber-Sicherheitsstrategie jedoch beim Vertrauen auf die selbst-regulierenden Kräfte des Marktes, die angesichts der Dominanz einiger weniger globaler IT-Unternehmen in Zweifel gezogen werden müssen. Hinsichtlich verpflichtender Regelungen oder der verpflichtenden IT-Produkthaftung - wie sie bspw. im Automobil-Bereich selbstverständlich sind - verweist die Strategie lediglich darauf, dass "*Vorgaben für eine angemessene Verteilung von Verantwortlichkeiten und Sicherheitsrisiken im Netz zum Beispiel durch Produkthaftungsregeln für IT-Sicherheitsmängel und Sicherheitsvorgaben für Hard und Softwarehersteller (..) geprüft [werden]*".

Zu Leitlinie 2: Gemeinsamer Auftrag Cyber-Sicherheit von Staat und Wirtschaft

Als Handlungsfelder der zweiten Leitlinie werden die folgende Aspekte identifiziert:

---

[8] https://de.wikipedia.org/wiki/Denial_of_Service
[9] https://de.wikipedia.org/wiki/Internet_der_Dinge
[10] http://cyber-peace.org/?p=2477
[11] https://de.statista.com/statistik/daten/studie/256790/umfrage/marktanteile-von-android-und-ios-am-smartphone-absatz-in-deutschland/
[12] https://de.wikipedia.org/wiki/Herdenimmunit%C3%A4t2

Kritische Infrastrukturen sichern
Unternehmen in Deutschland schützen
Die deutsche IT-Wirtschaft stärken
Mit den Providern zusammenarbeiten
IT-Sicherheitsdienstleister einbeziehen
Eine Plattform für vertrauensvollen Informationsaustausch schaffen

Ebenso wie für die Handlungsfelder aus Leitlinie 1 soll zugunsten der Kompaktheit hier auf eine eingehende Auswertung dieser Aspekte verzichtet werden. Einige Aspekte wie die Zusammenarbeit des BND mit IT-Providern zum Aufbau einer Erkennungs-Sensorik von Cyber-Angriffen für die Einleitung von Abwehrmaßnahmen[13], für das ein teilweises, ggf. inhaltliches Durchleuchten des kompletten Datenstroms notwendig wäre, oder der widersprüchliche Umgang mit Verschlüsselungs-Maßgaben sind aufgrund der Datenschutz- und Persönlichkeits-rechtlichen Implikationen kritisiert worden. Exemplarisch sei dazu dazu auf Kommentare bei heise.de[14] sowie netzpolitik.org[15] verwiesen.

Relevant im Sinne dieser Auswertung sind zum einen die verstärkten Maßnahmen zur Sicherung der kritischen Infrastrukturen. Obgleich die Strategie diese Aufgabe als von besonderer Bedeutung identifiziert, fehlen konkrete Maßnahmen und Ansätze, wie dieser Schutz verbessert werden soll. Beispielsweise fehlt, wie in ähnlichen Strategie-Konzepten der Jahre zuvor, eine Erklärung, wie eine Evaluation über die tatsächlichen Bedrohungen der Infrastrukturen, eine Identifikation der neuralgischen Punkte sowie eine Priorisierung der Verbesserung von Schutzmaßnahmen erfolgen soll. Soweit anhand öffentlich verfügbarer Quellen zu entnehmen, gibt es bisher keine umfassende Analyse des Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) oder des Bundesamt für Sicherheit in der Informationstechnik (BSI) über die konkrete Bedrohungslage sowie die Abhängigkeiten für den komplexen Bereich der kritischen Infrastrukturen, anhand dessen sich spezifische Handlungsempfehlungen ableiten lassen.

Neben diesem Aspekt verweist die Cyber-Sicherheitsstrategie erneut auf den Aspekt, dass im Bereich des Cyber-Schutzes kritischer Infrastrukturen "*innere und äußere Sicherheit (..) eng zusammenfallen*" ohne dies näher auszuführen. Folgt man diesem Argument, dann ist eine klare Erläuterung der Zuständigkeiten der einzelnen nationalen Ressorts, deren Zusammenarbeit und Koordination dringend geboten. Dies gilt umso mehr, da neben bestehenden Fähigkeiten bei Nachrichtendiensten in der vergangenen Monaten sowohl das BMVg, das BMI sowie das BfV den Aufbau von Cyber-Abwehr-Einheiten angekündigt und dabei unter anderem den Schutz kritischer Infrastrukturen als ein Kernaufgabe genannt haben. Angesichts der unterschiedlichen Befugnisse, des Geheimhaltungs-Vorgehens sowie der gesetzlichen Aufgaben und

[13] Dieses Vorhaben wird in Leitlinie 3 näher spezifiziert und dort als nachrichtendienstliche Maßnahme der "Signals Intelligence Support to Cyber Defense (SSCD)" bezeichnet
[14] https://heise.de/-3463416
[15] https://netzpolitik.org/2016/cybersicherheitsstrategie-der-regierung-widerspruechliche-verschluesselungsdiskussion-geht-weiter/

Grenzen der einzelnen Institutionen ist eine Klärung hier dringend geboten, insbesondere auch mit Blick auf die Interessen der Öffentlichkeit sowie der parlamentarischen Kontrolle. Die Richtlinien sehen das gemeinsame nationale Cyber-Abwehrzentrums in dieser Rolle als zentrale Koordinations- und Kooperationsplattform.[16] Allerdings gab es in der Vergangenheit mehrfach[17] Kritik unter anderem vom Bundesrechnungshof hinsichtlich der mangelhaften Effizienz dieser Einrichtung.

Zu Leitlinie 3: Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur

Leitlinie 3, ebenso wie Leitlinie 4, betreffen viele Aspekte die aus der hier fokussierten Sicht der Friedens- und Sicherheitsforschung von hoher Relevanz sind. Die Handlungsfelder der dritten Leitlinie sind:

> Das Nationale Cyber-Abwehrzentrum weiterentwickeln
> Die Fähigkeit zur Analyse und Reaktion vor Ort stärken
> Strafverfolgung im Cyber-Raum intensivieren
> Cyber-Spionage und Cyber-Sabotage effektiv bekämpfen
> Ein Frühwarnsystem gegen Cyber-Angriffe aus dem Ausland[18]
> Gründung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)
> Verteidigungsaspekte der Cyber-Sicherheit stärken
> CERT-Strukturen in Deutschland stärken
> Die Bundesverwaltung sichern
> Zwischen Bund und Ländern eng zusammenarbeiten
> Ressourcen einsetzen, Personal gewinnen und entwickeln

Ein wesentlicher Kern dieses Handlungsfeldes besteht im Ausbau des im Rahmen der Cyber-Sicherheitsstrategie 2011 eingerichteten nationalen Cyber-Abwehrzentrums. Dieses soll als Schlüsselelement einer "*gesamtstaatlichen, ressortübergreifenden Cyber-Sicherheitsarchitektur (..) organisatorisch gestärkt werden*". Für diese Aufgabe wird es zu einer "*ressortgemeinsame[n] Institution (..) unter Federführung des Bundesministeriums des Innern zur zentralen Kooperations- und Koordinationsplattform fortentwickelt. Das Cyber-AZ soll zukünftig mit eigenen Bewertungs- und Auswertungsfähigkeiten ausgestattet sein und über ein aktuelles Cyber-Lagebild verfügen, das die Cyber-Sicherheitslage in Deutschland widerspiegelt (..) Bei Cyber-Sicherheitsvorfällen, die bundesweit zahlreiche Institutionen betreffen, wächst das Cyber-AZ zu einem Krisenreaktionszentrum auf; in diesen Fällen können die Sicherung und Wiederherstellung der IT-Systeme sowie die Aufklärung und Abwehr von*

---

[16] Dazu mehr bei Leitlinie 3
[17] exempl.: http://www.sueddeutsche.de/news/wirtschaft/internet-rechnungshof-bezweifelt-nutzen-von-cyber-abwehrzentrum-dpa.urn-newsml-dpa-com-20090101-140607-99-01889 sowie https://www.welt.de/politik/deutschland/article148853713/Deutsche-Abwehr-gegen-Cyberangriffe-ist-unwirksam.html
[18] Siehe dazu die Anmerkungen und Verweise bei Leitlinie 1 zum Thema "Provider-Kooperationen"

Cyber-Angriffen nur durch abgestimmte Maßnahmen der nationalen Akteure erreicht werden. Diese operative Zusammenarbeit soll intensiver koordiniert werden."

Grundsätzlich erscheint es sinnvoll die verteilten Aktivitäten und Erkenntnisse der unterschiedlichen Akteure zu einem gemeinsamen ganzheitlichen Lagebild zusammen zu führen. Die Strategie lässt allerdings offen ob ein solches gemeinsames Lagebild explizit nur in Krisenzeiten oder dieses - wie es aus Sicht der Aufgabenerfüllung sinnvoll wäre - kontinuierlich erstellt wird. Offen bleibt auch, wie ein solches Lagebild-Szenario mit den unterschiedlichsten Quellen und Methoden der Informationsgewinnung den gesetzlichen Auflagen entsprechen und gleichzeitig effektiv und sinnvoll arbeiten kann. Diese Frage stellt sich auch angesichts der praktischen Steuerungsmöglichkeiten durch eine solche Ressort-übergreifende Institution in konkreten Krisenzeiten und den dabei gebotenen raschen Entscheidungen. Kernbehörden des Cyber-Abwehrzentrums waren bislang das BSI, das BfV sowie das BBK. Eine größere Einflußnahme des BMI als zukünftige federführende Institution und der damit zu erwartende Informationszusammenfluß im Innenministerium stellt darüber hinaus auch das verfassungsrechtliche Gebot der Dienste-Trennung in Frage.

Um angesichts von Cyberattacken besser vor Ort agieren zu können, Betroffenen bei der Abwehr und Bewältigung einer Attacke zu unterstützen sowie mit geeigneten Strafverfolgungs- und Nachrichtendienstlichen Maßnahmen reagieren zu können sollen in unterschiedlichen staatlichen Institutionen mobile IT-Einsatzteams aufgebaut werden. Folgende Einsatz-Teams sind geplant:

> BSI: „Mobile Incident Response Teams“ (MIRTs) für den konkreten technischen Supports bei relevanten Cyber-Vorfällen
> BKA: “Quick Reaction Force” (QRF) für unmittelbare und unaufschiebbare strafprozessuale Maßnahmen
> BfV: „Mobile Cyber-Teams“ für Analysen von Fälle mit nachrichtendienstlichem oder extremistischem/terroristischem Hintergrund sowie der Spionage/Sabotage-Abwehr. Im Fokus soll “die technische und fachliche Analyse sowie Bewertung der gegen Bundesbehörden und sonstige Ziele gerichteten Angriffe mit mutmaßlich nachrichtendienstlichem Hintergrund” stehen. Diese Aufgabendefinition umfasst nicht die von BfV-Präsident Maaßen unlängst geforderten Fähigkeiten zum aktiven Hacking-Back[19] bei Cyber-Attacken
> MAD: Analyse von Fällen mit nachrichtendienstlichem oder extremistischem/terroristischem Hintergrund sowie der Spionage/Sabotage-Abwehr im militärischen Bereich
> BND: Beobachtung der Vorbereitung und Durchführung von Angriffen sowie der potentiellen Datenabflüsse

Im Analogie zu den vorangegangenen Anmerkungen über den Ausbau des nationalen Cyber-Abwehrzentrums stellt sich angesichts des Aufbaus dieser vielen Task-Forces die

[19] http://cyber-peace.org/?p=2621

Frage, wie genau die praktische Koordination der Teams in konkreten Situationen erfolgen soll. Das Strategie-Papier betont mehrfach, dass bei Vorfällen im Cyberspace viele unterschiedliche Ebenen und damit die Aufgaben unterschiedlicher Institutionen betroffen sind, lässt hier jedoch offen wie Kompetenzüberschneidungen vermieden werden sollen, wie die Zusammenarbeit der Teams gesetzlich geregelt und die Möglichkeiten der parlamentarischen Kontrolle gewahrt werden sollen.

Ferner ist fraglich und bleibt im Strategiepapier offen, wie die Dienste das entsprechend notwendige Fachkräfte-Personal für ihre zusätzlichen Teams gewinnen wollen. Bislang fällt es selbst den bereits eingerichteten Cyber-Teams beim BKA, den LKAs sowie dem neuen Organisationsbereich der Bundeswehr schwer Fachkräfte zu akquirieren und attraktive Konditionen anzubieten. Es ist daher zu erwarten, dass diese Lücken durch den kostenintensiven Zukauf von externem Personal gefüllt werden und der nationale Sektor für IT-Sicherheitsdienstleistungen zusätzlichen Aufschwung erhalten wird.

Mit Blick auf die Fachkräfte-Situation schlägt die Cyber-Sicherheitsstrategie auch den Aufbau einer zivilen "Cyber-Reserve" nach dem Vorbild ähnlicher Bundeswehr-Planungen[20] vor, mit kurzfristig ausleihbaren Fachkräften aus der Wirtschaft.

Angesichts der technischen Erfordernisse an Hacking- und Analyse-Werkzeugen soll im Rahmen der Cyber-Sicherheitsstrategie 2016 die, dem BMI untergeordnete "*Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) (..) für die technische Unterstützung der Sicherheits- und Fachbehörden des Bundes einschließlich der Nachrichtendienste im Hinblick auf deren operativen Cyber-Fähigkeiten*" geschaffen werden. "*Schwerpunktmäßig ergeben sich die drei Aufgabengebiete Entwicklung, Unterstützung und Beratung der Sicherheitsbehörden. Die zu gründende Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) erarbeitet hierfür in enger Zusammenarbeit mit den genannten Behörden bedarfsbezogen und zukunftsorientiert Methoden, Produkte und (übergreifende) Strategien zur operativen Umsetzung in den Sicherheitsbehörden und entwickelt diese bedarfsgerecht fort.*" Eine solche Einrichtung zur technischen Entwicklung von Hacking-Hilfsmitteln soll möglicherweise auch dazu dienen, langfristig die technischen Abhängigkeiten von Produkten ausländischer Dienste, wie bspw. das auch vom BND[21] eingesetzte NSA-Produkt "XKeyScore", aufzulösen. Kritisch an einer solchen Einrichtung ist unter anderem die Zuständigkeit des Bundesinnenministeriums, dem auch das BSI untergeordnet ist, in dessen Aufgabenbereich nach dem IT-Sicherheitsgesetz von 2016 auch die zentrale Meldestelle von IT-Sicherheitsvorfällen und Sicherheitslücken aus der Wirtschaft fällt. Angesichts des Bedarfs an unbekannten Sicherheitslücken für die Entwicklung von Hacking-Werkzeugen ist zu befürchten, dass ZITiS als Bedarfsträger auf Informationen über gemeldete Cyber-Vorfälle Zugriff nehmen könnte und Sicherheitslücken eher gesammelt als durch das BSI behoben bzw. deren Behebung bei anderen betroffenen Unternehmen koordiniert

[20] http://cyber-peace.org/?p=2385
[21] https://de.wikipedia.org/wiki/XKeyscore

werden. Diese Kritik wurde angesichts der fehlenden Unabhängigkeit des BSI in den vergangenen Jahren immer wieder formuliert und bislang durch nicht ausgeräumt.

Die Cyber-Sicherheitsstrategie enthält in Leitlinie 3 auch einen Hinweis darauf, dass die Bundesregierung Möglichkeiten prüft, die bislang einzige Bundeswehr-Einheit mit offensiven Hacking-Fähigkeiten offiziell einzusetzen. Bislang soll diese sogenannte CNO-Einheit (Computer-Netzwerk-Operationen)[22], die dem Kommando Strategische Aufklärung untergeordnet ist, offiziellen Angaben zufolge nur in abgeschlossenen Übungsnetzwerken trainiert haben - Presseberichte widersprechen dem jedoch. Die Cyber-Sicherheitsstrategie enthält folgenden Verweis auf diese Bundeswehr-Einheit: "*Darüber hinaus sind schwerwiegende Cyber-Angriffe vorstellbar, gegen die mit den klassischen präventiven Maßnahmen in der notwendigen Zeit nicht nachhaltig vorgegangen werden kann. Die Bundesregierung wird daher prüfen, unter welchen rechtlichen Rahmenbedingungen und mit welchen technischen Möglichkeiten in diesen Fällen durch staatliche Stellen Netzwerkoperationen durchgeführt werden könnten"*.

Mit Blick auf die Aufgaben der Bundeswehr attestiert die Cyber-Sicherheitsstrategie, ebenso wie das Weißbuch 2016, dass "*Verteidigungsaspekte der gesamtstaatlichen Cyber-Sicherheit (..) originäre Aufgaben des Bundesministeriums der Verteidigung und der Bundeswehr [sind]. Cyber-Abwehr, Cyber-Außen- und internationale Cyber-Sicherheitspolitik sowie Cyber-Verteidigung sind drei ergänzende Mittel zum Erreichen von Cyber-Sicherheit*" und bekräftigt damit den Anspruch der Bundeswehr bei Krisensituation im Cyberspace unter Umständen auch im Inland tätig zu werden. "*Die Bundeswehr verfügt darüber hinaus über besondere Expertise, Fähigkeiten und Ressourcen, die in Form der Amtshilfe – im Rahmen der verfassungsrechtlichen Grenzen – auch anderen staatlichen Akteuren nutzbar gemacht werden können*".

Zu Leitlinie 4: Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik

Hinsichtlich dieser vierten Leitlinie identifiziert die Cyber-Sicherheitsstrategie 2016 die folgenden Handlungsfelder:

> Eine wirksame europäische Cyber-Sicherheitspolitik aktiv gestalten
> Die Cyber-Verteidigungspolitik der NATO weiterentwickeln
> Cyber-Sicherheit international aktiv mitgestalten
> Bilaterale und regionale Unterstützung und
> Kooperation zum Auf- und Ausbau von Cyber-Fähigkeiten (Cyber Capacity Building)
> Internationale Strafverfolgung stärken

[22] http://cyber-peace.org/?p=2621

Deutschland hat bereits im vergangenen Jahr im Rahmen des OSZE-Vorsitzes Cyber-Sicherheitspolitik als wichtige Aufgabe identifiziert und will diese Prozesse fortsetzen und aktiv mitgestalten.

Hinsichtlich des NATO-Engagements im Cyberspace sind die "*Resilienz des Bündnisses und der Schutz der NATO-eigenen Netze das zentrale Ziel. (..) Ziel ist es, die Resilienz der Alliierten und der Allianz insgesamt kontinuierlich zu erhöhen und nicht zuletzt im Kontext hybrider Bedrohungen die Abschreckungs- und Verteidigungsfähigkeiten zu steigern.*" Damit ist jedoch fraglich ob Abschreckung als Konzept im Cyberspace eine wirksame Komponente darstellt. Die aktuelle Cyber-Strategie des US Verteidigungsministerium[23] bspw. bezeichnet die Attribution im Cyberspace als ein wesentliches Element für eine erfolgreiche Abschreckung. Gleichfalls gilt Attribution nach wie vor als eines der ungelösten und möglicherweise unlösbaren Probleme im Cyberspace, das im besten Falle durch zeit- und ressourcenaufwendige IT-Forensik angegangen werden kann.

Hinsichtlich der Arbeit an völkerrechtlichen Fragen des Cyberspace "*wird sich Deutschland auch weiterhin engagiert an der Klärung zahlreicher neuer Fragestellungen zur Anwendung des Völkerrechts im Cyber-Raum und seiner Weiterentwicklung und für den Erhalt und die Stärkung eines offenen, sicheren und rechtlich gestalteten Cyber-Raums einsetzen*". Dazu zählen laut Cyber-Sicherheitsstrategie die:

> Entwicklung von Normen, Regeln, Prinzipien sowie weiteren Empfehlungen für verantwortliches Staatenverhalten im Cyber-Raum
> Stärkung der Kapazitäten der Vereinten Nationen
> Überlegungen, wie auf globaler Ebene mit dem Problem der Zuordnung von Cyber-Angriffen umgegangen und der in diesem Rahmen essenzielle Informationsaustausch gefördert werden kann
> Stärkung der Exportkontrollregime mit Blick auf Überwachungstechnologien aktiv unterstützen
> Maßnahmen zur Vertrauensbildung [umsetzen, weiterentwickeln und ausbauen]

Hinsichtlich der internationalen Strafverfolgung sowie der Möglichkeiten Cyber-Angriffe zurück zu verfolgen sollen "*unter Ausnutzung ausländischer Systeme (..) regelmäßig auch die Nutzung diplomatischer Kanäle neben Maßnahmen zum Schutz und zur Wiederherstellung der beeinträchtigten Systeme*" in Erwägung gezogen werden.

Ferner wird die "*Gründung eines deutschen Instituts für internationale Cyber-Sicherheit [initiiert]. Dessen Ziel soll es sein, Wirtschaft, Wissenschaft und staatliche Organisationen im Interesse von internationaler Stabilität und Krisenprävention einzubeziehen und Regierungen als verlässlicher und unabhängiger Kompetenzpartner beratend zur Verfügung zu stehen.*"

---

23 https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

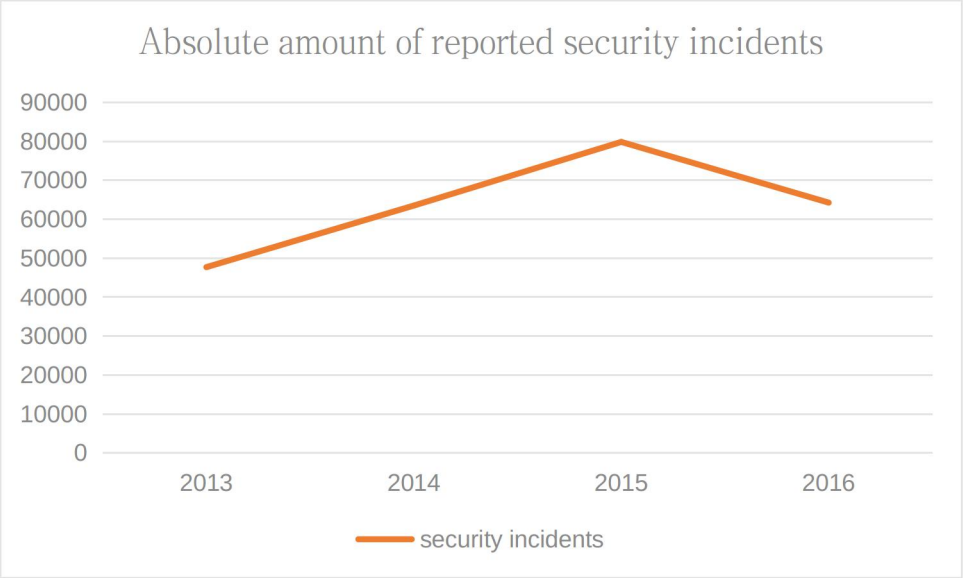
Ähnlich wie die vorangegangenen Überlegungen zur nationalen IT-Zertifizierung und dem Flächenausbau sicherer IT-Geräte und Produkte[24] soll im Rahmen der Cyber-Sicherheitsstrategie eine intensive "*Bilaterale und regionale Unterstützung und Kooperation zum Auf- und Ausbau von Cyber-Fähigkeiten (Cyber Capacity Building)*" durchgeführt werden. "*Cyber-Bedrohungen und -Angriffe können bestimmte Staaten und Bevölkerungsgruppen in ihrer wirtschaftlichen, sozialen und politischen Entwicklung stark einschränken oder zurückwerfen. Deutschland wird ausgewählte Partnerstaaten und -regionen beim Auf- und Ausbau ihrer präventiven und reaktiven Cyber-Sicherheitsfähigkeiten (Netzrobustheit und Netzresilienz) unterstützen. (..) Insbesondere dort, wo Menschen der Erstzugang zum Cyber-Raum dank entwicklungspolitischer Maßnahmen ermöglicht wird, müssen die Rahmenbedingungen und Kenntnisse für seine sichere und verlässliche Nutzung unterstützt werden.*" Diese Maßnahmen sind insofern wichtig und wirkungsvoll, da der Cyberspace als Allmende[25] verstanden werden kann, an dessen Sicherung, Erhalt und Ausbau alle beteiligten internationalen Akteure Interesse haben und von dessen stabiler Funktion alle profitieren. Ebenso basiert der Cyberspace auf einigen stark zentralisierten und eng vernetzen Prinzipien wie dem sog. Domain Name System[26] (DNS). Angriffe gegen zentrale DNS-Server (die sog. Root-Name-Server) oder zentrale DNS-Dienstleister können unmittelbar große Teile des Internet unerreichbar machen und aufgrund der Abhängigkeiten zwischen kritischen Infrastrukturen zu massiven Bedrohungen werden.

[24] Siehe Leitlinie 1
[25] https://de.wikipedia.org/wiki/Allmende
[26] https://de.wikipedia.org/wiki/Domain_Name_System

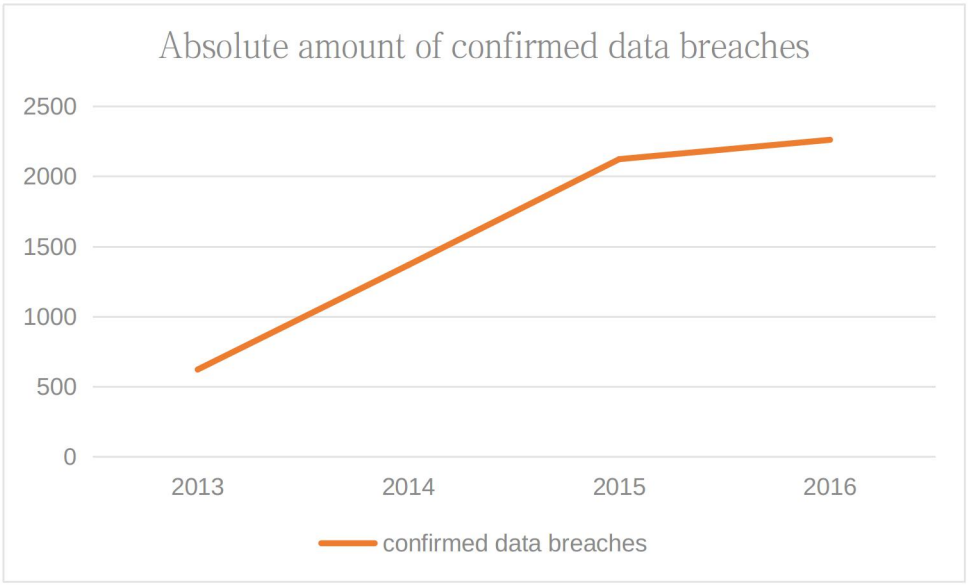
Anhang: Vergleich der Cyber-Vorfälle in den Verizon Data Breaches Reports

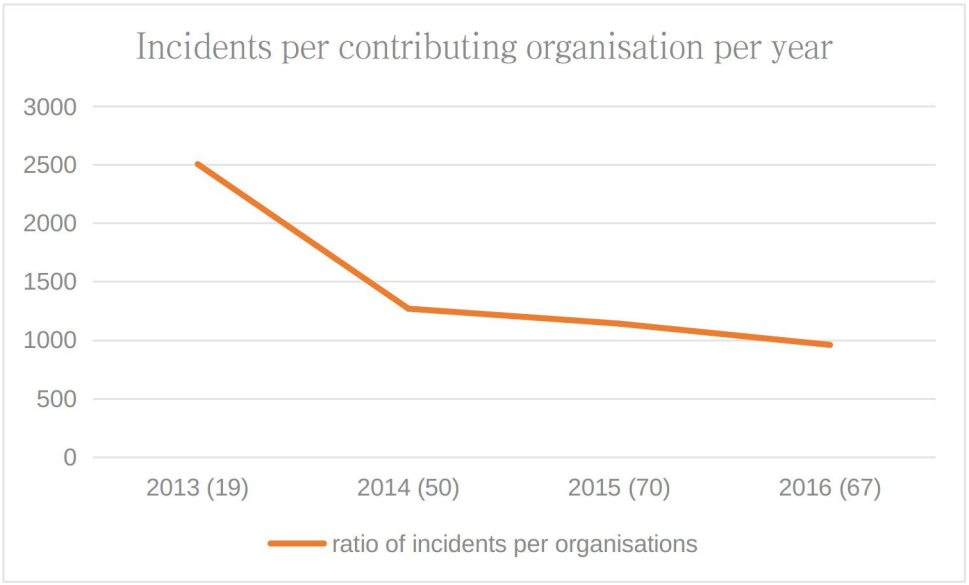
Die vom US-amerikanischen IT-Dienstleister Verizon herausgegebene Data Breach Reports[27] enthalten stellen seit Jahren die gesammelten Informationen über Cyber-Vorfälle, die davon betroffenen Wirtschafts-Sektoren und deren Schäden zusammen. Zu den Reports tragen unzählige internationale unabhängige Organisationen und IT-Sicherheitsfirmen bei und die Auswertungen haben ein hohes internationales Renommee.

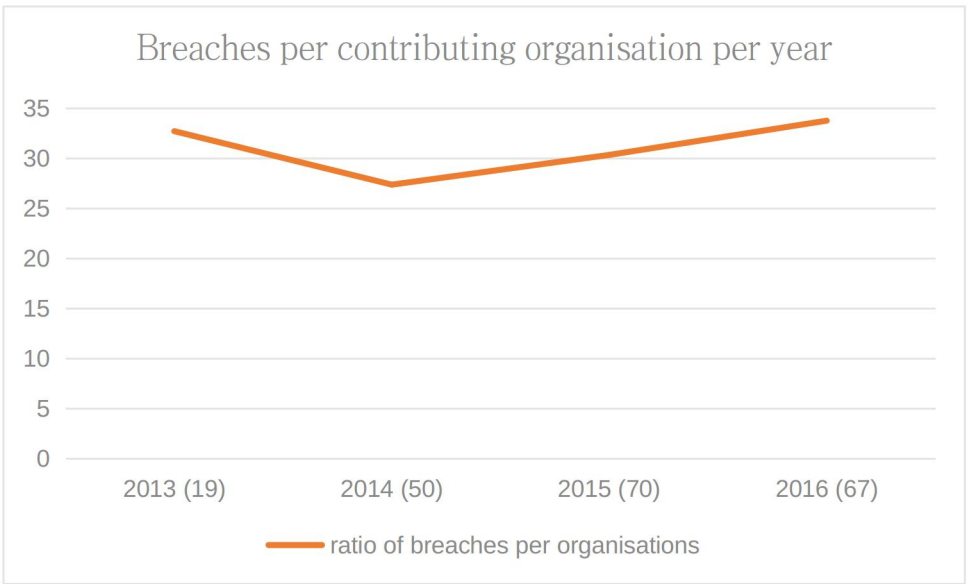
Die Analysten der Reports haben im Jahr 2013 unter anderem aufgrund der veränderten "Welt" digitaler Geräte und damit der typischen Cybervorfälle die Art und Weise ihrer Datenauswertung umgestellt. Die nachfolgenden Grafiken stellen daher für die vergangenen vier Jahre die reine Anzahl an gemeldeten Vorfällen (Incidents) und bestätigten Daten-Abflüssen (Breaches) einer Auswertung dieser absoluten Zahlen gemessen an der Anzahl an beteiligten Organisationen, die pro Jahr Informationen gemeldet haben gegenüber (Die Zahl in Klammern an der Jahres-Achse).



[27] http://www.verizonenterprise.com/verizon-insights-lab/dbir/


Absolute amount of confirmed data breaches
2500
2000
1500
1000
500
0
2013
2014
2015
2016
confirmed data breaches


Incidents per contributing organisation per year
3000
2500
2000
1500
1000
500
0
2013 (19)
2014 (50)
2015 (70)
2016 (67)
ratio of incidents per organisations


Breaches per contributing organisation per year
35
30
25
20
15
10
5
0
2013 (19)
2014 (50)
2015 (70)
2016 (67)
ratio of breaches per organisations