DSI | DIGITAL SOCIETY INSTITUTE BERLIN

ESMT BERLIN

DSI Industrial & Policy Recommendations (IPR) Series

Cybersicherheit 2018-2020: Handlungsvorschläge für CDU/CSU und SPD

Martin Schallbruch, Sandro Gaycken, Isabel Skierka (Digital Society Institute, ESMT Berlin)

Ausgabe 1, 2018

1. Ausgangslage

(a) Unkalkulierbares Risiko Cybersicherheit

Von 2013 bis 2017 hat sich die Lage der Cybersicherheit dramatisch verschlechtert. Während die Durchdringung aller Lebensbereiche mit digitaler Technologie immer schneller voranschreitet, ist die Qualität der Technologie in der Fläche nicht besser geworden. Unsichere Produkte aus der Office-Welt werden zunehmend auch in industriellen Anlagen eingesetzt. Neue Bereiche der Digitalisierung wie SmartHome oder IoT sind durch low-cost-Produkte mit erheblichen Sicherheitsmängeln gekennzeichnet. Hoher Druck durch Investoren zwingt Startups zu schneller Entwicklung ohne Qualitätssicherung, selbst in Bereichen mit höchsten Sicherheitsanforderungen wie Gesundheit und Finanzen. Komplexität der IT und Vernetzung wachsen ungebremst und erhöhen Unsicherheit exponentiell. Die Effektivität von Sicherheitsprodukten ist immer weniger belastbar; durch eigene Sicherheitslücken werden sie selbst zu Risiken. Trotz immer höherer Investitionen in IT-Sicherheit werden Risiken nicht messbar reduziert.

Gleichzeitig nehmen die Angriffe zu und werden immer gravierender. Gigantische Datendiebstähle und Erpressungsangriffe mit massenhaften Datenverlusten sind an der Tagesordnung. Kritische Infrastrukturen und Produktionsstraßen werden zunehmend angegriffen – einschließlich ihrer Mechanismen für Unfallschutz. Nachrichtendienstliche Angriffswerkzeuge gehen verloren. Alltagsgegenstände werden zu Angriffsplattformen.

Das exponentielle Wachstum der Verwundbarkeiten, die schlechte Effektivität der Sicherheitstechnik und die vielen Optionen für Angreifer lassen auf unabsehbare Zeit unklar, was Cybersicherheit ist und wie sie herzustellen ist. Cybersicherheit ist Bedingung der Digitalisierung und gleichzeitig ein unkalkulierbares Risiko für Wirtschaft und Gesellschaft.

(b) Politische Umsetzungsdefizite

Von 2013 bis 2017 konnten auf globaler Ebene bei der Cybersicherheit keine Fortschritte erzielt werden. Die Verhandlungen in der UNO sind gescheitert, multilaterale Anstrengungen und Multi-Stakeholder-Prozesse erzielten keine wirksamen Ergebnisse. Auf EU- und nationaler Ebene sind nur kleine Fortschritte erzielt worden. Die Verpflichtung kritischer Infrastrukturen zu Cybersicherheitsmaßnahmen und die Umsetzung der Datenschutz-Grundverordnung erzwingen für viele Unternehmen eine gründlichere Auseinandersetzung mit Cybersicherheit, heben aber aufgrund der niedrig angelegten Schutzziele, der Interpretationsoffenheit der Regelungen und der Implementierungsunsicherheiten die IT-Sicherheit faktisch nur auf ein geringfügig höheres Niveau. Die Sicherheitsbehörden sind mit besseren Befugnissen, mehr Personal und besseren Ausstattungen bedacht worden, aufgrund der dramatisch schlechten Personalsituation in der IT-Sicherheit und einem unterentwickelten Zuliefermarkt dennoch nur sehr begrenzt effizienter geworden. Eine Steigerung europäischer und nationaler Souveränität bei digitalen Technologien ist nicht feststellbar. Die Zusammenarbeit zwischen den Sicherheitsbehörden und zwischen Staat und Wirtschaft bei der Cyberabwehr ist nur marginal verbessert, Kompetenzgerangel kennzeichnet die gegenwärtige Cybersicherheitsarchitektur.

(c) Politische Chancen

Deutschland hat große Chancen, im Zeitraum 2018-2020 bei der Cybersicherheit entscheidend voranzukommen. Die gute wirtschaftliche Lage und die günstige Haushaltslage von Bund und Ländern erlauben erhebliche Investitionen in Cybersicherheit und sichere Digitalisierung. Cybersicherheitspolitik wird in einer großen Koalition im Bund politisch kaum strittig sein. Wesentliche Lebensbereiche werden in den kommenden Jahren grundlegend digitalisiert und bieten die Option, von Grund auf sichere Technologien zu entwickeln, ökonomisch zu skalieren und als Standards zu etablieren: die Verkehrssysteme, das Gesundheitswesen, die Energieversorgung, kommunale Infrastrukturen, staatliche Dienstleistungen.

Schon der Koalitionsvertrag von CDU/CSU und SPD im Jahr 2013 hatte die Cybersicherheit prominent adressiert, allerdings große Teile der damaligen Vorhaben noch nicht umgesetzt (siehe auch die Auswertung des Koalitionsvertrages 2013 im Anhang).

(d) Wirtschaftliche Chancen

Das Paradigma einer zuverlässig sicheren Digitalisierung kann globale wirtschaftliche Opportunitäten realisieren und einen glaubhaften und eigenen USP für die deutsche Wirtschaft auf den technischen Märkten etablieren. Die deutsche Wirtschaft kann in Kooperation mit dem Bund viele sinnvolle Entwicklungs- und Investitionsvorhaben umsetzen, allerdings muss die Effektivität der Sicherheitstechnik belegbar werden und der IT-Sicherheitsmarkt muss sehr viel dynamischer entwickelt werden.

2. Ziele

Die Cybersicherheitspolitik einer neuen Koalition im Bund sollte sechs Schwerpunkte setzen:

(a) Beweisbar sichere Technologien fördern

Nur mit einer langfristig angelegten Politik der Forderung und Förderung sicherer Technologien kann das Problem der Cybersicherheit gelöst werden. Die Forschungsanstrengungen und die Förderung der Industrialisierung hochsicherer Lösungen müssen erheblich verstärkt werden. Kern müssen Technologien und Systeme mit beweisbarer Sicherheit darstellen. Hype-Themen wie Big Data, KI oder Blockchain, die eher undeutlich oder kleine Beiträge zur Reduzierung der Cyberrisiken leisten, müssen kompetenter bewertet werden.

(b) IT-Sicherheit von Produkten gesetzlich vorschreiben

Die Verwundbarkeit der IT entsteht durch schlechte technische Qualität, die weitgehend vermeidbar wäre, deren Vermeidung allerdings kostenintensiv ist. Die mangelnde Regulierung dieser Qualitätsdefizite spart der IT-Industrie Entwicklungskosten auf Kosten der Sicherheit der privaten und industriellen IT-Anwender. Die Haftung für mangelnde Qualität muss daher verschärft werden, verfügbare Methoden der Qualitätssicherung und der Vermeidung von Schwachstellen gesetzlich vorgeschrieben werden.

Für die Digitalisierung von Technologien mit Gefahrenpotential für Leib und Leben müssen zwei Prinzipien festgehalten werden: (1) Safety First – Schutzmechanismen für Leib und Leben (Safety) dürfen in keiner Weise digital angreifbar sein. Ihre Cybersicherheit muss priorisiert und darf nur durch belegbar sichere Technologien als erfüllbar gelten. (2) Der Schutz von IT-Systemen gegen Angriffe und der Schutz gegen Unfälle muss gleich hoch sein, die Schutzziele beider Sicherheiten müssen kohärent sein.

(c) Sicherheit in Großprojekten der Digitalisierung kohärent festlegen

Digitalisierungsprojekte des Staates und der Wirtschaft sollten auf sicheren Architekturen beruhen und eine Nutzung hochsicherer Technologien vorsehen. Das betrifft beispielsweise die Digitalisierung von Verkehrssystemen, Gesundheitsversorgung, Energieversorgung, Gebäudetechnik und Industrieanlagen. Einer staatlichen Förderung von Marktlösungen mit besonders hohem Sicherheitsniveau sollte der Vorzug vor Eigenentwicklungen gegeben werden. Investitionen in Digitalisierungsprojekte des Staates sollten zugleich die parallele Entwicklung besonders vielversprechender IT-Sicherheitstechnologien fördern, so dass deren bessere Skalierung und Abnahme im Markt gewährleistet wird.

(d) Cyberabwehr besser koordinieren

Die Kompetenzstreitigkeiten bei der Cyberabwehr sollten durch eine neu definierte gemeinsame Struktur von

Bund (einschließlich Bundeswehr), Ländern und Wirtschaft gelöst werden. Es ist zu früh, eine abschließende und langfristige Definition der Cybersicherheitsarchitektur zu finden. Daher sollten die bisherigen Strukturen erhalten, jedoch besser (und straffer) koordiniert werden. Die Zusammenarbeit mit der Wirtschaft sollte auch operativ massiv ausgebaut werden.

(e) Offensive Fähigkeiten aktiv adressieren

Cyberwaffen sind – richtig entwickelt und gebraucht – ideale, nicht-letale militärische Wirkmittel. Sie können entscheidende Beiträge liefern, Konflikte frühzeitig zu vermeiden oder technisch undurchführbar zu machen. Hohe Abschreckungspotentiale oder über einen Cyberangriff abgeschaltete Waffensysteme helfen Kriege weniger gewaltsam zu machen. In der Strafverfolgung und nachrichtendienstlichen Aufklärung können Fähigkeiten des gezielten Hacking, eingebettet in sorgfältig gesetzten Befugnissen, eine hohe Zahl wertvoller Erkenntnisse liefern und helfen Verbrechen aufzuklären, zu vermeiden und Schäden zu reduzieren.

(f) Internationale Vorreiterrolle in Sicherheit und Datenschutz

Nach dem Scheitern der UNO-Bemühungen um Verbindlichkeit in der internationalen Cybersicherheit sollte sich Deutschland gemeinsam mit Frankreich, unseren europäischen Partnern und anderen Staaten um bilaterale Abkommen für verantwortungsvolles Verhalten der Staaten im Cyberraum mit einer eigenen Normenpolitik bemühen. Wir könnten den Startschuss geben für eine verstärkte internationale Akzeptanz von Regeln im Cyberraum. Dazu gehört auch die stärkere Verankerung des Schutzes der Privatheit in der internationalen Cyberpolitik. Datenschutz muss als Menschenrecht anerkannt, digitale Überwachungsstaaten von der Außenpolitik sichtbar gemacht und angeklagt werden.

3. Handlungsfelder

Zur Erreichung der oben genannten Ziele werden für die Koalitionsvereinbarung von CDU/CSU und SPD zehn Handlungsfelder vorgeschlagen:

(a) Sichere Technologien

1. Wir werden die Hersteller von Hardware und Software verpflichten, dem Einsatzzweck entsprechende, belegbar sichere Sicherheitsmaßnahmen zu ergreifen sowie für die Sicherheit ihrer Produkte längerfristig einzustehen, insbesondere Sicherheitsupdates und Sicherheitsinformationen bereitzustellen. Wer Geräte herstellt oder vertreibt, die zum Anschluss an das Internet gedacht sind, muss besondere Sorgfalt obwalten lassen. Die IT-Sicherheit digitaler Systeme mit Gefährdungspotential für Leib und Leben muss auf belegbar sicheren Ankern beruhen.

2. Wir werden die Förderung der Forschung und Entwicklung hochsicherer, insbesondere beweisbarer IT-Systeme erheblich ausbauen und in allen IT-Förderprogrammen die Berücksichtigung von Hochsicherheit begünstigen. Unternehmen, die nachvollziehbare Planungen zur Markteinführung hochsicherer Lösungen vorlegen, werden mit Investitionszuschüssen und Ausfallbürgschaften gefördert. Wir werden Anreize für Investoren zur Beteiligung an IT-Sicherheitsunternehmen schaffen. Voraussetzung sind belegbare Sicherheitseigenschaften der Produkte.

(b) Sichere Architekturen für die Digitalisierung

3. Wir werden Anbieter vertrauenswürdiger, europäischem Datenschutz- und IT-Sicherheitsrecht in besonderem Maße entsprechender Dienste fördern und diese bei staatlicher Beschaffung und in Infrastrukturprojekten (z.B. Verkehr, Gesundheit, Bildung, Energie) bevorzugt berücksichtigen. Für staatliche Anwendungen werden Vertrauens- und Zahlungsdienste europäischer Anbieter genutzt.

4. Wir werden das IT-Sicherheitsrecht um weitere Branchen erweitern und auch die öffentliche Verwaltung einbeziehen. Für IT-Systeme für wichtige staatliche Funktionen (z.B. Wahlen, Steuerverwaltung) sollen Sicherheitsbewertungen transparent gemacht werden.

5. Wir werden ein KfW-Förderprogramm „IT-Sicherheit der Industrie“ aufsetzen, welches nach dem Vorbild der Förderprogramme zur Energieeinsparung mit Beratungsleistungen, Investitionszuschüssen und zinsverbilligten Darlehen IT-Sicherheitsmaßnahmen in Unternehmen unterstützt. Dabei begünstigen wir Hochsicherheitstechnologien.

(c) Cyberabwehr besser koordinieren

6. Die Cyberabwehr werden wir gemeinsam mit den Ländern und der Wirtschaft umfassend neu organisieren. Wir stärken Polizeien, Nachrichtendienste und BSI in der Weiterentwicklung ihrer Cyberfähigkeiten und schaffen gleichzeitig eine Koordinierungseinheit für Cyberabwehr mit eigenem Personalkörper, in welche die Bundeswehr, Sicherheitsbehörden des Bundes und der Länder sowie Gemeinschaftseinrichtungen der Wirtschaft eingebunden sind. In ihr gehen die bisherigen Zusammenarbeitsstrukturen auf.

7. Wir schaffen eine gesetzliche Grundlage für die Sicherheitsbehörden des Bundes, zur Abwehr konkreter, von einem Cyberangriff ausgehender Gefahren für Leib und Leben oder die freiheitlich demokratische Grundordnung, aktive Maßnahmen der Cyberabwehr zu ergreifen. Bundeswehr und Sicherheitsbehörden werden ihre offensiven Fähigkeiten in enger Abstimmung miteinander und unter Beteiligung des Deutschen Bundestages und unabhängiger Experten ausbauen.

8. Die Nutzung von Schwachstellen in Hardware und Software schafft erhebliche Risiken für die Cybersicherheit. Soweit staatliche Stellen solche Schwachstellen für ihre Aufgaben nutzen, soll dies in einen gesetzlich geregelten Abwägungsprozess eingebunden sein.

(d) Spitzenkompetenz für Cybersicherheit

9. Der Bund wird den Ländern, der Wirtschaft und den Gewerkschaften ein Programm zur Förderung von Spitzenkompetenz in der Cybersicherheit vorschlagen, das Ausbildung, Weiterbildung, gemeinsame Personalentwicklung, Personaltausch zwischen Staat und Wirtschaft sowie Ausnahmeregelungen im Dienst- und Tarifrecht umfasst.

(e) Internationale Vorreiterrolle

10. Deutschland wird gemeinsam mit Frankreich, unseren europäischen und anderen internationalen Partnern einen Musterkodex für verantwortliches staatliches Verhalten im Cyberraum entwickeln und in bilaterale Verhandlungen und multilaterale Vereinbarungen einbringen. Der Kodex wird auch eindeutige Absagen an menschenrechtswidrige Massenüberwachungen und propagandistische Manipulationen demokratischer Prozesse enthalten.

Anhang

Koalitionsvertrag von CDU/CSU und SPD 2013, Aussagen zur IT-Sicherheit

Was wurde nicht, teilweise, ganz umgesetzt?

Eine zentrale Meldestelle für Phishing und ähnliche Delikte soll die Prävention verbessern und Ermittlungen erleichtern.

IT-Infrastruktur und digitaler Datenschutz
Wir schaffen ein IT-Sicherheitsgesetz mit verbindlichen Mindestanforderungen an die IT-Sicherheit für die kritischen Infrastrukturen und der Verpflichtung zur Meldung erheblicher IT-Sicherheitsvorfälle. Dafür setzen wir uns auch auf der EU-Ebene im Rahmen der europäischen Cybersicherheitsstrategie ein.

Um Freiheit und Sicherheit im Internet zu schützen, stärken und gestalten wir die Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum. Dazu treten wir für eine europäische Cybersicherheitsstrategie ein, ergreifen Maßnahmen zur Rückgewinnung der technologischen Souveränität, unterstützen die Entwicklung vertrauenswürdiger IT- und Netz-Infrastruktur sowie die Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie und begrüßen auch Angebote eines nationalen bzw. europäischen Routings.

Wir bauen die Kapazitäten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und auch des Cyber-Abwehrzentrums aus. Wir verbessern die IT-Ausstattung der deutschen Sicherheitsbehörden.

Um Bürgerdaten besser zu schützen und zu sichern, werden wir die Bündelung der IT-Netze des Bundes in einer einheitlichen Plattform „Netze des Bundes“ anstreben. IT- und TK-Sicherheit wollen wir zusammenführen.

Die Bundesbehörden werden verpflichtet, zehn Prozent ihrer IT-Budgets für die Sicherheit ihrer Systeme zu verwenden.

Um Vertrauen wieder herzustellen müssen die Standardisierungsgremien transparenter werden. Zudem muss sich Deutschland stärker in diesen und anderen internationalen Gremien beteiligen, besonders solchen der Internetarchitektur und Internet-Governance.

Wir prüfen, inwieweit ein Ausverkauf von nationaler Expertise und Know-how in Sicherheits-Schlüsseltechnologien verhindert werden kann.

Wir initiieren ein Spitzencluster „IT-Sicherheit und kritische IT-Infrastruktur".

Um zu gewährleisten, dass die Nutzerinnen und Nutzer über die Sicherheitsrisiken ausreichend informiert sind, sollen Internetprovider ihren Kunden melden, wenn sie Hinweise auf Schadprogramme oder ähnliches haben. Darüber hinaus streben wir einen sicheren Rechtsrahmen und eine Zertifizierung für Cloud-Infrastrukturen und andere sicherheitsrelevante Systeme und Dienste an.

Zur Wahrung der technologischen Souveränität fördern wir den Einsatz national entwickelter IT-Sicherheitstechnologien bei den Bürgerinnen und Bürgern.

Die Weiterentwicklung und Verbreitung von Chipkartenlesegeräten, Kryptographie, DE-Mail und sicheren Ende-zu-Ende-Verschlüsselungen sowie vertrauenswürdiger Hard- und Software gilt es erheblich auszubauen.

IT-Hersteller und -Diensteanbieter sollen für Datenschutz- und IT-Sicherheitsmängel ihrer Produkte haften.

Wir wollen das vom Bundesverfassungsgericht entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme mit Leben füllen. Die Nutzung von Methoden zur Anonymisierung, Pseudonymisierung und Datensparsamkeit müssen zu verbindlichen Regelwerken werden.

Die DSI Industrial & Policy Recommendations (IPR) Series wird herausgegeben vom Digital Society Institute der ESMT Berlin, http://dsi.esmt.org.