DSI | DIGITAL SOCIETY INSTITUTE BERLIN

ESMT BERLIN

DSI Industrial & Policy Recommendations (IPR) Series

Cybersecurity 2018–2020: Proposals for action for the CDU/CSU and SPD

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

Issue 1, 2018

1. Initial situation

(a) Incalculable cybersecurity risk

From 2013 to 2017, cybersecurity has deteriorated dramatically. While the penetration of all areas of life with digital technology is advancing ever faster, the quality of technology has not improved. Unsafe products from the office world are increasingly being used in industrial plants. New areas of digitalization such as the "Smart Home" and the "Internet of Things" (IoT) are characterized by low-cost products with significant safety flaws. High pressure from investors forces startups to develop quickly without quality assurance, even in areas with the highest security requirements, such as health and finance. The complexity of IT and networking is growing unchecked and growing insecurity exponentially. The effectiveness of IT security products is less and less resilient; through their own security vulnerabilities, they themselves become risks. Despite increasing investments in IT security, risks are not measurably reduced.

At the same time, cyber attacks are increasing and becoming more serious. Gigantic data theft and extortion attacks with massive data loss are commonplace. Critical infrastructures and production lines are increasingly under attack – including their accident prevention mechanisms. Intelligence cyberattack tools are lost. Everyday items become cyberattack platforms.

The exponential growth of vulnerabilities, the poor effectiveness of security technology, and the many options for cyber attackers make it unforeseeable for an indefinite time what cybersecurity is and how to create it. Cybersecurity is a pre-condition for digitization and at the same time poses an incalculable risk to the economy and society.

(b) Political implementation deficits

From 2013 to 2017, no progress could be made on cybersecurity at the global level. Negotiations at the UN have failed; multilateral efforts and multi-stakeholder processes have not produced effective results. Little progress has been made at EU and national levels. The commitment of critical infrastructures to cybersecurity measures and the implementation of the General Data Protection Regulation will force cybersecurity to be more thoroughly debated in many companies. In reality, it will only slightly raise the level of IT security, due to low protection goals as well as lack of clarity and uncertainties of regulations and implementation. Security authorities have assumed better powers, more staff, and better equipment, but have become very limited in their efficiency due to the dramatically poor staffing of IT security and an underdeveloped supply market. There is no discernible increase in European and national digital sovereignty. Collaboration between security agencies and between the state and industry on cyber defense has only marginally improved – the current cybersecurity architecture is characterized by competence wrangling.

(c) Political opportunities

Germany has great opportunities to make decisive progress in cybersecurity in the period 2018–2020. The good economic situation and the favorable budgetary situation of its federal and state governments allow considerable investments in cybersecurity and secure digitization. The cybersecurity policy of federal government's grand coalition will hardly be politically

controversial. Essential areas of life will be fundamentally digitized in the coming years and offer the option to develop, economically scale, and standardize safe technologies from the ground up: transport systems, health care, energy, municipal infrastructure, and government services.

Even the coalition agreement of the CDU/CSU and SPD in 2013 had prominently addressed cybersecurity but did not yet implement large parts of the former projects. (See also the evaluation of the coalition agreement 2013 in the annex.)

(d) Economic opportunities

The paradigm of reliable secure digitization can realize global economic opportunities and establish a credible and unique selling proposition for the German business community in technical markets. German industry, in cooperation with the federal government, can implement many meaningful development and investment projects. But the effectiveness of security technology must become verifiable, and the IT security market.

2. Objectives

The cybersecurity policy of a new coalition in the federal government should set six priorities:

(a) Promote demonstrable secure technologies

The issue of cybersecurity can only be resolved with a long-term policy of demanding and promoting secure technologies. Research efforts and the promotion of the industrialization of highly secure solutions need to be significantly strengthened. The core must be technologies and systems with verifiable security. Hot topics such as big data, AI, or blockchain, which make rather indistinct or small contributions to the reduction of cyber risks, must be assessed more competently.

(b) Legally require IT security of products

The vulnerability of IT arises from poor technical quality, which would be largely avoidable, but whose avoidance is costly. The lack of regulation of these quality deficiencies saves the IT industry development costs at the expense of the safety of private and industrial IT users. The liability for poor quality must be therefore strengthened, and available methods of quality assurance and the prevention of vulnerabilities must be required by law.

Two principles must be established for the digitization of technologies that hold potential danger for life and limb: (1) Safety first – protection mechanisms for health and safety must be in no way digitally vulnerable. Their cybersecurity needs to be prioritized and can only be considered as achievable through verifiably secure technologies. (2) The protection of IT systems against attacks and the protection against accidents must be the same; the protection objectives of both collaterals must be coherent.

(c) Coherently define security in large-scale digitization projects

State and business digitization projects should be based on secure architectures and use high-security technologies. This concerns, for example, the digitization of transport systems, health care, energy supply, building technology, and industrial facilities. State support for market solutions with a particularly high level of security should be given preference over in-house developments. Investments in state digitization projects should also foster the parallel development of particularly promising IT security technologies, ensuring their better scaling and market acceptance.

(d) Better coordinate national cyber defense

The competence disputes in cyber defense should be solved by a newly defined joint structure of the federal government (including the armed forces), the state governments, and industry. It's too early to find a final and long-term definition of cybersecurity architecture. Therefore, the previous structures should be preserved, although better coordinated (and tighter). Cooperation with the private sector should also be massively expanded.

(e) Actively address offensive capabilities

When properly developed and used, cyber weapons are ideal, non-lethal military weapons. They can provide crucial input to avoid conflicts at an early stage or make them technically impracticable. High deterrence potential or cyberattack weapon systems can help to make warfare less violent. In law enforcement and intelligence work, the capabilities of targeted hacking, embedded in carefully defined powers and authorities,

can provide a wealth of valuable insight and help clear up and prevent crime, and reduce damage.

(f) Establish international leadership in security and privacy

Following the failure of UN efforts to commit itself to international cybersecurity, Germany should work with France, our European partners, and other states for bilateral agreements on responsible behavior by states in cyberspace. We could give the go-ahead for greater international acceptance of rules in cyberspace. This includes strengthening the protection of privacy in international cyber policy. Data protection must be recognized as a human right, and digital surveillance states should be denounced on the world stage.

3. Action areas

In order to achieve the above goals, ten action areas are proposed for the CDU/CSU and SPD coalition agreement:

(a) Secure technologies

1. We will oblige manufacturers of hardware and software to take appropriate security measures in line with the product's intended purpose and to ensure the long-term security of their products, in particular, to provide security updates and security information. Anyone who manufactures or sells equipment that is intended for connection to the internet must take special care. The IT security of digital systems with the potential to threaten health and life must be based on proven safe anchors.

2. We will significantly expand the promotion of research and development of highly secure, especially verifiable IT systems and promote the consideration of high security in all IT support programs. Companies that present transparent plans for the market introduction of highly secure solutions are supported by investment grants and loss guarantees. We will create incentives for investors to invest in IT security companies. A prerequisite are verifiable safety features of the products.

(b) Secure architectures for digitization

3. We will promote providers of trustworthy services, which are compliant with European data protection and IT security law, and give them a high degree of preference and priority in government procurement and infrastructure projects (such as transport, health, education, energy). For government IT services, European trust and payment service providers will be used.

4. We will extend IT security legislation to other industries and also cover the public administration. For IT systems of important state functions (e.g., elections, tax administration), security assessments should be made transparent.

5. We will set up a KfW "IT Security Industry" funding program that supports IT security measures in companies (following the example of the energy-saving promotion programs) with consulting services, investment subsidies, and low-interest loans. We favor high-security technologies in this program.

(c) Better coordinate national cyber defense

6. We will completely reorganize cyber defense together with state governments and industry. We will strengthen the police forces, intelligence services, and the Federal Office for Information Security (BSI) in the further development of their cyber capabilities and, at the same time, will create a coordination unit for cyber defense with its own personnel, which integrates the military, security agencies of the federal and state governments as well as the private sector. It will incorporate existing cooperation structures.

7. We will create a legal basis for the federal security authorities to take active cyber-defense measures in cases of concrete dangers (to life and limb or the free democratic order) that emanate from a cyber attack. Military and security agencies will develop their offensive capabilities in close cooperation with each other, with the participation of the federal government and independent experts.

8. The use of hardware and software vulnerabilities creates significant cybersecurity risks. To the extent that government authorities use such vulnerabilities for the performance of their duties, this should be included in a statutory vulnerability equities process.

(d) Expertise for cybersecurity

9. The federal government will propose to state governments, business, and trade unions a program to promote cybersecurity expertise, comprising school education, professional training, joint human resources development, staff exchanges between government and business, and exemptions from civil service law.

(e) International leadership

10. Germany will work with France as well as our other European and international partners to develop a model code of good governance in cyberspace and to engage in bilateral negotiations and multilateral agreements. The code will also contain clear rejections of mass human rights violations and propaganda manipulations of democratic processes.

Annex

Coalition agreement of the CDU/CSU and SPD 2013, statements on IT security

What was not, partially, or fully implemented?

A central office for phishing and similar offenses should improve prevention and facilitate investigations.

IT infrastructure and digital data protection

We will create an IT security law with binding minimum requirements for IT security for critical infrastructures and the obligation to report significant IT security incidents. We are also committed to this at the EU level as part of the European cybersecurity strategy.

In order to protect freedom and security on the internet, we will strengthen and design the internet infrastructure of Germany and Europe as a trusted space. Therefore we are in favor of a European cybersecurity strategy, take action for recovery of technological sovereignty, support the development of trusted IT and network infrastructure as well as the development of secure software and hardware and secure cloud technology, and also welcome offers of national as well as European routing.

We are building the capacities of the BSI and the Cyber Defense Center. We will improve the IT equipment of the German security agencies.

In order to better protect and safeguard citizen data, we will strive to bundle the federal IT networks in a uniform "Federal Network" platform. We want to merge IT and telecommunications security.

Federal agencies will be required to use ten percent of their IT budgets for the security of their systems.

To restore confidence, standardization bodies must become more transparent. In addition, Germany must become more involved in these and other international bodies, especially those of internet architecture and internet governance.

We will examine the extent to which a sale of national expertise and know-how in key security technologies can be prevented.

We will initiate a top-level research cluster called "IT security and critical IT infrastructure".

To ensure that users are adequately informed about the security risks, internet service providers should re-port to their customers if they have evidence of mal-ware or the like. In addition, we will strive for a secure legal framework and a certification for cloud infra-structures and other security-related systems and ser-vices.

To safeguard technological sovereignty, we encour-age the use of nationally developed IT security tech-nologies by citizens.

The further development and distribution of chip card readers, cryptography, DE-Mail (the German e-government communications service), secure end-to-end encryption, and trustworthy hardware and software need to be considerably expanded.

IT manufacturers and service providers should be liable for data privacy and IT security flaws in their products.

We want to bring to life the right to guarantee confidentiality and integrity of information technology systems developed by the Federal Constitutional Court. The use of methods for anonymization, pseudonymization, and data economy must become binding rules.

The DSI Industrial & Policy Recommendations (IPR) Series is published by the Digital Society Institute of ESMT Berlin, http://dsi.esmt.org.

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.