Positionspapier der Arbeitsgruppe Inneres und der Arbeitsgruppe Digitale Agenda der SPD-Bundestagsfraktion

IT-Sicherheitsgesetz 2.0 muss das digitale Immunsystem stärken

Die Stärkung der IT-Sicherheit und die Wahrung der Vertraulichkeit der digitalen Kommunikation ist die zentrale Grundvoraussetzung für den Erfolg der digitalen Gesellschaft. Die vielen bekannt gewordenen Angriffe auf Unternehmen, den Deutschen Bundestag oder das Regierungsnetz, haben in aller Deutlichkeit die Verletzlichkeit der digitalen Gesellschaft aufgezeigt. Zuletzt haben die bislang vorliegenden Erkenntnisse zu dem Datenleak zum Jahreswechsel 2018/19, bei dem persönliche Daten hunderter von Politikern, Journalisten und Personen des öffentlichen Lebens ausgespäht und veröffentlicht wurden, gezeigt: Dem Schutz und der Sicherheit personenbezogener Daten aufseiten der Anbieter, aber auch aufseiten der Nutzer von Internetdiensten fehlt die notwendige Aufmerksamkeit. Der Vorfall hat auch deutlich gemacht, dass nach wie vor zentrale rechtliche Vorgaben, etwa zum aktuellen Stand der Technik oder zu Privacy-by-Design, zu wenig Beachtung finden. Dazu kommt noch immer ein erschreckender Mangel an planvollem und abgestimmtem Umgang der Behörden der Länder und des Bundes sowie innerhalb der Europäischen Union im Fall von Meldungen und Anzeigen von cyberkriminellen Vorfällen. So konnten offensichtlich Angriffe wie der jüngste Datenklau nicht in einen Kontext gebracht und Angriffsmuster nicht erkannt werden.

Zwar hat das Bundesverfassungsgericht bereits 2008 das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) festgeschrieben. Leider ist es der Politik jedoch bis heute nicht gelungen, dieses neue Grundrecht mit Leben zu füllen und daraus ein umfassendes Regelungsregime zum Schutz der persönlichen IT-Systeme zum Schutz der digitalen Identität zu entwickeln. Das IT-Grundrecht verankert IT-Sicherheit als verfassungsrechtliche Gewährleistungspflicht des Staates, welches ggfs. um den Schutz der digitalen Identität erweitert werden muss. Um diesem Verfassungsauftrag endlich Rechnung zu tragen, muss endlich eine umfassende und ebenenübergreifende IT-Sicherheitsstrategie entwickelt und das Klein-Klein beendet werden. Die SPD-Bundestagsfraktion drängt dabei auf eine strikt defensive Ausrichtung der staatlichen Cyber-Sicherheitsstrategie. Die Entwicklung und den Einsatz von Cyber-Angriffswerkzeugen und die Offenhaltung und Nutzung von IT-Sicherheitslücken durch den Staat lehnen wir ab, weil sie die allgemeine IT-Sicherheit beschädigen oder sogar gänzlich in Frage stellen.

Kernstück dieser umfassenden IT-Sicherheitsstrategie muss die anstehende Weiterentwicklung des IT-Sicherheitsgesetzes sein, mit dem wir in der letzten Legislaturperiode erste Maßnahmen zur Stärkung der IT-Sicherheit und zum besseren Schutz kritischer Infrastrukturen auf den Weg gebracht haben. Das IT-Sicherheitsgesetz 1.0 war nur auf den Staat und auf kritische Infrastrukturen bezogen. Die Fortentwicklung muss viel weitreichender sein und insbesondere auch den Schutz der Gesellschaft und Maßnahmen im Bereich digitaler Verbraucherschutz umfassen. Grundlegende Bedeutung kommt der Ausrichtung und dem weiteren Ausbau des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu. Im Koalitionsvertrag haben wir uns auf eine Fortschreibung des IT-Sicherheitsgesetzes und auf eine Erweiterung des Ordnungsrahmens verständigt, um den neuen Gefährdungen angemessen zu begegnen. Im Rahmen der Beratungen des IT-Sicherheitsgesetzes 2.0 wird zu klären sein, welche Maßnahmen es braucht, um

derartige Angriffe früher erkennen und diesen wirksam begegnen zu können. Dazu gehört auch die Frage, welche Maßnahmen die Diensteanbieter anbieten müssen, um den Schutz der Vertraulichkeit der Kommunikation sicherzustellen. Dazu gehören insbesondere die Verwendung von sicheren Passwörtern, eine 2-Faktor-Authentifizierung wo sie möglich ist und eine starke und vertrauenswürdige Verschlüsselung.

Die SPD-Bundestagsfraktion drängt auf eine schnelle Umsetzung des Koalitionsvertrages im Bereich der IT-Sicherheit und wird folgende Schwerpunkte einbringen:

1. Unabhängigkeit des BSI

Wir wollen das BSI als zentrale, unabhängige und vollständig präventiv ausgerichtete Cybersicherheitsbehörde ausbauen. Das BSI muss die erste und zentrale Anlaufstelle und der Anwalt in Fragen der IT-Sicherheit für Bürgerinnen und Bürger, Behörden und öffentliche Stellen, der Parlamente sowie für Unternehmen sein. Seine weisungsabhängige Eingliederung in den Geschäftsbereich und die Dienstaufsicht des BMI erschwert seine neutrale Aufgabenwahrnehmung gegenüber anderen Behörden des Bundes und als Ansprechpartner und Berater für Bürgerinnen und Bürger, Parlamenten und Bundesländern sowie Unternehmen. Deswegen ist die rechtliche und organisatorische Unabhängigkeit zwingend notwendig, um das Vertrauen der Bürgerinnen und Bürger nicht zu verlieren und um Interessenkonflikte zu vermeiden. Notwendig dafür ist eine Änderung des BSI-Gesetzes, in dem die Unabhängigkeit des BSI gesetzlich festgeschrieben werden muss. Im Koalitionsvertrag haben wir zudem vereinbart, dass die Beratungs- und Unterstützungsangebote des BSI für Bund und Länder, für Unternehmen und Einrichtungen sowie für Bürgerinnen und Bürger ausgebaut und dass der Verbraucher-schutz als zusätzliche Aufgabe des BSI etabliert werden soll. Zudem soll das BSI als zentrale Zertifizierungs- und Standardisierungsstelle für IT- und Cyber-Sicherheit fungieren. Auch müssen die Warn- und Untersuchungsbefugnisse des BSI erweitert und die Möglichkeiten des Monitorings und von Schwachstellenscans - unter Wahrung des Grundrechtsschutzes - ausgeweitet werden. Dabei sind für uns eine Aufwertung des BSI und insbesondere eine Ausweitung der Kompetenzen zwingend mit seiner Unabhängigkeit verbunden. Geprüft werden muss auch, welche weiteren Kompetenzen und Anordnungsbefugnisse das BSI als zentrale Cybersicherheitsbehörde in besonderen Gefahrenlagen braucht.

2. Schutzpflichten der Dienste- und Telekommunikationsanbieter

Es gibt bereits rechtliche Vorgaben hinsichtlich des aktuellen Standes der Technik, zu Privacy-by-Design bzw. -Default oder auch Security-by-Design. Wir werden prüfen, ob diese Vorgaben ausreichen und ob diese weiter konkretisiert werden müssen. Die jüngsten Sicherheitsfälle haben deutlich gemacht, dass diese zu oft ignoriert werden. Um die Verantwortung der Anbieter von Internetdiensten für den Schutz der Privatheit und der Daten der Nutzer zu stärken, setzt die SPD-Bundestagsfraktion dafür ein, dass die die Anbieter dazu verpflichtet werden:

- Maßnahmen für starke und sichere Passwörter zu etablieren und Schutzmaßnahmen wie die 2-Faktor-Authentifizierung anzubieten und ihre Verwendung anzubieten und voreinzustellen, ohne die anonyme Nutzungsmöglichkeit einzuschränken,

- bei den Einstellungen zur Sicherheit und zum Datenschutz die Privatheit grundsätzlich schützende Voreinstellungen vorzunehmen,
- für jede direkte Kommunikation als Option sichere und vertrauenswürdige Ende-zu-Ende-Verschlüsselung anzubieten und ihre Verwendung voreinzustellen.
- Fortschreibung des § 109 Telekommunikationsgesetz (TKG), um den besonderen Sicherheitsanforderungen von 5G, insbesondere mit Blick auf die neuen Architekturen, Rechnung zu tragen.

3. Weitere Maßnahmen zum Schutz der IT-Sicherheit

Darüber hinaus sind zahlreiche weitere Änderungen bzw. Fortschreibungen des IT-Sicherheitsgesetzes dringend geboten. Dazu zählen insbesondere:

- Die 24/7-Erreichbarkeit des BSI-Lagezentrums,
- die Ausweitung der Meldepflichten und Mindeststandards für weitere Bereiche der Wirtschaft, insbesondere auf weitere kritische Infrastrukturen,
- die Schaffung einer beim BSI angegliederten Meldestelle, bei entsprechende Lücken durch jeden – auch anonym oder pseudonym – gemeldet werden können,
- Verpflichtung von Cloud-Diensten, ihre Kunden über erkannte besonders schwere Angriffe zu informieren, damit diese ihren Schutz und ihre Selbstschutzinstrumente entsprechend anpassen können,
- die Einbeziehung der Soft- und Hardwarehersteller in die Meldepflicht, wenn Mängel oder Sicherheitslücken beim Anwender zu Schäden an Leib, Leben, Gesundheit, Vermögen und Eigentum führen können,
- die Verpflichtung der Hersteller und Anbieter, Sicherheitslücken zu bekannt machen und schnellstmöglich zu beheben,
- das BSI soll die Verpflichtung erhalten, öffentliche Warnungen unter Nennung des Produktes und Herstellers sowie gegebenenfalls der Sicherheitslücke auszusprechen, wenn nach Information an den Hersteller der Software und nach einem angemessenen Zeitablauf die Sicherheitslücke nicht geschlossen wurde,
- weitere Festschreibung von Mindeststandards und die Einführung eines IT-Sicherheitsgütesiegels für über die gesetzlichen Mindeststandards hinausgehenden IT-Sicherheitsstandard,
- die Verpflichtung zur Zertifizierung als Voraussetzung für den Einbau oder Einsatz in sicherheitsrelevanten Bereichen durch das BSI, beispielsweise bei Routern - wir wollen das Zulassungs- und Zertifizierungsregime für vertrauenswürdige und sichere Software und Hardware fördern und ähnlich wie bei den kritischen Infrastrukturen Mindestschutzstandards für sicherheitsrelevante Soft- und Hardware setzen,
- die gesetzliche Verankerung einer fairen Produkthaftung für digitale Güter, Umkehr der Beweislast,

- eine Kennzeichnungspflicht, wie lange Produkte mit sicherheitsrelevanten Updates versorgt werden sowie eine Verpflichtung, nur Produkte zu verkaufen, die noch mit Updates versorgt werden; die Updateverpflichtung bezieht sich folglich nicht auf die Dauer der Gewährleistung, sondern auf die vom Kunden erwartbare Lebensdauer des Produktes
- verstärkt auf offene und überprüfbare Standards zu setzen und diese verpflichtend vorzugeben,

4. Umgang der Sicherheitsbehörden mit cyberkriminellen Vorfällen

Die Erklärungen und Informationen der beteiligten Sicherheitsbehörden zum Umgang mit gehackten Accounts und veröffentlichten Daten haben erneut in erschreckender Weise deutlich gemacht, dass von einer klar definierten und abgestimmten Vorgehensweise und Kooperation der Behörden in Fällen der Cyber-Kriminalität keine Rede sein kann. Wenn eine Datenpanne gemeldet oder ein Daten- oder Identitätsdiebstahl angezeigt wird, wenn sich jemand meldet, dessen Account gehackt oder gekapert wurde, wenn jemand Opfer einer Malware oder Ransomware wurde, oder wenn das IT-System einer Einrichtung der kritischen Infrastruktur, der öffentlichen Verwaltung oder der Parlamente angegriffen wird, dann muss jede Dienststelle, jede Behörde einen strukturierten Plan haben, wie damit umzugehen ist.

Das Cyber-Abwehrzentrum muss daher – unter Wahrung des Trennungsgebotes zwischen polizeilicher und nachrichtendienstlicher Befugnisse sowie zwischen ziviler und militärischer Sicherheit und auf einer klaren rechtlichen Grundlage - als ständige Einrichtung weiterentwickelt und ausgebaut werden. Einbezogen werden müssen auch die Länder und die europäischen IT-Sicherheitsbehörden. Wir brauchen auch im Bereich der Cyberabwehr endlich eine klare Koordination und klare Zuständigkeiten.

Zudem ist dafür zu sorgen, dass dort zeitnah ein Konzept erarbeitet wird, welche Behörde (BfV, BSI, Polizeien aller Ebenen, möglicherweise auch die Datenschutz-Aufsichtsbehörden) im Falle einer Meldung bzw. Anzeige wen unterrichten und wer und wann welche Maßnahmen zum Schutz der Betroffenen, zur Beweissicherung und zur Strafverfolgung ergreifen muss und welche Fälle zwingend im Cyber-Abwehrzentrum eingebracht werden müssen. Das BSI soll unter der Wahrung des Datenschutzes der Betroffenen und unter der Aufsicht und Kontrolle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ein Register cyberkrimineller Vorfälle einrichten, um mögliche Angriffsmuster - und -ziele frühzeitig erkennen zu können.

Dabei müssen insbesondere folgende Fragen geklärt werden:

- Welche Informationen müssen beim Cyber-Abwehrzentrum zusammengeführt werden, damit Fachbehörden die Vorgehensweise des Täters analysieren können und mögliche Zusammenhänge und Muster mit anderen Fällen erkannt werden können? Auch die Datenschutzaufsichtsbehörden sollen bei Daten- und Identitätsklau und bei der unbefugten Veröffentlichung von personenbezogenen Daten in die Meldewege des Cyberabwehrzentrums und der Sicherheitsbehörden einbezogen werden, auch um die Nachteile für die Betroffenen so gering wie möglich zu halten. Zudem sollten auch sie Informationen über gemeldete Datenpannen in anonymisierter Form weiterzuleiten und so die allgemeine Sicherheit zu unterstützen.

- Es braucht klarere Vorgaben, was beim Opfer zur Schadensbegrenzung zu unternehmen ist (Gefährdungslage, Sicherungsmaßnahmen, Resilienz) und wer dabei unterstützen kann. Bisher scheint eine solche Ansprache, Unterstützung und Schutz des Opfers eher zufällig zu geschehen.
- Geklärt werden muss auch, welche weiteren Ermittlungen bei Bekanntwerden von Angriffen oder Hackerattacken zum Schutz des Opfers und / oder zum Schutz der allgemeinen Sicherheit anzustellen sind und welche konkreten anlassbezogenen Maßnahmen und Aktivitäten durch wen eingeleitet werden müssen, etwa ein anlassbezogenes Monitoring.

Hierzu zählt im Rahmen eines wirksamen Frühwarnsystems auch ein Monitoring von im Netz öffentlich zugänglichen Informationen und insbesondere von den für die Veröffentlichung von Leaks genutzten relevanten Plattformen, um möglichst frühzeitig Kenntnis von cyber-kriminellen Vorfällen zu erlangen. Das BSI sollte die Aufgabe bekommen, öffentlich verfügbare Informationen zu monitoren und – unter Beachtung datenschutzrechtlicher Vorgaben und Aufsicht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) – eine entsprechende Datenbank zu erstellen und zu pflegen.

Die SPD-Bundestagsfraktion macht in diesem Zusammenhang deutlich, dass ein flächendeckendes und anlassloses Monitoring des Internetverkehrs weit über das Ziel hinausschießen und den Freiheits- und Bürgerrechten fundamental widerspräche. Gleiches gilt für die Vorschläge auf europäischer Ebene, E-Mails und Messenger-Nachrichten auf unzulässige Inhalte verdachtslos und flächendeckend durchsuchen zu lassen – etwa zum Auffinden strafbarer Inhalte. Diese kämen einem Ende des Telekommunikationsgeheimnisses gleich und werden daher von uns grundsätzlich abgelehnt.

5. Bewusstsein der Nutzer für IT-sicheres Verhalten

Wir müssen die Menschen zur digitalen Selbständigkeit befähigen und sie beim digitalen Selbstschutz unterstützen. Um auch das Bewusstsein und das Wissen der Nutzerinnen und Nutzer von Internetdiensten für den Schutz ihrer Privatheit und ihrer Daten zu erhöhen, fordert die SPD-Bundestagsfraktion den Bundesminister des Inneren auf, eine umfassende, für die unterschiedlichen Zielgruppen und Kanäle wirksame Informationskampagne zu entwickeln und zu beauftragen. Eine solche Kampagne muss Informationen zu sicheren Passwörtern, die Verwendung von Passwortmanagern und andere Maßnahmen zur Sicherung von Zugängen wie die 2-Faktor-Authentifizierung enthalten. Sie muss über die Vorgehensweise von Phishing- und Man-in-the-Middle-Attacken aufklären, über Sicherungsmaßnahmen nach einem Angriff und darüber, wo der Nutzer Hilfe findet und den Angriff melden und zur Anzeige bringen kann.

Eine solche Kampagne muss auf Dauer angelegt sein und immer wieder auf den neuesten Stand gebracht werden. Sie soll Plakate und Radio- und TV-Formate umfassen, aber auch die Anbieter von Internetdiensten einbeziehen oder Medienschaffende wie z.B. prominente Youtuber und Gamer.

Das BMI wird darüber hinaus aufgefordert, eine Art „Landkarte“ bereits existierender Initiativen zur Sensibilisierung der Bürger zu erstellen und auf dieser Basis die Bündelung und Vernetzung bereits existierender Initiativen zu fördern. Es gibt bereits eine Reihe sehr guter (insbesondere

zivilgesellschaftlicher) Initiativen und Engagement, die aber überregional kaum bekannt sind. Die Vernetzung der Akteure untereinander könnte bereits Mehrwert erbringen.

Wir brauchen darüber hinaus ein Förderprogramm zur „Weiterentwicklung und Implementierung sicherer und vertrauenswürdiger Verschlüsselungsverfahren“, um Bürgerinnen und Bürgern aber auch Unternehmen wirksame und einfach zu nutzende Selbstschutzinstrumente an die Hand zu geben. Wenn es eine Erkenntnis aus den jüngsten Angriffen und Datenskandalen gibt, so lautet diese, dass allein sichere und vertrauenswürdige Verschlüsselungstechnologien einen weitgehenden Schutz der elektronischen Kommunikation bieten können. Dieses Projekt sollte anschließen an eine Förderung der Verschlüsselungstechnologie GnuPG des BMWi in seiner Entstehungsphase (1999 bis 2001). Heute genießt diese Verschlüsselungstechnologie hohe Akzeptanz und Vertrauen, ist Teil des IT-Grundschutzes des BSI und setzt einen wichtigen Verschlüsselungsstandard in der „freien Softwarewelt“ („Made in Germany“). Ziel dieser Förderung muss insbesondere die Weiterentwicklung und Implementierung in alle gängigen Mailprogramme sowie die einfache Nutzbarkeit für Jedermann sein.