CDU CSU

FRAKTIONSVORSITZENDENKONFERENZ

Stand 21.01.2019

Beschlussvorlage

„Gesamtplan einer länderübergreifenden Cybersicherheitsstrategie“

Telekommunikation, Telemedizin, intelligente Technik und Stromversorgung, Telebanking, GPS und autonomes Fahren - die Digitalisierung erfasst mehr und mehr Lebensbereiche unserer Gesellschaft. Sie macht das Leben an vielen Stellen komfortabler und leichter, macht jedoch die Gesellschaft als Ganzes wie auch den Einzelnen deutlich verwundbarer als wir alle dies in der analogen Welt gewohnt sind.

Wenn einerseits durch Technik riesige Datenmengen entstehen und andererseits sensible Daten quer über den Globus verschickt werden, können im Falle eines Datenmissbrauchs kriminelle Dritte von überall unbefugt auf diese zugreifen, oft sogar dann, wenn Absender und Empfänger Schutzmechanismen aktiviert haben. Nationale Grenzen verwischen vor diesem Hintergrund. Kriminelle fischen längst nicht mehr nur Bankdaten und Passworte im Netz ab und schädigen so Privatpersonen. Auch Wirtschaftsunternehmen, Betreiber kritischer Infrastrukturen und sensible Bereiche der staatlichen Verwaltung sehen sich tagtäglich den Attacken der Konkurrenz oder ausländischer Dienste aus dem Internet ausgesetzt. Dabei werden die verdeckten Angriffe in gleichem Maße komplexer, in dem die digitalen Schutzmauern höher gebaut werden. In einer virtuell eng vernetzten Welt gefährdet derjenige, der beim Schutz seiner Geräte und Netzwerke schläft, nicht nur sein eigenes Vermögen und Know-How, sondern eventuell sogar das seiner Freunde, Kontakte und Geschäftspartner. Die Sicherheit digitaler Daten ist damit längst nicht mehr die Sache eines jeden Einzelnen. Sie muss eingebunden werden in die IT-Sicherheitsstrategien von Unternehmen und des Staates.

I. Staatliche Aufgabenkoordinierung und Umsetzung

Die Schutzfunktion des Staates beschränkt sich nicht mehr nur auf die klassischen Aufgabenfelder der Sicherheits- und Ordnungsbehörden, sie umfasst auch den digitalen Schutz der Bürger, der Funktionsträger und der Unternehmen.

Wir setzen uns deshalb dafür ein, dass:

- die zuständigen Bundes- und Landesbehörden finanziell, technisch, personell und infrastrukturell so ausgestaltet werden, dass Cyberangriffe schnellstmöglich erkannt, betroffene Kreise gewarnt und identifizierte Schwachstellen schnellstmöglich umgehend beseitigt werden können.

- die Zusammenarbeit zwischen den beteiligten Stellen des Bundes und der Länder weiter verbessert wird.

- auf europäischer Ebene müssen Regelungen zu grenzüberschreitenden Informationswegen und zur Datenweitergabe erarbeitet und die europäischen Bemühungen um mehr Cybersicherheit weiter intensiviert werden (z.B Cybersecurity-Pakt).

- Ein Notfallplan, um innerhalb kurzer Zeit auf den Abfluss sensibler Daten, digitale Wirtschaftsspionage oder Sabotage reagieren zu können, ist dringend notwendig.

- der Bund und alle Länder geeignete kompatible Informations- und Koordinationssysteme vorhalten, die eine enge länderübergreifende Zusammenarbeit ermöglichen.

- in den zuständigen Institutionen ausreichend und gut ausgebildete Fachkräfte vorhanden sind. Anreize für die Ausbildung, beispielsweise durch Stipendien oder Studienzuschüsse, bzw. spezielle Anreize im Rahmen der Anwerbung von Fachkräften in der Informationstechnik sollten fester Bestandsteil des Personalmanagements werden.

- regelmäßige Krisenmanagementübungen zwischen den zuständigen Institutionen, auch länderübergreifend, etabliert werden.

- der Informationsfluss von den Institutionen an Betroffene von Cyberangriffen sowie der damit befassten Behörden untereinander möglichst umgehend erfolgt. Dabei ist der Schutz der Persönlichkeitsrechte zu gewährleisten.

- die Strafmaße für Cyberkriminalität erhöht werden. Neue Straftatbestände, z.B. für das Betreiben krimineller Infrastrukturen müssen geschaffen sowie strafprozessualen Vorschriften um Straftaten aus dem Bereich der Cyberkriminalität ergänzt werden. Mit Abschreckung und hohem Verfolgungsdruck können Erfolge zum Schutze Aller erzielt werden.
- die Anbieter von Internetdiensten und Hersteller von „Internet of Things (IoT)-Geräten“ stärker in die Pflicht genommen werden, um deren Angebote so zu gestalten, dass ausreichend starke Passworte von den Benutzern gewählt und diese regemäßig geändert werden müssen. Geräte sind so zu konfigurieren, dass sie den Anforderungen der Datensicherheit genügen.

II. Schutz der Wirtschaft vor digitalen Angriffen

Unsere Wirtschaftsunternehmen sind das Rückgrat unserer Gesellschaft. Hier liegen unser Know-How, unsere Innovationen mit allen davon abhängigen Arbeitsplätzen, unsere Zukunft, unsere Finanz- und Wirtschaftskraft. Diese zu schützen, sei es vor Diebstahl geistigen Eigentums und technischer Expertise oder gezielter Manipulation durch Cyberattacken, ist von enormer Bedeutung. Konkret setzen wir uns dafür ein, dass:

- regionale Sicherheitscluster von Wissenschaft, Wirtschaft, Hochschulen und den staatlichen Institutionen geschaffen und fortlaufend unterstützt werden. Die Erfahrungen aus den vorhandenen Modellregionen sind zu evaluieren und im weiteren Prozess zu berücksichtigen.

- die wissenschaftliche Forschung im Bereich der Informationssicherheit weiterhin intensiv vorangetrieben wird.

- in allen Ländern zentrale Anlaufstellen für die Wirtschaft etabliert werden. Im Fokus sollen hierbei der direkte Informationsaustausch sowie die schnelle Hilfe vor Ort stehen.

- fachspezifische Qualifizierungs- und Informationsangebote für klein- und mittelständische Unternehmen (KMU) bereitgestellt werden.

- die vernetzte Zusammenarbeit von KMU gefördert wird, um so zusätzliche Synergieeffekte beim Thema Cybersicherheit zu schaffen und damit die Gefährdungsrisiken zu minimieren.

- die von der Wirtschaft benötigte digitale Infrastruktur für den effektiven Schutz vor Cyberangriffen geschaffen wird (Digitalisierungsoffensive).

- verstärkte Investitionen in die Weiterentwicklung von Kryptographie-Verfahren und die Entwicklung von einfach zu bedienenden Verschlüsselungstechnologien getätigt werden.

- Förderung der IT-Sicherheitsbranche, damit weitere spezialisierte Anbieter im Bereich der IT-Sicherheit entstehen und den Unternehmen zur Verfügung stehen

- Vertrauensvolle, professionelle Zusammenarbeit zwischen Unternehmen und Behörden bei IT-Sicherheitsvorfällen (Informationsweitergabe)

- Förderung des digitalen Selbstschutzes der Unternehmen

III. Abwehr von Cyberattacken im privaten Bereich stärken

Die Verantwortung des Staates zum Schutz vor Cyberangriffen ersetzt nicht die Pflicht jedes Einzelnen für Datensicherheit zu sorgen und insbesondere seine Passworte sicher einzurichten und die technischen Verschlüsselungsmöglichkeiten für Daten zu nutzen. Wir setzen uns ergänzend dafür ein, dass:

- die zuständigen staatlichen Institutionen auf Bundes- und Länderebene zusätzliche Informationskampagnen und –materialien erstellen, um den Bürgern das Bewusstsein für den verantwortungsvollen Umgang mit ihren Daten nachhaltig zu vermitteln und effektive Hilfestellung zu geben.

- die Bildungseinrichtungen verstärkt in die Förderung der Medienkompetenz der Bevölkerung sowie die Entwicklung von altersgerechten Bildungsangebote (Für Jung und Alt) investieren.

- bundeseinheitliche gesetzliche Mindeststandards für die Sicherheit informationstechnischer Geräte insbesondere bei Endverbraucher-Geräten erarbeitet werden und auf dieser Grundlage auf einheitliche europäische Standards hingearbeitet wird.

- Softwarehersteller und Internetdienste der Sicherheit der Nutzerdaten und beim Schutz vor Datenmissbrauch stärker in die Pflicht genommen werden (Security by Design).

- Hersteller bzw. Anbieter kommerziell vertriebener Software für einen angemessenen Zeitraum zu Sicherheitsupdates verpflichtet werden.