

1

2 *Beschlussvorlage*

3

„Gesamtplan einer länderübergreifenden Cybersicherheitsstrategie“

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

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

24

25 **I. Staatliche Aufgabenkoordinierung und Umsetzung**

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

29 Wir setzen uns deshalb dafür ein, dass:

- 30
- die zuständigen Bundes- und Landesbehörden finanziell, technisch, personell und
31 infrastrukturell so ausgestaltet werden, dass Cyberangriffe schnellstmöglich erkannt,
32 betroffene Kreise gewarnt und identifizierte Schwachstellen schnellstmöglich
33 umgehend beseitigt werden können.

34

- 35 • die Zusammenarbeit zwischen den beteiligten Stellen des Bundes und der Länder
36 weiter verbessert wird.
37
- 38 • auf europäischer Ebene müssen Regelungen zu grenzüberschreitenden
39 Informationswegen und zur Datenweitergabe erarbeitet und die europäischen
40 Bemühungen um mehr Cybersicherheit weiter intensiviert werden (z.B Cybersecurity-
41 Pakt).
42
- 43 • Ein Notfallplan, um innerhalb kurzer Zeit auf den Abfluss sensibler Daten, digitale
44 Wirtschaftsspionage oder Sabotage reagieren zu können, ist dringend notwendig.
45
- 46 • der Bund und alle Länder geeignete kompatible Informations- und
47 Koordinationssysteme vorhalten, die eine enge länderübergreifende Zusammenarbeit
48 ermöglichen.
49
- 50 • in den zuständigen Institutionen ausreichend und gut ausgebildete Fachkräfte
51 vorhanden sind. Anreize für die Ausbildung, beispielsweise durch Stipendien oder
52 Stundenzuschüsse, bzw. spezielle Anreize im Rahmen der Anwerbung von Fachkräften
53 in der Informationstechnik sollten fester Bestandteil des Personalmanagements
54 werden.
55
- 56 • regelmäßige Krisenmanagementübungen zwischen den zuständigen Institutionen,
57 auch länderübergreifend, etabliert werden.
58
- 59 • der Informationsfluss von den Institutionen an Betroffene von Cyberangriffen sowie
60 der damit befassten Behörden untereinander möglichst umgehend erfolgt. Dabei ist
61 der Schutz der Persönlichkeitsrechte zu gewährleisten.
62
- 63 • die Strafmaße für Cyberkriminalität erhöht werden. Neue Straftatbestände, z.B. für das
64 Betreiben krimineller Infrastrukturen müssen geschaffen sowie strafprozessualen
65 Vorschriften um Straftaten aus dem Bereich der Cyberkriminalität ergänzt werden. Mit
66 Abschreckung und hohem Verfolgungsdruck können Erfolge zum Schutze Aller erzielt
67 werden.
- 68 • die Anbieter von Internetdiensten und Hersteller von „Internet of Things (IoT)-
69 Geräten“ stärker in die Pflicht genommen werden, um deren Angebote so zu gestalten,
70 dass ausreichend starke Passworte von den Benutzern gewählt und diese regelmäßig
71 geändert werden müssen. Geräte sind so zu konfigurieren, dass sie den Anforderungen
72 der Datensicherheit genügen.
73

75 II. Schutz der Wirtschaft vor digitalen Angriffen

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

- 81 • regionale Sicherheitscluster von Wissenschaft, Wirtschaft, Hochschulen und den
82 staatlichen Institutionen geschaffen und fortlaufend unterstützt werden. Die
83 Erfahrungen aus den vorhandenen Modellregionen sind zu evaluieren und im weiteren
84 Prozess zu berücksichtigen.
- 85
- 86 • die wissenschaftliche Forschung im Bereich der Informationssicherheit weiterhin
87 intensiv vorangetrieben wird.
- 88
- 89 • in allen Ländern zentrale Anlaufstellen für die Wirtschaft etabliert werden. Im Fokus
90 sollen hierbei der direkte Informationsaustausch sowie die schnelle Hilfe vor Ort
91 stehen.
- 92
- 93 • fachspezifische Qualifizierungs- und Informationsangebote für klein- und
94 mittelständische Unternehmen (KMU) bereitgestellt werden.
- 95
- 96 • die vernetzte Zusammenarbeit von KMU gefördert wird, um so zusätzliche
97 Synergieeffekte beim Thema Cybersicherheit zu schaffen und damit die
98 Gefährdungsrisiken zu minimieren.
- 99
- 100 • die von der Wirtschaft benötigte digitale Infrastruktur für den effektiven Schutz vor
101 Cyberangriffen geschaffen wird (Digitalisierungsoffensive).
- 102
- 103 • verstärkte Investitionen in die Weiterentwicklung von Kryptographie-Verfahren und
104 die Entwicklung von einfach zu bedienenden Verschlüsselungstechnologien getätigt
105 werden.
- 106
- 107 • Förderung der IT-Sicherheitsbranche, damit weitere spezialisierte Anbieter im Bereich
108 der IT-Sicherheit entstehen und den Unternehmen zur Verfügung stehen
- 109
- 110 • Vertrauensvolle, professionelle Zusammenarbeit zwischen Unternehmen und
111 Behörden bei IT-Sicherheitsvorfällen (Informationsweitergabe)
- 112
- 113 • Förderung des digitalen Selbstschutzes der Unternehmen
- 114

115 **III. Abwehr von Cyberattacken im privaten Bereich stärken**
116

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

- 121 • die zuständigen staatlichen Institutionen auf Bundes- und Länderebene zusätzliche
122 Informationskampagnen und –materialien erstellen, um den Bürgern das Bewusstsein
123 für den verantwortungsvollen Umgang mit ihren Daten nachhaltig zu vermitteln und
124 effektive Hilfestellung zu geben.
125
- 126 • die Bildungseinrichtungen verstärkt in die Förderung der Medienkompetenz der
127 Bevölkerung sowie die Entwicklung von altersgerechten Bildungsangebote (Für Jung
128 und Alt) investieren.
129
- 130 • bundeseinheitliche gesetzliche Mindeststandards für die Sicherheit
131 informationstechnischer Geräte insbesondere bei Endverbraucher-Geräten erarbeitet
132 werden und auf dieser Grundlage auf einheitliche europäische Standards hingearbeitet
133 wird.
134
- 135 • Softwarehersteller und Internetdienste der Sicherheit der Nutzerdaten und beim
136 Schutz vor Datenmissbrauch stärker in die Pflicht genommen werden (Security by
137 Design).
138
- 139 • Hersteller bzw. Anbieter kommerziell vertriebener Software für einen angemessenen
140 Zeitraum zu Sicherheitsupdates verpflichtet werden.