Juli 2018 · Tabea Breternitz und Dr. Sven Herpig

Zuständigkeiten und Aufgaben in der deutschen Cyber-Sicherheitspolitik

Eine Übersicht

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Die Cyber-Sicherheitsarchitektur

Der erste Grundstein für die deutsche Cyber-Sicherheitsarchitektur wurde bereits 1986 gelegt. In diesem Jahr wurde in der Vorgängerorganisation des Bundesamts für Sicherheit in der Informationstechnik (BSI), der *Zentralstelle für das Chiffrierwesen* (ZfCh) "[...] eine Arbeitsgruppe aufgebaut, die sich vor dem Hintergrund der schnellen Entwicklung der IuK-Technik mit den Sicherheitsfragen beschäftigte"[1]. Am 1. Januar 1991 nahm das *Bundesamt für Sicherheit in der Informationstechnik* nach Ausgründung aus dem *Bundesnachrichtendienst* (BND) seine Arbeit auf.

Es dauerte weitere zwanzig Jahre, bis die staatliche Sicherheitsarchitektur durch die Cyber-Sicherheitsstrategie für Deutschland[2] 2011 zum ersten Mal in den öffentlichen Fokus geriet. Hierbei lag das Augenmerk vor allem auf dem neu zu schaffenden *Nationalen Cyber-Abwehrzentrum* (Cyber-AZ/NCAZ). Seitdem hat sich einiges getan: Cyber-Sicherheit ist für die Sicherheitspolitik in Deutschland ein elementarer Bestandteil geworden, weswegen einige neue Akteure, wie zum Beispiel die *Zentrale Stelle für Informationstechnik im Sicherheitsbereich* (ZITiS) geschaffen und damit Bestandteil dieser Architektur wurden. Jedoch gab es auch in der aktualisierten Version der Cyber-Sicherheitsstrategie für Deutschland 2016[3] keine grafische oder anderweitige Übersicht über die immer komplexer werdende Architektur deutscher Behörden im Cyber-Raum. Für eine effektive und effiziente deutsche Aufstellung im Cyber-Raum ist, gerade auch vor dem Hintergrund begrenzter Ressourcen[4], eine strukturierte politische Herangehensweise unverzichtbar.

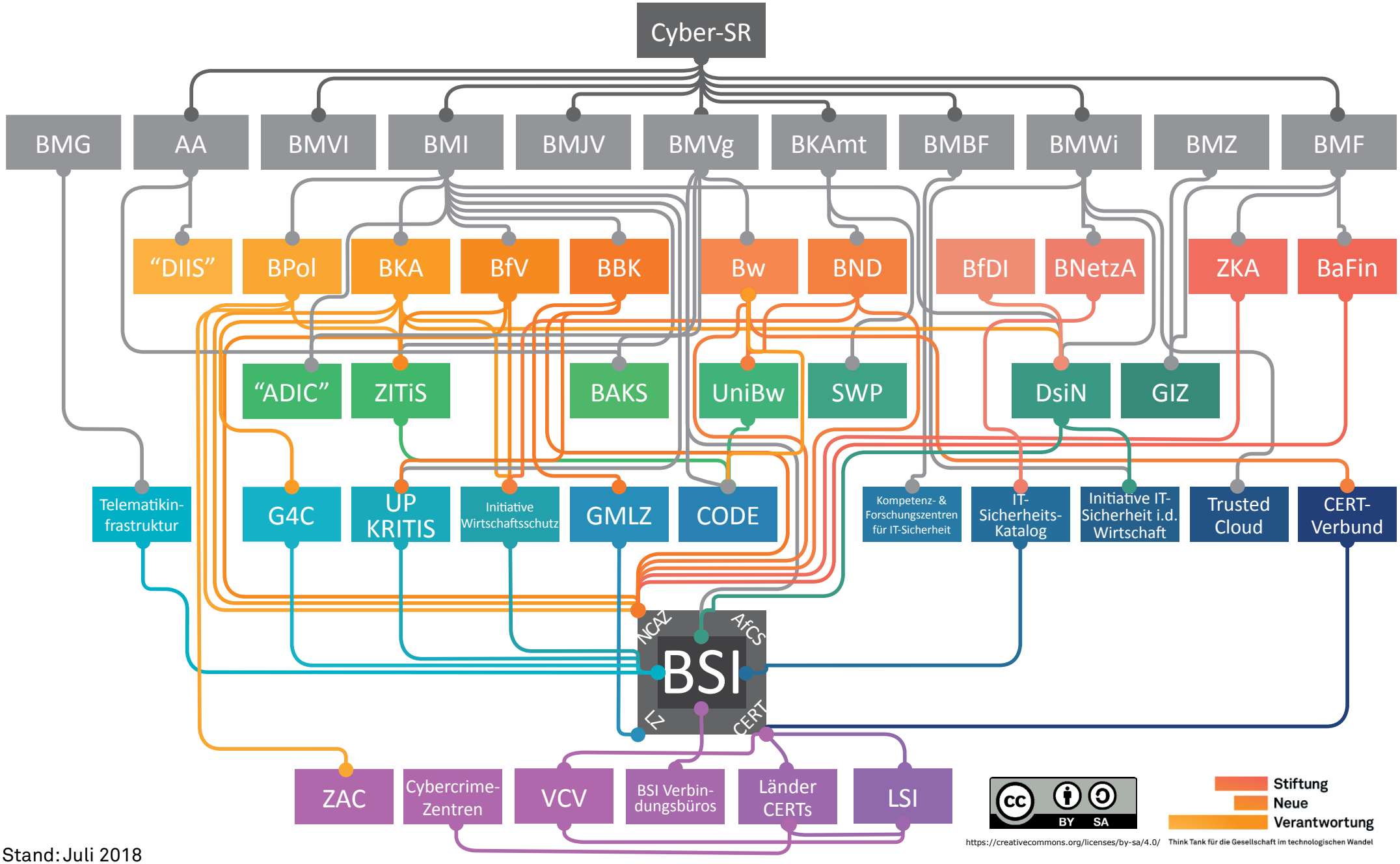
Aus diesem Grund wollen wir im Rahmen unserer Arbeit zu Cyber-Sicherheitspolitik an der Stiftung Neue Verantwortung hierzu einen Beitrag leisten. In dieser Veröffentlichung stellen wir eine grafische Abbildung der staatlichen Cyber-Sicherheitsarchitektur, ein Abkürzungs- und Akteursverzeichnis, sowie eine Erklärung der Verbindungen einzelner Akteure vor. Bis auf wenige Ausnahmen werden tiefergehende Länder- und Kommunalstrukturen, die internationale Ebene (UN, NATO, EU, etc.), sowie Akteure der Privatwirtschaft, Wissenschaft und Zivilgesellschaft nicht berücksichtigt. Das Dokument wird auch zukünftig periodisch aktualisiert um den neuesten Entwicklungsstand

1 Bundesamt für Sicherheit in der Informationstechnik, Jahresbericht 2003.
2 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland.
3 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.
4 Julia Schütze, Warum dem Staat IT-Sicherheitsexpert:innen fehlen.

abzubilden. Wir freuen uns daher über jeden Hinweis. Änderungs- und Ergänzungsvorschläge nimmt Dr. Sven Herpig gerne entgegen.

Die Verknüpfungen in der Visualisierung repräsentieren unterschiedliche Beziehungsaspekte und rangieren von der Entsendung von Mitarbeiter:innen in die verknüpfte Organisation, über eine Mitgliedschaft im Beirat, sowie finanziellen Zuwendungen bis hin zur Fach- und Rechtsaufsicht. Die Farben haben keine Bedeutung und dienen lediglich zur besseren Lesbarkeit.

Staatliche Cyber-Sicherheitsarchitektur



Stiftung Neue Verantwortung
Think Tank für die Gesellschaft im technologischen Wandel

Stand: Juli 2018

Akteure und Abkürzungen

AA	Auswärtiges Amt
ADIC	*Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien (in Gründung)*
AfCS / ACS	Allianz für Cyber-Sicherheit
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAKS	Bundesakademie für Sicherheitspolitik
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BKA	Bundeskriminalamt
BKAmt	Bundeskanzleramt
BMBF	Bundesministerium für Bildung und Forschung
BMF	Bundesministerium für Finanzen
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern, für Bau und Heimat
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BMVg	Bundesministerium der Verteidigung
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BMWi	Bundesministerium für Wirtschaft und Energie
BMZ	Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung
BND	Bundesnachrichtendienst
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BPol	Bundespolizei
BSI	Bundesamt für Sicherheit in der Informationstechnik

Bw	Bundeswehr
CERT	Computer Emergency Response Team des Bundes (CERT-Bund) und Bürger-CERT
CERT-Verbund	
CODE	Forschungszentrum Cyber Defence
Cybercrime-Zentren	*Cybercrime-Akteure in den Bundesländern, u. a. Hessen 3C und ZCB (Bayern)*
Cyber-SR	Cyber-Sicherheitsrat
DIIS	*Deutsches Institut für Internet Sicherheit / Deutsches Institut für Cyber-Sicherheit (in Gründung)*
DsiN	Deutschland sicher im Netz e.V.
G4C	German Competence Centre against Cyber Crime
GIZ	Gesellschaft für Internationale Zusammenarbeit
GMLZ	Gemeinsames Melde- und Lagezentrum
Initiative IT-Sicherheit in der Wirtschaft	
Initiative Wirtschaftsschutz	
IT-Sicherheitskatalog	
Kompetenz- und Forschungszentren für IT-Sicherheit	
Länder-CERTs	
LSI	Landesamt für Sicherheit in der Informationstechnik Bayern
LZ	Nationales IT-Lagezentrum
NCAZ / Cyber-AZ	Nationales Cyber-Abwehrzentrum
SWP	Stiftung Wissenschaft und Politik
Trusted Cloud	Kompetenznetzwerk Trusted Cloud
UniBw	Universität der Bundeswehr München
UP KRITIS	Umsetzungsplan Kritische Infrastrukturen
VCV	Verwaltungs-CERT-Verbund
ZAC	Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft

ZITiS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich
ZKA	Zollkriminalamt

Erläuterung

Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien (ADIC)
Die Einrichtung der Agentur für Disruptive Innovationen in der Cybersicherheit und Schlüsseltechnologien (ADIC) wurde im Koalitionsvertrag 2018 beschlossen. Sie soll unter der Federführung des BMI und BMVg sowie mithilfe eines IT-Sicherheitsfonds, die "technologische Innovationsführerschaft" im Bereich der sicherheitsrelevanten Schlüsseltechnologien gewährleisten.
Die ADIC soll sich unter Federführung des BMI und BMVg eingerichtet werden.[5]

Allianz für Cyber-Sicherheit (AfCS/ ACS)
Die Allianz für Cyber-Sicherheit (AfCS/ ACS) bietet einen vertrauensvollen Austausch zwischen den Mitgliedern und dem BSI zu Cyber-Bedrohungen, Schutzmaßnahmen und Vorfallsmanagement. Außerdem erhalten die Mitglieder Informationen zum Ausbau ihrer Cyber-Sicherheitskompetenzen. Mitglied kann jede Institution mit Sitz in Deutschland werden.
Die AfCS ist eine Public-Private-Partnership von BSI und BITKOM mit Wirtschaft, Behörden, Forschung und Wissenschaft.[6]

Auswärtiges Amt (AA)
Das Auswärtige Amt (AA) setzt sich im Rahmen seiner Cyber-Außenpolitik für internationale Cyber-Sicherheit, universelle Menschenrechte im digitalen Raum, sowie die Nutzung wirtschaftlicher Chancen durch die Digitalisierung ein. Dafür wurde 2011 der Koordinierungsstab für Cyber-Außenpolitik im Auswärtigen Amt geschaffen.
Das AA ist im Cyber-SR vertreten. Es strebt die Gründung des Deutschen Instituts für Internet Sicherheit (DIIS) an und stellt im Wechsel mit dem BMVg die Leitung der BAKS.[7]

Bundesakademie für Sicherheitspolitik (BAKS)
Die Bundesakademie für Sicherheitspolitik (BAKS) ist die zentrale Weiterbildungsstätte des Bundes für Sicherheitspolitik. In unterschiedlichen Veranstaltungsformaten, wie z. B. dem "Berliner Forum zur Cyber-Sicherheit", setzt sie sich mit den sicherheitspolitischen Herausforderungen im digitalen Raum auseinander.
Die BAKS gehört zum Geschäftsbereich des BMVg. Präsident und Vizepräsi-

5 Koalitionsvertrag zwischen CDU, CSU und SPD, Ein neuer Aufbruch für Europa Eine neue Dynamik für Deutschland Ein neuer Zusammenhalt für unser Land.

6 Bundesamt für Sicherheit in der Informationstechnik, ACS - Aktiv für mehr Cybersicherheit.

7 Auswärtiges Amt, Cyber-Außenpolitik.

dent kommen abwechselnd aus BMVg und AA.[8]

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
Die Aufgabe der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ist es ein funktionsfähiges, integres und stabiles Finanzsystem in Deutschland zu gewährleisten. Im Bereich der Wirtschaftskriminalität sieht die BaFin für Versicherer, Finanzdienstleister und Banken eine zunehmende Gefahr durch Cyber-Kriminalität.
Die BaFin gehört zum Geschäftsbereich des BMF und ist im Cyber-AZ vertreten.[9]

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) übernimmt eine wichtige Funktion im Gesamtkonzept der nationalen Sicherheitsarchitektur. In diesem Rahmen beschäftigt es sich zunehmend auch mit den Risiken von Cyber-Angriffen auf kritische Infrastrukturen. Das BBK ist im Cyber-AZ vertreten und sein Personal besetzt das Gemeinsame Melde- und Lagezentrum (GMLZ).
Die BBK gehört zum Geschäftsbereich des BMI und ist im GMLZ, UP KRITIS und Cyber-AZ vertreten.[10]

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Aufgabe die Sicherheit in der Informationstechnik des Bundes zu stärken. Als Behörde mit höchster technischer Expertise fördert es darüber hinaus die Informations- und Cyber-Sicherheit in Verwaltung, Wirtschaft und Gesellschaft durch zahlreiche Aktivitäten, Kooperationen und Initiativen. Um sich regional noch stärker zu vernetzen, baut das BSI aktuell deutschlandweit Verbindungsbüros auf.
Das BSI gehört zum Geschäftsbereich des BMI. In ihm beherbergt sind u.a. Cyber-AZ, AfCS, LZ, CERT-Bund und das Bürger-CERT.[11]

8 Bundesakademie für Sicherheitspolitik, Cyber-Realität zwischen Freiheit und Sicherheit.

9 Bundesanstalt für Finanzdienstleistungsaufsicht, Aufgaben & Geschichte der BaFin.

10 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Der Jahresbericht 2015. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Gemeinsames Melde- und Lagezentrum von Bund und Ländern.

11 Bundesamt für Sicherheit in der Informationstechnik, Bundesgesetzblatt Teil I Nr. 54, Jahrgang 2009, Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes. Bundesamt für Sicherheit in der Informationstechnik, Themen.

Bundesamt für Verfassungsschutz (BfV)
Das Bundesamt für Verfassungsschutz (BfV) untersucht wie neue technische Möglichkeiten beispielsweise von Extremisten, Terroristen oder ausländischen Nachrichtendiensten genutzt werden, um in Deutschland Spionage, politische Desinformation oder Computersabotage zu betreiben. Das BfV versucht Cyber-Angriffe auf staatliche und private Einrichtungen abzuwehren und aufzuklären.
Das BfV gehört zum Geschäftsbereich des BMI. Es ist im Cyber-AZ und der Initiative Wirtschaftsschutz vertreten und greift auf die Expertise von ZITiS zurück.[12]

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) berät und kontrolliert die Daten- und Informationsverarbeitung der öffentlichen Stellen des Bundes, sowie nicht-öffentlicher Stellen. Sie ist in der Ausübung ihres Amtes unabhängig und unterliegt nur der parlamentarischen Kontrolle durch den Bundestag.
Die BfDI ist im Beirat der DsiN vertreten.[13]

Bundeskanzleramt (BKAmt)
Das Bundeskanzleramt (BKAmt) unterstützt den/ die Bundeskanzler:in bei ihrer inhaltlichen Arbeit. Dazu unterhält es durch seine "Spiegelreferate" engen Kontakt zu den Bundesministerien. Mit Themen der Cyber-Sicherheit kommt es u. a. bei der Dienst- und Fachaufsicht des BND und der Finanzierung der SWP in Berührung.
Das BKAmt ist im Cyber-SR vertreten und ihm ist der BND nachgeordnet. Aus seinem Haushalt wird die institutionelle Zuwendung an die SWP gezahlt.[14]

Bundeskriminalamt (BKA)
Das Bundeskriminalamt (BKA) hat als Zentralstelle der deutschen Polizei sein Aufgabenfeld der nationalen Verbrechensbekämpfung auch auf den Cyber-Raum ausgeweitet. Es klärt Straftaten im Cyber-Raum auf, ermittelt und versucht Cyber-Kriminalität vorzubeugen.
Das BKA gehört zum Geschäftsbereich des BMI. Es ist im Cyber-AZ, sowie im G4C und der Initiative Wirtschaftsschutz vertreten. Es ist im DsiN Beirat und greift auf die Expertise von ZITiS zurück.[15]

12 Bundesamt für Verfassungsschutz, Cyberangriffe.
13 Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Aufgaben.
14 Bundeskanzleramt, Chef des Bundeskanzleramtes.
15 Bundeskriminalamt, Straftaten im Internet.

Bundesministerium der Justiz und für Verbraucherschutz (BMJV)
Das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) ist vor allem ein Gesetzgebungsministerium, das auch andere Bundesministerien bei ihren Rechtsetzungsvorhaben unterstützt. Innerhalb der Bundesregierung ist es für die wirtschaftliche Verbraucherpolitik zuständig. In diesem Rahmen beschäftigt es sich u. a. mit Themen wie dem Schutz von Bürgern und Onlinehändlern vor Cyber-Kriminalität oder Onlinemobbing.
Das BMJV ist im Cyber-SR vertreten.[16]

Bundesministerium der Verteidigung (BMVg)
Das Bundesministerium der Verteidigung (BMVg) ist für die militärische Verteidigung Deutschlands und somit auch für die Verteidigung Deutschlands im Cyber-Raum verantwortlich. Dafür setzt das BMVg auf nationale und internationale Kooperationen und Partnerschaften, zum Beispiel mit dem Cyber Innovation Hub oder dem Cooperative Cyber Defense Centre of Excellence der NATO. Im Ministerium ist die Abteilung Cyber- und Informationstechnik (CIT) für den Bereich Cyber-Verteidigung federführend zuständig.
Das BMVg ist im Cyber-SR vertreten. Ihm ist die Bw nachgeordnet und die BAKS gehört zu seinem Geschäftsbereich. ADIC soll unter Federführung des BMVg eingerichtet werden.[17]

Bundesministerium des Innern, für Bau und Heimat (BMI)
Das Bundesministerium des Innern, für Bau und Heimat (BMI) ist u. a. für die Sicherheit im Cyber-Raum zuständig. Die vom BMI vorgelegte "Cyber-Sicherheitsstrategie für Deutschland 2016" wurde im November 2016 vom Kabinett verabschiedet und bildet den ressortübergreifenden, strategischen Rahmen der Bundesregierung. Das BMI koordiniert die Umsetzung der Cyber-Sicherheitsstrategie durch den Bundesbeauftragten für Informationstechnik, der auch Vorsitzender des Cyber-Sicherheitsrates ist.
Das BMI ist im Cyber-SR vertreten. Seinem Geschäftsbereich sind BPol, BKA, BSI, BfV und BBK zugeordnet. Auf ein Erlass des BMI hin, wurde 2017 ZITiS gegründet. Das BMI ist in den Initiativen UP KRITIS, DsiN (Beirat), sowie der AfCS vertreten. ADIC soll unter Federführung des BMVG eingerichtet werden.[18]

16 Bundesministerium der Justiz und für Verbraucherschutz, Aufgaben und Organisation. Bundesministerium der Justiz und für Verbraucherschutz, Schutz von Bürgern und Onlinehandel vor Cyberkriminalität. Bundesministerium der Justiz und für Verbraucherschutz, Wir dürfen Cybermobbing nicht ignorieren.

17 Bundesministerium der Verteidigung, Cybersicherheit. Bundesministerium der Verteidigung, Cyber Innovation Hub. Koalitionsvertrag zwischen CDU, CSU und SPD, Ein neuer Aufbruch für Europa Eine neue Dynamik für Deutschland Ein neuer Zusammenhalt für unser Land.

18 Bundesministerium des Innern, für Bau und Heimat, IT & Cybersicherheit. Bundesministerium des Innern, für Bau und Heimat, Cyber-Sicherheitsstrategie für Deutschland.

Bundesministerium für Bildung und Forschung (BMBF)
Das Bundesministerium für Bildung und Forschung (BMBF) finanziert als Teil der Digitalen Agenda drei Kompetenzzentren für IT-Sicherheitsforschung. Mit dem CISPA (Saarbrücken), CRISP (Darmstadt) und KASTEL (Karlsruhe) soll die deutsche Forschungskapazität im Bereich der Cyber-Sicherheit nachhaltig erhöht werden.
Das BMBF ist im Cyber-SR vertreten und fördert die Kompetenzzentren für IT-Sicherheit.[19]

Bundesministerium für Finanzen (BMF)
Das Bundesfinanzministerium (BMF) ist vorrangig für die Steuer-, Haushalts- und Europäische Finanzpolitik zuständig. Es entwickelt zum Beispiel gemeinsam mit nationalen und internationalen Partnern Mindeststandards für die Cyber-Sicherheit in der Finanzdienstleistungsbranche.
Das BMF ist im Cyber-SR vertreten. Ihm nachgeordnet ist das ZKA und es hat außerdem die Rechts- und Fachaufsicht über die BaFin. BMZ und BMF sind Gesellschafter der GIZ.[20]

Bundesministerium für Gesundheit (BMG)
Das Bundesministerium für Gesundheit (BMG) ist vor allem für die Leistungsfähigkeit der Gesetzlichen Krankenversicherung sowie der Pflegeversicherung verantwortlich. Mit dem E-Health-Gesetz soll eine digitale Infrastruktur mit höchsten Sicherheitsstandards im Gesundheitswesen geschaffen werden.
Das BMG hat die gematik mit dem Aufbau einer Telematikinfrastruktur beauftragt, die Voraussetzung für eine sichere Vernetzung des Gesundheitswesens ist.[21]

Koalitionsvertrag zwischen CDU, CSU und SPD, Ein neuer Aufbruch für Europa Eine neue Dynamik für Deutschland Ein neuer Zusammenhalt für unser Land.

19 Kompetenz- und Forschungszentren für IT-Sicherheit, Über uns.

20 Bundesfinanzministerium, Themen.
Bundesfinanzministerium, Grundelemente zur Cyber-Sicherheit.

21 Bundesministerium für Gesundheit, E-Health-Gesetz.
Bundesministerium für Gesundheit, Aufgaben und organisation.

Bundesministerium für Verkehr und digitale Infrastruktur (BMVI)
Das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) ist für die Verkehrsinfrastruktur, -planung, -sicherheit sowie die digitale Infrastruktur verantwortlich. Aufgrund der sich daraus ergebenden Verantwortung für die zivile Notfallvorsorge bzw. Gefahrenabwehr, entwickelt das BMVI seine Krisenszenarien auch hinsichtlich möglicher Cyber-Angriffe auf digitale Infrastrukturen weiter.
Das BMVI ist im Cyber-SR vertreten.[22]

Bundesministerium für Wirtschaft und Energie (BMWi)
Das Bundesministerium für Wirtschaft und Energie (BMWi) hat es sich zum Ziel gesetzt für Wirtschaft, Gesellschaft und Staat den Zugang zu einer sicheren und vertrauenswürdigen IT zu schaffen, damit diese von der Digitalisierung bestmöglich profitieren können. Das BMWi setzt sich dabei vor allem für IT-Sicherheit in der Industrie 4.0 ein.
Das BMWi ist im Cyber-SR vertreten. Es hat die Initiative IT-Sicherheit in der Wirtschaft und Trusted Cloud ins Leben gerufen. Es ist im Beirat von DsiN vertreten; die BNetzA gehört zum Geschäftsbereich.[23]

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ)
Das Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ) ist für die Entwicklungszusammenarbeit der Bundesregierung verantwortlich. Dabei entwickelt das BMZ auch gesicherte IT-Lösungen für Partnerländer und unterstützt Cyber Capacity Building durch Bildungsprogramme vor Ort.
Das BMZ ist der wichtigste Auftraggeber der GIZ und neben dem BMF einer der beiden Gesellschafter.[24]

Bundesnachrichtendienst (BND)
Der Bundesnachrichtendienst (BND) ist der Auslandsnachrichtendienst der Bundesrepublik Deutschland und handelt im Auftrag der Bundesregierung. Im Ausland erfasst er Angriffe, die der Cyber-Spionage oder -Sabotage in Deutschland dienen sollen und warnt betroffene Akteure im Inland entsprechend vor, damit Abwehrmechanismen eingeleitet werden können. Bekannt ist dieser Teil seiner Arbeit auch unter dem Akronym SSCD - SIGINT Support

22 Bundesministerium für Verkehr und digitale Infrastruktur, Krisenmanagement.

23 Bundesministerium für Wirtschaft und Energie, IT-Sicherheit.
Bundesministerium für Wirtschaft und Energie, IT-Sicherheit für die Industrie 4.0.

24 Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, Grundsatzfrage: Warum brauchen wir Entwicklungspolitik?
Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung, Glossar - Digitalisierung und nachhaltige Entwicklung.

to Cyber Defense.
Der BND gehört zum Geschäftsbereich des BKAmt. Er ist an der Initiative Wirtschaftsschutz beteiligt und im Cyber-AZ vertreten. Sein Personal wird u.a. an der UniBw ausgebildet.[25]

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA)
Die Bundesnetzagentur (BNetzA) ist vorrangig für Regulierungs- und Wettbewerbsfragen in den Bereichen Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen zuständig. Da die Bedeutung von Cyber-Sicherheit in diesen Bereichen zunehmend an Bedeutung gewinnt, kümmert sich die BNetzA auch um IT-Sicherheitsanforderungen in den entsprechenden Sektoren.
Die BNetzA gehört zum Geschäftsbereich des BMWi. Gemeinsam mit dem BSI hat sie den IT-Sicherheitskatalog herausgebracht zu dessen Umsetzung alle Betreiber von Gas- und Stromnetzen verpflichtet sind.[26]

Bundespolizei (BPol)
Die Bundespolizei (BPol) übernimmt Aufgaben im Bereich des Grenzschutz, der Luftsicherheit, Bahnpolizei und Kriminalitätsbekämpfung. Da illegale Aktivitäten immer stärker auch im Internet oder mithilfe von Informationstechnik ausgeübt werden, bekämpft die BPol zunehmend auch Internet-Kriminalität.
Die BPol gehört zum Geschäftsbereich des BMI. Sie ist im Cyber-AZ vertreten und greift auf die Expertise von ZITiS zurück. Die ZAC sind bei den Polizeien des Bundes und der Länder angesiedelt.[27]

Bundeswehr (Bw)
Die Bundeswehr (Bw) ist u. a. für die Landes- und Bündnisverteidigung verantwortlich. Um dieser Aufgabe im digitalen Zeitalter gerecht zu werden, wurde im April 2017 der neue militärische Organisationsbereich Cyber- und Informationsraum (CIR) aufgestellt. Neben Heer, Luftwaffe und Marine ist die neue Organisation ganzheitlich für die Verteidigung des Cyber- und Informationsraums verantwortlich.
Die Bw gehört zum Geschäftsbereich des BMVg. Sie bildet Teile ihres Personals an der UniBw aus und ist im Cyber-AZ, sowie im CERT-Verbund vertreten.[28]

25 Bundesnachrichtendienst, Auftrag.
Bundesnachrichtendienst, Cyber-Sicherheit - Sicherung der nationalen Informationstechnik im Zeitalter globaler Vernetzung.

26 Bundesnetzagentur, Aufgaben und Struktur.
Bundesnetzagentur, IT-Sicherheit im Energiesektor.

27 Bundespolizei, Startseite.
Bundespolizei kompakt, 04/2015.

28 Bundeswehr, Auftrag und Aufgaben der Bundeswehr.

CERT-Bund / Bürger-CERT
Das Computer Emergency Response Team (CERT) des Bundes ist Notfallteam und Anlaufstelle für alle Bundesbehörden im Falle eines sicherheitsrelevanten IT-Vorfalls. Das Bürger-CERT ist ein Warn- und Informationsdienst für Privatpersonen, die vom Bürger-CERT neutral und kostenlos über aktuelle Sicherheitslücken informiert werden.
Das CERT des Bundes ist im BSI aufgehangen und kooperiert im Rahmen des Verwaltungs-CERT-Verbunds (VCV) mit den Länder-CERTs.[29]

CERT-Verbund
Der CERT-Verbund ist eine Allianz deutscher Sicherheits- und Computer-Notfallteams, die sich in Unternehmens-, Kommerziellen-, Akademischen- und Verwaltungs-CERTs auf Bundes- und Länderebene zusammengeschlossen haben.
Im CERT-Verbund sind u.a. die Bw und das BSI (mit dem CERT-Bund) vertreten.[30]

Cybercrime-Zentren
13 der 16 Bundesländer haben inzwischen Cybercrime-Zentren aufgebaut, die für die Bekämpfung und Aufklärung von Cyber-Kriminalität zuständig sind. Die Cybercrime-Zentren sind organisatorisch überwiegend im Polizeibereich der entsprechenden Landeskriminalämter oder bei den Staatsanwaltschaften aufgehangen.
Die Cybercrime-Zentren kooperieren mit den entsprechenden Länder-CERTs.[31]

Cyber-Sicherheitsrat (Cyber-SR)
Der nationale Cyber-Sicherheitsrat (Cyber-SR) wurde 2011 im Zuge der Cyber-Sicherheitsstrategie eingerichtet, mit dem Ziel als strategischer Ratgeber der Bundesregierung langfristige Handlungsnotwendigkeiten und Trends der Cyber-Sicherheit zu identifizieren und entsprechende Impulse anzuregen. Er bringt Vertreter der Bundesebene, der Länder und aus der Wirtschaft zusammen.
Im Cyber-SR sind BMI, BKAmt, AA, BMVg, BMWi, BMJV, BMF, BMBF und BMVI vertreten.[32]

Bundeswehr Karriere, Der Cyber- und Informationsraum.
29 Bundesamt für Sicherheit in der Informationstechnik, CERT-Bund.
30 Deutscher CERT-Verbund, Startseite.
31 Secupedia, Nationales Cyber-Abwehrzentrum.
32 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)
Die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) hilft der Bundesregierung bei der Realisierung ihrer Ziele zur internationalen Entwicklungszusammenarbeit. Sie unterstützt die Förderung von Informations- und Kommunikationstechnologien und plant in Zukunft auch Cyber-Sicherheit als Element der traditionellen Entwicklungszusammenarbeit aufzunehmen.
BMZ und BMF sind Gesellschafter der GIZ.[33]

Deutsches Institut für Internet Sicherheit / Cyber-Sicherheit (DIIS)
In der Cyber-Sicherheitsstrategie für Deutschland 2016 wurde die Gründung eines *Deutschen Instituts für Cyber-Sicherheit (DIIS)* angekündigt. Das Institut soll unterschiedliche Akteure einbeziehen, um an Cyber-Sicherheitsthemen mit Bezug zu internationaler Stabilität und Krisenprävention zu arbeiten. Dabei soll es Regierungen als internationaler Ansprechpartner zur Verfügung stehen.
Das DIIS soll vom AA gegründet werden.[34]

Deutschland sicher im Netz e.V. (DsiN)
Deutschland sicher im Netz e.V. (DsiN) wurde im Rahmen des 1. Nationalen IT-Gipfels gegründet, um die Bevölkerung, sowie kleine und mittlere Betriebe über IT-Sicherheit aufzuklären. In Kooperation mit seinen Mitgliedern und Partnern betreibt DsiN verschiedene Initiativen und Projekte, um konkrete Hilfestellungen für IT-Sicherheit zu leisten.
Das BMI, BMWi, BSI, BKA und BfDI sind im DsiN Beirat vertreten. DsiN kooperiert mit der Initiative IT-Sicherheit in der Wirtschaft.[35]

Forschungsinstitut Cyber Defence (CODE)
Das Forschungsinstitut Cyber Defence (CODE) an der Universität der Bundeswehr wurde vom BMVg mit dem Ziel gegründet, innovative technische Neuerungen für Bundeswehr und Bund zum Schutz von Daten, Software und Systemen zu verwirklichen. Darüber hinaus ist das interdisziplinäre, unabhängige Forschungsinstitut an die wissenschaftliche Aus-, Fort- und Weiterbildung der Universität der Bundeswehr angebunden. Hier baut es ein intersektorales Cyber-Cluster auf.
CODE ist das Forschungszentrum Cyber Defence an der UniBw, wo Bw Perso-

33 Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) GmbH, Bundesregierung.
Deutsche Gesellschaft für internationale Zusammenarbeit (GIZ) GmbH, IKT-Förderansatz der GIZ.
Hintergrundgespräche, 2018.

34 Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016.

35 Deutschland sicher im Netz, Presse.

nal wissenschaftlich ausgebildet wird. Es befindet sich im selben Gebäude wie ZITiS.[36]

Gemeinsames Melde- und Lagezentrum (GMLZ)
Das Gemeinsame Melde- und Lagezentrum (GMLZ) hat die Aufgabe für Bund, Länder und Fachbehörden ein einheitliches Lagebild für den Bevölkerungsschutz abzubilden. Dafür verfolgt und bewertet es rund um die Uhr relevante Geschehnisse im In- und Ausland und berichtet im täglichen Lagebericht oder gezielten Lagemeldungen.
Das GMLZ übernimmt nachts die Aufgaben des LZ. Das BBK ist im GMLZ vertreten.[37]

German Competence Centre against Cyber Crime (G4C)
Das German Competence Centre against Cyber Crime (G4C) ist ein Verein, der unterschiedliche Akteure in einer strategischen Allianz gegen Cyber-Kriminalität zusammenbringt. Durch einen täglichen Informationsaustausch zwischen den behördlichen Kooperationspartnern und den Mitgliedern, können diese geeignete Schutzmaßnahmen entwickeln.
Das G4C kooperiert mit dem BKA und dem BSI.[38]

Initiative IT-Sicherheit in der Wirtschaft
Die Initiative IT-Sicherheit in der Wirtschaft ist eine Initiative des BMWi für kleine und mittlere Unternehmen. Eine Vielzahl von Aktivitäten werden von der Initiative gebündelt. Die Mitglieder des Steuerkreises sind IT-Experten aus Verwaltung, Wissenschaft und Wirtschaft und beraten die Initiative IT-Sicherheit in der Wirtschaft bei der Umsetzung ihrer Projekte.
Die Initiative IT-Sicherheit in der Wirtschaft, ist eine Initiative des BMWi. In ihrem Rahmen wird u. a. das "Bottom-Up" Projekt von DsiN betrieben.[39]

Initiative Wirtschaftsschutz
Die Initiative Wirtschaftsschutz hat das Ziel den Schutz wichtiger Unternehmenswerte der deutschen Wirtschaft zu verbessern. Das BMI koordiniert die Zusammenarbeit von staatlichen Stellen und Wirtschaftsverbänden. Die Initiative bietet ein umfangreiches Schutzkonzept aus Maßnahmen, Handlungsempfehlungen und Seminaren.
Die Initiative Wirtschaftsschutz arbeitet auf staatlicher Seite mit dem BND,

36 Universität der Bundeswehr München, Forschungsinstitut CODE.

37 Bundesministerium des Innern, für Bau und Heimat, Das Gemeinsame Melde- und Lagezentrum von Bund und Ländern.

38 German Competence Centre against Cyber Crime e.V. (G4C), Über uns.

39 Bundesministerium für Wirtschaft und Energie, Steuerkreis. Bundesministerium für Wirtschaft und Energie, "Erste Berufsschulen in Niedersachsen setzen auf Bottom-Up für mehr IT-Sicherheit im Mittelstand".

BfV, BKA und dem BSI zusammen.[40]

IT-Sicherheitskatalog
Der IT-Sicherheitskatalog wurde gemeinsam von der BNetzA und dem BSI herausgebracht. Er verpflichtet alle Betreiber von Gas- und Stromnetzen dazu ein angemessenes Sicherheitsniveau ihrer Telekommunikations- und EDV-Systeme zu garantieren.
Beim IT-Sicherheitskatalog kooperieren BNetzA und BSI.[41]

Kompetenznetzwerk Trusted Cloud (Trusted Cloud)
Das Kompetenznetzwerk Trusted Cloud (Trusted Cloud) ist aus dem gleichnamigen Programm des BMWi entstanden, welches ein Gütesiegel für Cloud Services entwickelt und etabliert hat. Trusted Cloud dient als neutrale und branchenübergreifende Plattform für den Austausch zwischen Cloud-Anbietern und Anwendern.
Trusted Cloud wurde durch das BMWi ins Leben gerufen.[42]

Kompetenz- und Forschungszentren für IT-Sicherheit
Die drei Kompetenz- und Forschungszentren für IT-Sicherheit in Saarbrücken, Darmstadt und Karlsruhe sind Bestandteil der Digitalen Agenda des BMBF. Mit der Gründung der drei Forschungszentren hat die Bundesregierung die Forschung und Entwicklung im Bereich Cyber-Sicherheit und Schutz der Privatsphäre maßgeblich ausgeweitet.
Die drei Kompetenz- und Forschungszentren für IT-Sicherheit werden durch das BMBF gefördert.[43]

Länder-CERTs
Die Länder-CERTs sind die Computer Emergency Response Teams der einzelnen Bundesländer. Im Rahmen des Verwaltungs-CERT-Verbunds (VCV) kooperieren Bund und Länder beim Aufbau und Betrieb der Länder-CERTs.
Die Länder-CERTs kooperieren mit dem CERT-Bund im BSI.[44]

40 Initiative Wirtschaftsschutz, Aktuelles.

41 IT-Sicherheitskatalog, Kernforderungen und Inhalt des IT-Sicherheitskatalogs.

42 Bundesministerium für Wirtschaft und Energie, Das Kompetenznetzwerk Trusted Cloud.

43 Kompetenz- und Forschungszentren für IT-Sicherheit, Über uns.

44 Niedersächsisches Computer Emergency Response Team N-CERT, 2016, Kooperation der CERTS im Verwaltungs-CERT-Verbund (VCV).

Landesamt für Sicherheit in der Informationstechnik Bayern (LSI)
Das Landesamt für Sicherheit in der Informationstechnik Bayern (LSI) hat sich mit seiner Gründung im Dezember 2017 den Schutz staatlicher IT-Infrastrukturen zur Aufgabe gemacht. Es soll Kommunen und Bürger beratend unterstützen.
Das LSI ist Mitglied im VCV, beheimatet das Bayern-CERT und kooperiert mit dem BSI.[45]

Nationales Cyber-Abwehrzentrum (NCAZ/ Cyber-AZ)
Das Nationale Cyber-Abwehrzentrum (NCAZ oder Cyber-AZ) hat die Aufgabe die operative Zusammenarbeit hinsichtlich verschiedener Gefährdungen im Cyber-Raum zwischen staatlichen Stellen zu optimieren und entsprechende Schutz- und Abwehrmaßnahmen zu koordinieren. Dafür werden im Cyber-AZ, welches im BSI angesiedelt ist, alle Informationen zu Cyber-Angriffen auf IT-Infrastruktur gebündelt. Aktuell wird in der Regierung eine Ausweitung zum sogenannten "Cyber-AZ Plus" diskutiert.
Das Cyber-AZ ist eine Kooperationsplattform zwischen BSI, BPol, BKA, BfV, BBK, Bw, ZKA und MAD.[46]

Nationales IT-Lagezentrum (LZ)
Das Nationale IT-Lagezentrum (LZ) im BSI hat die Aufgabe 24 Stunden täglich ein IT-Lagebild zu erstellen, um auftretende IT-Sicherheitsvorfälle für staatliche Stellen und Wirtschaftsunternehmen schnell einschätzen zu können. Nachts übernimmt das GMLZ die Funktion.
Das LZ arbeitet eng mit dem GMLZ, CERT-Bund und Cyber-AZ zusammen.[47]

Stiftung Wissenschaft und Politik (SWP)
Die Stiftung Wissenschaft und Politik (SWP) berät Bundestag und Bundesregierung, sowie internationale Organisationen zu außen- und sicherheitspolitischen Fragen und ist dabei politisch unabhängig. Ihre Forschung umfasst auch Digitalisierungs- und Cyber-Sicherheitsthemen.
Die SWP erhält ihre institutionelle Zuwendung vom BKAmt.[48]

Umsetzungsplan Kritische Infrastrukturen (UP KRITIS)
Der Umsetzungsplan Kritische Infrastrukturen (UP KRITIS) hat die Aufgabe, die Versorgung durch Kritische Infrastrukturen zu erhalten. Dafür dient UP KRITIS als öffentlich-private Kooperation zwischen staatlichen Stellen,

45 Landesamt für Sicherheit in der Informationstechnik Bayern, Startseite.

46 Bundesamt für Sicherheit in der Informationstechnik, Cyber-Abwehrzentrum.

47 Bundesamt für Sicherheit in der Informationstechnik, Nationales IT-Lagezentrum.

48 Stiftung Wissenschaft und Politik, Cyber-Sicherheit.
Stiftung Wissenschaft und Politik, Über uns.

Betreibern Kritischer Infrastrukturen und ihren Verbänden. Da Informations- und Kommunikationstechnik einen immer größerer Bestandteil von Kritischen Infrastrukturen darstellt, kommt ihrem Schutz eine zentrale Rolle zu.
Im Rahmen des UP KRITIS kooperieren von staatlicher Seite BMI, BSI und BBK.[49]

Universität der Bundeswehr München (UniBw)
Die Universität der Bundeswehr München (UniBw) bildet Offiziere und Offiziersanwärter wissenschaftlich aus. Die Studiengänge umfassen aktuell Informatik, Cyber-Sicherheit, Mathematical Engineering und Wirtschaftsinformatik.
Die UniBw bildet Bw Personal wissenschaftlich aus und beheimatet CODE als fakultätsübergreifendes Forschungszentrum.[50]

Verwaltungs-CERT-Verbund (VCV)
Der Verwaltungs-CERT-Verbund (VCV) ist eine Plattform zum gegenseitigen Informationsaustausch zwischen dem CERT Bund und den vorhandenen Länder-CERTs. So soll die IT-Krisenprävention und -reaktion gestärkt und die IT-Sicherheit in der öffentlichen Verwaltung verbessert werden.
Am VCV beteiligt sind das BSI, Länder CERTs, sowie das LSI.[51]

Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft (ZAC)
Die Zentralen Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft (ZAC) stehen Unternehmen präventiv und reaktiv im Falle von Internetstraftaten zur Verfügung. In jedem Bundesland ermitteln speziell ausgebildete Polizeibeamte gemeinsam mit IT-Spezialisten.
Die ZAC sind u.a. bei der BPol angesiedelt.[52]

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)
Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) entwickelt, forscht, unterstützt und berät die deutschen Sicherheitsbehörden in den folgenden Bereichen: Digitale Forensik, Telekommunikations-

49 Internetplattform zum Schutz Kritischer Infrastrukturen, Zusammenarbeit im Rahmen des UP KRITIS.
Internetplattform zum Schutz Kritischer Infrastrukturen, UP KRITIS: Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen.

50 Universität der Bundeswehr München, Hintergrundinformationen.

51 Niedersächsisches Computer Emergency Response Team N-CERT, 2016, Kooperation der CERTS im Verwaltungs-CERT-Verbund (VCV).

52 Der Polizeipräsident in Berlin, Zentrale Ansprechstelle Cybercrime für die Wirtschaft im LKA Berlin.
Bundeskriminalamt, Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft.

überwachung, Krypto- und Big-Data-Analyse. Darüber hinaus arbeitet ZITiS auch zu technischen Fragen im Bereich der Kriminalitätsbekämpfung, Gefahren- und Spionageabwehr.
ZITiS wurde vom BMI gegründet. Sie versorgt BKA, BfV und BPol mit ihrer Expertise. Sie ist auf dem Campus der UniBw angesiedelt und befindet sich so auch in geographischer Nähe zu CODE.[53]

Zollkriminalamt (ZKA)
Das Zollkriminalamt (ZKA) gehört zum Geschäftsbereich des BMF und ist für die Prävention und Aufklärung von mittlerer, schwerer und organisierter Zollkriminalität verantwortlich. Dabei koordiniert das ZKA die Ermittlungen der einzelnen Zollfahndungsämter und kann in besonderen Fällen auch eigene Ermittlungen aufnehmen. Dies erstreckt sich auch auf den Cyber-Raum.
Das ZKA ist dem BMF nachgeordnet und ist im Cyber-AZ vertreten.[54]

53 Zentrale Stelle für Informationstechnik im Sicherheitsbereich, Aufgaben & Ziele.
54 Der Zoll, Die Aufgaben des Zolls.

Impressum

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Grafik:
Niña Duman

Free Download:

www.stiftung-nv.de