/ PD-Perspektiven /

Mehr Cybersicherheit durch Kooperationen auf Länderebene

1. Oktober 2021

/ Für die öffentliche Hand von morgen /

Inhaltsverzeichnis

Mehr Cybersicherheit durch Kooperationen auf Länderebene

Die zunehmende Digitalisierung der öffentlichen Verwaltung führt zu einer immer größeren Menge an Daten im digitalen Raum. Dadurch wächst auch die Gefahr von Cyberangriffen auf die öffentliche IT-Infrastruktur.

Erfolgreiche Kooperationen auf Länderebene zeigen, wie ein höheres Maß an Cybersicherheit erreicht werden kann. Die Zusammenarbeit kann dabei sowohl öffentlich-öffentlich als auch öffentlich-privat organisiert sein:

1. **Sicherheitskooperation Cybercrime**

Die seit 2011 existierende Sicherheitskooperation Cybercrime ist eine **öffentlich-private Kooperation**, an der mittlerweile **sechs Landeskriminalämter** teilnehmen und die durch den Digitalverband Bitkom koordiniert wird. Die Kooperation ist auf unbegrenzte Zeit angelegt und bietet eine Plattform, um das **Bewusstsein für die Gefahren durch Cybercrime** zu schärfen und diesen gemeinsam zu begegnen. Zu den Maßnahmen gehören beispielsweise **regelmäßige Sprechstunden für Unternehmen** oder **gegenseitige Hospitationen**.

2. **Kooperation zwischen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und den Ländern**

Seit 2017 unterhält das **BSI regionale Kooperationsvereinbarungen** mit den Ländern. Dies sind aktuell Hessen, Rheinland-Pfalz, Niedersachsen, Nordrhein-Westfalen, Berlin, Baden-Württemberg, Saarland, Sachsen, Thüringen, Brandenburg und Mecklenburg-Vorpommern. Durch seine Erfahrung **hilft das BSI den Ländern beim Aufbau länderspezifischer Informationssicherheitssysteme** und steht als **Ansprechpartner** bei Vorfällen zur Verfügung. Die Zusammenarbeit und der enge Austausch mit dem BSI erhöhen das Gesamtsicherheitsniveau in den Ländern.

3. **Organisationseinheiten zur Cyberabwehr auf Länderebene**

Auf der **Ebene der Länder** haben verschiedene Organisationseinheiten zur Cyberabwehr zu einer Ressourcen- und Kompetenzbündelung sowie einem erhöhten allgemeinen Sicherheitsniveau geführt: Die Cybersicherheitsagentur Baden-Württemberg (2020), Cyberabwehr Bayern (2020), das Hessen CyberCompetenceCenter (Hessen3C/2019) und die Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen (2020). Sie fungieren unter anderem als **Aufklärungs-, Informations- und Koordinierungsstelle** für **Unternehmen** und weitere **Behörden** in den Ländern.

*Hieraus ergeben sich **acht Empfehlungen für den Aufbau erfolgreicher Cybersicherheitskooperationen** in den Ländern:*

1. Im Vorfeld einer Kooperation sollten **Ziele definiert** und mit einem **konkreten Zeit- und Maßnahmenplan** sowie **eindeutigen Verantwortlichkeiten** hinterlegt werden. Um den nachhaltigen Erfolg zu gewährleisten, sollten zudem personelle und technische **Ressourcen gemeinsam genutzt** werden.

2. Die jeweiligen **Leitungsebenen** sollten bei der Anbahnung beziehungsweise Durchführung einer Kooperation **umfassend involviert** sein, um das **Bewusstsein** für die **Bedeutung der Zusammenarbeit** zu schaffen.

3. Die Verortung der Kooperation auf der Leitungsebene wird insbesondere vor dem Hintergrund der benötigten **Ressourcen zur Umsetzung der Kooperation** relevant.

4. Um Kooperationen zu institutionalisieren, braucht es **Personal**. Dabei kann die **Einrichtung einer koordinierenden Stelle** hier Entlastung schaffen.

5. Vor dem Hintergrund der sensiblen Daten, die im Bereich von Cybersicherheit ausgetauscht werden, ist für das Gelingen einer Kooperation **Vertrauen auf allen Ebenen der Teilnehmenden** essenziell.

6. Durch die **Kontinuität** der Teilnehmenden an der **Kooperation** kann dieses Vertrauen erzeugt werden.

7. Die Teilnehmenden sollten trotz der unterschiedlichen Hintergründe und Interessen **ein gewisses Maß an Neutralität** bewahren. Dies ist insbesondere bei öffentlich-privaten Kooperationen der Fall.

8. Durch die die Definition von Handlungsfeldern und Maßnahmen sollte die **Kooperation mit Leben erfüllt werden**. Diese Maßnahmen entscheiden schlussendlich auch über die **Tiefe der Kooperationen** und den damit verbundenen **Mehrwert** für den **Beitrag zur Cybersicherheit**.

Dr. Youssef Dhaibi
Direktor

Juri Denecke
Manager

Sie möchten mehr erfahren?

pd-g.de/pd-perspektiven-reihe/kooperationen-zur-cybersicherheit

PD – Berater der öffentlichen Hand
Friedrichstr. 149, 10117 Berlin

pd-g.de/

Stand: Oktober 2021

1 Einleitung

Die Digitalisierung ist eine aktuell anhaltende und sich stetig fortsetzende Entwicklung unserer Zeit[1] und birgt zahlreiche Vorteile für die Politik, Wirtschaft und Gesellschaft. Mit ihr geht die **fortschreitende Nutzung digitaler Anwendungen** und die verstärkte Produktion von privaten und staatlichen Daten einher. Längst wurden diese Daten und das damit verbundene **Schadenspotenzial** als aus Sicht der Angreifenden lukrative Ziele für Cyberattacken erkannt. Nicht nur persönliche Daten der Bürgerinnen und Bürger sind von hoher Relevanz für Datenmissbrauch, sondern insbesondere auch die staatliche, interministerielle Kommunikation, Berichte und Verschlusssachen.

Politik und Verwaltung beobachten diese Entwicklungen mit berechtigter Sorge. Um potenziellen Schaden vom Staat abzuwenden, wurde bereits eine Reihe von Maßnahmen ergriffen. Auf Bundesebene wurden im Rahmen der „**Cyber-Sicherheitsstrategie für Deutschland**“[2], die im September 2021 aktualisiert wurde, zahlreiche strategische und operative Maßnahmen identifiziert und umgesetzt. Auf Landes- und Kommunalebene werden aufgrund von Föderalismus und uneinheitlicher Ressourcenverfügbarkeit dezentrale Ansätze verfolgt. Diese sind zum Teil weniger weit gediehen, wenn es um die jeweilige Bedrohungsanalyse und die Maßnahmen zur Abwehr oder die grundsätzliche Steigerung systemischer Widerstandsfähigkeit geht.

Bei der Lösungssuche besteht auf der Bundes- und Föderalebene gleichermaßen Einigkeit, dass **Cybersicherheit nicht von einem einzigen Akteur gewährleistet** werden kann. Insbesondere auf Länderebene sind daher **Kooperationen in den Fokus** gerückt, da auf dieser Ebene weniger Ressourcen verfügbar sind. Dabei zeigt sich, dass die Zusammenarbeit dann besonders fruchtbar ist, wenn sie **durch eine zentrale Stelle auf Länderebene koordiniert** wird. Von den zahlreichen öffentlich-öffentlichen, aber auch öffentlich-privaten Kooperationen auf Länderebene werden in der **vorliegenden PD-Perspektiven-Veröffentlichung**[3] einige als Best Practices detaillierter vorgestellt. Sie können weiteren interessierten Ländern als Grundlage zum Aus- und Aufbau eigener kooperativer Strukturen dienen. Kooperationen ausschließlich zwischen Wirtschafts- beziehungsweise Forschungseinrichtungen werden hier nicht betrachtet.

Im öffentlichen Sektor **auf Länderebene** wird noch **großes Potenzial** bei der **Einrichtung und Nutzung von Kooperationen** gesehen. Auf diese Weise trägt dieser Beitrag dazu bei, die Literatur zur bestehenden Kooperationslandschaft zu erweitern. Es zeigt sich, dass Kooperationen Akteure übergreifend auf Länderebene gedacht werden sollten, um den größtmöglichen Nutzen in der Cyberabwehr herzustellen. Zusammenfassend kann festgestellt werden, dass Kooperationen auf Länderebene das Potenzial haben, die Cybersicherheit zu erhöhen.

Die PD empfiehlt daher, bei der Schaffung von zentralen Koordinierungsstellen den **Kooperationsgedanken** von Anfang an mitzudenken. Dazu gehören klare Kommunikationsstrukturen, die im Falle eines Angriffes eine schnelle, sichere und effiziente Krisenbewältigung innerhalb der Kooperation herstellen. Zentrale Stellen auf Länderebene, die Informationen in den jeweiligen Ländern bündeln, können als entscheidende Schnittstelle zum Bundesamt für Sicherheit in der Informationstechnik (BSI) agieren.

[1] Zukunftsinstitut (2020): Die Megatrends, https://www.zukunftsinstitut.de/dossier/megatrends/, abgerufen am 27.05.2021.

[2] Bundesministerium des Innern (2016): Cyber-Sicherheitsstrategie für Deutschland (2016): https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf, abgerufen am 27.05.2021.

[3] Als Basis für diese Veröffentlichung dienten – neben Recherchen – Interviews mit Mitgliedern der öffentlichen Verwaltung, Wirtschaft und Wissenschaft. Die Meinungen der Expertinnen und Experten sind in anonymisierter Form in den Bericht eingeflossen.

2 Bedrohungslage für die öffentliche Verwaltung

Die Bundesregierung definiert in der Cybersicherheitsstrategie (2011, 2016 und 2021 überarbeitet) Cybersicherheit als **„die IT-Sicherheit der im Cyber-Raum auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme**“.[4] Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen, IT-Netzen oder von Informationen ist dann gewährleistet, wenn das jeweilige System wie vorgesehen funktioniert. Ziel ist deshalb, die Verfügbarkeit der Systeme und Anwendungen möglichst hoch zu halten. In der Cybersicherheitsstrategie wird darauf hingewiesen, dass Angriffe auf staatliche Institutionen die Funktionsfähigkeit von Verwaltung, Streitkräften und Sicherheitsbehörden beeinträchtigen und somit erhebliche Auswirkungen auf die öffentliche Sicherheit und Ordnung in Deutschland haben können.

Immer mehr Cyberangriffe auf Verwaltungen

Tatsächlich wird der Verwaltungsapparat in Deutschland immer häufiger Ziel von Cyberangriffen. In den letzten Jahren ist die Zahl der Angriffe auf die Netze der öffentlichen Verwaltung kontinuierlich gestiegen. Dabei stand 2017 insbesondere die Bundestagswahl im Fokus von Cyberangriffen aus dem Ausland. So wurde beispielsweise die offizielle Webseite der CDU imitiert, um falsche Informationen zu verbreiten.[5] Die temporäre Abnahme der Angriffe im Jahr 2018 ist auf den starken Rückgang von „Ransomware“ (Erpressungssoftware) und „Distributed Denial of Service“-Angriffen[6] zurückzuführen. Doch im Jahr 2019 hat sich der Trend weiter fortgesetzt.[7]

Anzahl der E-Mails mit Schadprogrammen in Regierungsnetzen

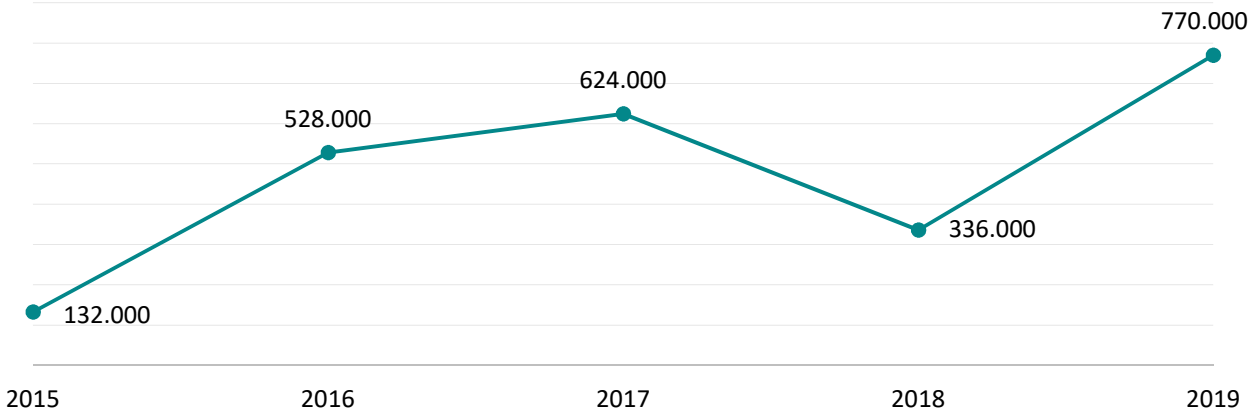


Abbildung 1: Zunahme der Angriffe durch E-Mails mit Schadprogrammen auf Regierungsnetze

[4] Bundesministerium des Innern (2016): Cyber-Sicherheitsstrategie für Deutschland (2016), https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html, abgerufen am 27.05.2021.

[5] Bundesministerium des Innern, für Bau und Heimat (2017): Verfassungsschutzbericht 2017, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/vsb-2017.pdf;jsessionid=3FDBB0AF164ABFCFC37F64558E89977C.1_cid295?__blob=publicationFile&v=11, abgerufen am 27.05.2021.

[6] Distributed Denial of Service = DDoS. Damit ist ein Cyberangriff gemeint, der durch mutwillig herbeigeführte Überlastung beispielsweise einer öffentlichen IT-Infrastruktur dafür sorgt, dass ein Onlinedienst nicht mehr oder nur noch eingeschränkt für die Nutzenden verfügbar ist.

[7] Bundesamt für Sicherheit in der Informationstechnik (2018): Die Lage der IT-Sicherheit in Deutschland 2018, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf;jsessionid=AB81F773C77F7BE65FE5B9FCF6616FE8.1_cid503?__blob=publicationFile&v=6, abgerufen am 27.05.2021.

Im Jahr 2017 wurde auch die öffentliche Verwaltung sowie die **kritische Infrastruktur**[8] zu Zielen und waren von Krypto-Ransomware durch „WannaCry“ und der Schadsoftware „NotPetya“ betroffen. Beide Programme nutzten Schwachstellen in Microsoft-Anwendungen aus, um bestimmte Nutzungsdateien zu verschlüsseln. Die Nutzenden wurden aufgefordert, innerhalb einer Frist **Lösegeld in Bitcoin** zu zahlen. Oft erhalten die Lösegeldzahlenden einen Code, um die verschlüsselten Nutzungsdateien wieder zu entschlüsseln. Durch eine Art Hintertür konnte das Schadprogramm in weitere Windows-Rechner eindringen. Schätzungen gehen davon aus, dass durch die **Schadsoftware „WannaCry“** weltweit **230.000 Systeme infiziert** wurden. Durch die niedrige Erpressungssumme von circa 425 Euro wurde die Schwelle für die Nutzenden absichtlich gering gehalten.[9]

Meldungen über Angriffe auf KRITIS-Einrichtungen

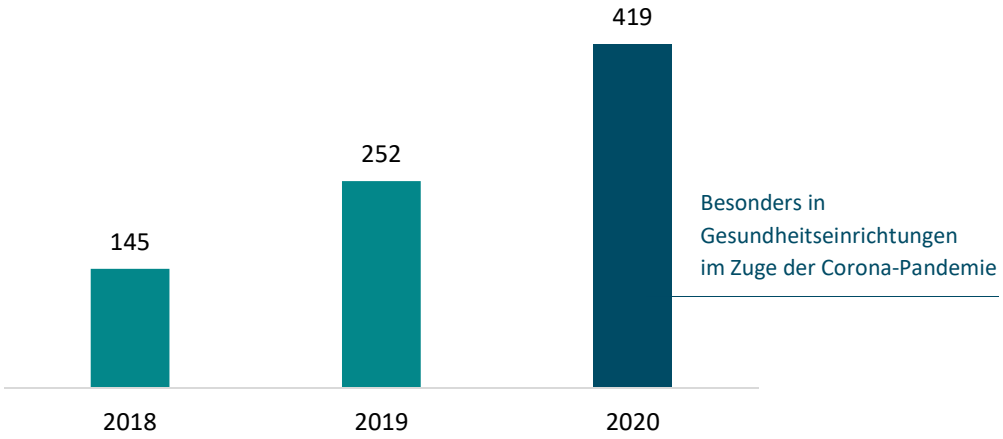


Abbildung 2: Meldungen über Angriffe auf KRITIS-Einrichtungen[10]

Das **BSI** – als **„Spinne im Netz“** – bündelt sämtliche **Meldungen und Informationen über Cyberangriffe** auf Verwaltungsstrukturen und **koordiniert deren Abwehr**. Der Staat bekommt innerhalb der innenpolitischen Dimension die Aufgabe, kritische Infrastruktureinrichtungen zu schützen, um die freiheitliche Sicherheit und Ruhe zu bewahren. Von den 1.500 Einrichtungen in Deutschland meldete knapp ein Drittel einen Cyberangriff. Die Dunkelziffer liegt wahrscheinlich noch viel höher.[11]

[8] Zur Definition von kritischen Infrastrukturen (KRITIS) siehe: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html (abgerufen am 21.09.2021)

[9] Bundeskriminalamt (2017): BKA stellt Bundeslagebild Cybercrime 2017 vor, https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2018/Presse2018/180927_BundeslagebildCybercrime.html, abgerufen am 27.05.2021.

[10] Bundesamt für Sicherheit in der Informationstechnik (2020): Die Lage der IT-Sicherheit in Deutschland 2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2, abgerufen am 27.05.2021.

[11] Bundesamt für Sicherheit in der Informationstechnik (2019): Die Lage der IT-Sicherheit in Deutschland 2019, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7, abgerufen am 27.05.2021.

Ein 2020 beispielhaft bekannt gewordener Fall ist die Infizierung von Rechnern des Berliner Kammergerichts mit der Schadsoftware „Emotet“[12/ 13]. Eine Untersuchung zeigt, dass die Schadsoftware über Tage hinweg auf den Systemen ungehindert Daten abziehen konnte.[14] Die Höhe des dadurch entstandenen Schadens kann bis heute nicht beziffert werden. Klar ist jedoch, dass der Aufbau einer neuen IT-Infrastruktur beim Berliner Kammergericht viel Zeit und Geld kosten wird.

Cyberkriminelle verfolgen meist eines oder mehrere der nachstehend genannten Ziele:

- Erpressung von Lösegeld
- Spionage
- Destabilisierung des politischen Systems
- Aufmerksam machen auf einen gesellschaftlichen Missstand

Aufgrund des derzeit noch jungen und fragmentierten Rechtsrahmens sind **Cyberangriffe** bislang nur **schwer attributierbare**, zuzuordnende und damit rechtlich zu sanktionierende **Formen der Kriminalität**. Die Chancen für eine effektive Strafverfolgung sind dementsprechend gering und Kriminelle profitieren von diesen Lücken im System.

Durch seine Neuartigkeit und die Fähigkeit, sich schnell weiterzuentwickeln, erhält das Phänomen Cyberkriminalität zusätzlichen Auftrieb durch die grenzüberschreitenden Möglichkeiten des „Internet of Things“[15]. Aktuell findet ein **„Wettlauf“** zwischen der Seite der **Angreifenden** und der Seite der **Verteidigenden** statt. Angreifende suchen fortwährend neue Angriffsflächen und Möglichkeiten, diese zu betreten. Die Verteidigenden hingegen müssen auf immer ausgeklügelter werdende Angriffe reagieren und diese – im besten Fall – antizipieren, um sie von vorneherein zu verhindern.

2.1 Einflussfaktoren für die aktuelle Bedrohungslage der öffentlichen Verwaltung

In den folgenden Unterabschnitten werden sechs Trends identifiziert, die sowohl einzeln als auch in Kombination einen ungemein schädigenden Einfluss auf die Cybersicherheit haben und somit die Bedrohungslage der öffentlichen Verwaltung im Bereich Cybersicherheit vergrößern.

2.1.1 Zunehmende Digitalisierung der öffentlichen Verwaltung

Die **Digitalisierung der Verwaltung** verläuft entlang zweier Stränge. Zum einen soll das Serviceangebot für die Bürgerinnen und Bürger sukzessiv digitalisiert werden. Wie im Onlinezugangsgesetz (OZG) festgelegt ist, sollen in den kommenden Jahren rund 575 Dienstleistungen verfügbar gemacht werden.[16] Dies bringt **viele Vorteile** für die **Bürgerinnen und Bürger** sowie die **Mitarbeitenden in den Behörden**. Verschiedene

[12] Haufe-Lexware GmbH & Co. KG (2020): Folgenschwere Cyber-Attacke auf das Kammergericht Berlin, https://www.haufe.de/recht/kanzleimanagement/cyber-attacke-auf-kammergericht-mit-emotet-malware_222_509238.html, abgerufen am 28.05.2021.

[13] Weitere Beispiele sind der Angriff auf High-Performance-Computing-Systeme (HPC) Anfang Mai 2020 sowie die Angriffe auf die Stadtverwaltungen von Potsdam und Brandenburg im Februar 2020. Siehe https://www.egovernment-computing.de/nach-cyberattacke-potsdamer-stadtverwaltung-offline-a-899249/; https://www.it-daily.net/shortnews/24714-best-of-hacks-highlights-mai-2020.

[14] Schmidt, Jürgen (27.01.2020): Emotet: IT-Totalschaden beim Kammergericht, https://www.heise.de/security/meldung/Emotet-IT-Totalschaden-beim-Kammergericht-Berlin-4646568.html, abgerufen am 27.05.2021.

[15] Zur Definition von „Internet der Dinge“ (IoT) siehe auch: https://de.wikipedia.org/wiki/Internet_der_Dinge

[16] IT-Planungsrat (2020): Flächendeckende Digitalisierung der Verwaltung Deutschlands bis 2022, https://www.it-planungsrat.de/DE/ITPlanungsrat/OZG-Umsetzung/OZG_Umsetzung_node.html, abgerufen am 27.05.2021.

Services können jederzeit ohne Wartezeiten und ressourcenschonend abgerufen werden. Die Bürgerinnen und Bürger können „Behördengänge“ bequem von zu Hause aus erledigen und sparen dadurch Zeit und Geld. Gleichzeitig haben die Mitarbeitenden in den Behörden mehr Zeit für die Präsenzkundschaft, wenn viele Arbeitsschritte automatisiert sind.

Zum anderen sollen aber auch wesentliche interne Ablauf- und Arbeitsprozesse der Verwaltung weiter digitalisiert und konsolidiert werden, wie zum Beispiel durch das Vorhaben „IT Konsolidierung Bund“. Dabei sollen für Bundesbehörden unter anderem technische Standardarchitekturen und -prozesse sowie IT-Betriebskonsolidierungen konzipiert und umgesetzt werden.[17]

Um nur ein weiteres prominentes Beispiel der Digitalisierungsbestrebung der Verwaltung zu nennen, ermöglicht die Einführung von E-Akten auf Basis des E-Government-Gesetzes von 2013 ein revisionssicheres und zeitgleiches Bearbeiten.

Effektiver Schutz gegen steigende Zahl von Cyberattacken nötig

Der Umzug von Verfahren und Prozessen in den digitalen Raum führt im Umkehrschluss zu einer ständigen digitalen Verfügbarkeit und Speicherung von Daten. Dies bedeutet eine sprunghafte Erhöhung der Anzahl potenzieller Angriffsziele. Somit bedarf es bei all den Digitalisierungsbestrebungen eines effektiven Grundschutzes für die durch Behörden vorgehaltenen Daten sowie deren Systeme und Netze.

Durch die vergleichsweise geringe Digitalisierungsquote im Vergleich zu anderen europäischen Staaten waren die deutschen Systeme in den letzten Jahren relativ gesehen nicht so stark von Angriffen betroffen. Laut „Index für digitale Wirtschaft und Gesellschaft in der EU (DESI) 2020“ liegt Deutschland auf Platz 12 der insgesamt 27 europäischen Länder und Großbritannien. Bei der **Digitalisierung der Verwaltungsdienste** erreicht **Deutschland nur noch den 21. Rang** und bleibt weit hinter den europäischen Spitzenreitern der digitalen Verwaltung wie Estland, Spanien, Dänemark, Finnland und Lettland[18] zurück. Dementsprechend ist davon auszugehen, dass mit der **fortschreitenden Digitalisierung der Verwaltung** die Zahl der **Angriffe weiter zunehmen** wird.

Auf **Länderebene** ergibt sich ein **heterogenes Bild**. Die Digitalisierung der öffentlichen Verwaltung verläuft mit unterschiedlicher Geschwindigkeit[19] und beeinflusst damit die Anzahl von Cybersicherheitsvorfällen und den Stellenwert von Cybersicherheit auf Länderebene. Aber auch die Spezifika eines jeden Bundeslandes (wie beispielweise Einwohner-, Wirtschafts- und Unternehmensstruktur) bestimmen die Bedrohungslage der Länderverwaltungen und deren unternommene Anstrengungen im Bereich der Cybersicherheit.

2.1.2 Künstliche Intelligenz

Die Bundesregierung hat Künstliche Intelligenz (KI) längst als eine der Zukunftstechnologien für Deutschland identifiziert und ist bereit, in deren Weiterentwicklung am Forschungsstandort Deutschland zu investieren. Dies belegt nicht nur die im Jahr 2018 verabschiedete „**Strategie Künstliche Intelligenz**“[20], sondern auch

[17] Bundesministerium der Finanzen (2020): IT-Betriebskonsolidierung des Bundes, https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Ministerium/abteilung-vi-it-betriebskonsolidierung-des-bundes.html, abgerufen am 27.05.2021.

[18] Europäische Kommission (2020): Deutschland im digitalen Vergleich in der EU an Platz zwölf, https://ec.europa.eu/germany/news/20200611-digitalisierung_de, abgerufen am 27.05.2021.

[19] Opiela, Nicole et al. (2019): Deutschland-Index der Digitalisierung 2019, Berlin: Kompetenzzentrum Öffentliche IT, http://www.oeffentliche-it.de/publikationen, abgerufen am 19.02.2021.

[20] Bundesregierung (2020): Strategie Künstliche Intelligenz, https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/strategie-kuenstliche-intelligenz-fortschreibung-2020.html#:~:text=Strategie%20K%C3%BCnstliche%20Intelligenz%20der%20Bundesregierung%20Fortschreibung%202020%20Download,%28KI%29%20seit%20Beschluss%20der%20Strategie%20im%20November%202018.

die zusätzlichen durch das Corona-Konjunkturprogramm zugewiesenen Mittel zur Umsetzung der Strategie[21].

Diese neue Technologie wird auch die **Bedrohungslage bei der Cybersicherheit** verschärfen. Ein Großteil der Angriffe auf ein Computernetzwerk wird nicht mehr komplett durch Menschenhand gesteuert. Eine viel beachtete Studie, herausgegeben vom „Future of Humanity Institute" der University of Oxford[22], identifiziert **drei mögliche Effekte** durch den Einsatz von **Künstlicher Intelligenz** bei **Cyberangriffen**:

1. Bisherige **Angriffsstrategien werden erweitert**, zum Beispiel durch automatisierte Recherche von Informationen.
2. Neue Bedrohungen entstehen, zum Beispiel durch gezielte Angriffe auf **KI-Systeme der öffentlichen Hand**.
3. Der Charakter der Angriffe verändert sich hin zu **effektiveren, effizienteren** und dadurch **skalierbaren Angriffen**.

Drei mögliche Szenarien, wie Cyber-Kriminelle Künstliche Intelligenz einsetzen können

1. Social Engineering:

Bei Social-Engineering-Angriffen werden Opfer dazu verleitet, **sensible Informationen freiwillig preiszugeben**[23], zum Beispiel indem sich der **Angreifende als Vertrauensperson** oder **Kollege beziehungsweise Kollegin** ausgibt. Die gefälschten E-Mails, insbesondere die Signatur und der Inhalt der Nachricht, sehen daher nicht nur täuschend echt aus, sie verleiten die adressierte Person auch dazu, die eingefügten Links oder Anhänge zu öffnen. Dies bereitet der dort hinterlegten Schadsoftware eine Tür in das Zielsystem.

Künstliche Intelligenz erweitert die **Möglichkeiten für Social Engineering** enorm, da Überwachungssysteme, die bereits über einen längeren Zeitraum auf dem Zielcomputer laufen, das Nutzungsverhalten beobachten und auf dessen Grundlage möglichst plausible Gründe für eine infizierte E-Mail finden. Die andauernden Angriffswellen des **Trojaners „Emotet"** zeigen das hohe Bedrohungspotenzial von **KI-gestützten „Fake-Mails"**. Dabei gilt: Je echter die Nachricht wirkt, desto höher ist die Klick-Rate. Chatbots können bei der Generierung solcher Informationen gezielt eingesetzt werden. Über Social-Engineering-Angriffe können sich Angreifende Zugang zu geheimen – da zu authentifizierenden – Informationen von Behörden verschaffen.

2. KI-basierte Analyse von Schwachstellen:

Künstliche Intelligenz kann die Analyse von **Schwachstellen** in der **öffentlichen IT**, sogenannte Exploits, vereinfachen und somit das **Gefahrenpotenzial** erhöhen. Bekannte Muster von Code-Schwachstellen können gelernt und adaptiert werden. So können Schwachstellen schneller und für die Angreifenden kostenschonender durchgeführt werden. Exploits in den Systemen der öffentlichen Verwaltung werden auf dem

[21] Koalitionsausschuss (2020): Corona-Folgen bekämpfen, Wohlstand sichern, Zukunftsfähigkeit stärken. Ergebnis Koalitionsausschuss 3. Juni 2020, unter Ziff. 43: Erhöhung der Mittel zur Umsetzung der Strategie von 3 auf 5 Milliarden Euro, https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Schlaglichter/Konjunkturpaket/2020-06-03-eckpunktepapier.pdf?__blob=publicationFile&v=6, abgerufen am 27.05.2021.

[22] Brundage, Miles et al. (2018): The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf, abgerufen am 27.05.2021.

[23] Security Insider: Floyd, Blue; Schmitz, Peter (17.08.2017): Was ist Social Engineering?, https://www.security-insider.de/was-ist-social-engineering-a-633582/, abgerufen am 27.05.2021.

Schwarzmarkt sehr hoch gehandelt, sodass durch die Multiplikationsmöglichkeiten von Künstlicher Intelligenz hier ein hohes Bedrohungspotenzial vorliegt.[24] Um dem entgegenzuwirken, ist der **Einsatz von Künstlicher Intelligenz** auf der **Verteidigungsseite** dringend zu empfehlen, um Angriffspraktiken zu identifizieren und eigene Exploits möglichst früh zu erkennen.

3. Aussetzung von Authentisierungsverfahren:

Mithilfe von KI-Systemen können Angreifende Bilder beziehungsweise **Videos manipulieren** oder **Stimmen imitieren** und somit sogenannte **Deep Fakes**[25] erzeugen. Deep Fakes können gezielt für die Übermittlung von Des- und Falschinformationen eingesetzt werden. Daher sind mehrere Authentifizierungssysteme notwendig, um auf mehr als einem Weg den Wahrheitsgehalt bestimmter Informationen verifizieren zu können. Verschlüsselungssysteme werden vor dem Hintergrund steigender Rechenleistung und – perspektivisch gesehen – durch den Einsatz von Quantenkryptografie von Bedeutung sein.

2.1.3 Gefährdung digitaler Souveränität durch Abhängigkeit von ausländischen Produkten

Aktuell nutzen deutsche Verwaltungen gängige **Standardsoftware kommerzieller Anbieter**. Dazu zählen vor allem Produkte von Microsoft, die in diesem Bereich Marktführer sind.[26] Durch die flächendeckende Nutzung von Standardsoftware entsteht eine **Abhängigkeit** von diesen **Anbietern**, die auch negative Auswirkungen auf die IT-Sicherheit haben kann. Diese beinhaltet die **mangelnde Souveränität** in Bezug auf die in der Verwaltung **erzeugten Daten**. So haben nicht-einsehbare Quellcodes zur Folge, dass die öffentliche Verwaltung die Informationssicherheit von Drittanbietern – in diesem Falle Microsoft – nicht überprüfen kann.[27]

Darüber hinaus müssen Nutzende von Microsoft-Produkten rechtliche Unsicherheiten in Kauf nehmen, da die Nutzung von Telemetriekomponenten, wie sie bei der Software häufig zum Einsatz kommen, auch die Übermittlung von personenbezogenen Daten beinhaltet, über die die nutzende Person nicht informiert wird.[28]

Das Bundesministerium des Innern, für Bau und Heimat hat die Reduktion der Abhängigkeit von kommerziellen Software-Anbietern auf die politische Agenda gesetzt. Als ein Lösungsschritt wird die Nutzung von **Open-Source-Software** genannt, wie sie auch auf Länderebene vereinzelt zum Einsatz kommt.[29] Um diese Lösung bundesweit auszurollen, erfordert es jedoch noch die Schaffung einheitlicher Standards für die Nutzung, um Harmonisierungs- und Effizienzpotenziale zu erzielen.

---

[24] Brundage, Miles et al. (2018): The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf, abgerufen am 27.05.2021.

[25] Ein bekanntes Beispiel ist das täuschend echte Video des ehemaligen US-Präsidenten Barack Obama, das mit der Stimme des Schauspielers und Regisseurs Jordan Peele überspielt wurde. Siehe Kerkmann, Christof (20.09.2019): So echt sehen Deepfake-Videos aus, https://www.handelsblatt.com/technik/digitale-revolution/manipulation-mit-ki-so-echt-sehen-deepfake-videos-aus/25036770.html?ticket=ST-152131-TXnPta0jY4d2fSyeflyb-ap1, abgerufen am 27.05.2021.

[26] Strategy& (2019): Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern. Abschlussbericht August 2019, https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile, abgerufen am 27.05.2021.

[27] Ebd., S. 17.

[28] Ebd., S. 17.

[29] Der Beauftragte der Bundesregierung für Informationstechnik (2020): Stärkung der Digitalen Souveränität in der Öffentlichen Verwaltung. Machbarkeitsnachweise zu alternativen IT-Lösungen, https://www.cio.bund.de/SharedDocs/Kurzmeldungen/DE/2020/20200330_Machbarkeitsnachweise_download.pdf?__blob=publicationFile, abgerufen am 27.05.2021.

2.1.4 Sukzessiv gewachsene Cybersicherheitsarchitektur

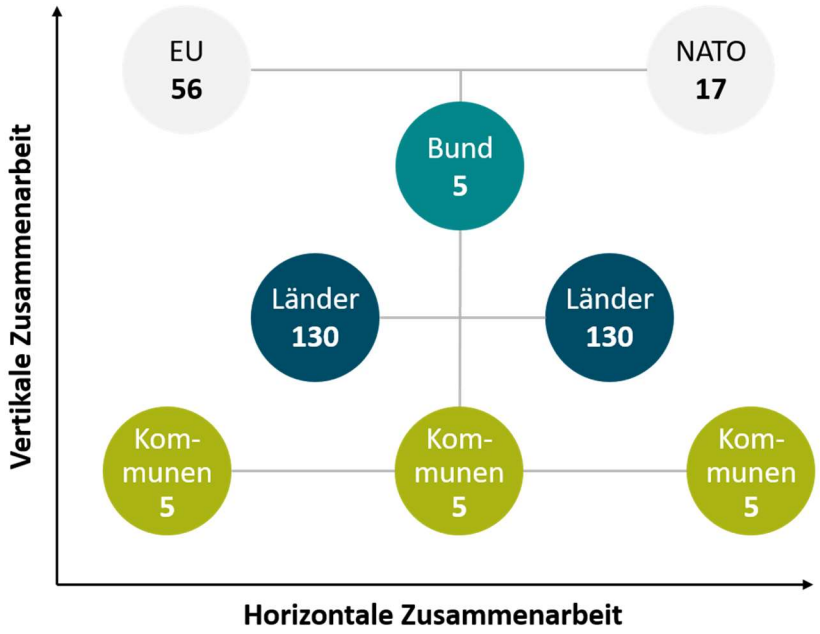


Abbildung 3: Vereinfachte Darstellung der staatlichen Cybersicherheitsarchitektur mit Anzahl der jeweiligen mit Cybersicherheit beauftragten Behörden[30]

Die Bedrohungen, die aus dem digitalen Raum für Staat, Wirtschaft und Gesellschaft ausgehen, sind durch die öffentliche Hand längst erkannt worden. Für eine effektive Prävention und **Bekämpfung von Cybersicherheitsangriffen** ist der Staat auf eine schlagkräftige und konsolidierte **Cybersicherheitsarchitektur** mit **effizienten Governance-Strukturen** angewiesen.

Heterogene IT-Sicherheitsarchitektur auf allen föderalen Ebenen

Die Strukturen sind über die Jahre jedoch nur teilweise koordiniert angewachsen. Die regelmäßig durch die Stiftung Neue Verantwortung bildlich dargestellte **Cybersicherheitsarchitektur** in **Deutschland** und auf **EU-Ebene** stellt die **Vielfalt und Komplexität** dar. Alleine die Anzahl der sich befassenden Behörden und Gremien ist dabei schon nennenswert.[31]

Vor dem Hintergrund der großen Anzahl an Gremien und Behörden erscheint ein koordiniertes Vorgehen herausfordernd bis unmöglich. Die **heterogene organisatorische Cybersicherheitsarchitektur** der einzelnen Länder erhöht nochmals das **Komplexitätsniveau**. So verfügt zum Beispiel das Land Bayern als einziges Bundesland über ein Landesamt für Sicherheit in der Informationstechnik, während bisher elf Bundesländer über ein Verbindungsbüro mit der äquivalenten Bundesbehörde, dem BSI, verfügen.

[30] Diese Grafik basiert auf der Cybersicherheitsarchitektur der SNV: https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur

[31] Stiftung Neue Verantwortung (2021): Staatliche Cybersicherheitsarchitektur. Version April 2021, https://www.stiftung-nv.de/sites/default/files/deu_visualisierung-deutschlands_staatliche_cybersicherheitsarchitektur_april_2021.pdf, abgerufen am 27.05.2021.

Weiterhin haben Baden-Württemberg und Bayern Cyberabwehrzentren, und Hessen hat mit dem „Hessen3C“ ein eigenes Cyberkompetenzzentrum eingerichtet.[32] Zusätzlich soll noch 2021 eine Cybersicherheitsagentur in Baden-Württemberg entstehen.[33/34]

Bereits im Jahr 2020 nahm hingegen im Land Nordrhein-Westfalen eine Koordinierungsstelle für landesweite Cybersicherheit ihre Arbeit auf.

Diese Beispiele zeigen, dass die immer **komplexer werdende Architektur** der deutschen Behörden einer gemeinsamen Führung und vor allem eines regen **Austausches** über die **Arbeitsergebnisse** der einzelnen Behörden bedürfen. Eine strategische Betrachtung, wie man die Akteure auf Bundes- und Länderebene miteinander vernetzt, könnte hier unterstützen. Nur so kann ein Beitrag zu mehr Cybersicherheit für Staat, Wirtschaft und Gesellschaft in Deutschland gewährleistet werden. Denn die unterschiedlichen Akteure auf Länderebene wissen oft voneinander, es fehlt allerdings an einer bündelnden Stelle, die die gemeinsame Arbeit strategisch ausrichtet. Die Grundidee einer **koordinierenden Stelle** erzielt somit langfristig mehr **Cyber-Resilienz** für die **deutsche Verwaltung**.

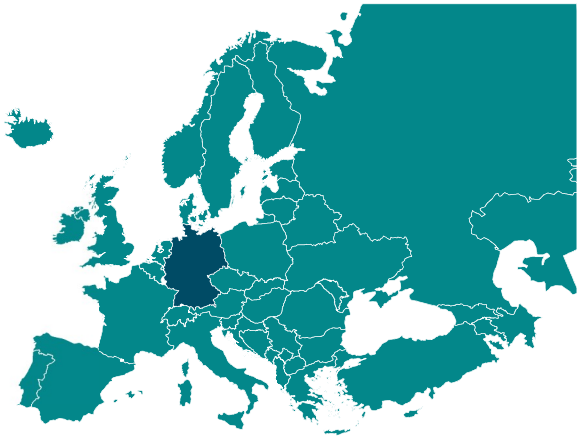
2.1.5 IT-Fachkräftemangel in der öffentlichen Verwaltung

Die Unerfahrenheit mit dem Thema Cybersicherheit lähmt die Zusammenarbeit und unterstreicht das Problem des IT-Fachkräftemangels in der öffentlichen Verwaltung. Obwohl der **IT-Fachkräftemangel** in der öffentlichen Verwaltung kein neues Phänomen ist, hat seine Bedeutung für die **Bedrohung der Cybersicherheit** mit der Zeit weiter zugenommen.

In Deutschland sind

124.000

Stellen unbesetzt



350.000

Cybersicherheitsexpertinnen und Cybersicherheitsexperten fehlen in Europa bis 2022

Abbildung 4: IT-Fachkräftemangel[35/36]

[32] Ebd.

[33] Stiebel (2020): Baden-Württemberg konstruiert Cyber-Sicherheitsarchitektur neu, https://issuu.com/behoerden_spiegel/docs/2020_m_rz/40.

[34] Diese Kooperationen werden im Abschnitt 4.2.2 im Detail vorgestellt.

[35] Europäische Kommission (2021): Women4 Cyber Registry – Database of European women in cybersecurity, https://ec.europa.eu/digital-single-market/en/news/women4cyber-registry-database-european-women-cybersecurity, abgerufen am 27.05.2021.

[36] Bitkom e. V. (2020): Erstmals mehr als 100.000 unbesetzte Stellen für IT-Experten, https://www.bitkom.org/Presse/Presseinformation/Erstmals-mehr-als-100000-unbesetzte-Stellen-fuer-IT-Experten, abgerufen am 27.05.2021.

Öffentlicher Dienst für viele IT-Fachkräfte wenig attraktiv

Wie eine deutschlandweite Befragung unter Studierenden ergab, begründet sich der Fachkräftemangel zum Teil darin, dass Absolventen und Absolventinnen mit Informatik- und/oder ähnlichen Abschlüssen am wenigsten eine Karriere im öffentlichen Dienst anstreben.[37] Neben der mangelnden Flexibilität bei den **Gehaltsstufen**, ausgelöst durch die Tarifbindung, vermissen **Informatik-Absolventen und -Absolventinnen** eine attraktive technische **Ausstattung beim öffentlichen Dienst**, weshalb die Mehrheit von ihnen eine **Karriere in der Privatwirtschaft** vorzieht.

Die als unzureichend wahrgenommenen Weiterbildungsmöglichkeiten sowie die hohen formalen Einstellungskriterien und die damit verbundene Bindung an feste Laufbahnstrukturen hindern die dringend benötigten Absolventen und Absolventinnen zusätzlich an einer Bewerbung im öffentlichen Dienst. Gerade für IT-Sicherheitsexperten und IT-Sicherheitsexpertinnen, die häufig nicht über die notwendigen formalen Voraussetzungen, jedoch über die nötige Berufs- und Praxiserfahrung verfügen, ist dies ein zentrales Ausschlusskriterium.[38]

Proaktivere Strategien zur Gewinnung von mehr IT-Personal notwendig

Der Staat hat diesen Missstand erkannt und bereits im Jahr 2016 den Leitfaden „IT-Personal für die öffentliche Verwaltung gewinnen, binden und entwickeln“ verabschiedet.[39] Dieser führt eine höhere und verbesserte Präsenz staatlicher **Behörden auf dem Bewerbungsmarkt**, einen offenen und ansprechenden Internetauftritt sowie den Beginn von Hochschulkooperationen auf. Zudem soll das verantwortliche Personal dahingehend geschult werden, **Active Sourcing** zu betreiben und **Talente anzuwerben**.

Einen entscheidenden Beitrag zur Entschärfung des IT-Fachkräftemangels auf Bundesebene könnte auch das im Januar 2020 in Kraft getretene **Besoldungsstrukturenmodernisierungsgesetz** (BesStMG) leisten, das Fachkräften im Einsatz für die Cybersicherheit auf Bundesebene, also zum Beispiel bei der Zentralen Stelle für Informationssicherheit (ZITiS), dem Informationstechnikzentrum Bund (ITZBund), der Bundeswehr (im Bereich Cyberverteidigung) und der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS), eine **höhere Vergütung** zugesteht.[40] Das Gesetz ist allerdings nur für die Besoldung auf Bundesebene anwendbar.

Fraglich ist, wie IT-Sicherheitsexperten und IT-Sicherheitsexpertinnen auf Länderebene, die auch ohne das neue Gesetz häufig einer niedrigeren Vergütungsstruktur unterliegen, gewonnen und langfristig gehalten werden können. Das Gesetz könnte somit den Fachkräftemangel auf Landes- und Kommunalebene verschärfen, da damit eine Beschäftigung beim Bund noch weiter an Attraktivität gewinnt.

---

[37] Next:Public Beratungsagentur (2019): Nachwuchsbarometer Öffentlicher Dienst 2019. Gradmesser der Attraktivität des Öffentlichen Dienstes als Arbeitgeber bei Studierenden aller Fachrichtungen bundesweit, https://www.nachwuchsbarometer-oeffentlicher-dienst.de/wp-content/uploads/2019/06/Inhaltsverzeichnis_verlinkt_Nachwuchsbarometer_Oeffentlicher_Dienst_2019.pdf, abgerufen am 27.05.2021.

[38] Stiftung Neue Verantwortung, Schuetze, Julia (Februar 2018): Warum dem Staat IT-Sicherheitsexpert:innen fehlen. Eine Analyse des IT-Sicherheitsfachkräftemangels im Öffentlichen Dienst, https://www.stiftung-nv.de/sites/default/files/it-sicherheitsfachkraeftemangel.pdf, abgerufen am 27.05.2021.

[39] IT-Planungsrat (Januar 2017): Leitfaden. IT-Personal für die öffentliche Verwaltung gewinnen, binden und entwickeln, https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/E-Gov-Kompetenz_Leitfaden_IT-Personal_2017.pdf?__blob=publicationFile&v=2, abgerufen am 27.05.2021.

[40] Bundesministerium des Innern, für Bau und Heimat (2020): Gesetz zur Modernisierung der Strukturen des Besoldungsrechts und zur Änderung weiterer dienstrechtlicher Vorschriften, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/besoldungsstrukturenmodernisierungsgesetz.html, abgerufen am 27.05.2021.

2.1.6 Der Mensch als Fehlerquelle

Der „**Faktor Mensch**“ nimmt eine, wenn nicht *die* zentrale Rolle beim Thema „Cybersicherheit“ ein. Seine Fehlbarkeit öffnet dabei das **Einfallstor für Cyberangriffe**.[41] Das zunehmend von Mitarbeitenden der öffentlichen Verwaltung in Anspruch genommene mobile Arbeiten stellt ein potenziell großes Einfallstor für Cyberangriffe dar. Dies ist insbesondere dann der Fall, wenn diese nicht ausreichend über die Risiken im Cyberraum aufgeklärt und sensibilisiert wurden und/oder nicht über die nötige technische Ausstattung verfügen, sodass sie sich gezwungen sehen, **private Endgeräte** zu nutzen, um auf interne **Verwaltungsnetze** zuzugreifen.

Der in einigen Bereichen durch die **Covid-19-Pandemie** unvorbereitete Umstieg in **dezentrales mobiles Arbeiten** wurde von Angreifenden verstärkt ausgenutzt. Zusätzlich zu den rund 160 Millionen **Phishing-Mails**, die täglich weltweit versendet werden, kamen nun rund 20 Millionen Corona-spezifische E-Mails hinzu, die etwa vorgaben, Informationen zum Virus, zu einem wirksamen Medikament oder Schutzmaßnahmen zu verbreiten. Obwohl der Großteil durch die Filter der E-Mail-Programme abgefangen wird, werden noch 18 Millionen Phishing-Mails täglich aussortiert.[42]

Täuschend echte Mails von angeblichen Vorgesetzten

Es kann davon ausgegangen werden, dass solche E-Mails im ungeschützten Raum, beispielsweise im eigenen Wohnzimmer, anders behandelt werden als in der Büroumgebung. Dabei sind insbesondere CxO-Fraud-Simulationen gefährlich, bei denen sich die Angreifenden als Vorgesetzte ausgeben. So werden angeblich streng vertrauliche Arbeitsaufträge aus höheren Hierarchiestufen an Mitarbeitende per E-Mail versendet. Die Nachricht erweckt den Eindruck als sei sie plausibel, weswegen in Simulationen durchschnittlich 83 Prozent der Personen den Anhang öffnen und so der Schadsoftware Zugriff auf den eigenen Computer gewähren.

Um eine solche Nachricht generieren zu können, bedarf es eines hohen Aufwands an **Social Engineering**. Es muss nicht nur die Arbeitsumgebung als solche kopiert werden, sondern **der Angreifende** muss sich auch in den **Hierarchiebeziehungen** auskennen, damit der **Arbeitsauftrag plausibel** erscheint.[43] Im Gegensatz zum Arbeiten in unmittelbarer räumlicher Nähe ist die Plausibilität von Arbeitsaufträgen beim mobilen Arbeiten nämlich um einiges schwieriger zu verifizieren.

[41] Crisis Prevention (17.02.2020): Faktor Mensch ist weiterhin größtes Einfallstor für Cyberangriffe. Cyber-Sicherheitsrat Deutschland e.V. startet Schulungs- und Awareness-Plattform für Unternehmen, https://crisis-prevention.de/kommunikation-it/faktor-mensch-ist-weiterhin-groesstes-einfallstor-fuer-cyberangriffe.html, abgerufen am 27.05.2021.

[42] Hellemann, N. (2020): Human Factor – Mit welchen psychologischen Tricks Hacker (besonders jetzt) erfolgreich sind. SoSafe. Vortrag beim Cyber Security Gipfel 2020.

[43] NoSpamProxy (kein Erscheinungsjahr): CxO Fraud und Corona Pandemie: So schützen sie sich, https://www.nospamproxy.de/de/cxo-fraud-und-corona-pandemie-so-schutzen-sie-sich/, abgerufen am 27.05.2021.

3 Ein Lösungsweg zu mehr Sicherheit: Kooperationen

In der Cybersicherheitsstrategie des Bundes von 2016 werden Kooperationen und Partnerschaften zwischen staatlichen, wirtschaftlichen und gesellschaftlichen Akteuren als einer der Schlüssel zu mehr Cybersicherheit genannt. Dabei liegt das Augenmerk auf Kooperationen zwischen Wirtschaft und öffentlicher Hand. **Kooperationen** als Mittel zur Steigerung der **Effizienz beim Verwaltungshandeln** liegen erkennbar im Trend. Sie werden in diesem Kontext als in der Regel freiwilliges, bewusst aufeinander abgestimmtes Vorgehen und Verhalten zwischen mindestens zwei eigenständigen Wirtschaftssubjekten verstanden. Diese können sowohl explizit – also vertraglich – vereinbart werden, oder implizit – und damit stillschweigend – vereinbart sein.

In der Regel werden Kooperationen nur dann von den Akteuren eingegangen, wenn beidseitig Vorteile in Aussicht gestellt werden können.[44] Man unterscheidet zwischen **öffentlich-privaten** und **öffentlich-öffentlichen** Kooperationen. Letztere können sowohl vertikal – zum Beispiel zwischen Bund, Ländern und Kommunen – als auch horizontal – zum Beispiel zwischen einzelnen Bundesländern oder zwischen jeweils einzelnen Kommunen – stattfinden. Kooperationen innerhalb eines Landes, an der mehrere Einrichtungen des Landes aktiv beteiligt sind, werden ebenfalls betrachtet.

Zusammenarbeit im Bereich Cybersicherheit bietet Zugang zu mehr Ressourcen

Die Vorteile von Kooperationen im Bereich der Cybersicherheit liegen auf der Hand. Es ergeben sich Spezialisierungs- und Größenvorteile sowie Synergieeffekte. Die Zusammenlegung identischer Prozesse **verringert Doppelstrukturen** bei der Aufgabenerfüllung, sodass langfristig kostensparende Verwaltungsstrukturen entstehen. Neben **Zeit- und Kosteneinsparungen** bieten Kooperationen **Zugang zu Ressourcen**, auf die man sonst keinen Zugriff hätte.

Dieses Argument fällt gerade im Kontext von Cybersicherheit ins Gewicht, da der Zugang zu spezialisiertem Know-how und den damit verbundenen Ressourcen ein Schlüssel zum Erfolg darstellt. Denn **spezialisiertes Fachpersonal** kann für **mehrere Verwaltungen** gleichzeitig eingesetzt werden und muss nicht jeweils neu und kostspielig auf dem Bewerbungsmarkt rekrutiert werden. Das Instrument der Kooperationen findet im Bereich der Cybersicherheit bereits durchaus Verwendung.

Nachfolgend wird der Blick ausschließlich auf die Kooperationen der Länderebene gerichtet, um dieses Potenzial weiter in den Blick zu rücken und zu erschließen. Bedingt durch den deutschen Föderalismus herrscht hier nicht nur ein dezentrales, sondern auch heterogenes Bild, das vielfältige Kooperationsmöglichkeiten mit anderen Behörden und der Wirtschaft begünstigt.

[44] Mühlenkamp, Holger (2012): Kooperation und Wettbewerb im öffentlichen Sektor, https://www.uni-speyer.de/fileadmin/Lehrstuehle/Muehlenkamp/2012KooperationundWettbewerbimoeffentlichenSektor_SB_.pdf, abgerufen am 27.05.2021.

3.1 Übersicht über bestehende Kooperationen

In Deutschland sind bereits auf Länderebene zahlreiche öffentlich-öffentliche, aber auch öffentlich-private Kooperationen zu finden. Für die einzelnen Bundesländer wurden folgende Kooperationen identifiziert und einige der hier aufgeführten Kooperationen als Best Practices genauer beleuchtet.

Tabelle 1: Übersicht über Kooperationen auf Länderebene

[1] Cyberkooperationen zwischen Behörden eines Landes
[2] Sicherheitskooperationen Cybercrime zwischen Landeskriminalämtern und Bitkom
[3] Kooperationsvereinbarung zwischen BSI und Land

1. Baden-Württemberg	Cyberwehr Baden-Württemberg **[1]**
	Sicherheitskooperation Cybercrime **[2]**
	Kooperation zwischen EnBw und dem Land Baden-Württemberg
	Gründung Cybersicherheitsagentur Baden-Württemberg **[1]**
	Kooperationsvereinbarung zwischen dem BSI und dem Land Baden-Württemberg **[3]**
	Cyberwehr-Austausch mit Bayern
2. Bayern	Cyberabwehr Zentrum **[1]**
	Cyberabwehr-Austausch mit Baden-Württemberg
	Themenplattform Cybersecurity des „Zentrum Digitalisierung.Bayern“
	IT-Sicherheitscluster
3. Berlin	Kooperationsvereinbarung zwischen dem BSI und dem Land Berlin **[3]**
4. Brandenburg	Kooperationsvereinbarung zwischen dem BSI und dem Land Brandenburg **[3]**
5. Bremen	Norship (North-German Research School for Information Security, Computer Forensics and Privacy)
6. Hamburg	Netzwerk für Standortsicherheit Hamburg
7. Hessen	Hessen Cyber Competence Center – Hessen3C **[1]**
	Kooperation zwischen Landesamt für Verfassungsschutz (LfV) und Vereinigung für die Sicherheit der Wirtschaft e. V. (VSW)
	Kommunales DL-Zentrum Cybersicherheit
	Sicherheitskooperation Cybercrime **[2]**
	Kooperationsvereinbarung zwischen dem BSI und dem Land Hessen **[3]**
	Kooperation mit dem Fraunhofer Institut
8. Mecklenburg-Vorpommern	Kooperationsvereinbarung zwischen dem BSI und dem Land Mecklenburg-Vorpommern **[3]**

9. Niedersachsen	Kooperationsvereinbarung zwischen dem BSI und dem Land Niedersachsen **[3]**
	Sicherheitskooperation Cybercrime **[2]**
	Kooperation zwischen CISPA – Helmholtz-Zentrum für Informationssicherheit und Leibniz Universität Hannover (LUH), gefördert durch das niedersächsische Wissenschafts- und Wirtschaftsministerium
10. Nordrhein-Westfalen	Kooperationsvereinbarung zwischen dem BSI und dem Land Nordrhein-Westfalen **[3]**
	Sicherheitskooperation Cybercrime **[2]**
	Koordinierungsstelle Cybersicherheit NRW
	Sicherheitspartnerschaft Nordrhein-Westfalen
11. Rheinland-Pfalz	Kooperationsvereinbarung zwischen dem BSI und dem Land Rheinland-Pfalz **[3]**
	Kooperationsvertrag zwischen dem Landeskriminalamt und der Hochschule Worms
	Sicherheitspartnerschaft Rheinland-Pfalz
	Sicherheitskooperation Cybercrime **[2]**
	Zusammenarbeit mit dem Saarland
12. Saarland	IT-Sicherheitsinitiative Saarland
	Kooperationsvereinbarung zwischen dem BSI und dem Saarland **[3]**
	Saarländisch-französische Kooperation: Intelligence Artificielle Territoriale
	Zusammenarbeit mit Baden-Württemberg auf dem Gebiet der Cyberkriminalität
	Zusammenarbeit mit Rheinland-Pfalz
13. Sachsen	Kooperationen des CERT des Landes Sachsen
	Kooperationsvereinbarung zwischen dem BSI und dem Land Sachsen **[3]**
	Sicherheitskooperation Cybercrime **[2]**
14. Sachsen-Anhalt	CyberSec Verbund Sachsen-Anhalt mit Cluster IT-Mitteldeutschland
15. Schleswig-Holstein	Service Point Cyber Security
	Sicherheitspartnerschaft Schleswig-Holstein
16. Thüringen	Kooperationsvereinbarung zwischen dem BSI und dem Land Thüringen **[3]**

Die aufgelisteten Kooperationen zeigen ein **heterogenes Bild der Kooperationslandschaft im Bereich Cybersicherheit auf Länderebene**. Neben zahlreichen lokal verankerten Kooperationen gibt es auch solche,

an denen mehrere Länder teilnehmen. So hat das BSI mittlerweile mit insgesamt elf Bundesländern eine Vereinbarung zu einer öffentlich-öffentlichen Kooperation geschlossen. Weitere sind in Vorbereitung.[45]

Die operative Zusammenarbeit zwischen dem BSI und den Ländern erfolgt über die Computer Emergency Response Teams (CERTs). Eine öffentlich-private Kooperation, an der insgesamt sechs Bundesländer teilnehmen, ist die Sicherheitskooperation Cybercrime, die durch den Digitalverband Bitkom vorangetrieben wird. Schließlich stehen die Bundesländer über den IT-Planungsrat und die darin eingerichteten Arbeitsgruppen in engem Austausch.

3.2 Best Practices

Nachfolgend stellen wir drei Arten besonders vielversprechender Kooperationen vor. Dazu zählen öffentlich-öffentliche sowie öffentlich-private Kooperationen. Die „Sicherheitskooperation Cybercrime“ ist die bisher einzige **öffentlich-private Kooperation**, die Bundesländer-übergreifend tätig ist.

Auf **öffentlich-öffentlicher** Seite haben hingegen fast alle Bundesländer eine Kooperationsvereinbarung mit dem BSI geschlossen, um die Bund-Länder-Zusammenarbeit zu bekräftigen. Mit dem BSI ist einer der wichtigsten Akteure in der Cybersicherheitslandschaft an diesen Kooperationen beteiligt.

Anschließend wird der Blick auf die **eigens gegründeten Organisationseinheiten** zur Verbesserung der Cybersicherheit in Baden-Württemberg, Bayern, Hessen und Nordrhein-Westfalen gerichtet. Solche Organisationseinheiten sind bisher selten auf Länderebene vertreten und werden aufgrund ihrer Koordinierungsfunktion als einzigartig dargestellt.

3.2.1 Sicherheitskooperation Cybercrime

Öffentlich-private Plattform	Seit 2011

Ziele:
- Wissensaustausch
- Prävention und Bekämpfung
- Warnmechanismus
- Austausch technischer Kompetenzen

Art und Teilnehmende der Kooperation

Die Sicherheitskooperation Cybercrime ist eine **öffentlich-private Kooperation**, an der mittlerweile **sechs Landeskriminalämter** teilnehmen. Die Kooperation bietet eine Plattform, um den Gefahren durch Cybercrime gemeinsam zu begegnen und wird durch den **Digitalverband Bitkom** koordiniert. Der Verband seinerseits vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, unter ihnen auch rund 1.000 Mittelständler und über 500 Start-ups. Unternehmensvertretende beteiligen sich in verschiedenen Arbeitskreisen, unter anderem dem Arbeitskreis „Sicherheit“.

[45] Bundesamt für Sicherheit in der Informationstechnik (2020) https://www.bsi.bund.de/DE/Das-BSI/Organisation-und-Aufbau/Abteilungen-inkl-Organigramm/Bund-Laender-Zusammenarbeit/bund-laender-zusammenarbeit_node.html

Beginn der Kooperation

Die Sicherheitskooperation Cybercrime ist auf unbegrenzte Zeit angelegt und entstand 2011 aus einer engen Zusammenarbeit des Bitkom und den Landeskriminalämtern Nordrhein-Westfalen sowie Baden-Württemberg. Durch die gemeinsame Willensbekundung, das bereits Erarbeitete zu institutionalisieren, entstand ein erstes Netzwerk. Mittlerweile ist daraus zusätzlich eine Austauschplattform für die Landeskriminalämter untereinander geworden – diese beinhaltet auch Themenfelder jenseits der Cybersicherheit.

Ziel der Kooperation

Die Sicherheitskooperation Cybercrime verfolgt durch den Austausch von Wissen und technischen Kompetenzen einen ganzheitlichen Ansatz zur Prävention und Bekämpfung von Cyberkriminalität. Sie hat das Ziel, ein Bewusstsein für das **Thema Cybersicherheit** im **Privatsektor** und in der **öffentlichen Verwaltung** zu verankern und zu erweitern. Zusätzlich soll vor neuartigen Gefahren gewarnt werden.

Neben einer Verbesserung der phänomenologischen Erkenntnisse der Landeskriminalämter steht auch eine Fortentwicklung der Prävention im Zielfokus dieser Partnerschaft. Durch Arbeitskreise mit der Privatwirtschaft werden die technischen Kompetenzen aller Teilnehmenden erweitert.

Rollen und Voraussetzungen der Kooperation

Die Rolle des Bitkom ist die eines Koordinators, der unter anderem durch die zuständige Bereichsleitung beziehungsweise Referenten und Referentinnen wahrgenommen wird. Der Verband dient zusätzlich als Kenner und Vertrauensgeber.

Aus der Privatwirtschaft kommen benötigte Impulse. Von öffentlicher Seite werden inhaltliche Vorgaben zu gefragten Inhalten benötigt. Erkenntnisse zu aktuellen Gefährdungen werden (in Abstimmung mit den kooperierenden Landeskriminalämtern) mit den Mitgliedern geteilt. Als **Erfolgsfaktoren** und Voraussetzungen der Kooperation dienen unter anderem die langfristige **Vertrauensbildung** zwischen dem Koordinator und den Landeskriminalämtern, aber auch die Wahrung von Neutralität der koordinierenden Stelle gegenüber allen Kooperationsteilnehmenden.

Erfolge der Kooperation

Durch die Sicherheitskooperation Cybercrime konnten bereits verschiedene Meilensteine erreicht werden. So gibt es beispielweise eine eigens für Unternehmen eingerichtete **regelmäßige Sprechstunde mit den Landeskriminalämtern** sowie einen Single Point of Contact (SPOC) in allen teilnehmenden Landeskriminalämtern. Zusätzlich werden **gegenseitige Hospitationen** bei Unternehmen beziehungsweise den Landeskriminalämtern durchgeführt. Die Kooperation bietet die Möglichkeit für eine gemeinsame Lösungssuche.

Neben den Vorstellungen bei Jahrestagungen führt die Kooperation verschiedene mehrstufige Awareness-Maßnahmen durch und gibt ad hoc Warnhinweise an die Bitkom-Mitglieder weiter. Mit einzelnen Unternehmen werden zusätzlich weitere Formate im Rahmen der Kooperation beschlossen und durchgeführt.

3.2.2 Kooperation zwischen dem BSI und den Ländern

Öffentlich-öffentlich	Seit 2017

Ziele:
- Wissensaustausch
- Prävention und Bekämpfung
- Beratung

Art und Teilnehmende der Kooperation

Das BSI unterhält im Rahmen des nationalen Verbindungswesens **regionale Kooperationsvereinbarungen** mit den Bundesländern Hessen, Rheinland-Pfalz, Niedersachsen, Nordrhein-Westfalen, Berlin, Baden-Württemberg, Saarland, Sachsen, Thüringen, Brandenburg und Mecklenburg-Vorpommern. Es gibt **feste Kontakte**, die angesprochen werden und beim Aufbau eines **regionalen Netzwerkes** aus Verwaltung, Wirtschaft und Gesellschaft unterstützen. Zurzeit sitzen diese in Wiesbaden (für das Rhein-Main Gebiet), in Berlin, Dresden (für Ostdeutschland), Stuttgart (für Süddeutschland) und in Hamburg (für Norddeutschland).

Beginn der Kooperation

Mit den Ländern Hessen und Rheinland-Pfalz hat das BSI bereits im Jahr 2017 Modellpartnerschaften initiiert, 2018 folgten Niedersachsen, Nordrhein-Westfalen, Berlin, das Saarland, Baden-Württemberg, Sachsen und Thüringen. Brandenburg und Mecklenburg-Vorpommern kamen im darauffolgenden Jahr dazu. Laut Aussage des BSI sind weitere Kooperationsvereinbarungen in der Vorbereitung.[46]

Ziel der Kooperation

Die operative Zusammenarbeit mit den Ländern wird vereinheitlicht. So soll ein **Mindestniveau der IT-Sicherheit gewährleistet** werden. Die Verbindungsbüros ermöglichen eine physische Nähe zu den Ländern. Beispielsweise liegt im Falle von Baden-Württemberg das Verbindungsbüro im selben Gebäude wie die Büros der Länder-CIO. So wird der Aufbau regionaler Netzwerke strategisch verbessert und gefördert.

Über den Verwaltungs-CERT-Verbund (VCV, Computer Emergency Response Team) wird der Informationsaustausch verbessert, um länderübergreifend effizienter **IT-Angriffe abwehren** und die **Verteidigungsstrukturen** stärken zu können.

Rollen und Voraussetzungen der Kooperation

Das BSI übernimmt gemäß § 3 BSIG in erster Linie eine beratende Rolle gegenüber den Ländern. Darüber hinaus kann es auf Ersuchen der Länder bei der Verteidigung und Abwehr unterstützen. Gemeinsame Grundlage hierfür ist das „Konzept zur zukünftigen Koordination von Maßnahmen der IT-Sicherheit zwischen Bund und Ländern unter Berücksichtigung der Rolle des BSI“.

Die Basis der Kooperationsvereinbarungen ist ein Katalog von 40 Produkten aus dem BSI-Portfolio, der sich speziell an dem jeweiligen Land orientiert. Das BSI agiert als CERT-Verbund als zentrale Einheit bei sicher-

[46] Bundesamt für Sicherheit in der Informationstechnik (2020): Bund-Länder-Zusammenarbeit, https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Zusammenarbeit_mit_Bund_und_Laendern/bund-laender-zusammenarbeit_node.html, abgerufen am 28.05.2021.

heitsrelevanten Vorfällen, Angriffen und Risiken. Durch seine Erfahrungen hilft das BSI beim Aufbau **länderspezifischer Informationssicherheitssysteme** und steht als **Ansprechpartner** bei Vorfällen allen Ländern und Akteuren der Verwaltung jederzeit zur Verfügung.

Erfolge der Kooperation

Durch die direkten Kommunikations- und Meldewege an das BSI werden die IT-Standards der Länder erhöht und an den Bund angeglichen. So wird das **Gesamtsicherheitsniveau wesentlich gehoben**. Durch die engere Zusammenarbeit und den regelmäßigen Austausch wird die vom IT-Planungsrat beschlossene Bund-Länder-Meldepflicht noch einfacher umgesetzt. Seit dem 1. Januar 2010 sind Bundesbehörden gemäß § 4 Abs. 3 BSIG dazu verpflichtet, Informationen, die zur Abwehr von Gefahren für die Sicherheit der Informationstechnik relevant sind, unverzüglich dem BSI zu melden.

3.2.3 Einrichtung von Organisationseinheiten zur Cyberabwehr auf Länderebene

Baden-Württemberg: Cybersicherheitsagentur

Öffentlich-private Kontakt- und Beratungsstelle	Seit 2020

Ziele:
- Aufbau von Infrastruktur
- Prävention und Verteidigung
- Beratung

Art und Teilnehmende der Kooperation

Das Land Baden-Württemberg hat zur Bekämpfung und Aufklärung eine **Kontakt- und Beratungsstelle** für **kleine und mittlere Unternehmen** des Landes sowie eine **Koordinierungsstelle** bei Hacker-Angriffen eingerichtet. Diese werden durch das Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg gefördert. Die Teilnehmenden dieser Zusammenarbeit sind die Zentrale Ansprechstelle Cybercrime (ZAC) beim Landeskriminalamt, das Landesamt für Verfassungsschutz im Bereich der Cyberspionage, das CERT BW Baden-Württemberg und das Forschungszentrum Informatik am Karlsruher Institut für Technologie (KIT). Die Cyberwehr, die insbesondere Unternehmen bei Cyberangriffen berät, ist ebenfalls Teils der Cybersicherheitsarchitektur.

Ziel der Kooperation

Die Cyberabwehr in Baden-Württemberg verfolgt mehrere Ziele. Das langfristige Ziel entspricht dem landesweiten Aufbau von regionalen Infrastrukturen zur Leistung von **Ersthilfe** im Falle eines **IT-Sicherheitsvorfalles**. Weiterhin soll die Cyberabwehr Soforthilfe bei Hacker-Angriffen für kleinere und mittelständische Unternehmen leisten. Im nächsten Schritt soll die Cybersicherheitsagentur zur landesweiten Koordinierungsstelle für Hacker-Angriffe in Baden-Württemberg werden.

Beginn der Kooperation

Die Kooperation ist auf unbegrenzte Zeit angelegt und begann zunächst mit einer Pilotphase für die Cyberabwehr in den Stadt- und Landkreisen Karlsruhe, Rastatt und Baden-Baden. Im Laufe des Jahres 2022 soll

sie in ganz Baden-Württemberg operativ tätig werden. Die Haushaltsmittel stehen dafür bereits zur Verfügung. Als einen weiteren Schritt soll die Verankerung der Einheit im Innenministerium stattfinden.

Erfolge der Kooperation

Die Kooperation beendete eine erfolgreiche Pilotphase im September 2020. Dabei wurden positive Rückmeldungen von Unternehmen und Anfragen über die Pilotregion hinaus empfangen. Aus der erfolgreichen **Testphase** ergibt sich nun eine **Erweiterung des Service** auf ganz Baden-Württemberg. Dabei stand der Fokus auf der Gewährleistung einer durchgängigen Erreichbarkeit für die baden-württembergische Landes- und Kommunalverwaltung und für kleine und mittelständische Unternehmen.

Bayern: Cyberabwehr Bayern

Öffentlich-öffentliche Kooperation zwischen Landesbehörden	Seit 2020

Ziele:
- Kontakt zum Bund und dem Nationalen Cyber-Abwehrzentrum
- Informationsbeschaffung und Lagebilderstellung

Art und Teilnehmende der Kooperation

Bei der Cyberabwehr Bayern handelt es sich um eine öffentlich-öffentliche Kooperation zwischen verschiedenen Landesbehörden, die Anfang 2020 aus der Sicherheitsstrategie des Landes Bayern[47] hervorgegangen ist. Die Cyberabwehr Bayern fungiert als behördeninterne **Informations- und Kooperationsplattform** für alle bayerischen Landesbehörden mit Cybersicherheitsaufgaben.

Teilnehmende an dieser Kooperation sind das Cyber-Allianz-Zentrum (CAZ) im Bayerischen Landesamt für Verfassungsschutz, die Zentrale Ansprechstelle Cybercrime (ZAC) im Bayerischen Landeskriminalamt, die Zentralstelle Cybercrime Bayern (ZCB) bei der Generalstaatsanwaltschaft Bamberg, das Landesamt für Sicherheit in der Informationstechnik (LSI), das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) und die Landesbeauftragte für den Datenschutz (LfD). Organisatorisch verankert ist die Kooperation beim Bayerischen Landesamt für Verfassungsschutz.

Ziele der Kooperation

Mit dieser Kooperation werden mehrere Ziele verfolgt. Die Cyberabwehr Bayern soll als **zentrale Ansprechstelle** für das auf Bundesebene eingerichtete **Nationale Cyber-Abwehrzentrum** bei Cybersicherheitsvorfällen als **Schnittstelle** zwischen dem Bund und dem Land Bayern dienen. Zudem werden durch regelmäßige Lagebesprechungen Informationen, Kompetenzen und Ressourcen gebündelt. Durch diesen Austausch zu aktuellen Ereignissen und zu ergreifenden Maßnahmen kann ein Cyber-Lagebild des Landes Bayern erstellt werden.

[47] Bayerisches Staatsministerium des Innern (11.04.2013): Regierungserklärung des Bayerischen Staatsministers des Innern, Joachim Herrmann, am 11. April 2013 im Bayerischen Landtag, Thema „Bayern digital – Sicherheit im Internet“, https://www.stmi.bayern.de/assets/stmi/med/reden/stm_reg-erklaerung_cybersicherheit_130411.pdf; Bayerischer Rechts- und Verwaltungsreport (BayRVR), Kohnen, Klaus (08.01.2019): StK: Bayerische Cybersicherheitsstrategie wird stetig fortentwickelt – Schutz für Bürger, Unternehmen und staatliche Stellen stärken, https://bayrvr.de/2019/01/08/stk-bayerische-cybersicherheitsstrategie-wird-stetig-fortentwickelt-schutz-fuer-buerger-unternehmen-und-staatliche-stellen-staerken/, beide Quellen abgerufen am 27.05.2021.

Beginn der Kooperation

Die Cyberabwehr Bayern wurde Anfang 2020 von der Bayerischen Staatsregierung ins Leben gerufen und ist auf unbestimmte Zeit angelegt. Zuvor – seit Mai 2013 – hatte das Bayerische Staatsministerium des Innern, für Sport und Integration die Koordinierung im Rahmen der gegründeten „Initiative Cybersicherheit Bayern“ übernommen. Im Juli 2013 folgte das Cyber-Allianz-Zentrum als erste institutionelle Umsetzung dieser Initiative. Das Cyber-Allianz-Zentrum unterstützt Unternehmen und Betreiber kritischer Infrastrukturen (KRITIS) bei der Prävention und Abwehr von elektronischen Angriffen.

Erfolge der Kooperation

Das durch die Cyberabwehr Bayern erstellte Lagebild hat sich während der ersten Jahreshälfte 2020 – insbesondere durch die steigenden Angriffszahlen im Zuge der **Covid-19 Pandemie** – als gute Basis zur **Verhinderung von Angriffen** gezeigt.[48]

Hessen: Hessen CyberCompetenceCenter (Hessen3C)

Öffentlich-öffentliche Kooperation zwischen Landesbehörden	Seit 2019

Ziele:
- Prävention und Verteidigung
- Schaffung von Synergien
- Informationsaustausch

Art und Teilnehmenden der Kooperation

Beim Hessen Cyber Competence Center handelt es sich um eine **öffentlich-öffentliche** institutionalisierte Kooperation zwischen Landesbehörden.[49] Hessen3C ist als zentrale Kompetenzstelle zur interdisziplinären Zusammenarbeit und institutionalisierten Kooperation hessischer Behörden ins Leben gerufen worden. An der Kooperation sind Spezialisten und Spezialistinnen im Bereich Cybersicherheit aus dem Computer Emergency Response Team (CERT) des Landes, der Hessischen Polizei und des Landesamtes für Verfassungsschutz Hessen beteiligt. Die organisatorische Verankerung liegt beim Hessischen Ministerium des Innern und für Sport.

Ziel der Kooperation

Das Hessen3C soll zur Erhöhung der **Sicherheit in der Informationstechnik** beitragen, cyberspezifische Gefahren abwehren, die Effizienz bei der Bekämpfung von Cyberkriminalität erhöhen sowie Synergien schaffen. Diese Ziele sollen durch die Übernahme verschiedener Aufgaben umgesetzt werden. Dazu zählen unter anderem ein regelmäßiger **Informationsaustausch**, die Erstellung eines **Lagebildes für Hessen** sowie die Unterstützung des zentralen **Informationssicherheitsbeauftragten** der Landesverwaltung.

[48] BR24 (13.07.2020): Bilanz der "Cyberabwehr Bayern": Deutliche Cybercrime-Zunahme, https://www.br.de/nachrichten/bayern/bilanz-der-cyberabwehr-bayern-deutliche-cybercrime-zunahme,S4dYdfX, abgerufen am 27.05.2021.

[49] Hessisches Ministerium des Innern und für Sport (2021): Hessen CyberCompetenceCenter. Hessen3C, https://innen.hessen.de/sicherheit/hessen3c/hessen-cyber-competence-center, abgerufen am 27.05.2021.

Darüber hinaus nimmt Hessen3C Koordinierungsaufgaben zur Umsetzung des IT-Sicherheitsgesetzes in der hessischen Landesverwaltung und bei der Zusammenarbeit aller mit Cybersicherheit befassten Dienststellen der Landesverwaltung wahr. Das Hessen3C vertritt auch das Land Hessen im Bereich Cybersicherheit in den entsprechenden Bund-Länder-Gremien und ist seit 2020 für den Betrieb der Zentralen Meldestelle „HessenGegenHetze“ für Hass-Kommentare zuständig.

Beginn der Kooperation

Die Kooperation besteht seit April 2019 und ist aus der Stabsstelle Kompetenzzentrum Cybersicherheit im hessischen Ministerium des Innern und für Sport hervorgegangen. Sie ist auf unbestimmte Zeit angelegt. Die durchgängige Erreichbarkeit ist sowohl für die **hessische Landes- und Kommunalverwaltung** als auch für **kleine und mittelständische Unternehmen** gewährleistet.

Erfolge der Kooperation

Durch diese Kooperation konnten bereits **Informationen, Kompetenzen und Ressourcen** in den Bereichen Cyber Security, Cyber Intelligence und Cyber Crime gebündelt werden. Zudem werden regelmäßige **Lageberichte** erstellt und daraus Maßnahmen abgeleitet. Zurzeit sind für das „Hessen3C“ 20 Expertinnen und Experten im Einsatz. Bis Ende 2020 soll sich diese Zahl auf 50 und bis Ende 2021 auf 100 Experten und Expertinnen erhöhen.

Nordrhein-Westfalen: Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen

Öffentliche Koordinierungsstelle	Seit 2020

Ziele:
- Ausbau der Infrastruktur
- Koordinierung und Strukturierung des Informationsflusses

Art und Teilnehmende der Kooperation

Das Land Nordrhein-Westfalen hat zur Erhöhung des Cybersicherheitsniveaus eine „Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen“ eingerichtet, die im Ministerium des Innern des Landes Nordrhein-Westfalen angesiedelt ist. Die **Koordinierung und Strukturierung** der Informationsflüsse zum Thema Cybersicherheit zwischen den teilnehmenden Ressorts der Ministerien des Landes, die das Thema Cybersicherheit bearbeiten, stellen dabei Hauptaufgaben dar.

Weiterhin dient die Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen als Verantwortliche für die inhaltliche und organisatorische Umsetzung des „Interministeriellen Ausschusses Cybersicherheit NRW“ (IMA Cybersicherheit). Am IMA Cybersicherheit nehmen alle Ressorts mit Aufgaben im Bereich der Cybersicherheit teil, die dadurch gleichzeitig Teilnehmende der Kooperation sind.

Ziele der Kooperation

Ziel der Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen ist es, das **Niveau der Cybersicherheit** im Land zu erhöhen und **relevante Daten** und **Informationen** für die verschiedenen Aufgabentragenden und Akteure bereitzustellen. Weiterhin bündelt die Stelle die Position des Landes im Bereich Cybersicherheit und kommuniziert sie an Bund und Länder.

Das Land Nordrhein-Westfalen verspricht sich von der Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen eine **strategische Neuausrichtung** beim Kampf gegen Cyberkriminalität, bei gleichzeitiger Wahrung der Aufgabenerfüllung durch die Ressorts. Dafür wird in einem ersten Schritt, unter Einbeziehung der Kooperationsteilnehmenden, auch eine **gemeinsame Strategie** der Cybersicherheit für das Land erstellt.

Beginn der Kooperation

Die Kooperation wurde im August 2020 durch einen Kabinettsbeschluss der Landesregierung Nordrhein-Westfalen angenommen und nahm daraufhin ihre Arbeit auf. Auf Ebene der Landesregierung gab es bislang keine übergreifende Koordinierung aller Aspekte von Cybersicherheit.

Erfolge der Kooperation

Durch die bessere Vernetzung der Ressorts untereinander wird ein effizienteres Arbeiten ermöglicht. Mit der Ansiedlung im Ministerium des Innern ist es der Landesregierung gelungen, die **Zusammenarbeit mit den Sicherheitsbehörden** im Rahmen der Cybersicherheit zu vertiefen, wodurch das **Gesamtsicherheitsniveau** nochmals angehoben wurde. Die Koordinierungsstelle für Cybersicherheit Nordrhein-Westfalen flankiert hier die bereits vorhandenen Ressorts und intensiviert die Zusammenarbeit.

3.3 Erfolgsfaktoren für die Einrichtung von Kooperationen

Kooperationen im Bereich Cybersicherheit können einen entscheidenden Faktor zur Verbesserung der Sicherheitslage der deutschen Verwaltung leisten. Damit eine Kooperation möglichst wirkungsvoll verläuft, sollten vor neuen Kooperationsvereinbarungen nachstehende Erfolgsfaktoren beachtet werden. Vor Beginn einer Kooperation sollten **(1) die Ziele definiert**, auf eine **Zeitachse** (kurz-, mittel- und langfristige Ziele) gelegt und mit konkreten Handlungsfeldern beziehungsweise Maßnahmen hinterlegt werden. Dabei sollten auch die Aufgaben, Kompetenzen und Verantwortlichkeiten der einzelnen Kooperationsteilnehmenden genau definiert werden.

Um einen langfristigen und vor allem nachhaltigen Erfolg zu sichern, sollten für Kooperationen **konkrete Handlungsschritte** – vor allem was die Kooperationstiefe beinhaltet –, beschrieben werden. Dabei können und sollen Kooperationen weit über den üblichen regelmäßigen Austausch von Informationen hinausgehen. Hospitationen, die gemeinsame Projektarbeit sowie das Teilen von Personal und technischem Equipment sollten fester Bestandteil dieser Kooperationen sein.

Die jeweilige Leitungsebene sollte bei Anbahnung beziehungsweise Durchführung der Kooperation umfassend involviert sein, um das **Bewusstsein (2)** für die **Bedeutung der Zusammenarbeit** zu schaffen. Dies wird insbesondere auch vor dem Hintergrund der **benötigten Ressourcen (3)** zur Umsetzung der Kooperation relevanter. Um Kooperationen zu institutionalisieren, erfordert es den Einsatz von Personal. Dabei kann die Einrichtung einer **koordinierenden Stelle (4)** hier Entlastung schaffen.

Vor dem Hintergrund der sensiblen Daten, die im Bereich von Cybersicherheit ausgetauscht werden, ist für das Gelingen einer Kooperation **Vertrauen** auf allen Ebenen **der Teilnehmenden** essenziell **(5)**. Dieses kann durch die **Kontinuität** der Teilnehmenden an der Kooperation erzeugt werden **(6)**. Die einzelnen Teilnehmenden – und dies ist insbesondere bei öffentlich-privaten Kooperationen der Fall –, müssen trotz der unterschiedlichen Hintergründe und damit verbundenen Interessen ein gewisses **Maß an Neutralität (7)** bewahren.

Schließlich sollte die Kooperation **mit Leben ausgestaltet (8)** werden, das bedeutet, dass Handlungsfelder und Maßnahmen zu definieren sind, die Inhalt der Kooperation sind. Diese Maßnahmen entscheiden

schlussendlich auch über die Tiefe der Kooperationen und den damit verbundenen Mehrwert für den Beitrag zur Cybersicherheit.

Nachfolgende Abbildung zeigt die vorgestellten Schritte auf einen Blick.

Abbildung 5: Erfolgsfaktoren einer Kooperation

Es wird empfohlen, Kooperationen **langfristig und allumfassend** zu denken. Der **Kooperationsgedanke** sollte bei der Gründung von Koordinierungsstellen von Anfang an mitgedacht werden, sodass ein **hohes Maß an Vertrauen** generiert wird. Dazu gehören ebenfalls **klare Kommunikationsstrukturen**, die im Falle eines Angriffs eine **schnelle, sichere und effiziente Krisenbewältigung** innerhalb der Kooperation gewährleisten. Zentrale Stellen auf Länderebene, die Informationen in den jeweiligen Ländern bündeln, können als entscheidende **Schnittstelle zum BSI** agieren.

Darüber hinaus wird empfohlen, ein **einheitliches Sprachbild** nach innen sowie nach außen zu pflegen. Durch eine einheitliche Kommunikation wird ein erhöhtes Bewusstsein für Kooperationen erschaffen. Bei Cyberangriffen ist es wichtig, dass alle Akteure mit der gleichen Sprache sprechen, um möglichst schnell und effizient agieren zu können.

4 Ausblick

Die zunehmende Digitalisierung der Verwaltung erhöht die Gefährdung der öffentlichen Hand im Bereich der Cybersicherheit. **Kooperationen** können dabei helfen, diese zu entschärfen, indem sie Angriffe verhindern und die **„Response-Zeit“** bei tatsächlichen Angriffen verkürzen. Dabei werden Bedrohungsszenarien durch die Verfügbarkeit von Technologien, wie Künstliche Intelligenz, weiter verschärft. Dieser Entwicklung entgegen steht eine sukzessiv **gewachsene Cybersicherheitsarchitektur** der öffentlichen Hand mit einer vergleichsweise **geringen Anzahl** von Cybersicherheitsfachkräften.

In diesem Spannungsfeld gilt es, Lösungen für die aktuelle Bedrohungslage zu finden und die Voraussetzungen zu verbessern, um künftigen Bedrohungen wirkungsvoll begegnen zu können. Kooperationen kommt hierbei unter den beschriebenen Rahmenbedingungen eine entscheidende Rolle zu. Sie ermöglichen es Akteuren der öffentlichen Hand, schnell auf vielfältige Informationen zugreifen zu können und damit ein aktuelles Lagebild der Bedrohung zu erstellen, Zugriff auf begrenzte personelle Ressourcen zu erhalten und dadurch die Effektivität des eigenen Handelns zu steigern.

Die vorliegende Analyse hat gezeigt, dass die Kooperationslandschaft auf Länderebene noch **recht jung und heterogen** ist. Es gibt viele lokale Kooperationen, aber auch bundesweit übergreifende Kooperationen. Diese werden von einem Akteur, wie zum Beispiel dem BSI oder dem Bitkom, initiiert und koordiniert.

Die eigens gegründeten **Organisationseinheiten** für die Vernetzung der Akteure aus dem Bereich Cybersicherheit in den Ländern **Baden-Württemberg, Bayern und Hessen** sind im Hinblick auf die Teilnehmenden, die Ziele und die organisatorische Verankerung unterschiedlich ausgestaltet. Daher besteht insbesondere noch Potenzial hinsichtlich der **Tiefe der Kooperationen**, auch wenn dies vor dem Hintergrund der Heterogenität der Behörden eine Herausforderung darstellt.

Neben dem häufig stattfindenden reinen Informationsaustausch, der zentral für die Aufklärung der Bedrohungslage ist, sollten auch weitere Möglichkeiten genutzt werden. Hierzu zählen vor allem **Hospitationen** von Mitarbeitenden**, Bündelung von Aufgaben, gemeinsame Nutzung von Infrastruktur** und auch die gemeinsame Nutzung von den nur äußerst begrenzt vorhandenen Fachkräften. Gemeinsam durchgeführte Projekte können schließlich dazu beitragen, personelle Kompetenzen zu bündeln und Kosten einzusparen.

Auch mit Blick auf das Verständnis der unterschiedlichen Organisationskulturen darf hier von einem positiven Effekt ausgegangen werden. Dabei scheinen **Kooperationen besonders lebendig** zu sein, wenn diese durch eine **Stelle koordiniert** werden. Aus diesem Grund wird empfohlen, dies vor Einrichtung einer neuen Kooperation zu bedenken.

Die aktuell **laufenden Kooperationen** sollten daraufhin überprüft werden, ob sie **weiter vertieft** werden können, um einen noch effizienteren beziehungsweise effektiveren Beitrag zur Cybersicherheit in Deutschland zu leisten. Weiterhin sollten die Erkenntnisse aus den einzelnen lokalen Kooperationen den anderen Bundesländern zur Verfügung gestellt werden. Eine flächendeckende Studie könnte hier den Anfang machen. Neben der Vertiefung von Kooperationen auf Länderebene sollten auch weitere Wege zur Erhöhung der Cybersicherheit der öffentlichen Verwaltung überprüft werden. Mit Blick auf Bundesländer übergreifende Kooperationen kann hier das „**Einer für Alle Prinzip**“ (EfA) von Nutzen sein. Dieses Prinzip „bedeutet, dass ein Land oder eine Allianz aus mehreren Ländern eine Leistung zentral entwickelt und betreibt – und

diese anschließend anderen Ländern und Kommunen zur Verfügung stellt, die den Dienst dann mitnutzen können.“[50]

Dem **EfA-Prinzip** kommt in Deutschland bereits bei der OZG-Umsetzung eine tragende Rolle zu, doch auch im Kontext von **Cybersicherheit** kann das EfA-Prinzip doppelten Aufwand vermeiden und Synergien fördern. So lässt sich spezialisiertes Know-How für alle Bundesländer zugänglich machen. Zusätzlich können durch die Zusammenlegung identischer Prozesse Betriebskosten geteilt und Doppelstrukturen vermieden werden. Beispielsweise könnten Cybersicherheitsübungen und -weiterbildungen von einem Bundesland entwickelt und von allen nachgenutzt werden.

Das gleiche gilt für **Open-Source-Software**. Mit der Schaffung von einheitlichen Standards für die Nutzung dieser Open-Source-Software könnte ein Bundesland die Software entwickeln und zur Weiterverwendung für die anderen Bundesländer bereitstellen, dabei werden die Kosten umverteilt. Das EfA-Prinzip ließe sich auf Grund der genannten Beispiele im Bereich der Cybersicherheit zur Verringerung der Bedrohungslage für die öffentliche Verwaltung einführen, was beim Aufbau von Kooperationen auf Länderebene unterstützt. Jedoch bedarf die Umsetzung des EfA-Prinzips einer zentralen bundesweiten Steuerungseinheit, die in dieser Form in Deutschland noch nicht existiert. Eine weitreichendere Prüfung, ob das **EfA-Prinzip** auch auf den **Kooperationsgedanken** anwendbar ist, muss künftig und an anderer Stelle detailliert betrachtet werden.

[50] Bundesministerium des Innern, für Bau und Heimat (2020): Wie funktioniert EfA?, https://www.onlinezugangsgesetz.de/Webs/OZG/DE/umsetzung/nachnutzung/efa/efa-node.html#:~:text=%22Einer%20f%C3%BCr%20Alle%22%20bedeutet%2C%20dass%20ein%20Land%20oder,sich%20die%20angeschlossenen%20L%C3%A4nder%20und%20Kommunen%20%28siehe%20Abbildung%29, abgerufen am 28.06.2021

Kontakt

Juri Denecke
Manager
T +49 30 25 76 79-308
M +49 162 245 22 41
Juri.Denecke@pd-g.de

Darya Schwarz-Fradkova
Managerin
T +49 30 25 76 79-330
M +49 170 562 38 85
Darya.Schwarz-Fradkova@pd-g.de

Michelle Busch
Consultant
M +49 174 692 75 64
Michelle.Busch@pd-g.de

Elisabeth Faria Lopes
Consultant
T +49 30 25 76 79-218
M +49 162 101 05 85
Elisabeth.FariaLopes@pd-g.de

Philip Schönfelder
Consultant
M +49 162 635 35 58
Philip.Schoenfelder@pd-g.de

pd-g.de/pd-perspektiven-reihe/kooperationen-zur-cybersicherheit