digital@bw

CYBERSICHERHEITSSTRATEGIE BADEN-WÜRTTEMBERG

– Perspektive 2026 –

Baden-Württemberg

digital@bw

CYBERSICHERHEITSSTRATEGIE BADEN-WÜRTTEMBERG

– PERSPEKTIVE 2026 –

www.digital-bw.de/cybersicherheitsstrategie

VORWORT

Unser Leben wird immer digitaler – und die Digitalisierung verändert die Welt. Smartphones, Streaming, vernetzte Küchengeräte, selbstfahrende Autos, Künstliche Intelligenz (KI) und vieles mehr prägen diesen Wandel. Daraus ergeben sich nicht nur viele Chancen, sondern auch Risiken. Mit zunehmender Digitalisierung steigt auch die Gefahr von Angriffen auf die digitalisierten Daten, Dienste oder Infrastrukturen, die zu Bedrohungen, Datenmissbrauch, Spionage oder Sabotage führen können. Basis für den digitalen Transformationsprozess und das Vertrauen in ihn ist daher die Sicherheit des Cyberraumes.

Cybersicherheit ist folglich die Voraussetzung für eine erfolgreiche Digitalisierung und damit wesentlicher Bestandteil unserer **Digitalisierungsstrategie digital@bw**. Sie dient der **digitalen Souveränität von Menschen, Staat, Wirtschaft und Wissenschaft** und umfasst nach § 2 Absatz 11 des Gesetzes für die Cybersicherheit in Baden-Württemberg „alle Aspekte der Sicherheit in der Informationstechnik und den Schutz gesellschaftlich relevanter Prozesse vor Angriffen im gesamten Cyberraum". Für die Sicherheit in der Informationstechnik muss der Staat zum Schutz der Grundrechte Verantwortung übernehmen.

Die **Cybersicherheitsstrategie der Europäischen Union für die digitale Dekade** wurde am 16. Dezember 2020 vorgelegt. Sie bildet einen der Eckpfeiler des Maßnahmenpakets für die digitale Dekade und benennt konkrete Maßnahmen, die bei der Umsetzung nationaler Cybersicherheitsstrategien zu beachten sind.

Daran anknüpfend hat am 8. September 2021 die Bundesregierung ihre überarbeitete **Cybersicherheitsstrategie 2021** beschlossen. Danach können die vielfältigen staatlichen Aufgaben im Cyberraum nur durch eine gemeinsame Anstrengung von Bund und Ländern erfüllt werden. Eine intensive Verzahnung der Aktivitäten der Bundes- und Landesebene auf dem Wege einer kooperativen und komplementären Zusammenarbeit ist hierbei unumgänglich.

Bereits zuvor erarbeiteten bundesweit alle Länder zusammen im Interesse der nachhaltigen Stärkung einer föderal geprägten Cybersicherheitsarchitektur eine **Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien.** Sie wurde auf der Ständigen Konferenz der Innenminister und -senatoren der Länder – kurz **Innenministerkonferenz (IMK)** – vom 16. bis 18. Juni 2021 in Rust behandelt. Ziel der Leitlinie ist eine Empfehlung hinsichtlich Aufbau und Weiterentwicklung der Cybersicherheitsarchitektur in den Ländern, um durch Harmonisierung, größere Interoperabilität und fachlichen Austausch den nötigen Raum für Innovationen zu eröffnen. Diese **Leitlinie**, unser **Leitbild und Eckpunkte für eine Cybersicherheitsstrategie Baden-Württemberg** und der **Koalitionsvertrag 2021-2026 von BÜNDNIS 90/DIE GRÜNEN Baden-Württemberg und der CDU Baden-Württemberg** bilden die Grundlage für die baden-württembergische Cybersicherheitsstrategie.

Als Landesregierung leitet uns die **Vision, dass Menschen, Staat, Wirtschaft und Wissenschaft die Chancen der Digitalisierung ohne erhebliche Gefährdungen durch Cyberangriffe nutzen können.** Der Schutz vor Cyberbedrohungen wird immer wichtiger, weil Störungen der digitalen Technik unser Leben deutlich beeinträchtigen können.

Um unsere Vision Wirklichkeit werden zu lassen, wollen wir als Landesregierung die **Verbesserung des allgemeinen Cybersicherheitsniveaus** durch eine ganzheitliche Cybersicherheitsstrategie erreichen, die alle gesellschaftlichen Bereiche umfasst. Deshalb haben wir in neun Handlungsfeldern unsere konkreten Ziele und Maßnahmen formuliert:

1. **Vernetzung der Cybersicherheitsakteure**
2. **Staatliche Verwaltung und Kommunen**
3. **Gefahrenabwehr- und Strafverfolgungsbehörden**
4. **Wirtschaft und Kritische Infrastrukturen (KRITIS)**
5. **Digitale Kompetenzen**
6. **Awareness und Verbraucherschutz**
7. **Fachkräfte**
8. **Innovative Forschung und Entwicklung**
9. **Nationale und internationale Kooperationen**

Die meisten **Ziele** der Strategie sind SMART (spezifisch, messbar, akzeptiert, realistisch, terminiert) formuliert worden, um die Erreichung der Ziele und den Erfolg der Strategie sicherzustellen.

Die Cybersicherheitsstrategie wollen wir in den nächsten **fünf Jahren** umsetzen. Herausforderung dabei wird sein, dass alle zusätzlichen finanzwirksamen Maßnahmen aktuell unter Haushaltsvorbehalt stehen. Bei der Umsetzung wollen wir systemübergreifend alle relevanten Akteure einbinden. So werden wir uns auch weiterhin für eine Digitalisierung einsetzen, die die Menschen in den Mittelpunkt stellt und sicher ist.

INHALT

1. Vernetzung der Cybersicherheitsakteure 8

2. Staatliche Verwaltung und Kommunen 10
2.1 Informationssicherheitsmanagement 12
2.2 Analyse- und Reaktionsfähigkeit vor Ort stärken 13
2.3 Gemeinsame Abwehr von IT-Angriffen 14
2.4 IT-Notfallmanagement 14
2.5 Rechtliche Rahmenbedingungen 15
2.6 Security by Design und Sicherheitsgütesiegel 15

3. Gefahrenabwehr- und Strafverfolgungsbehörden 16
3.1 Staatliche Handlungsfähigkeit und Stärkung der Gefahrenabwehrbehörden 16
3.2 Stärkung der Strafverfolgungsbehörden 18
3.3 Ganzheitliche Lagebilderstellung 19

4. Wirtschaft und Kritische Infrastrukturen (KRITIS) 20
4.1 Schutz der Wirtschaft vor Spionage und Sabotage 21
4.2 Erhöhung der Resilienz gegen Cyberangriffe speziell bei den KMU 22
4.3 Öffentlich-private Partnerschaften (ÖPP) 23
4.4 Kritische Infrastrukturen (KRITIS) und ähnliche Einrichtungen 24

5. Digitale Kompetenzen 26
5.1 Schulen 27
5.2 Hochschulen 28
5.3 Weiterbildung 28

6. Awareness und Verbraucherschutz 29

7. Fachkräfte 30

8. Innovative Forschung und Entwicklung 31
8.1 Stärkung der Spitzenforschung und Ausbildung des Nachwuchses 32
8.2 Stärkung der Forschungsverbünde 32
8.3 Förderung der anwendungsorientierten, wirtschaftsnahen Forschung und Entwicklung sowie des wechselseitigen Wissens- und Technologietransfers zwischen Wissenschaft und Wirtschaft 33
8.4 Schnelle Entwicklung durch Start-ups 34

9. Nationale und internationale Kooperationen 35
9.1 Ziel: Synergien für mehr Cybersicherheit nutzen 35
9.2 Sachstand 35
9.2.1 Internationale Kooperationen 36
9.2.2 Bund 36
9.2.3 Hessen 37
9.2.4 Kooperation mit EnBW 37
9.2.5 Kooperationen innerhalb der Verwaltung in Baden-Württemberg 38
9.3 Geplante Maßnahmen mit Leistungskennzahlen 38

10. Zusammenfassung der Ziele 39
10.1 Vernetzung der Cybersicherheitsakteure 40
10.2 Staatliche Verwaltung und Kommunen 40
10.3 Gefahrenabwehr- und Strafverfolgungsbehörden 41
10.3.1 Staatliche Handlungsfähigkeit und Stärkung der Gefahrenabwehrbehörden 41
10.3.2 Stärkung der Strafverfolgungsbehörden 41
10.3.3 Ganzheitliche Lagebilderstellung 41
10.4 Wirtschaft und Kritische Infrastrukturen (KRITIS) 42
10.4.1 Schutz der Wirtschaft vor Spionage und Sabotage 42
10.4.2 Erhöhung der Resilienz gegen Cyberangriffe speziell bei den KMU 42
10.4.3 Öffentlich-private Partnerschaften (ÖPP) 42
10.4.4 Kritische Infrastrukturen (KRITIS) und ähnlich schutzbedürftige Stellen 43
10.5 Digitale Kompetenzen 43
10.6 Awareness und Verbraucherschutz 44
10.7 Fachkräfte 44
10.8 Innovative Forschung und Entwicklung 44
10.9 Nationale und internationale Kooperationen 45

Impressum 46

1.

VERNETZUNG DER CYBERSICHERHEITSAKTEURE

Zur **Verbesserung des Informationsstands und der Reaktionsfähigkeit** der mit Cybersicherheit betrauten Akteure, Behörden und Gremien ist eine Intensivierung der Vernetzung notwendig. Auf diese Weise können frühzeitig Bedrohungen erkannt, gemeinsam bewältigt sowie Präventionsstrategien ausgebaut und weiterentwickelt werden. Dabei legen wir auf eine enge, komplementäre Zusammenarbeit mit zuständigen Einrichtungen des Bundes, insbesondere dem **Bundesamt für Sicherheit in der Informationstechnik (BSI)**, und den übrigen Ländern und der Europäischen Union Wert. Plattformen, in denen sich Baden-Württemberg – direkt oder in Kooperation mit anderen Ländern bundesweit – einbringen und Interessen artikulieren kann, wollen wir identifizieren, uns mit ihnen vernetzen und kooperieren. Aktivitäten wollen wir insbesondere im Hinblick auf das Nationale Cyber-Abwehrzentrum (NCAZ) als gemeinsame, behörden- und institutionsübergreifende Plattform des Bundes entfalten. Bislang ist im NCAZ keine Beteiligung der Länder institutionalisiert, obwohl insbesondere die Polizei bereits wesentliche Mehrwerte dazu hätten beitragen können.

Als zentrale Koordinierungs- und Meldestelle in Baden-Württemberg wurde die Cybersicherheitsagentur Baden-Württemberg (CSBW) durch das Cybersicherheitsgesetz errichtet. Die CSBW wird zur Vernetzung der Akteure in Baden-Württemberg den **Aufbau einer zentralen Informations- und Kommunikationsplattform** gestalten. Vertrauenswürdige Akteure sollen von dieser Plattform Informationen abrufen und über eine abgesicherte Chatfunktion miteinander kommunizieren können. Bestehende Akteure, Gremien und Strukturen sollten gestärkt und, wo immer möglich, gebündelt werden. Großes Potenzial liegt in der Intensivierung des Austauschs der CSBW mit den Kommunalen Landesverbänden und der Komm.ONE, um die Prozesse und Abläufe im Interesse der kommunalen Einrichtungen gemeinsam bestmöglich zu gestalten. Die CSBW unterstützt auch bereits bestehende Gremien bei Fachthemen der Cybersicherheit. Dazu gehören beispielsweise die länderoffene Arbeitsgruppe (LAG) Cybersicherheit, die Koordinierungsgruppe Informationssicherheit (KG InfoSic) und die Koordinierungsgruppe Cybersicherheit der Interministeriellen Arbeitsgruppe Digitalisierung. Die CSBW pflegt eine enge Zusammenarbeit mit der oder dem

Das **Gesetz für die Cybersicherheit in Baden-Württemberg** (Cybersicherheitsgesetz – CSG) vom 4. Februar 2021 ist das erste Gesetz in der Bundesrepublik Deutschland, welches einen ganzheitlichen Ansatz zur Verbesserung der Cybersicherheit verfolgt. Dazu haben wir die **Cybersicherheitsagentur Baden-Württemberg (CSBW)** errichtet.

Baden-Württemberg
CYBERSICHERHEITSAGENTUR

Chief Information Security Officer (CISO) der Landesverwaltung, der Justiz, der Polizei und den Nachrichtendiensten, dem BSI sowie mit den europäischen Einrichtungen (z. B. **ENISA**) und internationalen Partnern. Davon ausgenommen sind die existenten, fachspezifischen Gremienstränge der Polizei und der Nachrichtendienste.

Überdies will das Innenministerium mit einem operativ ausgerichteten Fachbeirat Cybersicherheit zentrale Akteure an der Weiterentwicklung der Cybersicherheitsarchitektur in Baden-Württemberg beteiligen. Mit dem Fachbeirat Cybersicherheit will das Innenministerium durch die CSBW externen Sachverstand zusammenführen und konkrete Fragestellungen bearbeiten. Unter Vorsitz des Innenministeriums sollen darüber hinaus in einem strategischen Fachbeirat Zusammenhänge mit übergeordneten Themen der Digitalisierung erörtert werden. So will das Innenministerium erreichen, dass ein ganzheitliches Bild zu aktuellen Fragestellungen der Cybersicherheit in Baden-Württemberg entsteht und neue Entwicklungen frühzeitig aufgenommen werden.

Der Vernetzung dienen auch die Veranstaltungen des Innenministeriums zur Cybersicherheit. Im Jahr 2021 hat bereits das **3. CyberSicherheitsForum (CSF)** stattgefunden. Beim CSF tauschen sich nationale wie auch internationale Expertinnen und Experten aus Sicherheitsbehörden, Wirtschaft und Wissenschaft über exzellente Lösungen und Zukunftsfragen der Cybersicherheit aus. Nachdem in den Jahren zuvor ca. 400 Personen vor Ort in der Landeshauptstadt angemeldet waren, konnten sich 2021 insgesamt über 500 Personen digital zuschalten. Künftig soll bei Vernetzungsveranstaltungen des Landes die **Anzahl der Teilnehmenden jährlich über 500** liegen.

„Mit neueren Projekten wie der Cybersicherheitsagentur verfolgt Baden-Württemberg u. a. das Ziel, die Vernetzung verschiedener Akteure zu verbessern, Sicherheitsstandards durchzusetzen und Systemsicherheiten zu gewährleisten. Um einen langfristigen Erfolg der Einrichtung zu gewährleisten, sind klare Definitionen und Verantwortlichkeiten genauso relevant wie eine noch effizientere Einbindung aller Akteure der Cybersicherheit in Baden-Württemberg."
ZEW, Zentrum für Europäische Wirtschaftsforschung, Metastudie – Chancen und Herausforderungen der Digitalisierung in Baden-Württemberg, 2021.

Der **„Fachbeirat Cybersicherheit"** wurde unter Leitung des ehemaligen Chief Information Officer (CIO) im Bundesministerium der Verteidigung im Jahr 2019 zur Überarbeitung der Cybersicherheitsarchitektur in Baden-Württemberg ins Leben gerufen. Die Besetzung des Beirats erfolgte zur fachlichen Prüfung der Konzepte mit hochrangigen Expertinnen und Experten aus Wirtschaft und Wissenschaft. Mit der Gründung der CSBW im Februar 2021 hat der Fachbeirat seine originäre Aufgabe erfüllt und soll nunmehr in der neuen Legislaturperiode weiterentwickelt werden. Um die Erfahrungen, Bedürfnisse und Vorstellungen von Wirtschaft, Forschung, Wissenschaft und Fachverbänden bei der Cybersicherheit aufzunehmen und zu diskutieren, werden wir den Fachbeirat in eine strategische und eine operative Sparte unterteilen.

2.

STAATLICHE VERWALTUNG UND KOMMUNEN

Um ein hohes Sicherheitsniveau in der staatlichen Verwaltung und den Kommunen zu erreichen, müssen Prozesse und Fachverfahren sowie die jeweiligen IT-Infrastrukturen auf professionellem Niveau und stets unter Berücksichtigung aktueller Entwicklungen abgesichert werden. Dabei wird die CSBW zum zentralen Ansprechpartner für die Landesverwaltung und für die Kommunen. Dazu arbeitet sie fachlich eng mit den Kommunalen Landesverbänden und dem Kommunalen IT-Dienstleister Komm.ONE zusammen.

Für eine Vielzahl bereits digitalisierter und noch zu digitalisierender Verwaltungsprozesse werden Bürgerinnen und Bürger sowie Unternehmen künftig ebenenübergreifende Verfahren nutzen. So werden in den Gemeinden, Städten und Landkreisen Bürgerdaten digital erfasst, um dann in Systemen des Landes verarbeitet oder über das Landesverwaltungsnetz weitergeleitet zu werden, um am Ende zentral in Bundesregistern gespeichert zu werden. Das betrifft Leistungen des Staates von A bis Z: Von der Verwaltung von Asylanträgen bis hin zur Zulassung von Fahrzeugen. Daher gilt es, die Zusammenarbeit zwischen Kommunen, Ländern und dem Bund hinsichtlich der Informationssicherheit zu vertiefen und damit wahrnehmbar zu stärken. Hierzu beteiligt sich das **Innenministerium als Fachaufsicht der CSBW** auf der strategischen Ebene aktiv in der Länderarbeitsgemeinschaft (LAG) Cybersicherheit der Innenministerkonferenz (IMK) sowie in der Arbeitsgemeinschaft (AG) Informationssicherheit des IT-Planungsrats. Auf der operativen Ebene erfolgt eine länderübergreifende Zusammenarbeit insbesondere über den **Verwaltungs-CERT-Verbund** (VCV). Eine Anbindung der Kommunen an diese Informationsflüsse über die CSBW wäre hier zielführend.

Die dem Handlungsfeld „Staatliche Verwaltung und Kommunen" zugehörigen Themenblöcke und Aufgabenstellungen orientieren sich an der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung 2018 des IT-Planungsrats **(Beschluss 2019/04 des IT-Planungsrats)**. Dort sind die Handlungsfelder mit konkreten Maßnahmen und messbaren Zielen unterlegt sowie ein fortlaufendes jährliches Berichtswesen der AG Informationssicherheit an den IT-Planungsrat festgelegt.

Der **IT-Planungsrat** fungiert als zentrales politisches Steuerungsgremium zwischen Bund und Ländern in Fragen der Informationstechnik und der Digitalisierung von Verwaltungsleistungen.
Durch die Beschlüsse des IT-Planungsrats erhalten Bund und Länder eine verbindliche Grundlage für die gemeinsamen föderalen Digitalisierungsaktivitäten.

Ein Computer Emergency Response Team (**CERT**) unterstützt bei der Analyse und Bewertung von Sicherheitsvorfällen.

Die darin benannten Handlungsfelder sind:

- Informationssicherheitsmanagement
- Absicherung der IT-Netzinfrastruktur der öffentlichen Verwaltung
- ein einheitliches Sicherheitsniveau für ebenenübergreifende IT-Verfahren
- gemeinsame Abwehr von IT-Angriffen
- IT-Notfallmanagement

Daran anknüpfend wird die CSBW die Einrichtungen der Landesverwaltung und Kommunen insbesondere bei den in den folgenden Abschnitten aufgeführten Themenstellungen, Aufgaben und Herausforderungen unterstützen.

Über die Ausgestaltung dieser Handlungsfelder mit konkreten Maßnahmen hinaus gilt es, bei der Entwicklung neuer digitaler Prozesse, IT-Anwendungen und Systeme einen Paradigmenwechsel herbeizuführen: Die Aspekte der Cybersicherheit müssen bereits von Anfang an berücksichtigt werden (siehe dazu den Abschnitt **2.6 Security by Design und Sicherheitsgütesiegel).**

Nur so gelingt es, die Cybersicherheit zukunftsorientiert und nachhaltig und auf dem erforderlichen Niveau auszugestalten.

Cybersicherheit umfasst nach § 2 Absatz 11 des Cybersicherheitsgesetzes „alle Aspekte der Sicherheit in der Informationstechnik und den Schutz gesellschaftlich relevanter Prozesse vor Angriffen im gesamten Cyberraum."

Informationssicherheit umfasst nach § 2 Absatz 9 des Cybersicherheitsgesetzes „alle technischen und nichttechnischen Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen."

2.1 Informationssicherheitsmanagement

Ein wichtiger Baustein zur Verbesserung der Cybersicherheit ist der Aufbau und Betrieb eines Informationssicherheitsmanagementsystems (ISMS) in jeder Behörde, Dienstelle oder Einrichtung. Das ISMS ist ein wichtiges Werkzeug für die Steuerung und Lenkung der Informationssicherheit für die jeweilige Leitungsebene. Damit wird Informationssicherheit / Cybersicherheit zur Chefsache. Es gilt, Aufgaben, Aktivitäten und Maßnahmen zu planen, umzusetzen, regelmäßig zu überprüfen und zu verbessern. Die Dokumentation der Maßnahmen in einem hierfür zur Verfügung stehenden ISMS-Tool macht Umsetzungsstände transparent, messbar und steuerbar. Die Landesbehörden in Baden-Württemberg orientieren sich an der VwV Informationssicherheit des Landes (bzw. der noch zu entwickelnden Rechtsvorschrift). Zur Umsetzung der hieraus resultierenden umfangreichen organisatorischen und technischen Maßnahmen **zum Erreichen und Aufrechterhalten eines angemessenen Sicherheitsniveaus müssen weiterhin dezentrale personelle und finanzielle Ressourcen aufgebracht werden.**

Die CSBW kann für den Aufbau und Betrieb eines ISMS sowie bei der Umsetzung der Standards des BSI in den Behörden, Dienststellen und Einrichtungen des Landes wertvolle Unterstützung für die oder den CISO leisten. Dies betrifft in einem ersten Schritt das wichtige Handlungsfeld der Schulung der Fachkräfte.

Überdies plant die CSBW durch Beratung und Mustervorlagen zu unterstützen. Daran anknüpfend wird das **Innenministerium den Dienststellen und Einrichtungen der Landesverwaltung die Dokumentation von Sicherheitskonzepten für Systeme und Anwendungen in einer zentralen Dokumentationssoftware,** bei der jedes Ressort ausschließlich auf seine ISMS-Inhalte zugreifen kann, **ermöglichen.**

Um ebenenübergreifend ein hohes und somit möglichst einheitliches Sicherheitsniveau zu erreichen, sollen zukünftig auch die Kommunen Unterstützung durch die CSBW bei der Anwendung der Standards des BSI erfahren. Dazu sind insbesondere Beratungsleistungen und Schulungen durch die CSBW sowie ein Partizipieren an den Sensibilisierungsmaßnahmen geplant.

Chief Information Security Officer (**CISO**) haben eine Steuerungs-, Koordinierungs-, Prüf- und Beratungsfunktion innerhalb der Organisation. Sie sind übergreifend verantwortlich für das Informationssicherheitsmanagement sowie dessen strategische Weiterentwicklung.

2.2
Analyse- und Reaktionsfähigkeit vor Ort stärken

Zur Bewältigung der Herausforderungen der gestiegenen Bedrohungslage für informationstechnische Systeme können die Landesbehörden künftig die Unterstützung durch die CSBW in Anspruch nehmen.

Zunehmend spielt auch der Einsatz von auf Künstlicher Intelligenz (KI) basierten Technologien, Mechanismen und Detektionsmöglichkeiten im Bereich der Cybersicherheit eine Rolle. Die CSBW wird sich stets auf Augenhöhe mit aktuellen Entwicklungen bewegen und entsprechende Handlungsempfehlungen ausgeben.

Die in den Rechenzentren der Landesverwaltung begonnenen Projekte zum Einsatz sogenannter „Security Information and Event Management (SIEM)" – Systeme werden konsequent fortgesetzt. In sogenannten „Security Operation Center" (SOC) lassen sich Anomalien und Angriffe erkennen und Abwehrmaßnahmen einleiten. Hierbei kommt der CSBW künftig eine weitere bedeutende Rolle zu.

Bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems kann künftig ein Mobile Incident Response Team (MIRT) der CSBW vor Ort unterstützen.

Überdies sind weitere **dezentrale Maßnahmen** bei den staatlichen und kommunalen Stellen erforderlich, um die Kompetenz und Ressourcen für die IT-Sicherheit zu stärken. Die CSBW wird dafür einen Katalog an Dienstleistungen und Produkten unter bestmöglicher Berücksichtigung der von den Kommunalen Landesverbänden gemeldeten Bedarfe der Gemeinden, Städte und Landkreise sowie Erfahrungen der Komm.ONE erstellen. So wird die CSBW **jährlich mindestens sechs Untersuchungen mit Schwachstellenscans für öffentliche Stellen** mit **anschließender Beratung einschließlich einer Maßnahmenplanung** anbieten.

2.3
Gemeinsame Abwehr von IT-Angriffen

Im Hinblick auf die Zunahme der professionellen und gezielten Angriffe ist die Früherkennung von Sicherheitslücken im Vorfeld von Cyberangriffen besonders wichtig. Die Beseitigung der Sicherheitslücken und die Abwehr der Angriffe wird strategisch durch eine operative Zusammenarbeit von Bund (BSI) und Ländern über den Verwaltungs-CERT-Verbund (VCV) gefördert. Hierüber wird der Informationsaustausch verbessert und Unterstützung angeboten, um effektiver und schneller auf IT-Angriffe reagieren zu können. In den dafür geschaffenen CERT-Strukturen werden u. a. sicherheitskritische Themen erörtert, bewertet und regelmäßige Warnungen über aktuelle Gefahren ausgegeben.

Wir werden die gemeinsame Abwehr von IT-Angriffen, insbesondere durch den **Aufbau einer Plattform** bei der CSBW, stärken. Dadurch wird der **Austausch von Indicators of Compromise** mit autorisierten Beteiligten verbessert.

Indicators of Compromise sind technische Informationen, die zur Detektion einer Infektion mit Schadsoftware oder einer anderweitigen Kompromittierung verwendet werden können.

2.4
IT-Notfallmanagement

Um die Folgen eines erfolgreichen Cyberangriffs oder anderweitig herbeigeführter Störungen möglichst gering und beherrschbar zu halten, bedarf es zur besseren Vorbereitung auf Notfälle einer strukturierten Herangehensweise in Form eines Notfallvorsorgekonzepts und eines Notfallbehandlungsplans in Form von Notfallhandbüchern. Dazu gehören nicht nur die Maßnahmen zur Vorbeugung von Notfällen sowie die Schritte der Notfallbewältigung an sich, sondern auch die Benennung der Notfallverantwortlichen in den jeweiligen öffentlichen Stellen, deren Aufgaben sowie die Beschreibung der Melde- und Alarmierungswege. Dies ermöglicht im Falle eines Notfalls eine schnelle Reaktion. Das IT-Notfallmanagement ist Teil des ganzheitlichen Notfallmanagements der jeweiligen Organisation.

Neben Sensibilisierungen und Notfallschulungen durch die CSBW werden insbesondere **Notfallvorsorgekonzepte für die zentralen, landesweiten Systeme und Fachverfahren,** wie z. B. den Messaging-Dienst, die E-Akte BW und Service-bw, erstellt.

2.5
Rechtliche Rahmenbedingungen

Zu der Erhöhung der allgemeinen Cybersicherheit auf Landesebene ist ein belastbarer, normativer Rahmen als eine unerlässliche Voraussetzung zur Schaffung notwendiger Befugnisse zu betrachten.
Der Landtag hat am 4. Februar 2021 das Gesetz zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften beschlossen, deren Hauptregelungen das **Gesetz für die Cybersicherheit in Baden-Württemberg** (Cybersicherheitsgesetz – CSG) enthält. Die Auswirkungen dieses Cybersicherheitsgesetzes werden wir nach einem Erfahrungszeitraum von drei Jahren evaluieren. Dies erfolgt unter Mitwirkung der kommunalen Landesverbände, der oder des Landesbeauftragten für den Datenschutz und ggf. weiterer sachverständiger Personen. Auf Basis der **Evaluation** wird zu entscheiden sein, ob Anpassungen erforderlich sind.

Um den normativen Rahmen weiter zu konkretisieren, wird das Innenministerium in Abstimmung mit dem Arbeitskreis Informationstechnik (AK-IT) und im Einvernehmen mit dem IT-Rat Baden-Württemberg eine **Rechtsverordnung nach dem Cybersicherheitsgesetz erlassen.** Über diese Rechtsverordnung werden wir die flächendeckende Umsetzung einheitlicher Standards in Baden-Württemberg voranbringen.

2.6
Security by Design und Sicherheitsgütesiegel

Um die Cybersicherheit besser zu verwirklichen, sollen Sicherheitskonzepte nicht erst am Ende der Prozesskette ansetzen, sondern bereits bei der Entwicklung und Beschaffung von Produkten und Dienstleistungen soll der Grundsatz Security by Design berücksichtigt werden.
In diesem Zusammenhang sind die vom **BSI** eingeführten **Sicherheitsgütesiegel** einschließlich Zertifizierungen zu beachten. Überdies prüfen wir, inwieweit der Grundsatz **Security by Design** und auch der Einsatz von Produkten mit **Sicherheitsgütesiegeln** stärker im Rahmen der Beschaffung und der IT-Vorhaben berücksichtigt werden kann. Anknüpfungspunkte hierfür sind insbesondere die Weiterentwicklung der Verwaltungsvorschrift Beschaffung und der Verwaltungsvorschrift IT-Standards.

Nach dem Grundsatz **Security by Design** werden Sicherheitsaspekte als integraler Bestandteil in allen Phasen der Entwicklung berücksichtigt, um Schwachstellen erst gar nicht entstehen zu lassen.

3.

GEFAHRENABWEHR- UND STRAFVERFOLGUNGSBEHÖRDEN

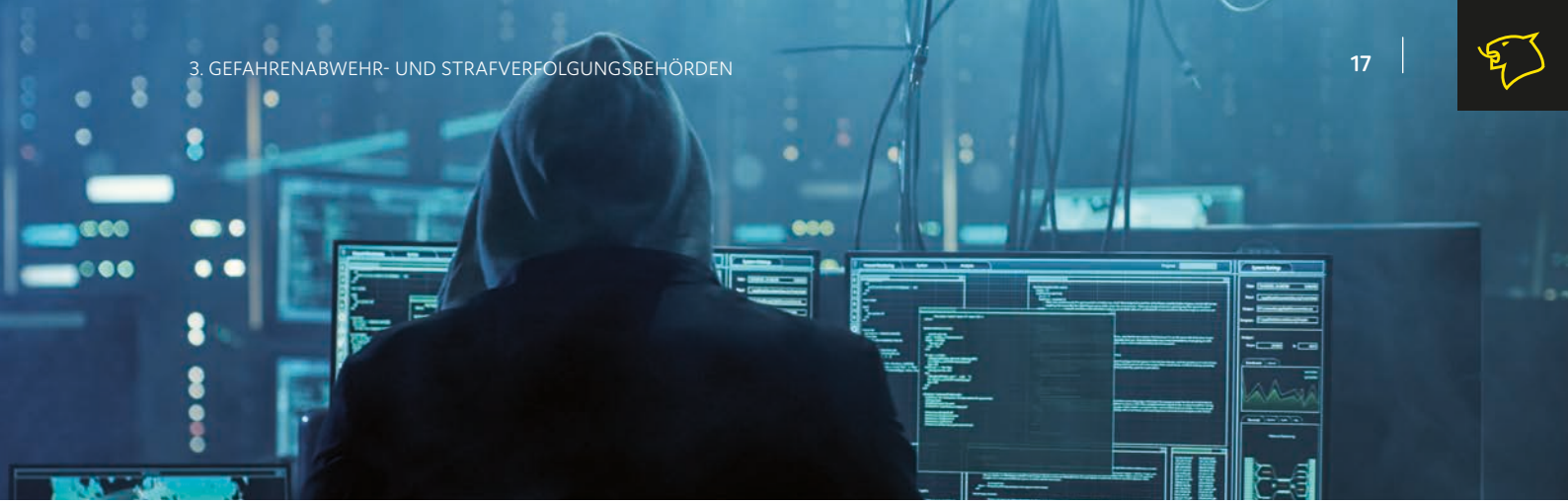
Die Rolle der Gefahrenabwehr- und Strafverfolgungsbehörden ist im Bereich Cybercrime, -spionage und -sabotage und der physischen Sicherheit elementar.

3.1 Staatliche Handlungsfähigkeit und Stärkung der Gefahrenabwehrbehörden

Da die Handlungsfähigkeit des Staates immer mehr von sicheren IT-Systemen und -Netzen abhängt, müssen Strukturen geschaffen werden, die der Verantwortung für die Funktionsfähigkeit der staatlichen IT-Nutzung gerecht werden. Diese Herausforderung kann nur als gesamtstaatliche Aufgabe, also in der Zusammenarbeit aller Akteure, sichergestellt werden.

Zentraler Akteur ist dabei die CSBW, deren Aufgaben in § 3 des Cybersicherheitsgesetzes beschrieben sind:

1. Abwehr von Gefahren für die Cybersicherheit,
2. Schutz gesellschaftlicher Prozesse vor Angriffen im Cyberraum,
3. Mitwirkung an der Entwicklung und Setzung von Standards für die Cybersicherheit sowie Überprüfung der Einhaltung der geltenden Standards für die Cybersicherheit,



4. zentrale Koordinierungs- und Meldestelle,

5. Kontaktstelle im Rahmen des Verfahrens zu § 8b des BSI-Gesetzes und Unterrichtung der zuständigen Aufsichtsbehörden, obersten Landesbehörden sowie der Koordinierungsstelle Kritische Infrastrukturen über die Informationen, die sie als Kontaktstelle erhalten hat,

6. Information und Beratung zur Cybersicherheit und

7. Kompetenzzentrum für Sensibilisierungen und Schulungen zur Cybersicherheit.

Insbesondere durch die regelmäßig und anlassbezogen stattfindenden Lagebesprechungen Cybersicherheit der CSBW wird ein fortlaufender Austausch aller zuständigen Behörden sichergestellt, namentlich mit dem Landeskriminalamt Baden-Württemberg (LKA BW) und dem Landesamt für Verfassungsschutz.

Im Hinblick auf diese vielfältigen Aufgaben und die jährlich ansteigende Anzahl der Cybersicherheitsbedrohungen ist eine angemessene Stellenausstattung der CSBW unerlässlich. Aus Sicht des Innenministeriums ist angezeigt, die **CSBW personell zu stärken.**

Auch das Landesamt für Verfassungsschutz bildet eine tragende Säule in der Cybersicherheitsarchitektur des Landes. Speziell die Bereiche Cyberspionage und -sabotage sollen daher ebenfalls personell verstärkt werden. Das Landesamt baut die technischen Möglichkeiten hinsichtlich der Analyse von Cyberangriffen mit mutmaßlich nachrichtendienstlichem Hintergrund weiter aus. Ferner sollen die Sensibilisierungs- und Beratungsgespräche in Kombination aus Wirtschaftsschutz und Cyberabwehr intensiviert werden. Darüber hinaus steht das Landesamt für Verfassungsschutz im Rahmen der gesetzlichen Aufgabenstellung bei allen Fragestellungen zu Cyberspionage und -sabotage fremder Staaten als Ansprechpartner zur Verfügung.

Die Polizei ist entsprechend ihres gesetzlichen Auftrags neben der Strafverfolgung auch für die Abwehr von Gefahren für die Cybersicherheit mit polizeilichen Mitteln zuständig. Durch diese Doppelfunktionalität liegen der Polizei Informationen aus Ermittlungsverfahren vor, die zur Abwehr von Gefahren für die Cybersicherheit verwendet werden können.

„Mit der neu geschaffenen Cybersicherheitsagentur rüstet sich Baden-Württemberg noch besser gegen Angriffe im Netz. Diese wollen wir weiter personell stärken."
Koalitionsvertrag 2021-2026 von BÜNDNIS 90/DIE GRÜNEN Baden-Württemberg und der CDU Baden-Württemberg.

3.2
Stärkung der Strafverfolgungsbehörden

Bedingt durch die massiv voranschreitende Digitalisierung stiegen die Fallzahlen bei der Cyberkriminalität in den vergangenen Jahren enorm an. Zudem zeigen sich qualitative Veränderungen. Ein besonderes Bedrohungspotential ergibt sich aus der zunehmenden Fokussierung von Cyberkriminellen auf bedeutsame Ziele, wie wirtschaftlich starke Unternehmen, Kritische Infrastrukturen und öffentliche Einrichtungen.

Hinzu kommt, dass die Polizei im Zusammenhang mit den neuen Meldepflichten nach dem Netzwerkdurchsetzungsgesetz künftig eine Vielzahl von im Internet begangenen Straftaten zusätzlich zu bearbeiten hat.

Wir treten dieser Entwicklung mit einer effektiven Strafverfolgung entgegen. In diesem Sinne wollen auch die Parteien der Regierungskoalition die Polizei und Justiz personell und technisch kräftig stärken. Insbesondere setzen sich das Innenministerium und das Justizministerium dabei für die zusätzliche Einstellung von **Digitalexpertinnen und -experten** sowie Ermittlungsassistentinnen und -assistenten **für die Polizei** sowie für die Besetzung von **korrespondierenden neuen Stellen bei der Justiz,** vorrangig im Bereich der Staatsanwaltschaften, ein. Neben der Gewinnung neuen Fachpersonals behält das Innenministerium dabei auch die fortlaufende fachliche Qualifikation der Polizeibeamtinnen und Polizeibeamten im Blick. Der Koalitionsvertrag sieht überdies zur weiteren Stärkung der bereits sehr guten Zusammenarbeit von Ermittlungs- und Justizbehörden und der bestehenden schlagkräftigen Strukturen zur Bekämpfung der Cybercrime in Baden-Württemberg – insbesondere der Zentralstelle für die Bekämpfung von Informations- und Kommunikationskriminalität sowie der bestehenden Schwerpunktstaatsanwaltschaften – die Einrichtung eines Cybercrime-Zentrums vor.

> „Wir stärken die Sicherheitsbehörden bei der Strafverfolgung im digitalen Raum und statten sie personell und technisch so aus, dass sie auch weiterhin entschlossen gegen Cybercrime, Cyberspionage, Cybersabotage und Cyberwar vorgehen können."
> Koalitionsvertrag 2021-2026 von BÜNDNIS 90/ DIE GRÜNEN Baden-Württemberg und der CDU Baden-Württemberg.

Cyberermittlungen, aber auch die IT-basierte Beweissicherung, sind mit sich dynamisch entwickelnden technologischen Herausforderungen, ständig wachsenden Datenmengen und komplexer werdenden digitalen Spuren konfrontiert. Vor diesem Hintergrund ist es aus Sicht des Innenministeriums und des Justizministeriums angezeigt, das Technikbudget der Polizei spürbar zu erhöhen, um gezielte Investitionen in die technische Ausstattung zu ermöglichen und den Betrieb sicherzustellen.

Neben einem starken, kompetenten Personalkörper und einer guten technischen Ausstattung der Strafverfolgungsbehörden ist für die erfolgreiche Bekämpfung der Cyberkriminalität insbesondere auch entscheidend, dass die Strafverfolgungsbehörden über ausreichende rechtliche Befugnisse verfügen, um ihre Aufgaben im digitalen Raum ebenso effektiv wahrnehmen zu können, wie in der analogen Welt.

Bei Straftaten, die über das Internet begangen werden, handelt es sich bei der von Tatverdächtigen verwendeten IP-Adresse um einen

wichtigen Ermittlungsansatz. Vor diesem Hintergrund setzen sich das Innenministerium und das Justizministerium dafür ein, die Möglichkeiten der Strafverfolgungsbehörden zur Identifizierung von tatverdächtigen Personen im Internet zu verbessern.

Bei der Telekommunikationsüberwachung (TKÜ) handelt es sich ebenfalls um ein unverzichtbares, bewährtes Instrument zur Verfolgung schwerer Straftaten. Allerdings findet relevante Kommunikation zwischenzeitlich oftmals nicht klassisch per Telefon und SMS, sondern per Internettelefonie sowie mittels internetbasierten Messenger-Diensten statt. Diese Kommunikation wird von den Anbietern standardmäßig mit der sogenannten Ende-zu-Ende-Verschlüsselung versehen, welche den rechtmäßigen und auf eindeutigen Rechtsgrundlagen fußenden Zugriff zur Verfolgung schwerer Straftaten meist unmöglich macht. Die Verschlüsselung internetbasierter Kommunikationsdienste durch die Anbieter leistet einen wichtigen Beitrag für eine sichere Kommunikation. Das Innenministerium und das Justizministerium setzen sich dafür ein, dass die Anbieter dazu verpflichtet werden, selbst die technischen Voraussetzungen zu schaffen, um den Strafverfolgungsbehörden zum Schutz gewichtiger Rechtsgüter sowie auf Basis eines richterlichen Beschlusses die Kommunikationsinhalte vom Anbieter unverschlüsselt in Echtzeit zur Verfügung stellen zu können und unterstützen in diesem Zusammenhang bereits bestehende Bemühungen auf Ebene der Europäischen Union. Eine solche Verpflichtung muss technikoffen formuliert sein, um den Anbietern auch weiterhin die Entwicklung und Anbietung verschlüsselter Kommunikationsprodukte zum Schutz vor unberechtigten Zugriffen zu ermöglichen.

3.3 Ganzheitliche Lagebilderstellung

Als Grundlage zielgerichteten Handelns zur Verbesserung der Cybersicherheit dient den Gefahrenabwehr- und Strafverfolgungsbehörden ein ganzheitliches Lagebild. Hierbei kann es sich sowohl um ein strategisches Lagebild mit dem Ziel einer strategischen Entscheidungshilfe für die Zukunft als auch um ein operatives Lagebild mit dem Ziel, Kenntnis relevanter Gegebenheiten als Grundlage operativer Entscheidungen in der jeweiligen Situation zu erlangen, handeln.

Die Expertinnen und Experten der CSBW erstellen dazu ein umfassendes Lagebild, basierend auf aktuellen Informationen aus allen zur Verfügung stehenden Informationsquellen. Dazu sammeln sie Daten zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen aus Informationsquellen von Staat, Wirtschaft und Wissenschaft. Hierfür werten sie auch die direkt bei ihnen eingegangenen Meldungen von Betroffenen aus. Aus den Informationen werden zielgerichtete, operative Maßnahmen zur Wiederherstellung des Normalzustandes der IT-Services oder strategische Entscheidungen abgeleitet.

Die CSBW wird ein **Lagebild zumindest fünfzigmal im Jahr erstellen** und im Rahmen eines Warn- und Informationsdienstes an die im Cybersicherheitsgesetz benannten Stellen verteilen.

4.

WIRTSCHAFT UND KRITISCHE INFRASTRUKTUREN (KRITIS)

Unser Ziel ist es, ein hohes Sicherheitsniveau für Unternehmen zu schaffen, insbesondere für solche, die zu den Kritischen Infrastrukturen (KRITIS) zählen, und im Sinne der Daseinsvorsorge die Handlungsfähigkeit des Staates zu schützen.

4.1 Schutz der Wirtschaft vor Spionage und Sabotage

Die Wirtschaft wollen wir vor Cyberspionage und -sabotage schützen. Vor allem kleinere und mittlere Unternehmen (KMU), viele davon Weltmarktführer, stehen im Fokus nachrichtendienstlich gesteuerter Cyberangriffe. Die digitale Verwundbarkeit ist, im Vergleich zu größeren und vielfach besser geschützten Unternehmen sowie Konzernen, oftmals höher, da meist die nötigen personellen wie finanziellen Ressourcen zur Absicherung fehlen. Nicht immer steht bei Attacken auf KMU der Know-how-Gewinn im Vordergrund: Gerade die vermeintlich kleineren und „schwächeren" Firmen geraten aufgrund ihres Kundenkreises oder der geschäftlichen Verbindungen zu größeren Unternehmen in den Fokus. Dabei ist davon auszugehen, dass nachrichtendienstliche Akteure unter anderem die Strategie verfolgen, sich über elektronische Verbindungswege „von klein nach groß" Zugriff auf die IT-Systeme der eigentlichen Ziele zu verschaffen.

88 Prozent der befragten Unternehmen waren in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen.
Bitkom, Wirtschaftsschutz 2021.

Unsere Bemühungen für den Wirtschaftsschutz werden wir deshalb intensivieren und vermehrt auf Spionage- und Sabotagebedrohungen aufmerksam machen. Zudem werden wir, wie etwa im Rahmen der „SiFo-Studie 2018/19: Gefährdungen in baden-württembergischen Unternehmen durch Ausspähungen, Know-how-Abflüsse und Datenmanipulationen", weiter praxistaugliche Empfehlungen zur Prävention erarbeiten. Das Landesamt für Verfassungsschutz steht im Rahmen seiner gesetzlichen Aufgabenstellung bei allen Fragen zu Cyberspionage- und -sabotage fremder Staaten als Ansprechpartner für sämtliche Stellen im Land zur Verfügung. Es bestehen bereits vielfältige und etablierte Kontakte zwischen dem Landesamt für Verfassungsschutz und Unternehmen, insbesondere zu solchen, die sich in der Geheimschutzbetreuung des Bundes oder des Landes Baden-Württemberg befinden oder sich im Rahmen des Sicherheitsforums Baden-Württemberg – Die Wirtschaft schützt ihr Wissen – engagieren.

Auf geeigneten Fachkonferenzen und Symposien werden wir verstärkt den Kontakt zu Wirtschaftsvertreterinnen und Wirtschaftsvertretern suchen und weiterhin **bedarfsorientierte Beratungen im Bereich der Spionage- und Sabotageabwehr anbieten.**

4.2 Erhöhung der Resilienz gegen Cyberangriffe speziell bei den KMU

KMU stehen im Fadenkreuz von Cyberkriminellen wie nie zuvor. Wir werden uns daher zunehmend darauf konzentrieren, wirksame Schutzschirme gegen Angriffe aus dem Cyberraum zu entwickeln bzw. zu unterstützen, um so die Resilienz der Wirtschaftsunternehmen, speziell der KMU, gegen Cyberangriffe weiter zu verbessern.

Ausgeklügelte Notfallmanagementsysteme sind längst nicht mehr nur den Großkonzernen vorbehalten. Auch KMU müssen Cyber-Resilienz aufbauen und verstärkt in wirkungsvolle Maßnahmen der Prävention investieren. Derartige Ansätze umfassen nicht nur die IT-Infrastruktur, sondern zielen auch auf das sicherheitsbewusste Verhalten der Mitarbeitenden ab und gehen bis hin zu einem sicherheitsorientierten Notfallmanagement für den Fall der Fälle. Diese Bemühungen wollen wir aktiv unterstützen und Maßnahmen fördern, die darauf abzielen, einen Schaden erst gar nicht entstehen zu lassen sowie mit Störungen aller Art professionell umzugehen. Dabei unterstützen wir KMU, den Regelbetrieb möglichst schnell wieder aufnehmen zu können. Cyber-Resilienz bewerben wir als eine der Kernkompetenzen bei den Cyber-Sicherheitsmaßnahmen einer Organisation. Wir wollen erreichen, dass so viele KMU wie möglich Initiativen ergreifen, um mehr Cyber-Resilienz zu erlangen. Neben der technischen Abwehr gehören dazu das Erlangen von Know-how zum Wiederanlauf und zur Wiederherstellung sowie konsequente Reaktionsmöglichkeiten auf Cyberangriffe. Geschädigten Unternehmen wird die CSBW eine niederschwellige Vorfallsannahme und Empfehlungen zur weiteren Vorgehensweise anbieten – und das rund um die Uhr.

Mit der CSBW haben wir einen neuen Ansprechpartner für die baden-württembergische Wirtschaft geschaffen. Als neues Herzstück der Cybersicherheitsarchitektur fungiert die CSBW als zentrale Koordinierungs- und Meldestelle im Bereich Cybersicherheit. Davon unberührt bleiben die Zuständigkeit der Polizei bei der Bekämpfung der Cyberkriminalität, insbesondere der beim LKA BW angesiedelten Zentralen Ansprechstelle Cybercrime, die u. a. Hinweise auf Cyberangriffe entgegennimmt und zeitnahe polizeiliche Erstmaßnahmen veranlasst, und die Zuständigkeit des Landesamts für Verfassungsschutz Baden-Württemberg insbesondere in den Bereichen Spionageabwehr und geheimschutzbetreute Wirtschaft.

Die am FZI Forschungszentrum Informatik erlangten Erfahrungen in dem vom Innenministerium geförderten Projekt „Cyberwehr Baden-Württemberg“ werden weiter genutzt. Seit 2018 ist hier wertvolle Grundlagenarbeit für eine Kontakt- und Beratungsstelle bei Cyber-

„Wir sehen die Gefahr von Cyberattacken auf baden-württembergische Unternehmen mit Sorge. Um Selbstständige und KMU besser bei der Cybersicherheit zu begleiten, bieten wir eine Erstberatung über die Cybersicherheitsagentur an. Ziel ist es, unsere Unternehmen zu sensibilisieren und Lösungswege für mehr Sicherheit in einer sich digitalisierenden Welt aufzuzeigen.“
Koalitionsvertrag 2021-2026 von BÜNDNIS 90/DIE GRÜNEN Baden-Württemberg und der CDU Baden-Württemberg.

angriffen geleistet worden, die in den Betrieb der Cyberhotline der CSBW einfließen soll. Kein Malerbetrieb und keine Apotheke soll im Falle eines Cyberangriffs alleingelassen werden. So wollen wir die Zusammenarbeit zwischen Staat und Wirtschaft (z. B. im Bereich Wirtschaftsschutz und Cybercrime) sowie Unterstützungs- und Beratungsleistungen für Unternehmen ausbauen. Wir nehmen uns vor, **bedarfsorientierte Hilfestellungen für KMU sowohl in präventiver Hinsicht als auch nach einem Sicherheitsvorfall** anzubieten.

Bei Cyberangriffen oder anderen Vorfällen hilft die CSBW Landesbehörden, Städten, Gemeinden und Landkreisen – ganz konkret auch bei der Wiederherstellung der Systeme nach einem Angriff. In begründeten Einzelfällen können auch andere Organisationen mit wichtiger Bedeutung für das öffentliche Gemeinwesen Hilfe erhalten.

4.3 Öffentlich-private Partnerschaften (ÖPP)

Neben den Behinderungen im Organisationsablauf, im Betrieb sowie den psychischen Belastungen für die Mitarbeitenden stehen KMU im Falle eines Cyberangriffs häufig vor der Herausforderung, zur Wiederherstellung der Systeme ein passendes IT-Sicherheitsunternehmen mit entsprechenden IT-Schwerpunkten zu finden. Jede Reaktion auf einen Angriff erfordert besondere und spezifische Erfahrungen und Kenntnisse. Für das effiziente Zusammenführen von Geschädigten mit IT-Sicherheitsdienstleistern zur Wiederherstellung sowie zur Umsetzung der präventionsorientierten Erstberatung werden wir eine Vermittlungsstelle etablieren, die IT-Sicherheitsdienstleistern diskriminierungsfreien Zugang gewähren soll. Wir werden prüfen, ob eine öffentlich-private Partnerschaft (ÖPP) als vertraglich geregelte Zusammenarbeit zwischen öffentlicher Hand und IT-Unternehmen der Privatwirtschaft in einer Zweckgesellschaft diese Aufgabe übernehmen kann. Auf die in Karlsruhe geleistete Vor- und Grundlagenarbeit werden wir zurückgreifen und das kompetente Partnernetzwerk der Cyberwehr Baden-Württemberg einbeziehen. Unser Ziel ist die Vermittlungsstelle nach Gründung bedarfsorientiert stetig auszubauen und weitere IT-Profile zur Bewältigung eines wirkungsvollen Präventions- und Notfallmanagements zu hinterlegen. **Dazu sollen zumindest 15 IT-Dienstleister pro Jahr neu in das Netzwerk aufgenommen werden.**

Damit KMU zur Prävention von schädigenden Cyberattacken bzw. im Fall eines Cyberangriffs genau diejenigen IT-Sicherheitsdienstleister an die Hand bekommen, die die Expertise zur Herstellung ihrer Systeme haben, prüfen wir die Möglichkeit einer ÖPP, die diese Zusammenführung vornimmt. Sie pflegt das passende IT-Netzwerk und sichert den diskriminierungsfreien Zugang.

4.4 Kritische Infrastrukturen (KRITIS) und ähnliche Einrichtungen

Organisationen und Einrichtungen mit herausragender Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung es zu nachhaltigen Versorgungsengpässen oder anderen dramatischen Folgen kommen kann, werden nachfolgend als Kritische Infrastrukturen, kurz KRITIS, bezeichnet. Eine zunehmende Bedrohung sind Cyberangriffe gegen solche Einrichtungen wie beispielsweise Unternehmen aus den Bereichen Transport und Verkehr, Energieversorgung, Wasserversorgung, Medien und Kultur, Unternehmen der Informations- und Kommunikationstechnik sowie die gerade zur Bewältigung der Corona-Krise notwendigen Krankenhäuser. Eine Störung oder der Ausfall von IT-Infrastrukturen in solchen Einrichtungen kann gravierende Folgen für Staat und Gesellschaft haben.

Unser **zentrales Ziel** ist, die Betreiber zu unterstützen, ein angemessen hohes Sicherheitsniveau im Cyberraum für Kritische Infrastrukturen (KRITIS) zu gewährleisten. **Wir unterstützen die Betreiber in Baden-Württemberg bei der Erstellung von Notfallvorsorgekonzepten und Notfallbehandlungsplänen, insbesondere auch solche, die aus Sicht des Landes zu den KRITIS zählen, jedoch nicht von der BSI-Kritisverordnung des Bundes erfasst werden.**

Die zunehmende Professionalisierung und Internationalisierung der Cybercrime, -spionage und -sabotage sowie die daraus entstehenden Gefahren für Wirtschaft und Gesellschaft stellen die Betreiber Kritischer Infrastrukturen und Ermittlungsbehörden gleichermaßen vor wachsende Herausforderungen. Deshalb ist die Förderung der Sicherheit bei der Nutzung von Informationstechnologien durch die Betreiber Kritischer Infrastrukturen sowie eine erfolgreiche Vorbeugung und Bekämpfung von Cybercrime eines unserer zentralen Anliegen.

Bei Angriffen auf Kritische Infrastrukturen sind eine effektive Krisenkommunikation und eine schnelle Reaktion erfolgskritische Faktoren für eine professionelle Vorfallbearbeitung. Wir setzen uns dafür ein, dass jedes KRITIS-Unternehmen in Baden-Württemberg über ein Notfallvorsorgekonzept und einen Notfallbehandlungsplan verfügt.

Klare Strukturen, **Melde- und Alarmierungswege** sind festzulegen und konsequent umzusetzen. Im Fall einer Cyberkrise ist ein effizienter und kontinuierlicher Informationsfluss zwischen den verantwortlichen öffentlichen und privaten Stellen erfolgsentscheidend.

Kritische Infrastrukturen im Sinne des BSI-Gesetzes sind „Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und

2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden."

Die nähere Bestimmung erfolgt durch Rechtsverordnung. In vielen Sektoren liegt der Regelschwellenwert für eine Kritische Infrastruktur bei 500 000 versorgten Personen.

Die Identifikation konkreter Kritischer Infrastrukturen erfolgt grundsätzlich unabhängig von der BSI-Kritisverordnung individuell durch die jeweils zuständige administrative Ebene. Aus Landessicht ist die BSI-Kritisverordnung ein hilfreicher erster Ansatzpunkt zur Identifikation Kritischer Infrastrukturen. Aufgrund ihrer Bedeutung für das Funktionieren des Gemeinwesens können in Baden-Württemberg jedoch auch Einrichtungen und Unternehmen zu den Kritischen Infrastrukturen zählen und Unterstützung durch das Land erhalten, die nicht die Schwellenwerte der BSI-Kritisverordnung erreichen. Gleiches gilt für Einrichtungen und Unternehmen, die zu KRITIS-Sektoren gehören, die nicht von der BSI-Kritisverordnung erfasst sind.

Da die Zuständigkeit für die verschiedenen KRITIS-Sektoren wie Energie, Transport und Verkehr oder Gesundheit dem Ressortprinzip folgend bei verschiedenen Ministerien liegt, wurde im Innenministerium bereits vor mehreren Jahren eine Koordinierungsstelle Kritische Infrastruktur (KoSt KRITIS) eingerichtet, welche als Informationsdrehscheibe die Fäden aus den einzelnen Ressorts zusammenführt und beispielsweise auch mit dem Bund und den anderen Ländern vernetzt ist. Übergeordnetes Ziel aller Aktivitäten ist der Schutz und die Resilienz Kritischer Infrastrukturen. Im Sinne des dabei verfolgten „All-Gefahren-Ansatzes" ist der Schutz Kritischer Infrastrukturen vor Cyberbedrohungen ein Baustein von mehreren, dem jedoch aufgrund seines Querschnittscharakters – wachsende IT-Durchdringungen bei den Kritischen Infrastrukturen nahezu aller Sektoren – eine besondere Bedeutung zukommt.

Die CSBW wird daher gegenüber dem BSI im Sinne von § 8b BSI-Gesetz als zentrale Kontaktstelle des Landes für alle KRITIS-Sektoren fungieren und Meldungen des BSI im Kontext Kritischer Infrastrukturen entgegennehmen, gegebenenfalls für Menschen mit wenig IT-Fachkenntnissen aufbereiten und an die KoSt KRITIS sowie die jeweils fachlich betroffenen Ressorts und Stellen weitersteuern.

Die Verantwortung für den Schutz Kritischer Infrastrukturen liegt in erster Linie bei den Betreibern selbst. Da aber nur ein vernetztes und gemeinsames Handeln die Cyberkriminalität eindämmen kann, beteiligt sich auch das LKA BW auf Bundesebene und länderübergreifend durch Kooperationen mit anderen Behörden, der Wirtschaft sowie der Wissenschaft und Forschung, um die polizeiliche Gefahrenabwehr (siehe dazu oben **3.1 Staatliche Handlungsfähigkeit und Stärkung der Gefahrenabwehrbehörden)** und die Strafverfolgung (siehe dazu oben **3.2 Stärkung der Strafverfolgungsbehörden**) im Land auf höchstem Niveau sicherzustellen.

Gleichzeitig warnt und sensibilisiert das Landesamt für Verfassungsschutz potenziell betroffene Stellen bzw. Unternehmen im Bereich der Kritischen Infrastruktur bereits im Vorfeld vor möglichen physischen wie digitalen Angriffen. Die Arbeitsbereiche Cyberabwehr und Wirtschaftsschutz betreuen diesbezüglich insbesondere die sich im Geheimschutz befindlichen Unternehmen und Institutionen bzw. Forschungsinstitute aus dem KRITIS-Bereich. Diese werden regelmäßig vor Ort aufgesucht und auf vertraulicher Basis über Gefahren und Risiken der Spionage informiert und sensibilisiert.

Ergänzend hat das Innenministerium mit der EnBW Energie Baden-Württemberg AG eine Kooperationsvereinbarung zur Stärkung der Cybersicherheit im Land abgeschlossen. Die EnBW verfügt als bedeutender Betreiber Kritischer Infrastrukturen über eine herausragende Expertise in diesem Bereich. Durch die Kooperationsvereinbarung soll die Zusammenarbeit intensiviert und damit eine effektivere Bekämpfung der Cyberkriminalität und der Schutz systemkritischer Infrastrukturen, wie z. B. Energie- und Wasserversorger, gestärkt werden.

Zur operativen Umsetzung der Kooperation wurden vier Handlungsfelder festgelegt, die im Rahmen einer turnusmäßigen Jahresplanung mit Maßnahmen hinterlegt werden und das Arbeitsprogramm der Kooperation bilden: Dazu gehört ein Informationsaustausch im Rahmen eines zweimonatigen Jour fixe mit LKA BW, Innenministerium und EnBW, gemeinsame Veranstaltungen zur Awareness und Übungen, die Ausbildung von Cybersicherheitsexpertinnen und -experten durch einen Studiengang an der Dualen Hochschule Baden-Württemberg (DHBW) am Standort Heilbronn sowie die Zusammenarbeit in Notfällen.

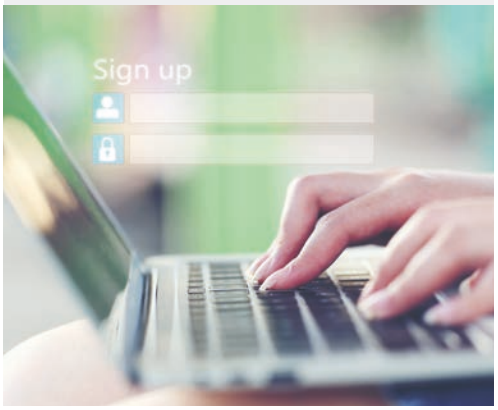
Kooperationsvereinbarungen (dazu mehr bei **9. Nationale und internationale Kooperationen**) dieser Art stellen einen wichtigen Baustein der Cybersicherheitsstrategie dar.

5.

DIGITALE KOMPETENZEN

Zum besseren Umgang mit Cybersicherheitsrisiken ist es erforderlich, dass die handelnden Personen über angemessene digitale Kompetenzen verfügen. Die deutliche Zunahme von Sicherheitsvorfällen im Land hat die Dringlichkeit bei der Umsetzung von Präventionsmaßnahmen gesteigert. Klassische Schulungsangebote wie etwa Präsenzschulungen erreichen jedoch nur wenige Menschen gleichzeitig bei relativ hohem Aufwand für die Lehrenden. Wir müssen somit alternative Lehrformen und Lernkonzepte unterstützen, die besser skalieren. Als Lehrformen sind beispielsweise Lernvideos, Web-Based-Trainings und weitere E-Learning-Angebote geeignet. Der Einsatz von Lernplattformen, mit denen die Organisation, die Durchführung und der Abschluss solcher Lehrangebote effizient durchgeführt werden können, muss aufgebaut und gefördert werden. Wir wollen die auf den Lernplattformen verfügbaren, skalierbaren Lernangebote für eine sowohl möglichst breite als auch große Zielgruppe unkompliziert zur Verfügung stellen. In diesem Zusammenhang wollen wir Projekte fördern, die dazu beitragen, dass wir neue und bessere Lehr- und Lernkonzepte erhalten, mit denen wir die nötigen digitalen Kompetenzen vermitteln können. Ergebnisse sollen neue innovative Ansätze sein und auch konkrete Schulungsmaterialien – insbesondere der CSBW –, die einer bestimmten Zielgruppe, z. B. Kommunen, bei der Prävention von Cybersicherheitsvorfällen konkret und praktisch helfen.

„Der kontinuierliche Anstieg von Cyberkriminalität erfordert von Nutzerinnen und Nutzern immer mehr Bewusstsein und Wissen über effektive Schutzmaßnahmen wie Antivirensoftware, Passworthygiene und Multi-Faktor-Authentifizierung."
Initiative D21, Digital Skills GAP, 2021.



5.1 Schulen

Um die digitalen Kompetenzen zur Reduzierung von Cybersicherheitsrisiken frühzeitig zu vermitteln, müssen wir bereits bei der Ausbildung junger Menschen ansetzen. Eine umfangreiche und detailliert belegbare Überprüfung der Bildungspläne 2016 auf Übereinstimmung mit dem Kompetenzrahmen der Kultusministerkonferenz(KMK)-Strategie „Bildung in der digitalen Welt" hat hierzu u. a. ergeben, dass in den Bildungsplänen in Übereinstimmung mit dieser KMK-Strategie verschiedene Aspekte der Themen Informations- und Cybersicherheit sowie Datenschutz bereits vielfach verankert sind.

Anschlussmöglichkeiten für weitere Maßnahmen ergeben sich für die allgemein bildenden Schulen durch die verpflichtend umzusetzende Leitperspektive Medienbildung und deren Konkretisierungen vor allem in den Bereichen Jugendmedienschutz, informationelle Selbstbestimmung und Datenschutz, für die beruflichen Schulen durch die Leitziele „Digitale Medien als Lernwerkzeuge nachhaltig einsetzen" und „Auf das Leben in einer sich dynamisch wandelnden, pluralistischen und demokratisch verfassten Gesellschaft vorbereiten".

Auch sind in der Lehrkräftebildung aller Lehrämter die **Themen Informations- und Cybersicherheit sowie Datenschutz** in der 2. Phase verankert. Verschiedene Maßnahmen **im Bereich der Aus- und Fortbildung der Lehrkräfte** werden durch das Zentrum für Schulqualität und Lehrerbildung Baden-Württemberg (ZSL) angeboten. Aus fachlicher Sicht sollen künftig die bestehenden Fortbildungsmaßnahmen **weiterentwickelt und die Angebote intensiviert werden.**

An die Lehrkräfte werden in gleich drei Bereichen hohe Anforderungen gestellt: Erstens ist eine fachliche Expertise in dem Bereich Cybersicherheit notwendig, um die Lehrinhalte überzeugend zu vermitteln. Zweitens dient das didaktische Wissen dem Aufbereiten und der Darstellung von sachgerechten und verständlichen Lehrinhalten. Drittens ist das technische Wissen für die Erstellung von Lehrmaterialien erforderlich. Das Kultusministerium wird darauf achten, in all diesen drei Kompetenzbereichen bestehende Fachkräfte aufzubauen, zu fördern und auch aus anderen Bereichen für das Thema Cybersicherheit zu gewinnen. Regelmäßige Schulungen der Lehrkräfte und die Erstellung definierter Schulungsprozesse werden hierfür vorausgesetzt, wofür die CSBW hier einen wesentlichen Beitrag leisten wird.

5.2 Hochschulen

An den Hochschulen findet das Thema Cybersicherheit in den Curricula von Informatikstudiengängen, aber auch als Teil von Vertiefungslinien von Studiengängen anderer Disziplinen zunehmend Berücksichtigung. Darüber hinaus werden mit Blick auf den Fachkräftebedarf im Rahmen der Hochschulfinanzierungsvereinbarung 2021 - 2025 insgesamt 150 zusätzliche Studienanfängerplätze im Bereich IT/Digitalisierung eingerichtet.

Zum Schutz ihrer eigenen Sicherheit und der bei ihnen liegenden sensiblen Daten haben die Hochschulen untereinander ein Kompetenznetzwerk geknüpft, das neben Sensibilisierung, Schulungen und Prävention auch eine schnelle Reaktionsfähigkeit bei Cyberangriffen garantiert. Die bereits bestehende Kooperation der Hochschulen mit der CSBW wird weiter vertieft werden.

5.3 Weiterbildung

Bestehende Angebote zur Weiterbildung hinsichtlich digitaler Kompetenzen, die die Cybersicherheit im Land stärken, müssen wir besser bekannt machen und bestehende Anbieter dazu zunehmend vernetzen. Hierzu ist es notwendig, dass wir zentrale Plattformen schaffen und fördern, in denen zielgruppenspezifisch über Weiterbildungsangebote informiert wird. Ein erfolgreiches, bestehendes Beispiel, das jedoch über das Thema Cybersicherheit hinausgeht, ist die Weiterbildungsplattform **www.fortbildung-bw.de** des Wirtschaftsministeriums. Wir werden über dieses **Weiterbildungsportal die Informationen und die Transparenz zu den vielfältigen, derzeit über 100 Qualifizierungsangeboten im Themenfeld Cybersicherheit weiter verbessern.** Überdies soll die **Anzahl der Bediensteten in der Landesverwaltung, die an mindestens einer Schulung zur Cybersicherheit teilgenommen haben, auf 15.000 jährlich steigen.** Dazu zählen auch die Teilnahme an entsprechenden E-Learning-Angeboten. Zudem hat im Februar 2021 die Landesregierung eine ressortübergreifende Weiterbildungsoffensive WEITER.mit.BILDUNG@BW unter der Koordination des Staatsministeriums auf den Weg gebracht. Wirtschafts-, Kultus- und Wissenschaftsministerium tragen unter einem gemeinsamen Dach die berufsbezogene Weiterbildung im Land zusammen mit den Weiterbildungspartnern vor Ort in die Fläche und stärken die Weiterbildungseinrichtungen beim Ausbau der Digitalisierung.

6.

AWARENESS UND VERBRAUCHERSCHUTZ

Um Cybersicherheitsrisiken rechtzeitig zu erkennen sowie früh und angemessen darauf zu reagieren, wollen wir nicht nur die digitalen Kompetenzen, sondern auch das Bewusstsein (Awareness) von Cyberrisiken erhöhen. Präventionsmaßnahmen, die zum Thema Cybersicherheit sensibilisieren und schulen, leisten einen entscheidenden Beitrag hierfür. Wir wollen regelmäßig Möglichkeiten zur Verringerung der Cybersicherheitsrisiken den handelnden Personen als Mitarbeiterinnen und Mitarbeiter in der Landesverwaltung, den Kommunen, der Wirtschaft und der Wissenschaft sowie als Verbraucherinnen und als Verbraucher aufzeigen. Dabei werden wir uns auf die Gruppen fokussieren, bei denen bislang die Schutzmaßnahmen weniger verwendet werden. Dazu werden wir die **Bevölkerung – insbesondere Verbraucherinnen und Verbraucher sowie Beschäftigte – und Unternehmen über die Gefahren im Cyberraum mit Hilfe konkreter Sensibilisierungsmaßnahmen informieren, um sie vor Schäden zu schützen.**

Überdies wird die 2021 errichtete CSBW beim Angebot von Sensibilisierungsveranstaltungen für Bürgerinnen und Bürger die Zusammenarbeit mit Kommunalen Landesverbänden, Komm.ONE, Polizei, Verbraucherzentralen, Volkshochschulen sowie der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit intensivieren.

„63 Prozent der Onlinerinnen und Onliner insgesamt nutzen für unterschiedliche Dienste auch unterschiedliche Passwörter. Dabei gibt es große Unterschiede zwischen denjenigen, die einen Schreibtisch- bzw. **Bürojob** haben **(drei von vier)** und denjenigen, die keinen Bürojob haben (nur etwa die Hälfte). Auch zwischen den Geschlechtern gibt es Unterschiede: Während rund **zwei von drei Männern** angeben, verschiedene Passwörter zu nutzen, sind es bei den **Frauen mit 57 Prozent** etwas weniger."
„Je nach formalen Bildungsabschluss unterscheidet sich die Kompetenz, für unterschiedliche Dienste auch unterschiedliche Passwörter zu nutzen deutlich.
Unter denjenigen, die eine **geringe formale Bildung** haben, stimmt **weniger als die Hälfte** zu, dies zu tun. Bei denjenigen mit **hoher Bildung** hingegen geben **drei von vier** Onlinerinnen und Onliner an, unterschiedliche Passwörter zu nutzen."
Initiative D21, Digital Skills GAP, 2021.

7.

FACHKRÄFTE

Für den Umgang mit Cybersicherheitsrisiken werden zunehmend hochqualifizierte Fachkräfte in Verwaltung, Wirtschaft und Wissenschaft benötigt. Wir werden zielgruppenorientierte Personalgewinnungs- und Entwicklungskonzepte etablieren, landesweit aufeinander abstimmen und umsetzen. Als Basis dient die Förderung der digitalen Kompetenzen (siehe oben **5. Digitale Kompetenzen**). Für den Wissenschaftsbereich werden Möglichkeiten der Aus- und Fortbildung als Teil der Innovativen Forschung und Entwicklung näher erörtert (siehe nachfolgend **8. Innovative Forschung und Entwicklung**). Durch die Entwicklung von Personal im Kreislauf von Wissenschaft, Start-Ups, Unternehmen und Verwaltung wird das Innovationspotential gefördert. Verbesserte staatliche Anreize könnten die Gewinnung von Fachkräften im öffentlichen Dienst zusätzlich vereinfachen.

Als Maßnahmen zur Nachwuchskräftegewinnung kooperieren die CSBW und das LKA BW mit der DHBW am Standort Heilbronn und beide werden **jährlich jeweils mindestens zwei berufsbegleitende Studienplätze** ermöglichen.

Überdies werden **jährlich 60 ausgebildete Fachkräfte** in der Landesverwaltung im IT-Grundschutz des BSI bzw. in vertiefenden Cybersicherheitsthemen fortgebildet, um das Cybersicherheitsniveau zu erhöhen. Zur Gewährleistung der Informationssicherheit liefert die Fortbildung ein fachlich solides Fundament sowie ein umfangreiches Arbeitswerkzeug.

Zentral beim **IT-Grundschutz des BSI** ist ein ganzheitlicher Ansatz zur Informationssicherheit: Neben technischen Aspekten werden auch infrastrukturelle, organisatorische und personelle Themen betrachtet.
Dies ermöglicht ein systematisches Vorgehen, um notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen.

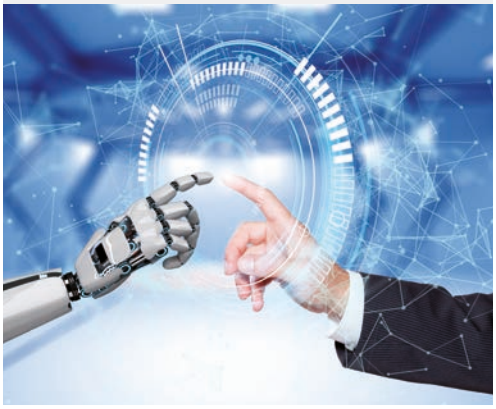
8.

INNOVATIVE FORSCHUNG UND ENTWICKLUNG

Damit wir bei der Abwehr von Cyberbedrohungen auf dem möglichst neuesten Stand sind, fördern wir die innovative Forschung und Entwicklung im Land. Gleichzeitig wird der Wirtschaftsstandort Baden-Württemberg durch innovative, sichere Produkte sowie Dienstleistungen gestärkt. Die baden-württembergische Forschung und Entwicklung im Bereich Cybersicherheit hat hier ein erhebliches Innovations- und Wertschöpfungspotenzial.

Um relevante Erkenntnisse zur Cybersicherheit zu erlangen, streben wir eine stärkere Nachwuchsförderung an Hochschulen, Universitäten und Forschungseinrichtungen sowie für Start-ups, etablierte Unternehmen und forschende öffentliche Einrichtungen an. Ziel ist, **die anwendungsorientierte Forschung und Entwicklung in diesem Bereich an den Hochschulen und außeruniversitären Forschungsinstituten in Baden-Württemberg sowie den wechselseitigen Wissens- und Technologietransfer zwischen Wissenschaft und Wirtschaft zu fördern.**

„In Anbetracht der zunehmenden und sich stetig verändernden Cyberrisiken besteht ein hoher Bedarf, diesen Risiken mit innovativen Cybersicherheitslösungen zu begegnen. Innovationen in der Cybersicherheit ermöglichen sowohl die Erhöhung des Schutzniveaus als auch eine Ausweitung von Wertschöpfungspotenzialen."
Expertenkommission Forschung und Innovation (EFI), Gutachten, 2020.



8.1
Stärkung der Spitzenforschung und Ausbildung des Nachwuchses

In dem dynamischen Feld der digitalen Technologien wachsen die Anforderungen an sichere Anwendungen kontinuierlich. Es ist deshalb unerlässlich, die entsprechenden Forschungskapazitäten aufzubauen und damit Grundlagen und Methoden auf aktuellstem Stand zu entwickeln. Ein international anerkanntes Zentrum für Informationssicherheit ist KASTEL am KIT (Institut für Informationssicherheit und Verlässlichkeit). KASTEL steht nicht nur für exzellente Forschung, sondern bildet auch wissenschaftlichen Nachwuchs für Wissenschaft und Wirtschaft auf höchstem Niveau aus. Außerdem können Studierende studiengangsübergreifend das KASTEL-Zertifikat im Cybersicherheitsbereich erwerben. Das Zertifikat ist eine mit einem spezialisierten Master vergleichbare Qualifikation. Darüber hinaus ermöglicht das Wissenschaftsministerium im Rahmen der Landesgraduiertenförderung Unterstützung bei Promotionsvorhaben. Das Margarete-von-Wrangell-Programm unterstützt qualifizierte Wissenschaftlerinnen, sich für die Berufung auf eine Professur zum Beispiel auch im Bereich Cybersicherheit zu qualifizieren.

Das **KASTEL** – Institut für Informationssicherheit und Verlässlichkeit ist aus dem Kompetenzzentrum für Angewandte Sicherheitstechnologie hervorgegangen und ist seither Teil der KASTEL Security Research Labs. Das Institut repräsentiert die Forschung und Lehre im Bereich der Informationssicherheit und Verlässlichkeit am Karlsruher Institut für Technologie (KIT).

8.2
Stärkung der Forschungsverbünde

Die Cybersicherheitsforschung am Hochtechnologiestandort Baden-Württemberg ist weiter voranzutreiben. Auch im Bereich der Cybersicherheitsforschung gilt, dass wissenschaftliche Exzellenz wiederum talentierte Köpfe aus aller Welt anzieht und damit insbesondere für den Nachwuchs eine inspirierende Umgebung geschaffen wird. Bestehende Forschungsverbünde oder Schwerpunkte mit großer Ausstrahlungskraft wie zum Beispiel das Kompetenzzentrum KASTEL am KIT spielen von daher eine zentrale Rolle; die Kooperation mit geeigneten Forschungspartnern ist dabei wichtig, um die eigenen Kompetenzen zu ergänzen und zusätzliche Themenfelder zu erschließen.

8.3 Förderung der anwendungsorientierten, wirtschaftsnahen Forschung und Entwicklung sowie des wechselseitigen Wissens- und Technologietransfers zwischen Wissenschaft und Wirtschaft

Neben der universitären Forschung ist zentrales Anliegen von Wirtschaftsministerium und Wissenschaftsministerium die anwendungsorientierte, wirtschaftsnahe Forschung sowie den Technologie- und Wissenstransfer aus der Forschung in die Wirtschaft zu fördern, um damit Unternehmen bei der Entwicklung cybersicherer Hard- und Softwarelösungen zu unterstützen. Auf diese Weise leisten wir einen Beitrag dazu, Innovations- und Wertschöpfungspotenziale im Bereich Cybersicherheit zu heben: So wurde am FZI Forschungszentrum Informatik ein IT-Sicherheitskompetenzzentrum aufgebaut, welches als Anlaufstelle zur anwendungsorientierten IT-Sicherheitsforschung für den Mittelstand dient. Ein weiteres Beispiel sind die vom Wirtschaftsministerium geförderten Forschungs- und Transferprojekte „CyberProtect“ und „RoboShield“: Darin wurde die Entwicklung und Anwendung innovativer Sicherheitstechnologien speziell für die Produktion gefördert, durch deren Einsatz Unternehmen den Herausforderungen einer zunehmend vernetzten Wertschöpfungskette besser begegnen können. Seit dem Abschluss der Projekte führen die beteiligten Forschungsinstitute ihre Aktivitäten u. a. in Form von Test-, Schulungs- und Beratungsangeboten für Unternehmen fort. Mit ihren Aktivitäten stärkt die Allianz Industrie 4.0 Baden-Württemberg die Sensibilisierung und Wissensvermittlung zur Cybersicherheit im Kontext von digital vernetzten Wertschöpfungsketten in der Industrie.

Mit dem Aufbau der neuen Institute für Quantentechnologien und für KI-Sicherheit des Deutschen Zentrums für Luft- und Raumfahrt (DLR) leistet der Standort Ulm als Innovationszentrum der DLR-Quantencomputing-initiative einen zentralen Beitrag dazu, innovative Anwendungen mit quantenbasierten Hard- und Softwarelösungen in Baden-Württemberg und Deutschland voranzutreiben. Dies schließt die anwendungsorientierte Erforschung und Entwicklung von KI in praxisrelevanten Anwendungen mit hohen Sicherheitsanforderungen ein.

Anknüpfend an diese Beispiele ist Ziel, auch künftig die **anwendungsorientierte, wirtschaftsnahe Forschung und Entwicklung sowie den Wissens- und Technologietransfer zwischen Wissenschaft und Wirtschaft zu fördern.**

8.4
Schnelle Entwicklung durch Start-ups

Cybersicherheit und Datenschutz sind als Qualitätsmerkmal und Wettbewerbsvorteil bei Produkten und Dienstleistungen „made in Baden-Württemberg" noch stärker zu etablieren. Dies trägt dazu bei, dass Produkte und Dienstleistungen von Start-ups eine schnelle Marktreife erlangen. Erkenntnisse, wie beispielweise innerhalb der KI-Forschung sowie der Forschung an kryptografischen Verfahren (z. B. Quantentechnologie), tragen letztendlich zur Stärkung des Wirtschaftsstandorts Baden-Württemberg bei. KASTEL oder der Start-up BW Accelerator CyberLab HighTech BW des Cyberforum e.V. bieten hierzu fachliche Beratungen an. Das CyberLab unterstützt beispielsweise die Unternehmensentwicklung von Start-ups aus der IT- und Hightech-Branche. Innerhalb von sechs bis acht Wochen werden die jungen Unternehmen mit Modulen, Sprechstunden, Vorträgen und Workshops auf den Markteintritt vorbereitet.

Zusätzlich erhalten Gründungsinteressierte sowie Start-ups und forschungsbasierte Spin-offs durch verschiedene Beratungs- und Förderprogramme, die unter anderem unter dem Dach der Landeskampagne Startup BW firmieren, eine individuelle Unterstützung sowie einen Zugang zu den relevanten Unternehmenssnetzwerken. Vor allem in dem Bereich der KI treffen baden-württembergische Start-ups u. a. im Innovationscampus „Cyber Valley" auf einen ausgezeichneten Nährboden. Hierbei kann die fachliche Betreuung dazu verhelfen, dass die jungen Unternehmen von Beginn an relevante Erkenntnisse in der Cybersicherheitsforschung und -entwicklung erlangen und schließlich maktfähige Produkte entwickeln können.

Damit wir die baden-württembergischen Innovations-und Wertschöpfungspotenziale mit und durch Cybersicherheit langfristig festigen können, plant das Wirtschaftsministerium **mindestens einen Start-up-BW-Accelerator, in dem das Thema Cybersicherheit behandelt wird, zu fördern.**

9.

NATIONALE UND INTERNATIONALE KOOPERATIONEN

9.1 Ziel: Synergien für mehr Cybersicherheit nutzen

Um Synergien für mehr Cybersicherheit durch nationale und internationale Kooperationen zu nutzen, arbeiten wir mit zahlreichen Partnern zusammen, die sich ebenfalls mit dem Thema Cybersicherheit beschäftigen. Es liegt in der Natur der Sache, dass der Cyberraum nicht an nationalen oder internationalen Grenzen haltmacht. Die Vernetzung der beteiligten Akteure muss demnach grenzüberschreitend sein. Es besteht die Notwendigkeit zum effektiven und effizienten Austausch zur Prävention und Bewältigung von Herausforderungen im Bereich der Cybersicherheit – der Länder untereinander, zwischen Baden-Württemberg und dem Bund genauso wie zwischen Baden-Württemberg und internationalen Partnern. Über die aktive Mitarbeit in Gremien und über den Abschluss bi- oder multilateraler Kooperationsvereinbarungen werden wir die Cybersicherheit in Baden-Württemberg ganzheitlich und verbindlich weiter gestalten.

9.2 Sachstand

Die nachfolgend dargestellten Vereinbarungen sind wichtige Bausteine, um dieses Ziel zu erreichen. Sie benennen die Kooperationsfelder zwischen dem Innenministerium oder dessen nachgeordnetem Bereich für die Thematik Cyber- und Informationssicherheit und geben der Zusammenarbeit einen verbindlichen Rahmen. Der kooperative Ansatz umfasst unter anderem den Austausch mit Akteuren aus Verwaltung, der Wissenschaft und der Wirtschaft, um Perspektiven unterschiedlicher Fachdisziplinen in die Arbeit einfließen zu lassen und gemeinsam an innovativen Lösungskonzepten zu arbeiten.

9.2.1
Internationale Kooperationen

Neben mehreren Kontakten auf internationaler Ebene wurde mit dem im Februar 2021 geschlossenen Memorandum of Understanding zwischen dem Israel National Cyber Directorate (INCD) und dem Innenministerium die Partnerschaft zwischen Israel und Baden-Württemberg auf ein neues Fundament gestellt. Beide Partner wollen künftig noch enger in folgenden Bereichen zusammenarbeiten:

- Informationsaustausch zu Cybersicherheit, Lagebildern und Maßnahmen zur Abwehr von Cyberangriffen,
- Erfahrungsaustausch und Austausch von Informationen zur Förderung der Widerstandsfähigkeit und Erhöhung der digitalen Souveränität,
- Austausch von Informationen über „best practices“,
- Vernetzung von nationalen und internationalen Cyberpartnern,
- Expertentreffen und Hospitationen sowie
- gegenseitige Besuche und gemeinsame Veranstaltungen.

9.2.2
Bund

Mit der **Eröffnung des Verbindungsbüros** in Stuttgart im Frühjahr 2019 wurde eine Vereinbarung umgesetzt, die das BSI und das Land Baden-Württemberg im Rahmen der im Oktober 2018 unterzeichneten Absichtserklärung zur engeren Zusammenarbeit in Fragen der Cybersicherheit getroffen hatten. Das Verbindungsbüro Süd ist sowohl für Baden-Württemberg als auch Bayern zuständig.

Um einem einheitlich hohen IT-Sicherheitsniveau für alle Akteure näherzukommen, wollen wir zeitnah eine weitergehende Kooperationsvereinbarung mit dem BSI unterzeichnen. Dazu wird die Zusammenarbeit in den Bereichen Informationsaustausch, Sensibilisierung und Fortbildung ausgebaut sowie die gegenseitige Unterstützung bei der Umsetzung von Cybersicherheitsmaßnahmen intensiviert. Ebenfalls findet ein Austausch zum Einsatz von Systemen und Lösungen zur Erhöhung und Sicherung der Cybersicherheit statt. Bereits heute arbeitet das Land Baden-Württemberg in verschiedenen Gremien vertrauensvoll mit der zentralen Meldestelle für IT-Sicherheit innerhalb der Bundesverwaltung zusammen. Mit der Kooperationsvereinbarung werden wir dies auf ein neues und nachhaltiges Fundament stellen.

9.2.3 Hessen

Die Länder Hessen und Baden-Württemberg stehen gemeinsam vor der Herausforderung, die zunehmende Verlagerung des öffentlichen Lebens in den Cyberraum sicher zu gestalten und die Risiken zu minimieren, ohne die damit einhergehenden Chancen einzuschränken. Durch die Einrichtung des Hessen CyberCompetenceCenter (Hessen3C) und die Errichtung der CSBW haben beide Länder bereits wegweisende und innovative Strukturen für eine Stärkung und Optimierung der Cybersicherheit geschaffen.

Aufbauend auf diesen Strukturen hat eine Kooperationsvereinbarung die Grundlage für eine länderübergreifende Zusammenarbeit geschaffen. Der hieraus folgende Austausch der Cybersicherheitsakteure aus Baden-Württemberg und Hessen ist die Basis für weitere Schritte, welche die professionellen Strukturen der Cybersicherheitsarchitektur in beiden Ländern weiter verbessern werden. Ziel der Vereinbarung ist es, Synergien nutzbar zu machen und Kräfte zu bündeln.

Die folgenden Kooperationsfelder bilden die Grundlage für zukünftige gemeinsame Aktivitäten der Länder Hessen und Baden-Württemberg:

- Intensivierung des Erkenntnis- und Wissenstransfers bei länderübergreifenden Cyberlagen,
- Stärkung der Aus- und Fortbildung von Cybersicherheitsexperten sowie
- Beratung und Unterstützung bei strategischen Fragestellungen und operativen Anforderungen.

9.2.4 Kooperation mit EnBW

Da die Cyberkriminalität zunehmend professioneller und internationaler wird, wachsen die Aufgaben der Stellen, die mit der Abwehr und der Ermittlung von Cyberkriminalität befasst sind. Aus diesem Grund ist das Innenministerium eine Public-Private-Non-Profit-Partnership (PPNPP) mit dem Unternehmen EnBW eingegangen. Ziel der Initiative ist die Verbesserung der Cybersicherheit für Städte, Gemeinden, Landkreise, Wirtschaft und Gesellschaft sowie Stadtwerke und das Gesundheitswesen in Baden-Württemberg.

Der Kooperationsvertrag zielt neben der Schaffung eines Bewusstseins um die Gefahren von Cyberkriminalität vor allem auf gemeinsame Präventionsmaßnahmen, Wissenstransfer, Vernetzung von Expertinnen und Experten und eine standardisierte Aus- und Weiterbildung. Darüber hinaus soll ein Lagebild „Cybersicherheit Kritische Infrastrukturen“ für Baden-Württemberg erstellt werden.

9.2.5
Kooperationen innerhalb der Verwaltung in Baden-Württemberg

Auch innerhalb der Landesregierung nutzen wir bereits geschaffenes Know-How im Bereich Cybersicherheit. Je digitaler unser Leben, unsere Arbeit und die Welt um uns herum werden, desto mehr Angriffsstellen gibt es für Cyberkriminelle – auch in der Landesverwaltung. Daher haben wir Cybersicherheit als eines der grundlegenden Querschnittsthemen der Digitalisierungsstrategie digital@bw definiert. Zahlreiche Aspekte der Cybersicherheit betreffen alle Ressorts. Die Start-Up-Förderung im IT-Sicherheitsbereich ist für das Innenministerium, das Wirtschaftsministerium und gegebenenfalls auch für das Wissenschaftsministerium relevant. Alle drei Ministerien identifizieren herausragende Querschnittsbereiche und – wo immer sinnvoll und notwendig – arbeiten wir in den Ressorts noch enger zusammen.

Auch bei Angeboten für breite Zielgruppen wie etwa Sensibilisierungsthemen und Informationsangebote ist eine Kooperation innerhalb der Landesverwaltung und mit den Kommunen besonders relevant, insbesondere, wenn Verwaltung, Kommunen, Wirtschaft sowie Bürgerinnen und Bürger betroffen sind. Um Doppelstrukturen zu vermeiden, ist es angezeigt, im Rahmen von Kooperationsvereinbarungen festzulegen, welche Informations- und Schulungsangebote wie geteilt und über weitere Kanäle verbreitet werden können. Dabei ist auch über Ländergrenzen hinweg ein Austausch sinnvoll, wie z. B. bei einer Zusammenarbeit mit dem BSI zu Schulungs- und Sensibilisierungsthemen der Cybersicherheit.

9.3
Geplante Maßnahmen mit Leistungskennzahlen

Das Netzwerk an Partnern soll durch **neue Kooperationsvereinbarungen** erweitert und bestehende Kontakte sollen vertieft werden. Die getroffenen Vereinbarungen sollen während ihrer Laufzeit **überprüft und gegebenenfalls an neue Rahmenbedingungen angepasst** werden. Zu diesem Zweck werden sich die Kooperationspartner von Zeit zu Zeit über die Aktualität und dabei insbesondere über die Aufnahme weiterer Kooperationsfelder im Wege einer Änderung der Vereinbarungen austauschen. Die konkrete Ausgestaltung der Kooperationsfelder wird regelmäßig zwischen den Partnern abgestimmt. Außerdem wollen wir erreichen, dass die CSBW **jährlich mindestens 50 Lagebilder mit diesen Partnern austauscht.** Darüber hinaus nehmen wir uns vor, pro Jahr **mindestens drei Hospitationen von Beschäftigten der Landesverwaltung bei Kooperationspartnern und umgekehrt zu ermöglichen.**

10.

ZUSAMMENFASSUNG DER ZIELE

Um die Erreichung der Ziele und den Erfolg der Strategie sicherzustellen, sind die meisten Ziele SMART (spezifisch, messbar, akzeptiert, realistisch, terminiert) formuliert worden. Wir wollen als Landesregierung die Ziele innerhalb der nächsten fünf Jahre umsetzen.

Dabei wird die Realisierung finanzwirksamer Maßnahmen der Cybersicherheitsstrategie im Rahmen einer nachhaltigen und vorausschauenden Finanzpolitik erfolgen. Eine solche Finanzpolitik erfordert einen verantwortungsgerechten Umgang mit den finanziellen Ressourcen. Im Hinblick auf die im Grundgesetz und in der Landesverfassung verankerte Schuldenbremse und die Priorisierungen durch den Haushaltsgesetzgeber kann es zu Verzögerungen bzw. zu Abweichungen kommen, weil alle zusätzlichen finanzwirksamen Maßnahmen unter Haushaltsvorbehalt stehen. Für neue Maßnahmen wird daher zunächst Spielraum durch Umschichtung im Rahmen vorhandener Mittel / Stellen zu schaffen sein. Es ist außerdem Sache des jeweils zuständigen Ressorts, zu prüfen, ob die jeweilige Maßnahme – soweit Kommunen berührt sind – Konnexität auslöst, und bei Bedarf die entsprechenden Folgerungen zu ziehen. Final bleibt die Bereitstellung von Ressourcen dem Haushaltsgesetzgeber vorbehalten und wird in den jeweiligen Haushaltsaufstellungsverfahren entschieden. Im Rahmen dieser Möglichkeiten werden wir uns auch weiterhin für eine Digitalisierung einsetzen, die die Menschen in den Mittelpunkt stellt und sicher ist.

10.1
Vernetzung der Cybersicherheitsakteure

Zur Verbesserung des Informationsstands und der Reaktionsfähigkeit der mit Cybersicherheit betrauten Akteure, Behörden und Gremien strebt das Innenministerium im Schulterschluss mit den Ministerien eine Intensivierung der Vernetzung der Cybersicherheitsakteure an. Dies soll mit Hilfe des **Aufbaus von erweiterten Kommunikationskanälen** durch die Cybersicherheitsagentur Baden-Württemberg (CSBW) und **Vernetzungsveranstaltungen des Landes mit jährlich über 500 Teilnehmenden** erfolgen.

10.2
Staatliche Verwaltung und Kommunen

Um die Gefahren durch Cyberangriffe und deren Auswirkungen auf die staatliche Verwaltung und die Kommunen zu reduzieren, werden wir

- den Dienststellen und Einrichtungen der Landesverwaltung die **Dokumentation von Sicherheitskonzepten für Systeme und Anwendungen in einer zentralen Dokumentationssoftware,** bei der jedes Ressort ausschließlich auf seine ISMS-Inhalte zugreifen kann, ermöglichen,
- die **Analyse- und Reaktionsfähigkeit vor Ort stärken**, indem jährlich mindestens sechs Untersuchungen mit Schwachstellenscans durch die CSBW für öffentliche Stellen mit anschließender Beratung und Maßnahmenplanung angeboten werden,
- die **gemeinsame Abwehr von IT-Angriffen** fördern, indem die CSBW eine Plattform aufbaut, auf der ein Austausch von Indicators of Compromise stattfinden kann,
- das **IT-Notfallmanagement** durch die Erstellung von Notfallkonzepten für alle zentralen, landesweiten Systeme und Fachverfahren stärken,
- die **rechtlichen Rahmenbedingungen** durch eine mit dem AK-IT abgestimmte, und im Einvernehmen mit dem IT-Rat Baden-Württemberg vom Innenministerium erlassene Rechtsverordnung konkretisieren und nach der Evaluation des Cybersicherheitsgesetzes ggf. anpassen sowie
- prüfen, inwieweit der Grundsatz **Security by Design** und der Einsatz von Produkten mit **Sicherheitsgütesiegeln** stärker im Rahmen der Beschaffung und der IT-Vorhaben berücksichtigt werden kann.

10.3 Gefahrenabwehr- und Strafverfolgungsbehörden

10.3.1 Staatliche Handlungsfähigkeit und Stärkung der Gefahrenabwehrbehörden

Gegen Angriffe im Netz haben wir uns mit der CSBW noch besser gerüstet. Im Hinblick auf diese vielfältigen Aufgaben und die jährlich ansteigende Anzahl der Cybersicherheitsbedrohungen ist eine angemessene Stellenausstattung der CSBW unerlässlich. Aus Sicht der Parteien der Regierungskoalition und des Innenministeriums ist angezeigt, diese weiter mit **neuen Beschäftigten** personell zu stärken.

10.3.2 Stärkung der Strafverfolgungsbehörden

Zur Verbesserung der Cybersicherheit tragen die Strafverfolgungsbehörden vor allem über die bei der Aufklärung von Angriffsmodalitäten in Ermittlungsverfahren gewonnenen Erkenntnisse und die Abschreckungswirkung von drohenden Sanktionen bei. Aus diesem Grund wollen die Parteien der Regierungskoalition die Polizei und Justiz personell und technisch kräftig stärken. Insbesondere setzen sich das Innenministerium und das Justizministerium dabei für die zusätzliche Einstellung von **Digitalexpertinnen und -experten** sowie Ermittlungsassistentinnen und -assistenten **für die Polizei** sowie für die Besetzung von **korrespondierenden neuen Stellen bei der Justiz,** vorrangig im Bereich der Staatsanwaltschaften ein. Die rechtlichen Rahmenbedingungen müssen dabei so ausgestaltet sein, dass die Strafverfolgungsbehörden auch im digitalen Raum handlungsfähig bleiben.

10.3.3 Ganzheitliche Lagebilderstellung

Als Grundlage zielgerichteten Handelns zur Verbesserung der Cybersicherheit dient den Gefahrenabwehr- und Strafverfolgungsbehörden ein umfassendes Lagebild. Die CSBW wird ein **Lagebild zumindest fünfzigmal im Jahr erstellen** und im Rahmen eines Warn- und Informationsdienstes an im Cybersicherheitsgesetz benannten Stellen verteilen.

10.4 Wirtschaft und Kritische Infrastrukturen (KRITIS)

10.4.1 Schutz der Wirtschaft vor Spionage und Sabotage

Zum Schutz der Wirtschaft werden wir neben dem Warn- und Informationsdienst weiterhin **bedarfsorientierte Beratungen im Bereich der Abwehr von Spionage und Sabotage** anbieten.

10.4.2 Erhöhung der Resilienz gegen Cyberangriffe speziell bei den KMU

Um Selbstständige und KMU besser bei der Cybersicherheit zu begleiten, bieten wir **bedarfsorientierte Hilfestellungen sowohl in präventiver Hinsicht als auch nach einem Sicherheitsvorfall** an. Dabei werben wir aktiv dafür, dass Cyber-Resilienz als Leitbild in die Unternehmenskultur aufgenommen wird.

10.4.3 Öffentlich-private Partnerschaften (ÖPP)

Damit KMU im Fall eines Cyberangriffs genau diejenigen IT-Sicherheitsdienstleister finden, die die Expertise zur Wiederherstellung ihrer Systeme haben, prüfen wir die Möglichkeit einer ÖPP, die diese Zusammenführung vornimmt. Dazu sollen **zumindest 15 IT-Dienstleister pro Jahr neu in das Netzwerk** aufgenommen werden.

10.4.4
Kritische Infrastrukturen (KRITIS) und ähnlich schutzbedürftige Stellen

Unser zentrales Ziel ist die Betreiber zu unterstützen, ein angemessen hohes Sicherheitsniveau im Cyberraum für Kritische Infrastrukturen (KRITIS) zu gewährleisten. Wir **unterstützen die Betreiber in Baden-Württemberg bei der Erstellung von Notfallvorsorgekonzepten und Notfallbehandlungsplänen,** insbesondere auch solche, die aus Sicht des Landes zu den KRITIS zählen, jedoch nicht von der BSI-Kritisverordnung des Bundes erfasst werden.

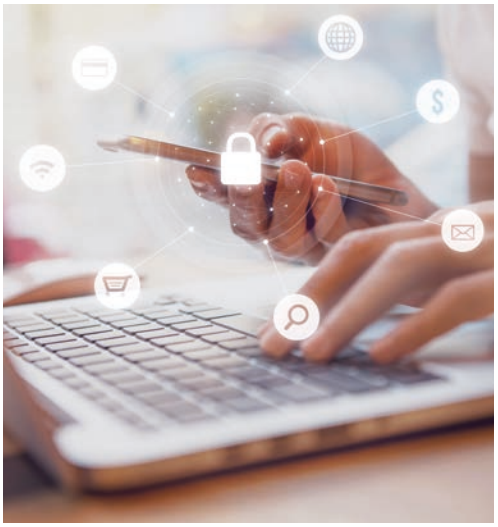
10.5
Digitale Kompetenzen

Zum besseren Umgang mit Cybersicherheitsrisiken ist es erforderlich, dass die handelnden Personen angemessene digitale Kompetenzen verfügen. Dazu sollen die betroffenen Fachressorts:

- die in der Lehrkräftebildung aller Lehrämter in der 2. Phase bereits **verankerten Themen Informations- und Cybersicherheit sowie Datenschutz in den entsprechenden Konzeptionen und Maßnahmen im Bereich der Aus- und Fortbildung der Lehrkräfte** durch das Zentrum für Schulqualität und Lehrerbildung Baden-Württemberg (ZSL) künftig aus fachlicher Sicht **weiterentwickeln und die Angebote intensivieren,**

- über das **Weiterbildungsportal www.fortbildung-bw.de** die Informationen und die Transparenz zu den vielfältigen, derzeit über 100 Qualifizierungsangeboten im Themenfeld Cybersicherheit weiter verbessern, und

- **jährlich mindestens für 15.000 Bedienstete der Landesverwaltung** Fortbildungen zur Cybersicherheit anbieten.



10.6
Awareness und Verbraucherschutz

Um Cybersicherheitsrisiken rechtzeitig zu erkennen sowie früh und angemessen darauf zu reagieren, wollen wir das Bewusstsein von Cyberrisiken (Awareness) erhöhen. Dazu werden wir **die Bevölkerung – insbesondere Verbraucherinnen und Verbraucher sowie Beschäftigte – und Unternehmen über die Gefahren im Cyberraum mit Hilfe konkreter Sensibilisierungsmaßnahmen informieren, um sie vor Schäden zu schützen.**

10.7
Fachkräfte

Für den Umgang mit Cybersicherheitsrisiken werden Fachkräfte benötigt. Dazu werden wir neben den allgemeinen Maßnahmen zur Verbesserung der digitalen Kompetenzen speziell bei der CSBW und dem LKA BW in Kooperation mit der DHBW am Standort Heilbronn **jährlich jeweils mindestens zwei berufsbegleitende Studienplätze anbieten.** Überdies werden **jährlich 60 ausgebildete Fachkräfte in der Landesverwaltung im IT-Grundschutz des BSI bzw. in vertiefenden Cybersicherheitsthemen fortgebildet,** um das Cybersicherheitsniveau zu erhöhen.

10.8
Innovative Forschung und Entwicklung

Damit wir bei der Abwehr von Cyberbedrohungen auf dem möglichst neuesten Stand sind, wollen wir die innovative Forschung und Entwicklung im Bereich der Cybersicherheit durch

- die Stärkung bereits sichtbarer Standorte ausbauen,
- die Förderung der **anwendungsorientieren, wirtschaftsnahen Forschung und Entwicklung sowie des wechselseitigen Wissens- und Technologietransfers zwischen Wissenschaft und Wirtschaft stärken,** und
- die Förderung von mindestens einem **Start-up-BW-Accelerator** durch das Wirtschaftsministerium, in dem das Thema Cybersicherheit behandelt wird, umsetzen.

10.9
Nationale und internationale Kooperationen

Um Synergien für mehr Cybersicherheit durch nationale und internationale Kooperationen zu nutzen, wollen wir

- die **Anzahl der Kooperationsvereinbarungen** erhöhen,
- die **bestehenden Kooperationsvereinbarungen überprüfen** und ggf. an neue Rahmenbedingungen anpassen,
- innerhalb der bestehenden Kooperationen **jährlich mindestens 50 Lagebilder austauschen,** sowie
- **jährlich mindestens drei Hospitationen von Beschäftigten** der Landesverwaltung bei Kooperationspartnern und umgekehrt zu ermöglichen.

IMPRESSUM

Bildnachweis

S. 1: Fingerprint Scanning Identification System © blackboard - stock.adobe.com
S. 4: Minister des Inneren, für Digitalisierung und Kommunen Thomas Strobl © Leif Piechowski
S. 9: Smart city and Wireless communication network concept ... © Yingyaipumi - stock.adobe.com
S. 11: Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg © Dr. Alfred Gustav Debus
S. 13: Cyber security concept, authentication screen on computer, confidential business data © NicoElNino - stock.adobe.com
S. 17: Dangerous Hooded Hacker Breaks into Government Data Servers and Infects Their System with a Virus. © Gorodenkoff - stock.adobe.com
S. 20: netz © vegefox.com - stock.adobe.com
S. 26: Young woman using laptop computer and sign up or log in username password ... © Monthira - stock.adobe.com
S. 30: Portrait of modern young man holding laptop ... © Seventyfour - stock.adobe.com
S. 31: Businessman Robot Hands Connection HUD Network © Alexander Limbach - stock.adobe.com
S. 32: Young people having business meeting in modern office © Pixel-Shot - stock.adobe.com
S. 34: Technician holding computer part with lancet ... © motortion - stock.adobe.com
S. 39: Cybersecurity and information or network protection. © kras99 - stock.adobe.com
S. 43: Woman using smartphone and laptop with icon graphic Cyber security network of connected devices and personal data security © oatawa - stock.adobe.com
S. 45: Futuristic cyber security concept with glowing low polygonal shield with access and world map © Inna - stock.adobe.com

Herausgeber
Ministerium des Inneren, für Digitalisierung und Kommunen
im Auftrag der Landesregierung Baden-Württemberg

Grafische Umsetzung
büro punkt. für visuelle Gestaltung

Stand
Dezember 2021

www.digital-bw.de