Baden-Württemberg

JAHRESBERICHT 2022

DER CYBERSICHERHEITSAGENTUR
BADEN-WÜRTTEMBERG

CSBW

CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

JAHRESBERICHT 2022

DER CYBERSICHERHEITSAGENTUR
BADEN-WÜRTTEMBERG

CSBW
CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

VORWORT

Thomas Strobl: Stellvertretender Ministerpräsident und Minister des Inneren, für Digitalisierung und Kommunen.

Meine sehr verehrten Damen und Herren,
liebe Leserinnen und Leser,

wenn wir auf das Jahr 2022 zurückblicken, sehen wir ein außergewöhnliches und erneut ein herausforderndes Jahr: Weltweite Krisen, geopolitische Herausforderungen und die fortdauernden Auswirkungen der COVID-19-Pandemie. All das sorgte im Jahr 2022 auch für drastische Entwicklungen im Bereich der Cybersicherheit. Der völkerrechtswidrige Angriff Russlands auf die Ukraine hat gezeigt: Kriege werden heute auch über das Netz geführt. Deshalb sind sichere und zuverlässige IT-Dienste für uns von entscheidender Bedeutung. Hinzu kommt eine zunehmende Professionalisierung der Angreifer: „Cybercrime-as-a-Service“ wurde zu einem Geschäftsmodell der organisierten Kriminalität. Zugleich weitet sich die IT-Landschaft und damit auch die Angriffsfläche immer weiter aus: Unsichere Cloud-Dienste, unzureichend gesicherte Heimnetzwerke

oder nicht gepatchte Systeme sind willkommene Einfallstore für Angreifer. Kaum eine Stelle oder ein Unternehmen kann heute noch von sich behaupten, nicht bereits in das Fadenkreuz der Angreifer gekommen zu sein – einige prominente Beispiele gab es für das Berichtsjahr mit Angriffen auf Unternehmen, Hochschulen und Kommunen, aber auch auf Krankenhäuser und Presseverlage im Land. In Baden-Württemberg vergeht kaum ein Tag, an dem öffentliche Verwaltungen, Unternehmen oder die kritische Infrastruktur nicht von Cyberkriminellen angegriffen werden.

Cybercrime, Cyberspionage und Cybersabotage haben wir bereits vor Jahren zum Top-Thema in Baden-Württemberg gemacht und frühzeitig Pionierarbeit geleistet. Mit der Cybersicherheitsagentur Baden-Württemberg (CSBW) haben wir im Frühjahr 2021 eine zentrale Einrichtung zur Abwehr von Gefahren für die Cybersicherheit geschaffen. Schon im ersten Jahr nach Errichtung hat die CSBW bei einer Vielzahl von Cyberangriffen vor Ort unterstützt – angefangen von der Koordination der beteiligten Akteurinnen und Akteure, über die forensische Analyse der IT-Systeme bis hin zur Krisenkommunikation und der Hilfestellung bei der Wiederherstellung der Systeme. Auch im Bereich der Prävention hat die CSBW mit verschiedenen Sensibilisierungsmaßnahmen „Awareness“ geschaffen. Dies ist besonders wichtig, denn 99 % aller Angriffe nehmen ihren Ursprung in der „Schwachstelle Mensch“.

Seit Anfang August 2022 ist die CSBW zudem zentrale KRITIS-Kontaktstelle für das Bundesamt für Sicherheit in der Informationstechnik und gibt die erhaltenen Informationen an die betreffenden Stellen im Land weiter. Mit der Übernahme des CERT BWL im selben Monat wurde schließlich ein weiterer Meilenstein in Richtung „Zentrale Koordinierungs- und Meldestelle“ für die Cybersicherheit im Land erreicht.

Die Mitarbeitenden der Cybersicherheitsagentur haben sich all diesen Herausforderungen mit großer Einsatzbereitschaft angenommen und tragen mit ihrer engagierten Arbeit zur Absicherung des Cyberraums bei, wofür ich mich ganz herzlich bedanke.

Ihr
Thomas Strobl

www.cybersicherheit-bw.de

INHALT

INTERVIEW MIT DEM FÜHRUNGSDUO DER CSBW: RALF ROSANOWSKI UND DR. CLAUDIA WARKEN

Frage 1:

Ralf Rosanowski, Präsident der CSBW

Was waren aus Ihrer Sicht die größten Herausforderungen des Jahres 2022 für die Cybersicherheit in Baden-Württemberg?

Ralf Rosanowski:
Der russische Angriffskrieg auf die Ukraine hat auch uns in vielfältiger Weise gefordert. Die Sicherheitsmaßnahmen in der Landesverwaltung mussten kurzfristig verschärft werden und der erheblich gestiegene Informationsbedarf auf vielen Ebenen erforderte einen besonders intensiven Austausch mit allen anderen Akteurinnen und Akteuren – zum Teil auch an Wochenenden.
In diesem Jahr war der deutliche Anstieg an Cyberangriffen auf öffentliche Einrichtungen in Baden-Württemberg auffällig. Dadurch waren wir zeitweise in vielen Bereichen extrem gefordert. Gleichzeitig hat dieser Trend aber auch deutlich gemacht: Für das Team der CSBW wird es auch in Zukunft noch viel zu tun geben. Die zunehmende Digitalisierung dürfte hierbei als Beschleuniger wirken.
Letztendlich hatten wir über das ganze Jahr verteilt eine große Zahl an schwerwiegenden Sicherheitslücken zu bewältigen. Die zunehmend komplexer werdende IT-Landschaft lässt auch in diesem Feld keine Entspannung erwarten.

Frage 2:

Was hat die CSBW als neue Landesoberbehörde in ihrem Aufbau am meisten geprägt?

Ralf Rosanowski:
Aus meiner Sicht haben uns die Bewältigung der Aufbauarbeit und die gleichzeitige Erledigung der operativen Aufgaben in besonderem Maße gefordert. Beide Aspekte beeinflussen sich gegenseitig. Wäre nicht noch Aufbauarbeit zu leisten, dann wären wir im operativen Leistungsportfolio stärker. Umgekehrt gilt natürlich auch: Wäre nicht zeitweise der operative Betrieb zu priorisieren, wären unsere Fortschritte im Aufbau größer.

Dr. Claudia Warken, Vizepräsidentin der CSBW

Frage 3:

Was ist Ihr jeweils persönliches Resümee aus dem ersten Jahr als CSBW?

Ralf Rosanowski:
Ich ziehe eine ausgesprochen positive Bilanz. Wir haben sehr viel bewegt – insbesondere unter den bereits angesprochenen Rahmenbedingungen. Die Fortschritte in den verschiedenen Projekten, aus dem Aufbau der Behörde und aus dem operativen Bereich, belegen das. Natürlich hätte auch ich mir gewünscht, dass wir in diesem Jahr in ein eigenes Bürogebäude einziehen können – aber wie bei zahlreichen Themen aus allen möglichen Lebensbereichen, gibt es auch hier vielfältige externe Faktoren, die Auswirkungen auf das Gesamtziel haben.

Dr. Claudia Warken:
Wir haben 2022 in allen Fachbereichen viele Meilensteine erreicht, aber auch vieles von dem, was wir uns vorgenommen haben, aus unterschiedlichen Gründen noch nicht verwirklichen können. Wichtig ist, dass wir uns davon nicht entmutigen lassen. Es gibt kein Handbuch zum Aufbau einer neuen Landesoberbehörde und gerade weil wir es gut machen wollen, müssen wir permanent nachsteuern, neu priorisieren und gegebenenfalls auch korrigieren. Die Fähigkeit dazu ist ein Zeichen von Stärke.

Nur aufgrund des großen persönlichen Einsatzes der Mitarbeitenden und ihrer herausragenden Leistungsbereitschaft haben wir es geschafft, unter teilweise extrem widrigen Bedingungen (lange Zeit ungeklärter Standort, Raumnot und fehlende IT-Ausstattung – um nur einige zu nennen) nicht den Fokus zu verlieren. Wir werden bereits jetzt als wichtiger Player im Land und im Bund wahrgenommen, überzeugen mit Fachkompetenz und Verbindlichkeit. Das Vertrauen, das uns unsere Zielgruppen entgegenbringen, wächst mit jedem Tag. Ein konstruktiver Dialog in verschiedene Richtungen und positives Feedback von außen sprechen für sich und sind keinesfalls selbstverständlich.

In vielen persönlichen Gesprächen innerhalb des Teams habe ich die uns verbindende Leidenschaft für die Sache und ein echtes Interesse am Thema Cybersicherheit gespürt. Ich wünsche mir, dass uns beides immer erhalten bleibt.

Frage 4:

Wie hat die CSBW den Grat zwischen weiterer Aufbauarbeit und operativem Betrieb gemeistert?

Ralf Rosanowski:
Das hat in der Tat von allen Mitarbeitenden sehr viel abverlangt. Einzelne Bereiche haben häufig an der Kapazitätsgrenze gearbeitet. Zudem mussten sich teilweise Mitarbeitende auch flexibel mit Themen befassen, die nicht zu ihren primären Aufgabenbereichen zählen. Doch auch hier ist meine Bilanz positiv. Wir haben das gemeinsam gut geschafft. Ich danke allen Mitarbeitenden der CSBW für ihren tatkräftigen Beitrag!

Dr. Claudia Warken:
Sehr gut! Wir haben die Chance, eine Behörde mit herausragender gesellschaftlicher Bedeutung neu zu denken und „so richtig gut" aufzubauen. Die Kehrseite dieser Gestaltungsfreiheit sind manche (noch) fehlenden Strukturen und Prozesse, anfänglich unzureichende Sachmittel und unerwartet lange Zeitläufe für viele Dinge, die gebraucht werden. Das kann frustrierend und demotivierend sein, weil die meisten von uns darauf brennen, endlich loszulegen und ihre fachlichen Fähigkeiten einzubringen.

Die CSBW-ler aus sämtlichen Bereichen gehen mit dieser Situation professionell, mit viel Einsicht und noch mehr Ausdauer um. Praktikable und teilweise auch unkonventionelle Lösungen bringen uns Schritt für Schritt unserem großen Ziel – einer innovativen, modernen Vorzeigebehörde – näher, das wir zu keinem Zeitpunkt aus den Augen verlieren dürfen. Diese innere Haltung und ein ergebnisorientiertes Miteinander zeichnen das CSBW-Team aus.

Frage 5:

**Die CSBW wächst auch 2023 weiter:
Welche Menschen suchen Sie für das Team?**

Ralf Rosanowski:
Nun, zunächst müssen die Menschen natürlich die Skills mitbringen, die für die jeweilige Aufgabe benötigt werden.

In den operativen Bereichen sind wir sehr stark fremdbestimmt. Hier brauchen wir Menschen, die bereit sind, auch dann zu arbeiten, wenn andere das Wochenende oder den Feiertag genießen können.

Wichtig ist mir, dass alle Mitarbeitenden den nötigen Idealismus mitbringen, um das Thema Cybersicherheit insgesamt voranzubringen. Das bezieht sich ausdrücklich auf alle Bereiche in der CSBW und nicht nur auf die IT-Fachkräfte.

Dr. Claudia Warken:
Für alle Bereiche brauchen wir Menschen, die das gemeinsame Ziel teilen, eine innovative, moderne Behörde aufzubauen; Menschen, die geistig offen und lösungsorientiert sind und die erkennen, dass wir als Team mehr erreichen als die Summe aller Einzelbeiträge. Ich wünsche mir Kolleginnen und Kollegen, die Dinge hinterfragen, die den Mut haben, Neues auszuprobieren und damit eventuell auch zu scheitern, und die Freude und Stolz für das empfinden, was wir gemeinsam schaffen.

1.0

CSBW: Zentrale Anlaufstelle für Cybersicherheit im Land

Verwaltung, Kommunen, Wirtschaft – die Gefahr, Opfer eines Cyberangriffs zu werden ist so hoch wie nie zuvor. Ein Blick auf die Betroffenen zeigt: Es kann alle treffen.
Mit der Cybersicherheitsagentur Baden-Württemberg (CSBW) hat das Land Baden-Württemberg eine zentrale Koordinierungs- und Meldestelle, die im ständigen Austausch mit allen relevanten Sicherheitsbehörden sowie weiteren Akteurinnen und Akteuren steht. Dadurch werden die Bekämpfung und Abwehr von Sicherheitsbedrohungen im digitalen Raum effektiver und effizienter.

1.1
ZWECK UND AUFGABEN DER CSBW

Die CSBW wurde mit Inkrafttreten des Cybersicherheitsgesetzes am 17.02.2021 gegründet. Bereits während der Aufbauphase 2021 begegnete das stetig wachsende und interdisziplinär aufgestellte Team der CSBW den immer größer werdenden Gefahren von Cyberangriffen. Zentrale Aufgabe der CSBW ist es, die Cybersicherheit und die damit zusammenhängenden Aspekte der Informationssicherheit in Baden-Württemberg zu fördern. Im Fokus steht dabei vor allem die Landesverwaltung. Der Ansatz der CSBW deckt die Handlungsfelder Prävention (Vorbeugen), Detektion (Erkennen) und Reaktion (Reagieren) ab, welche auch die Fachabteilungen der Behörde bilden.

Die zentralen Aufgaben der CSBW im Überblick:

- Sie ist die **zentrale Koordinierungs- und Meldestelle** für die Zusammenarbeit der öffentlichen Stellen in Angelegenheiten der Cybersicherheit in Baden-Württemberg
- Die CSBW erstellt wöchentliche sowie anlassbezogene Berichte zur **Cybersicherheitslage in Baden-Württemberg.** Über dieses Lagebild informiert die CSBW beispielsweise andere Behörden, sodass diese geeigneten Maßnahmen zur Gefahrenabwehr vornehmen können
- Bei konkreten, herausgehobenen Cyberangriffen kann die CSBW Landesbehörden, Städte, Gemeinden und Landkreise bei der **Angriffsbeendigung oder der Wiederherstellung kompromittierter Systeme** nach einem Angriff helfen. In begründeten Einzelfällen können auch andere Organisationen mit wichtiger Bedeutung für das öffentliche Gemeinwesen Hilfe erhalten
- **Die CSBW vernetzt** Staat, Verwaltungen, Kommunen, Wirtschaft, Wissenschaft und Forschung im Bereich der Cybersicherheit sowie die maßgeblichen behördlichen Organisationen der Cybersicherheit im Land, wie Strafverfolgungsbehörden und Sicherheitseinrichtungen. Polizeiliche Aufgaben wie die **Strafverfolgung nimmt die CSBW nicht wahr**
- Vorrangig Personen aus der Verwaltung, den kleinen und mittelständischen Unternehmen und dem Hochschulbereich in Baden-Württemberg werden von der CSBW zum Thema Cybersicherheit sensibilisiert
- Bei der **Aus- und Fortbildung zu Cybersicherheitsthemen** in der staatlichen **Verwaltung, in den Kommunen, in der Wirtschaft und für die Bürgerinnen und Bürger unterstützt die CSBW aktiv**
- Seit dem 1. August 2022 ist die CSBW **zentrale Kontaktstelle nach § 8b des BSI-Gesetzes** und gibt die vom BSI erhaltenen Informationen über meldepflichtige Vorfälle bei Unternehmen der Kritischen Infrastruktur (KRITIS) an die betreffenden Stellen weiter
- Momentan pilotiert die CSBW ein **Beratungsangebot** für von Cybersicherheitsvorfällen betroffene Unternehmen, Behörden, Institutionen, aber auch Bürgerinnen und Bürger

Der weitere Auf- und Ausbau der Angebote und Serviceleistungen, sowohl im präventiven wie auch im reaktiven Bereich, erfolgt stufenweise.

1.2
VISION, LEITBILD UND STRATEGIE

Die CSBW soll maßgebliche Anlaufstelle und impulsgebend für die Cybersicherheit in Baden-Württemberg werden und einen nachhaltigen, gesamtgesellschaftlichen Nutzen schaffen.

Diese Vision führt die CSBW zum Leitbild einer modernen Führungskultur und einem Team aus hochkompetenten und leistungsfähigen Spezialistinnen und Spezialisten, um ein Schutzschild für die öffentlichen Stellen in Baden-Württemberg im Cyberraum zu bilden.

Um ihre Vision zu erreichen und dem Leitbild entsprechend zu handeln, hat die CSBW eine Strategie für die Jahre 2022-2025 entwickelt, die den Fokus auf fünf strategische Handlungsfelder setzt.
Die Führungsebene leitet aus diesen jährlich Ziele ab, die allen CSBW-Mitgliedern in ihren Entscheidungen und ihrer täglichen Arbeit als Maßgabe und Orientierung dienen soll.

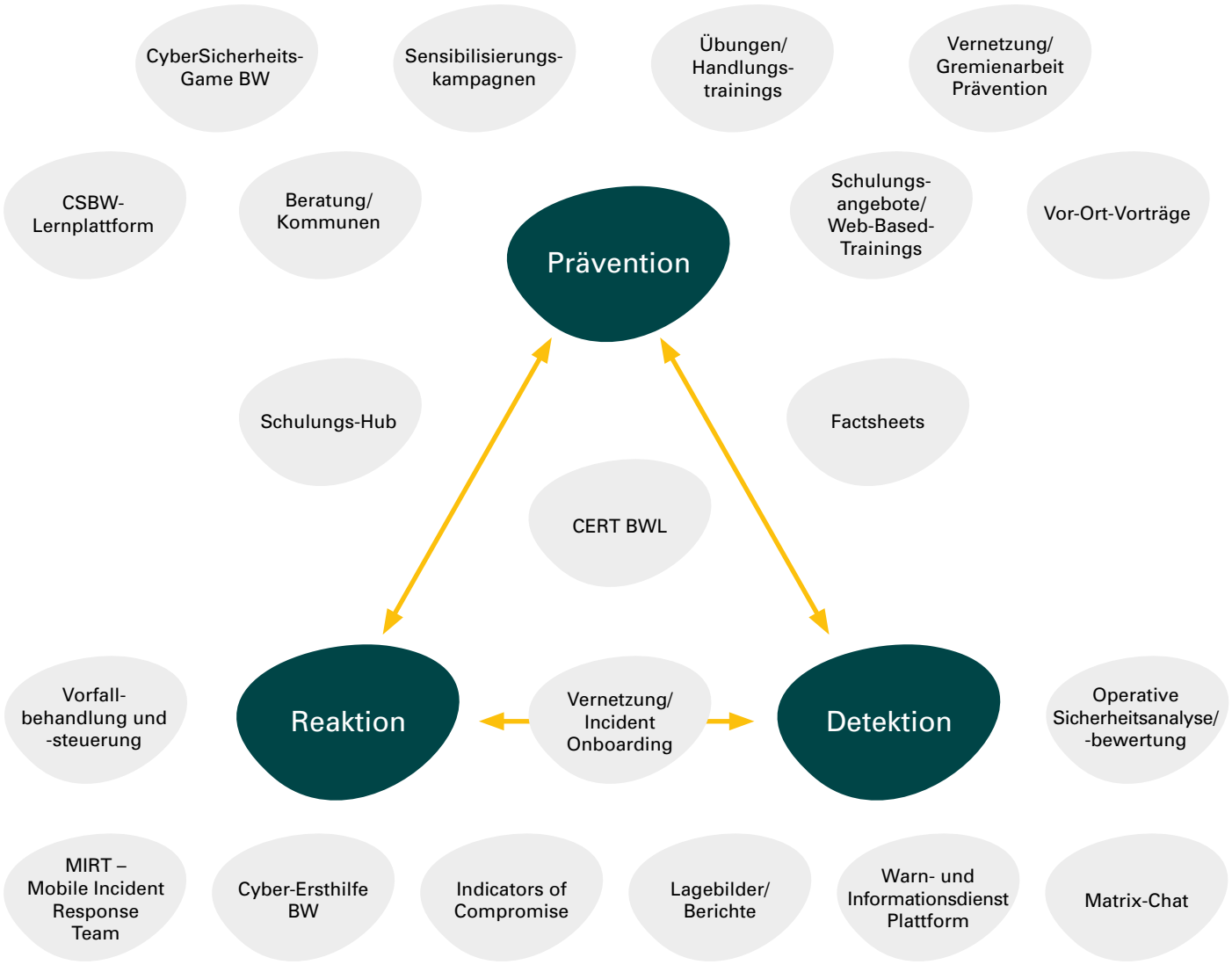
1. **Sinnstiftung**
   Dieses strategische Handlungsfeld beschäftigt sich mit der wichtigsten Ressource – den Menschen in der CSBW. Deren Leistung hängt maßgeblich von einem motivierenden und zufriedenstellenden Arbeitsumfeld ab.
2. **Innovation und Führung**
   Das Thema Cybersicherheit ist hochdynamisch und fordert eine entsprechende Flexibilität. Der Einsatz neuer Methoden und Werkzeuge – sowohl technologisch wie auch in der Führung – ist Voraussetzung, um in diesem Umfeld wirksam agieren zu können.
3. **Vernetzung und Sichtbarkeit**
   Um die Cybersicherheit des Landes zu stärken, ist die Zusammenarbeit mit weiteren Akteurinnen und Akteuren unerlässlich. Aus diesem Grund befindet sich die CSBW in regem fachlichen Austausch und arbeitet selbst am Aufbau entsprechender Strukturen.
4. **Vertrauen in die CSBW**
   Zum Schutz vor Cyberangriffen beziehungsweise um angemessen reagieren zu können, bedarf es einer hohen fachlichen Kompetenz. Die Mitglieder der CSBW halten sich stets auf dem aktuellsten Stand der Entwicklung und tragen durch ihre Einsätze und fachlichen Beiträge zum Vertrauen in die Leistungsfähigkeit der CSBW bei.
5. **Kontinuierliche Weiterentwicklung**
   Als junge Behörde befindet sich die CSBW, neben dem operativen Betrieb, zwar weiterhin in der Aufbauphase, dennoch gilt es die kontinuierliche Weiterentwicklung der Services und die dauerhafte Verbesserung der Prozesse der CSBW von Beginn an mitzudenken und als Ziel der Optimierung zu verfolgen.

Cybersicherheit in einer volatilen, unsicheren, komplexen und mehrdeutigen Umgebung herzustellen, ist die Herausforderung, der sich die CSBW stellen muss. Die definierten strategischen Handlungsfelder geben Orientierung und lassen gleichzeitig genug Spielraum, um flexibel agieren zu können.

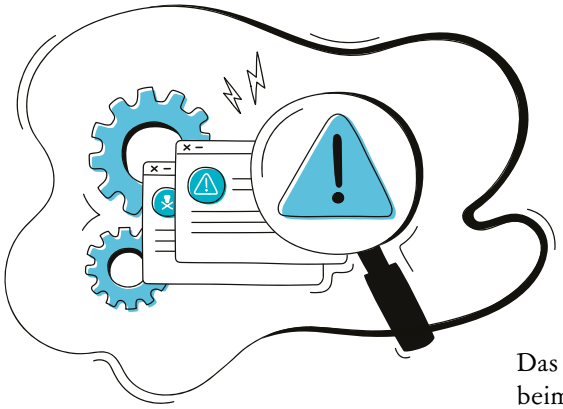
1.3
DIE CSBW-HANDLUNGSFELDER

Für die Cybersicherheit in Baden-Württemberg ist ein umfassender Ansatz erforderlich, der die Sicherheit von der Prävention über die Detektion bis hin zur Reaktion behandelt und entsprechende Angebote bereitstellt. Dabei entstanden sind die beiden Fachabteilungen („Prävention“ sowie „Detektion und Reaktion“), die sich mit ebendiesen operativen Handlungsfeldern beschäftigen.

Folgende Darstellung zeigt auf, wie umfassend und breit die Cybersicherheitsagentur Baden-Württemberg aufgestellt ist und welche Dienstleistungen und Produkte das Angebot umfasst.



Handlungsfelder und Angebote der Fachabteilungen der CSBW



Das **operative Handlungsfeld Prävention** setzt auf Sensibilisierung beim Thema Cybersicherheit, um Vorfälle im besten Fall gar nicht erst entstehen zu lassen. Für den Fall, dass es bereits zu einem Vorfall gekommen ist, vermittelt das Handlungsfeld das erforderliche Wissen, wie durch eine angemessene Reaktion Schadensbegrenzung betrieben werden kann. Neben den klassischen Schulungsangeboten umfasst das Portfolio der Abteilung unter anderem Kampagnen und Übungen zur Sensibilisierung, ein „Serious Game“ (Lernspiel) für die Landesverwaltung, spezielle Beratungsangebote sowie handliche Factsheets, die Informationen zu den häufigsten Risiken auf einen Blick liefern und die zielgruppenübergreifend bereitgestellt werden.

Das Ziel des **operativen Handlungsfelds Detektion** ist es, Vorfälle möglichst frühzeitig zu erkennen. Um akute Schwachstellen und Risiken zu erörtern und betroffene Akteurinnen und Akteure rechtzeitig zu warnen, ist das Lagezentrum der CSBW im engen Austausch unter anderem mit den Ressorts, Rechenzentren und Sicherheitsbehörden des Landes. Regelmäßige und fallbezogene Lagebilder und Führungsinformationen sorgen zudem dafür, dass alle relevanten Akteurinnen und Akteure über den aktuellen Stand der Cybersicherheit im Land in Kenntnis gesetzt sind, sodass rechtzeitig und angemessen reagiert werden kann.

Sollte es im schlimmsten Fall doch zu einem Vorfall kommen beziehungsweise ein Verdachtsfall vorliegen, kommt die Expertise im **operativen Handlungsfeld „Reaktion“** zum Einsatz. Die forensische Vorfallbehandlung – mit mobilem Team vor Ort oder remote[1] – sowie Hilfe zur Selbsthilfe sind die wesentlichen Unterstützungsleistungen des seit Juli 2022 bei der CSBW angesiedelten CERT BWL (Computer Emergency Response Team des Landes Baden-Württemberg).

In allen Handlungsfeldern setzt die CSBW auf eine enge und konstruktive Zusammenarbeit unter anderem mit Hochschulen, Rechenzentren, Sicherheitsbehörden und Kommunen. Der Austausch von Wissen und Erfahrungen führt bei allen Beteiligten zur Erhöhung der Cyber-Resilienz und damit zu einer immer leistungsfähigeren Cybersicherheitsarchitektur in Baden-Württemberg.

[1] **remote** = Homeoffice beziehungsweise an einem anderen Ort als im Büro

1.4
ORGANISATION / AUFBAUSTAB

Präsident der Cybersicherheitsagentur Baden-Württemberg ist seit dem 15. September 2021 Ralf Rosanowski. Die Leitung der Stabsstelle hat die Vizepräsidentin Dr. Claudia Warken inne. Präsident und Vizepräsidentin tragen als Führungsduo die Gesamtverantwortung für den weiteren Auf- und Ausbau der CSBW.

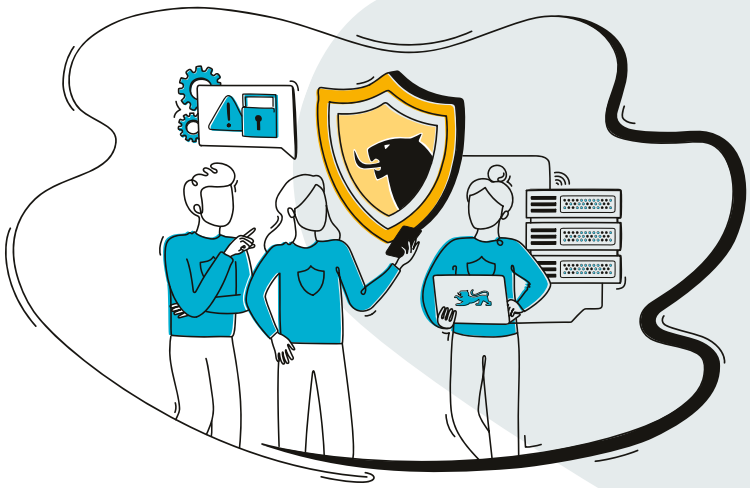
Ihnen obliegt im Zusammenspiel mit dem Innenministerium die strategische Steuerung und Koordination der Aktivitäten des Landes im Bereich der Cybersicherheit. Sie sollen unter anderem die diversen Akteurinnen und Akteure im Themenfeld Cybersicherheit im Land Baden-Württemberg zusammenbringen, Projekte zur Umsetzung der Cybersicherheitsstrategie entwickeln und Partnerschaften zu Cybersicherheitsagenturen auf nationaler und internationaler Ebene aufbauen.

In der **Stabsstelle** sind die Themen „Grundsatz und Strategie“ sowie „Kommunikation und Öffentlichkeitsarbeit“ angesiedelt.

Die Mitarbeitenden der **Abteilung 1 – Prävention** kümmern sich um die Themen Sensibilisierung und Schulung, Beratung, Innovationsmanagement, Informationssicherheitssystem und Übungen.

In der **Abteilung 2 – Detektion und Reaktion** sind das Lagezentrum, die Operative Sicherheitsanalyse, die Vorfallbehandlung sowie die Cyber-Ersthilfe BW verortet.

Die Sachgebiete Haushalt und Vergabe, Personal, Recht, die IT der CSBW, die Registratur und E-Akte sowie die Servicestelle sind in **Abteilung 3 – Querschnitt** angesiedelt.



2.0
Handlungsfeld „Prävention“

Ein elementarer Bestandteil der Arbeit der Cybersicherheitsagentur Baden-Württemberg (CSBW) liegt in der Prävention.
Denn: Das wahrscheinlichste Einfallstor bei einem Cyberangriff ist weiterhin der Mensch. Wie sieht ein sicheres Passwort aus? Was ist bei einem Cybernotfall zu tun? Wie kann jede Einzelperson sich schützen?
Die CSBW richtet sich perspektivisch an ihre verschiedenen Zielgruppen mit einem breiten Angebot vielseitiger Informationsmaterialien, Schulungen sowie Sensibilisierungsmaßnahmen.

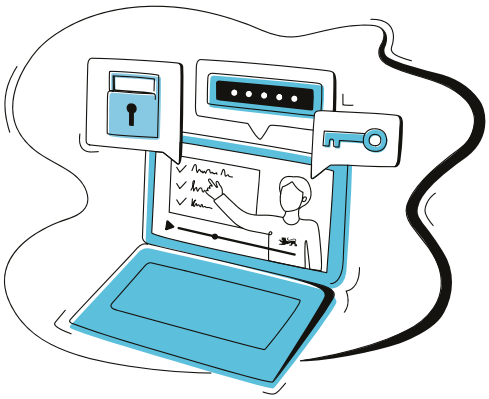
2.1
CSBW-FACTSHEETS INFORMIEREN ZU THEMEN DER CYBERSICHERHEIT

Bei den Factsheets handelt es sich um einseitige, kompakte „Wissensblätter“ zu verschiedenen Themen der Cybersicherheit. Ziel ist es, mit kurzen Anleitungen und Handlungsempfehlungen, leicht verständlich und informativ, Orientierung für den digitalen Alltag zu geben.

Jedes Factsheet behandelt genau ein Thema zur Cybersicherheit, welches übersichtlich auf einer Seite präsentiert wird. Die Themen sind sehr vielfältig und decken sowohl den dienstlichen als auch den privaten Bereich ab. Themen sind zum Beispiel „Wie sieht ein sicheres Passwort aus?“, „Wie schützt man sich vor Phishing-E-Mails?“ oder „Wie richtet man den Home-Router ein, damit alles sicher ist?“.

Auch zu speziellen landesverwaltungsinternen Themen werden Verhaltensempfehlungen an die Hand gegeben. Die Reihe der CSBW-Factsheets wird sukzessive und anlassbezogen ergänzt. Oft gibt ein aktuelles Cybersicherheitsthema den Anstoß, konkrete Tipps und Handlungsempfehlungen in einem CSBW-Factsheet zusammenzufassen und der Öffentlichkeit zugänglich zu machen.

Die CSBW-Factsheets sind auf der CSBW-Website www.cybersicherheit-bw.de veröffentlicht und für den Download freigegeben.



Exemplarische Factsheets der CSBW

2.2 SCHULUNGEN

Neben der Sensibilisierung zum Thema Cybersicherheit über diverse Angebote liegt ein weiteres Augenmerk des Bereichs „Prävention“ auf dem Themenkomplex der Schulungen. Durchdachte, innovative Schulungen und eine nutzerfreundliche Bündelung der Schulungsangebote, sollen dazu führen, dass die Wissensaneignung im Bereich der Cybersicherheit vereinfacht wird.

Die CSBW baut aktuell ein vielfältiges Angebot an Schulungen, Trainings und Präventionsangeboten auf. Dabei richtet sie sich vor allem an die Mitarbeitenden der Landes- und Kommunalverwaltung. Darüber hinaus spricht die CSBW mit einigen Formaten auch weitere Zielgruppen an, wie beispielsweise Bürgerinnen und Bürger sowie KMU (Kleine und mittlere Unternehmen). Zudem werden für alle neuen Beschäftigten der CSBW interne Schulungs- und Trainingsangebote konzipiert und angeboten.

Das derzeit vorgeschlagene Schulungsangebot reicht von der klassischen Präsentation über interaktive Web-Based-Trainings bis hin zu Schulungsvideos mit Live-Demonstration des Schulungsinhalts. Thematische Schwerpunkte liegen beispielsweise in der sinnvollen Nutzung eines Passwort-Managers zur sicheren Verwaltung von Passwörtern. Aber auch grundlegende Themen zur Cybersicherheit werden in den Schulungsangeboten aufgegriffen und weiter vertieft. Hierzu zählen insbesondere der Umgang mit sicheren Passwörtern, Phishing-Mails, Social Engineering, Cybersicherheit im Homeoffice und im Büro, aber auch die richtige Reaktion bei dem Verdacht, Opfer eines IT-Sicherheitsvorfalls geworden zu sein.

Die von der CSBW konzipierten Schulungen und Präventionsmaterialien werden auf der CSBW-Lernplattform Moodle zur Verfügung gestellt, um den interessierten Zielgruppen einen zeit- und ortsunabhängigen Zugriff zu ermöglichen. Die Plattform befindet sich seit November 2022 im zunächst internen Pilotbetrieb. Auf Moodle können Schulungen angelegt, verwaltet, gebucht, durchgeführt und ausgewertet werden. Neben der nutzerfreundlichen Bereitstellung liegt insbesondere in der Verwaltung und Auswertung ein erhebliches Potenzial, das Angebot stetig auszubauen und zielgruppengerecht zu verbessern.

Ein weiterer Vorteil der Bereitstellung über Moodle ist die Eröffnung der Möglichkeit zum selbstgesteuerten Lernen, das sich flexibel in den individuellen Arbeitsalltag integrieren lässt. Innerhalb der Landes- und Kommunalverwaltung können perspektivisch alle Mitarbeitenden Schulungen auf dieser Plattform selbst durchführen und an das individuelle Lerntempo anpassen. Externe Personen sind als Gäste willkommen und erhalten über einen Gastzugang Zugriff auf die Schulungen zur Cybersicherheit. Für das Jahr 2023 plant die CSBW, nach der initialen Freischaltung, eine sukzessive Erweiterung der Angebotspalette im Schulungs-, Trainings- und Präventionsbereich.

2.3
CYBERSICHERHEITSGAME BW

In Kooperation mit dem Innenministerium Baden-Württemberg entstand unter Federführung der Cybersicherheitsagentur Baden-Württemberg das „CyberSicherheitsGame BW“.

Das Projekt wird den Mitarbeitenden der Landes- und Kommunalverwaltung zukünftig als Teil des E-Learning-Angebots der CSBW zur Verfügung stehen.

Es definiert sich als „Serious Game[2]“. Als Ergänzung zum sonstigen Schulungsangebot werden Lerninhalte adäquat in die Spiellogik übersetzt und laden auf insgesamt 14 Levels dazu ein, sich spielerisch mit Themen wie „Social Engineering“, „Phishing-E-Mails“ oder „Passwortsicherheit“ auseinanderzusetzen.

Das „CyberSicherheitsGame BW“ vereint hierfür die Vorteile von Präsenzschulungen und E-Learning-Angeboten und animiert dazu, selbst aktiv zu werden und mit dem Spiel zu interagieren. Es entführt die Spielenden in die Welt der beiden Computerchips Cypher und Divio, aus der sie sich nur mithilfe ihres Wissens zu Cybersicherheitsthemen befreien können. Um wieder nach Hause zurückkehren zu können, müssen sie verschiedene Aufgaben und Herausforderungen meistern, die Cypher ihnen stellt. Divio steht ihnen dabei mit Rat und Tat zur Seite.

Über verschiedene Zwischenziele, wie zum Beispiel Sterne sammeln oder Level abschließen, kommen die Spielenden stückweise dem Hauptziel näher, das Reich von Cypher und Divio wieder zu verlassen. Zeitgleich erhalten sie hierdurch aber auch kontinuierlich Rückmeldung zum eigenen Lernerfolg. Das Spiel kann abgeschlossen werden, indem die Nutzerinnen und Nutzer eine Mindestanzahl an Sternen und Schildern sammeln. Die Level lassen sich jedoch beliebig oft wiederholen, auch nach Abschluss des Spiels.

Mit dem „CyberSicherheitsGame BW“ sollen die Mitarbeitenden der Landes- und Kommunalverwaltung für das Thema Cybersicherheit anwenderorientiert und nachhaltig sensibilisiert werden. Das langfristige Ziel ist, den Transfer zwischen Lernen und Anwenden zu ermöglichen und damit eine anhaltende Verhaltensänderung zu erreichen.

Avatar aus dem CyberSicherheitsGame BW

[2] **Serious Game:**
Ein Videospiel, das der Vermittlung von Wissen dient und dabei dem didaktischen Ansatz der Gamification folgt.

2.4
LANDESWEITE KAMPAGNE: FÜR CYBERSICHERHEIT SENSIBILISIEREN

Mit einer landesweiten Sensibilisierungskampagne zur Cybersicherheit beabsichtigt die CSBW den Mitarbeitenden der Landes- und Kommunalverwaltung das Thema Cybersicherheit näher zu bringen. Der Faktor Mensch steht dabei im Mittelpunkt. Es geht darum, die möglichen Gefahren aufzuzeigen, aber gleichzeitig auch deutlich zu machen, dass jede einzelne Person mit konkretem Handeln zur Cybersicherheit beitragen kann. Angelehnt an den CSBW-Slogan: „Mit uns. Mit Ihnen. Mit Sicherheit.“

Einzelne Kampagnenprodukte geben den Zielgruppen gut verständliche Informationen an die Hand, um sich der Gefahr von Cyberangriffen bewusst zu werden und bei Angriffen richtig reagieren zu können. Konkrete Handlungsempfehlungen regen zu richtigem Handeln an.

Eine erste außenwirksame Aktion der Kampagne war die „Advents-Aktion 2022“. Das Ziel der Aktion war, auf die Gefahren im Cyberraum insbesondere zur Weihnachtszeit hinzuweisen. Über die Informationssicherheitsbeauftragten der Landes- und Kommunalverwaltung wurden insgesamt vier Sensibilisierungs-E-Mails zu den Themen „Phishing-E-Mails“, „Online-Shopping“, „Homeoffice“ und „Passwortverwaltung“ mit konkretem Weihnachtsbezug an deren Belegschaft verschickt.

Als weiteres Produkt der Sensibilisierungskampagne wird derzeit an einem Quick-Guide gearbeitet, der sich als Broschüre im Handtaschenformat präsentiert. In illustrierter Form werden darin die wichtigsten Bereiche der Cybersicherheit sowie die Gefahren des Cyberraums aufgezeigt und Handlungsempfehlungen gegeben. Den Zielgruppen wird die kleine Broschüre in digitaler Form zur Verfügung gestellt. Zusätzlich wird sie für Veranstaltungen als Printversion realisiert.

Für das Quartal 2/2023 ist der eigentliche Roll-out der Kampagne mit weiteren digitalen und analogen Sensibilisierungsprodukten geplant. In diesem Rahmen wird auch der Quick-Guide zum Einsatz kommen.

Advents-Kampagne zur Sensibilisierung für Gefahren im Cyberraum

2.5 BERATUNG

Neben den Bereichen Sensibilisierung und Schulung wird seit der zweiten Jahreshälfte 2022 der Bereich Beratung aufgebaut. Zwei Mitarbeitende befassen sich in diesem Zusammenhang intensiv mit der spezifischen Beratung von Kommunen in Baden-Württemberg, konzipieren hierfür ein spezielles Beratungsangebot und setzen einen Schulungs-Hub auf.

Mehrere Kommunen in Deutschland und auch in Baden-Württemberg wurden im Jahr 2022 Opfer von Cyberangriffen. Zusätzliche Schutzmaßnahmen für Kommunen haben deshalb einen hohen Stellenwert im Aufgabenspektrum der CSBW. Für die Entwicklung eines Beratungskonzeptes wurde eine Bedarfsermittlung bei Kommunen durchgeführt, welche einen Überblick über die aktuelle Situation liefert und umfangreiche Herausforderungen aufzeigt. Auf der Basis dieser Bedarfsermittlung wurden als Teil des Beratungskonzeptes konkrete Beratungsangebote näher definiert. Diese werden im Laufe des Jahres 2023 für die Kommunen bereitgestellt.

Auch bei den Kommunen gilt: Das Wissen über die Risiken und Einfallstore von Cyberangriffen kann helfen, sich im digitalen Raum sicherer zu bewegen. Demnach ist auch hier ein weiterer, wichtiger Aspekt für einen besseren Schutz von Kommunen die Schulung von Mitarbeitenden. Zur Unterstützung dieses Aspekts startete im zweiten Halbjahr 2022 das Projekt zur Erstellung eines Schulungs-Hubs. Dieser wird als Bestandteil der CSBW-Website in diese integriert und informiert über Schulungsangebote im Bereich der Cybersicherheit. Grundsätzlich kann jede staatliche, institutionelle und private Bildungseinrichtung mit Schulungsangeboten in Baden-Württemberg in den Schulungs-Hub aufgenommen werden, wodurch den Lernwilligen der Überblick über die verschiedenen Schulungsmöglichkeiten erleichtert und eine bessere Orientierung ermöglicht wird. Der Schulungs-Hub soll im Laufe des Jahres 2023 bereitgestellt werden.

2.6 HOCHSCHULEN

Mit dem Hochschul- und Innovationsmanagement stehen die Vernetzung und der intensive Austausch mit Universitäten und Hochschulen in Baden-Württemberg im Bereich der Cybersicherheit im Vordergrund. Zukünftig sollen Schulungs- und Sensibilisierungsprodukte, wie beispielsweise E-Learning-Angebote und Informationsmaterialien, für den Hochschulbereich bereitgestellt werden.

Die CSBW hat eine Partnerschaft mit der Dualen Hochschule Baden-Württemberg Heilbronn (DHBW) und stellt im Jahr 2023 zwei Studienplätze der Fachrichtung Wirtschaftsinformatik mit dem Schwerpunkt Software Engineering zur Verfügung. Die Ausbildungskooperation besteht gemeinsam mit dem Landeskriminalamt und der EnBW AG. Teil dieser Kooperation ist ein Austauschprogramm, in dessen Rahmen die dualen Studierenden insgesamt zwei Praxisphasen bei einem der Kooperationspartner verbringen dürfen. Die erste Rotationsphase startete im Dezember 2022, in welcher zwei Studierende der EnBW AG ihre Praxisphase bei der CSBW begonnen haben. Das Ziel ist, die Ausbildung der nächsten Generation von Cybersicherheits-Fachkräften aktiv zu begleiten und zu unterstützen sowie Synergien durch die Nähe der CSBW zum Hochschulbereich zu schaffen.

Interesse an einem DHBW-Studium bei der CSBW?
Unser Personal-Team beantwortet gerne Ihre Fragen.

2.7
CYBERSICHERHEITSÜBUNGEN

Der Bereich „Übungen“ der CSBW beschäftigt sich mit der Konzeption, Planung und Durchführung von internen und externen Übungen sowie situativen Handlungstrainings.

Übungen sind dabei kontrollierte und zielgerichtete Aktivitäten zur Überprüfung, Bewertung und Verbesserung von Prozessen oder Fähigkeiten. Es werden hierbei reale Ereignisse simuliert, um auf diese vorzubereiten und die Situationswahrnehmung zu verbessern. Übungen sind je nach Zielsetzung und Institution individuell zu planen und durchzuführen. Korrekt durchgeführt haben Übungen viele Vorteile und einen nachhaltigen Nutzen, wie beispielsweise die Steigerung der Cyber-Resilienz und der Reaktionsfähigkeit oder auch die Überprüfung von Prozessen, Planungen und der Technik.

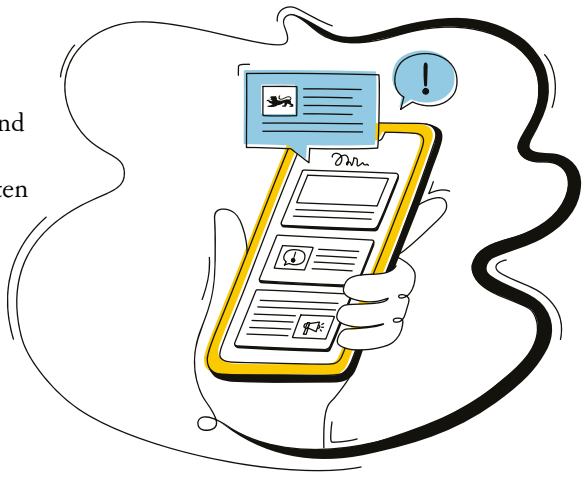
Auch die Planungs-Beteiligung an extern durchgeführten Übungen gehört zum Aufgabenbereich. Hierzu gehört beispielsweise die Länder- und Ressortübergreifende Krisenmanagementübung (Exercise) LÜKEX[3], welche regelmäßig alle zwei Jahre in Deutschland stattfindet.
Handlungstrainings stellen dagegen eine Form von Präventionsmaßnahme dar, bei der im Gegensatz zu Übungen ohne das Vorliegen eines konkreten Prozesses sensibilisiert beziehungsweise geschult und praktisch trainiert wird.

Der Fokus bei Handlungstrainings liegt auf praxisrelevanten Bedrohungen aus dem Cyber- und Informationsraum, denen die Beschäftigten der Zielgruppe bei ihrer täglichen Arbeit ausgesetzt sein können, wie zum Beispiel Phishing-E-Mails oder auch Social-Engineering-Angriffen. Durch die Steuerung von entsprechend realitätsnah ausgestalteten Aktionen, lernen die Beschäftigten diese Bedrohungen in unterschiedlicher Form kennen und trainieren gleichzeitig das korrekte Verhalten in solchen Situationen.

Dadurch kann das Handlungstraining ein nachhaltiges Bewusstsein für Gefahrensituationen sowie Handlungssicherheit schaffen. Zudem steigert es die Aufmerksamkeit für mögliche Bedrohungen und ermöglicht so eine frühzeitige Detektion durch aufmerksame Beschäftigte.

Ein erstes Handlungstraining wurde im zweiten Halbjahr pilotweise CSBW-intern geplant, durchgeführt und ausgewertet. Anhand der Ergebnisse konnte das Team weiteren Sensibilisierungsbedarf ableiten und wertvolle Erkenntnisse für ein nächstes Handlungstraining gewinnen.
Die Resonanz der Teilnehmenden war durchweg positiv und es konnten einige Aha-Momente bei den Beschäftigten erzielt werden.

[3] **LÜKEX-Übungen** sind so genannte strategische Krisenmanagementübungen (vgl. Homepage des BBK).



3.0
Handlungsfeld „Detektion und Reaktion“

Das Team der Abteilung „Detektion und Reaktion“ behält die Cybersicherheits-Lage im Blick und deckt mit ihrem Angebot ein breites Spektrum in diesem Bereich ab.
Die Abteilung beinhaltet das Lagezentrum mit dem Warn- und Informationsdienst und der Vorfallsteuerung. Ebenso sind die Vorfallbehandlung, die operative Sicherheitsanalyse sowie die Cyber-Ersthilfe BW dort angesiedelt. Alle Bereiche sind eng miteinander verzahnt und agieren unter dem Dach des CERT BWL.

3.1
DAS CERT DES LANDES BADEN-WÜRTTEMBERG

Das CERT BWL[4] ist Teil der CSBW und die zentrale Stelle für Cybersicherheit in der Landesverwaltung. Es ist auch zuständig für alle Dienststellen und Einrichtungen des Landes Baden-Württemberg. Die Cybersicherheitsagentur Baden-Württemberg (CSBW) hat das CERT im Sommer 2022 von der IT Baden-Württemberg (BITBW) übernommen und damit ihre Rolle als Schlüsselfigur für Cybersicherheit im Land gestärkt.

Zum CERT-Expertenteam gehören IT-Spezialistinnen und IT-Spezialisten aus verschiedenen Fachbereichen mit unterschiedlichen Qualifikationen und Schwerpunkten, wodurch ein breites Leistungsspektrum bei der Cybersicherheit abgedeckt wird. Das CERT BWL steht in stetigem Austausch mit Institutionen der Cybersicherheit auf Landes- und Bundesebene; unter anderem mit den CERTs der anderen deutschen Bundesländer und dem Bundesamt für Sicherheit in der Informationstechnik in Bonn, dem BSI.

Nach einem erfolgreichen Cyber-Angriff unterstützen die CERT-Expertinnen und -Experten der Vorfallbehandlung und der Vorfallsteuerung bei der Analyse von betroffenen Systemen und bieten bedarfsgerechte Beratung und Hilfe an. Bei Bedarf rückt das **M**obile **I**ncident **R**esponse **T**eam (MIRT) aus, um direkt am Einsatzort mit Rat und Tat zur Seite zu stehen.

Aufgaben des CERT BWL
Das Leistungsspektrum des CERT BWL wird stets den neuen Herausforderungen der IT-Bedrohungslage angepasst und weiter ausgebaut. Das aktuelle Aufgabengebiet des CERT BWL umfasst insbesondere:

- Beratung zu sicherheitsrelevanten Themen wie zum Beispiel Malware[5], SPAM- und Phishing-Mails, Angriffsvektoren oder Aktivitäten von Cyberkriminellen
- Präventive Handlungsempfehlungen zur Schadensvermeidung
- Hinweise auf Risiken für die Cybersicherheit, insbesondere zu Schwachstellen in der Informationstechnik
- Betrieb eines Warn- und Informationsdienstes, insbesondere Alarmierung der öffentlichen Stellen bei akuten Gefährdungen
- Analyse eingehender Vorfallmeldungen sowie die Erstellung daraus abgeleiteter Empfehlungen
- Empfehlungen von reaktiven Maßnahmen zur Schadensbegrenzung oder Schadensbeseitigung und zur Behebung von Sicherheitslücken
- Durchführung von operativen Schwachstellenscans
- Nach § 8b BSIG zentrale Kontaktstelle für Einrichtungen der Kritischen Infrastruktur (KRITIS)
- Unterstützung bei der Reaktion auf IT-Sicherheitsvorfälle aus dem CERT und bei Bedarf vor Ort mit einem mobilen Einsatzteam

Diese unterschiedlichen Aufgaben des CERT BWL werden im Bereich „Detektion und Reaktion“ innerhalb der verschiedenen Bereiche bearbeitet.

[4] **CERT =** Computer Emergency Response Team; **BWL =** Behördenkurzzeichen für Baden-Württemberg Land

[5] **Malware =** bösartige Sofware

3.2 KUNDENKREIS ABTEILUNG DETEKTION UND REAKTION

Die Abteilung „Detektion und Reaktion“ der Cybersicherheitsagentur Baden-Württemberg bedient mit ihren verschiedenen Bereichen einen umfassenden Kundenkreis, der in seiner gesamten Breite folgende Zielgruppen umfasst:

- Die Landesverwaltung Baden-Württemberg mit allen nachgeordneten Bereichen, die einen Personalkörper von circa 80.000 Mitarbeiterinnen und Mitarbeitern repräsentiert. Deren zentraler IT Dienstleister ist die BITBW mit einem Großrechenzentrum
- 1.101 Kommunen in Baden-Württemberg mit einem Personalkörper im mittleren sechsstelligen Bereich. Die Größe der Kommunen ist dabei sehr heterogen. Zentraler IT-Dienstleister mit Angeboten für die Kommunen ist die Komm.ONE
- Staatliche Schulen, Hochschulen und Universitäten des Landes
- Unternehmen mit Landesbeteiligung, in kommunaler Trägerschaft oder von besonderem öffentlichem Interesse
- die Öffentlichkeit als solche

3.3
DAS LAGEZENTRUM – WARN-/INFORMATIONSDIENST UND VORFALLSTEUERUNG

Das Lagezentrum ist eine zentrale Kommunikationsstelle der CSBW bei Themen der Cybersicherheit. Es setzt sich aus den beiden Bereichen Warn- und Informationsdienst sowie der Vorfallsteuerung zusammen und bündelt zudem den Informationsaustausch aller relevanten Akteurinnen und Akteure der Cybersicherheit in Baden-Württemberg.

Der Warn- und Informationsdienst (WID)
Der WID sammelt, analysiert und verteilt Informationen zu aktuellen Cybersicherheitsthemen, um die Cybersicherheit des Landes Baden-Württemberg zu erhöhen. Konkret bedeutet das:

- **Daten sammeln und analysieren**
  Aus öffentlichen und internen Quellen sammelt der WID permanent Informationen zu Themen wie Software-Schwachstellen, Angriffsvektoren von Hacker-Gruppierungen oder Malware-Kampagnen. Diese Informationen werden seitens des WID gesichtet, eingeordnet und bewertet. Dazu steht der WID in engem Kontakt zu den zuständigen Anlaufstellen der anderen Bundesländer und dem Bundesamt für Sicherheit in der Informationstechnik (BSI)
- **Informationen aufbereiten und verteilen**
  Die Hauptaufgabe des WID besteht darin, alle Akteurinnen und Akteure zu vernetzen, den Informationsfluss zu gewährleisten und die gewonnenen Informationen zielgruppengerecht aufzubereiten und weiterzugeben. So entstehen verschiedene Informationsprodukte wie zum Beispiel Warnmeldungen zu Software-Schwachstellen oder Handlungsanweisungen, um nicht Opfer aktueller Betrugskampagnen zu werden. Die Informationen werden aktuell noch per E-Mail an die verschiedenen Zielgruppen verteilt. Dieses Medium wird 2023 von der WID-Plattform abgelöst. Der WID bietet dann eine Plattform, auf die ausschließlich die berechtigten Empfänger der WID-Meldungen Zugriff haben. So lässt sich eine zielgruppengerechte, stets aktuelle und dynamische Informationsverteilung sicherstellen. Zudem können über die Plattform Sicherheitsvorfälle unkompliziert gemeldet werden.

Vorfallsteuerung
Nach einem Cyberangriff geraten die Betroffenen in Konfrontation mit vielen komplexen Fragen. Eine hohe Reaktionsgeschwindigkeit und die Fähigkeit, Entscheidungen mit kühlem Kopf treffen zu können, sind in solchen Krisen ausschlaggebend, um diese schnellstmöglich und erfolgreich überwinden zu können. In diesen Situationen unterstützt und berät die CSBW die Betroffenen individuell unter Berücksichtigung der fallspezifischen Besonderheiten.

Die Vorfallsteuerung der CSBW nimmt mit den Betroffenen für ein Erstgespräch Kontakt auf. Hierbei werden erste Informationen über die aktuelle Situation ausgetauscht. In der weiteren Zusammenarbeit wird gemeinsam ein Plan erarbeitet, wie die CSBW die Betroffenen unterstützen kann. Ziel dabei ist es, Orientierung zu geben und den Vorfall bestmöglich zu bewältigen. Den Schaden gering zu halten, ist hier besonders relevant. Die Vorfallsteuerung stellt nach dem Erstgespräch mit den Betroffenen den „Single Point of Contact“ für alle Beteiligten dar und steht den Betroffenen während der gesamten Krisensituation in beratender Rolle zur Seite. Besonders dann, wenn Entscheidungen getroffen werden müssen. Die Entscheidungsbefugnis und Verantwortung bleibt während der gesamten Fallbearbeitung bei den Betroffenen. Die CSBW nimmt eine unabhängige und objektive Perspektive ein, die die öffentlichen Stellen in Baden-Württemberg sowie die dazugehörigen Netze schützen will. In herausragenden Fällen unterstützt die CSBW auch darüber hinaus.

3.4
BEHANDLUNG VON CYBERSICHERHEITSVORFÄLLEN

Bei Bedarf wird die **Vorfallbehandlung** in die Unterstützung eingebunden. Dieser Bereich der Abteilung „Detektion und Reaktion“ bietet im Rahmen der Behandlung von Cyber-Sicherheitsvorfällen auch IT-Forensik als Dienstleistung an. Während einer IT-forensischen Untersuchung können idealerweise der Angriffsvektor und der Ablauf des Sicherheitsvorfalls rekonstruiert und aufgeklärt werden. Aus den Analyseergebnissen können Rückschlüsse auf die Ursache gezogen sowie Verbesserungsmaßnahmen für den weiteren Betrieb abgeleitet werden.

Hierbei hat das Team der CSBW den Anspruch, dass das Vorgehen über den gesamten Ablauf der Vorfallbehandlung den forensischen Grundsätzen entspricht, um ein qualitativ hochwertiges und belastbares Ergebnis zu erzielen. Das bedeutet:

- Jeder Schritt ist nachvollziehbar und wiederholbar
- Die Integrität der Daten ist jederzeit gewährleistet. Das heißt, die Daten wurden nicht nachträglich verändert
- Die Analyseergebnisse sind gerichtsverwertbar

Die Ergebnisse und Erkenntnisse der forensischen Analyse werden dabei in themenspezifischen Austausch-Runden geteilt. Diese Runden werden von der Vorfallsteuerung organisiert und koordiniert, sodass ein transparenter und reibungsloser Daten- und Informationsfluss zwischen allen Beteiligten gewährleistet ist.

Herausforderungen

Die verwendeten Werkzeuge bei Angriffen werden stets raffinierter: Viren und Trojaner passen sich an, um ihre Erkennungsmerkmale zu verschleiern. Dies bringt klassische Antiviren-Lösungen an ihre Grenzen. Bis vor einigen Jahren war es in den meisten Fällen noch ausreichend, im Nachgang die Daten aus den für die dauerhafte Speicherung ausgelegten Medien (beispielsweise Festplatten) zu sichern. Da moderne Angriffswerkzeuge ihre Spuren jedoch verwischen, ist deren Vorhandensein teilweise nur noch in flüchtigen Daten ersichtlich. Diese sind beispielsweise im Arbeitsspeicher ansässig und verschwinden nach jedem Neustart.
Doch auch der Wandel in der IT-Infrastruktur beinhaltet viele Herausforderungen: Systeme verlagern sich zunehmend von statischen Serverlandschaften hin zu dynamischen Cloud-Plattformen. Gerade in Zeiten des ortsunabhängigen Arbeitens ist es nicht immer einfach, den Überblick über das interne Netzwerk zu behalten. Die zunehmende Vernetzung und Mobilität erleichtern die tägliche Arbeit, vergrößern allerdings gleichzeitig auch die Angriffsfläche.

Abschluss eines Vorfalls

Ist die akute Gefahr eines Datenabflusses, einer Verschlüsselung oder weiterer Störungen überwunden, steht der Wiederaufbau der benötigten IT-Landschaft im Fokus. Hierbei unterstützt die CSBW die Betroffenen weiter und teilt ihre Erfahrung unter anderem zu Sicherheitskonzepten. Nach dem Abschlussgespräch zwischen allen Beteiligten zieht sich die CSBW aus der Bearbeitung des Cyberangriffs zurück.

3.5 VERBESSERUNG DER CYBERSICHERHEIT IN BADEN-WÜRTTEMBERG

Moderne Sicherheitsarchitekturen umfassen eine immer größer werdende Anzahl an Systemen zur Erkennung von Angriffen. Diese liefern zwar hilfreiche Informationen, erdrücken aber ihre Benutzerinnen und Benutzer in einer Datenflut. Die Bewertung, ob es sich bei auftretenden Warnungen um tatsächliche Alarme oder False-Positives[6] handelt, ist zeitaufwendig und komplex. Nur wer einen kühlen Kopf bewahrt und sich auf das Wesentliche konzentriert, behält hier den Überblick. Auch wenn Maßnahmen der IT-Forensik meist erst dann ergriffen werden, wenn bereits ein Vorfall geschehen ist: Ohne die daraus gewonnenen Erkenntnisse könnte eine Kompromittierung der Systeme jederzeit wieder stattfinden. Auf diese Weise tragen sie zum erklärten Ziel der CSBW bei, die Cybersicherheit im Land Baden-Württemberg nachhaltig zu verbessern.

Hierzu wurden mehrere Tätigkeitsfelder identifiziert:

- Übergreifende Workshops: Unter Moderation der CSBW werden mit den Fachexpertinnen und -experten der Kunden (unter anderem Rechenzentren) die jeweiligen Sicherheitsarchitekturen bewertet und mögliche Schritte zur Erhöhung des Sicherheitsniveaus beraten. Insbesondere wird hierdurch auch der fachliche Austausch gestärkt. Außerdem werden hier Bedarfe aus besonderen aktuellen Bedrohungslagen heraus erörtert, unter anderem die Überprüfung der Infrastrukturen auf aktuelle Indicators of Compromise (IoCs)[7] der CSBW
- Unterstützung der Kunden durch IT-Sicherheitsrahmenarchitektur: Die CSBW hat ein Architektur-Grundkonzept erarbeitet und stellt dieses ihren Kunden bei Bedarf zur Verfügung, damit diese ihre eigene Umsetzung der Handlungspunkte bewerten können. Hierbei unterstützt die CSBW mit ihrer Erfahrung zur Erhöhung des Sicherheitsniveaus
- Schwachstellen-Scans: Einige Schwachstellen-Scans konnten durch die CSBW bereits durchgeführt werden. Das Angebot befindet sich aktuell im weiteren Ausbau. Perspektivisch sollen Penetrationstests[8] und Red-Teamings[9] ebenfalls angeboten werden

[6] Ein **False-Positive** liegt vor, wenn bei einer Überprüfung fälschlicherweise eine positive Übereinstimmung mit vorher definierten Kriterien festgestellt wird, obwohl diese nicht gegeben ist.

[7] **IoCs** sind technische Informationen, die zur Detektion einer Infektion mit Schadsoftware oder einer anderweitigen Kompromittierung verwendet werden können (vgl. BSI-Glossar).

[8] Ein **Penetrationstest** ist ein gezielter, in der Regel simulierter, Angriffsversuch auf ein IT-System. Er wird als Wirksamkeitsprüfung vorhandener Sicherheitsmaßnahmen eingesetzt (vgl. BSI-Glossar).

[9] Ein **Red-Team** führt als beauftragte Dienstleistung echte Angriffe auf Infrastrukturen durch, um komplexe Einfallswege zu identifizieren.

3.6
CYBER-ERSTHILFE BADEN-WÜRTTEMBERG

Die Cyber-Ersthilfe Baden-Württemberg ist die zentrale Kontakt- und Meldestelle für Cybervorfälle in Baden-Württemberg. Hat beispielsweise ein kleines- oder mittelständisches Unternehmen den Verdacht, Opfer eines Cyberangriffs geworden zu sein, kann es den Service der Cyber-Ersthilfe Baden-Württemberg erreichen. Die Cyber-Ersthilfe Baden-Württemberg hilft bei der Einordnung der gemeldeten Cyber-Verdachtsfälle, gibt erste Hilfestellungen und nennt zielgruppenspezifische Anlaufstellen für weitere Unterstützungsleistungen. Im Anschluss an das Telefonat bekommen die Betroffenen eine zusammenfassende Erstanalyse, fallbezogene Handlungsoptionen sowie Informationen zu Anlaufstellen zur Verfügung gestellt.

Ablauf eines Beratungsgesprächs bei der Cyber-Ersthilfe Baden-Württemberg:
Um den Hilfesuchenden bestmöglich und effizient zu helfen, stellt die Cyber-Ersthilfe Baden-Württemberg ihnen verschiedene Fragen. Diese folgen einem bestimmten Ablauf, um die Informationen zielgerichtet aufzunehmen und schnelle Hilfe zu ermöglichen. Neben der reinen Erhebung der Stammdaten (unter anderem Kontaktdaten, Funktion der Institution, Sektor des Unternehmens oder Adresse) folgen Fragen zur Kategorisierung des Verdachtsfalls sowie der Schwere und des Schadens. Dadurch verschaffen sich die Mitarbeitenden der Cyber-Ersthilfe Baden-Württemberg während des Gesprächs einen schnellen Überblick über die vorliegende Situation und führen eine Erstbewertung durch. Basierend auf dieser Einordnung zeigen sie verschiedene Handlungsoptionen auf und benennen passende Anlaufstellen.

Gewährleistung der Vertraulichkeit
Angriffe auf die Cybersicherheit sind ein sensibles Thema. Die Befürchtung ist häufig, dass das Bekanntwerden eines Vorfalls je nach Kontext – neben finanziellen Schäden – auch zu Imageschäden bei der jeweiligen Organisation führen kann. Vor diesem Hintergrund ist die Vertraulichkeit der Daten ein besonders wichtiges Anliegen der Cyber-Ersthilfe Baden-Württemberg.
Die Verarbeitung der Daten erfolgt auf Grundlage von Art. 6 Abs. 1 lit. e, Abs. 3 Satz 1 lit. b DSGVO, § 12 Abs. 1, § 3 Abs. 1 Satz 2 Nrn. 1 und 6 CSG zum Zweck der Abwehr von Gefahren für die Cybersicherheit und zur Information und Beratung zur Cybersicherheit.

4.0
Informationen rund um die CSBW

Die Bandbreite der dargestellten Handlungsfelder innerhalb der Cybersicherheitsagentur Baden-Württemberg (CSBW) zeigt den Bedarf an hochqualifizierten Fachkräften auf. Die Gewinnung geeigneten Personals war in 2022 eine der großen Herausforderungen.
Dies vor allem aufgrund der aktuellen Arbeitsmarktlage sowie der Konkurrenz mit wirtschaftlich starken Unternehmen der Region. Das Kapitel gibt einen Überblick über die personelle Entwicklung und die Beschäftigtenstruktur der CSBW sowie die dafür notwendige Ausstattung mit Haushaltsmitteln.

4.1
PERSONAL UND HAUSHALT DER CSBW

Um den weiteren Aufbau der Cybersicherheitsarchitektur in Baden-Württemberg mit allen geplanten Themenfeldern bestmöglich voranzubringen, waren der Cybersicherheitsagentur im Haushaltsplan 2022 insgesamt 86,5 Stellen zugewiesen. Die ausschließliche Zuweisung als Beamtenstellen macht dabei den hohen Stellenwert der Cybersicherheit für das Land Baden-Württemberg deutlich. Zum Ende des Kalenderjahres 2022 waren davon insgesamt 60 Stellen besetzt.

Der Anteil der Beamtinnen und Beamten an der Gesamtbelegschaft betrug zum Jahresende 46,7 %. Ein nicht unerheblicher Teil der Fachkräfte und IT-Expertinnen und -Experten im tariflichen Angestelltenverhältnis konnte von Unternehmen der freien Wirtschaft gewonnen werden. Auch das ist ein Indikator für das große Interesse am Thema Cybersicherheit und seiner Relevanz auf dem Arbeitsmarkt sowie an der CSBW als attraktivem öffentlichen Arbeitgeber.

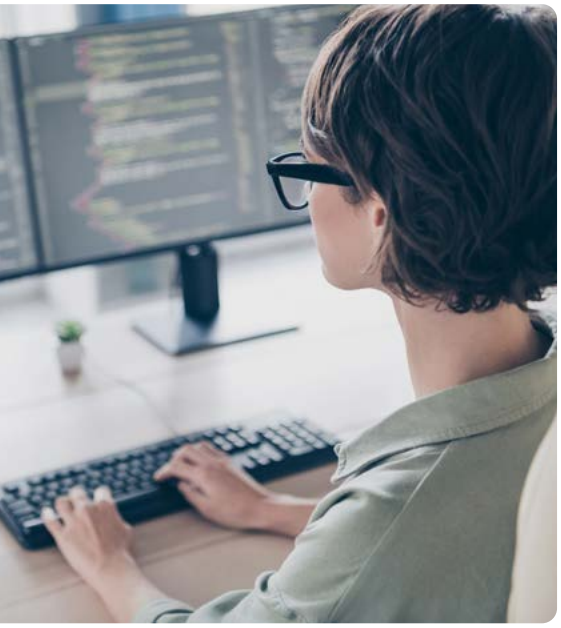
Zum 31.12.2022 waren 34 von den 60 Beschäftigten der CSBW dem höheren Dienst, 21 dem gehobenen Dienst und fünf dem mittleren Dienst zugeordnet, beziehungsweise jeweils gleichwertig beschäftigt.

Die CSBW hat einen Anteil von 46,7 % weiblicher Beschäftigter an der Gesamtbelegschaft. Und das Thema Chancengleichheit steht bei der CSBW ebenso im Fokus wie die Gestaltung eines Arbeitsumfeldes, das die Vereinbarkeit von Familie und Beruf in bestmöglicher Art und Weise unterstützt. So wird beispielsweise allen Beschäftigten die Möglichkeit geboten, einen nicht unwesentlichen Teil der Arbeitszeit remote[9] zu erbringen. Die benötigte IT-Ausstattung wurde zur Verfügung gestellt. Zum Stichtag betrug die Teilzeitquote 13,3 %.

Mit Ablauf des Kalenderjahres stieg die Anzahl der Beschäftigten mit Schwerbehinderung beziehungsweise anerkannter Gleichstellung auf insgesamt drei. Das entspricht einem Anteil von 5 % der Gesamtbeschäftigtenzahl.

Arbeitsverhältnisse im Rahmen einer geringfügigen Beschäftigung bestanden im Jahr 2022 nicht.

Alle freien und besetzbaren Stellen der CSBW sind zur Wieder- oder erstmaligen Besetzung vorgesehen. Insgesamt wurden im abgelaufenen Kalenderjahr 29 Stellenbesetzungsverfahren durchgeführt. Auch wenn nicht alle der ausgeschriebenen Stellen tatsächlich besetzt werden konnten, so bildet die Diversität der fachlichen Qualifikationen aller Mitarbeitenden eine hervorragende Basis für die weitere Entwicklung der CSBW an sich und deren Leistungsspektrum. Dass die CSBW Stellen nicht besetzen kann, liegt vor allem an der geringen Zahl von Bewerbungen und der mangelnden Eignung der Bewerberinnen und Bewerber. Dies betraf insbesondere die Stellenausschreibungen im IT-Bereich sowie im Bereich der Nachwuchsgewinnung im Rahmen des DHBW-Studiums.



Um die Zahl und Qualität von Bewerbungen zu erhöhen, wurde der Großteil der Besetzungsverfahren erfolgreich auf Bewerberinnen und Bewerber im Bereich der Tarifbeschäftigung ausgeweitet.

Ein weiterer wesentlicher Fokus – neben der Gewinnung von Fachpersonal – lag auf der Definition von Strukturen und Prozessen der Abteilung „Querschnitt". Mit dem operativen Start der CSBW wurden alle notwendigen Aufgaben beschrieben und zugewiesen. Mit zunehmendem Personalaufbau wurde ein strukturierter Onboarding-Prozess definiert und umgesetzt, der eine schnelle und professionelle Einarbeitung neuer Kolleginnen und Kollegen sowie die Umsetzung der notwendigen Projekte in den Fachabteilungen unterstützt. Die Optimierung und Standardisierung der personalinternen Verfahren erfolgt kontinuierlich. Mit Beginn des Jahres 2023 ist der Personalbereich vollständig besetzt.

Der Aufbau des Finanz- und Haushaltsbereichs wurde im Mai 2021 mit nur einem Mitarbeitenden gestartet. Mit mittlerweile drei Mitarbeitenden in diesem Bereich ist der Aufbau fast abgeschlossen. Sowohl bei der Planung des Haushalts, aber auch bei Projekten wie dem landesweiten SAP-Projekt (Repro), wurde das Team bereits eingebunden. Innerhalb kurzer Zeit wurden entsprechende Systeme und Prozesse, wie die Rechnungsbearbeitung (E-Rechnung), Dienstreisemanagement oder auch ein internes Verwaltungssystem einschließlich notwendiger Dokumentationen aufgebaut.

Für das Haushaltsjahr 2022 wurde für die CSBW ein eigenes Kapitel zur selbstständigen Bewirtschaftung im Landeshaushalt geschaffen. Das Kapitel 0308 aus dem sich die CSBW ab 2022 finanziert, wurde im Haushaltsplan für das Jahr 2022 mit einem Gesamtbudget in Höhe von 8.754.700,00 € ausgestattet. Auch die künftige Finanzierung ist durch den Doppelhaushalt 2023/24 gesichert und verschafft der CSBW eine große Planungssicherheit.

Im Rahmen der Haushaltsplanungen für die Jahre 2023 und 2024 wurde eine Erhöhung der Haushaltsmittel beschlossen, die vor allem dem Personalausgabenbudget zu Gute kommt. Somit erhöhen sich die verfügbaren Haushaltsmittel für das Jahr 2023 auf insgesamt 8.803.300,00 € und für das Jahr 2024 auf insgesamt 8.806.400,00 €. Der weitaus größte Anteil mit ca. 70 % entfällt dabei auf die Kosten für das Personal.

Die Verteilung des Budgets auf Personal-, Sach- und Investitionsmittel wird in folgender Übersicht deutlich:

Haushalt	2022	2023	2024
Personal	6.151.200 €	6.289.500 €	6.289.500 €
Sachausgaben	2.333.500 €	2.254.000 €	2.256.800 €
Investitionen	270.000 €	259.800 €	260.100 €
Summe	8.754.700 €	8.803.300 €	8.806.400 €

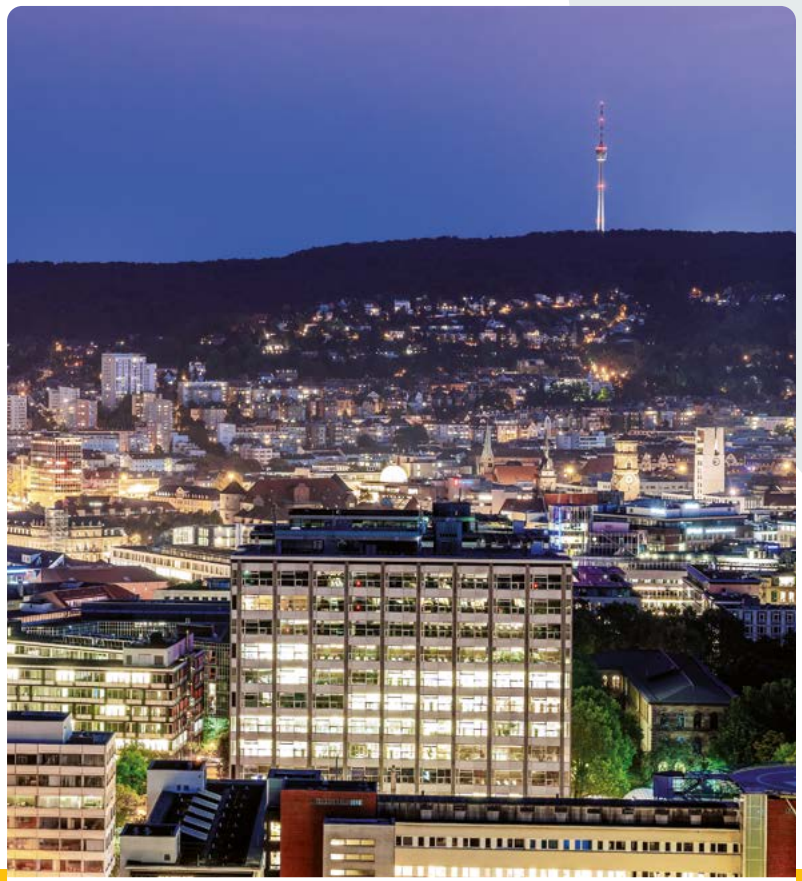
4.2
STANDORT DER CSBW

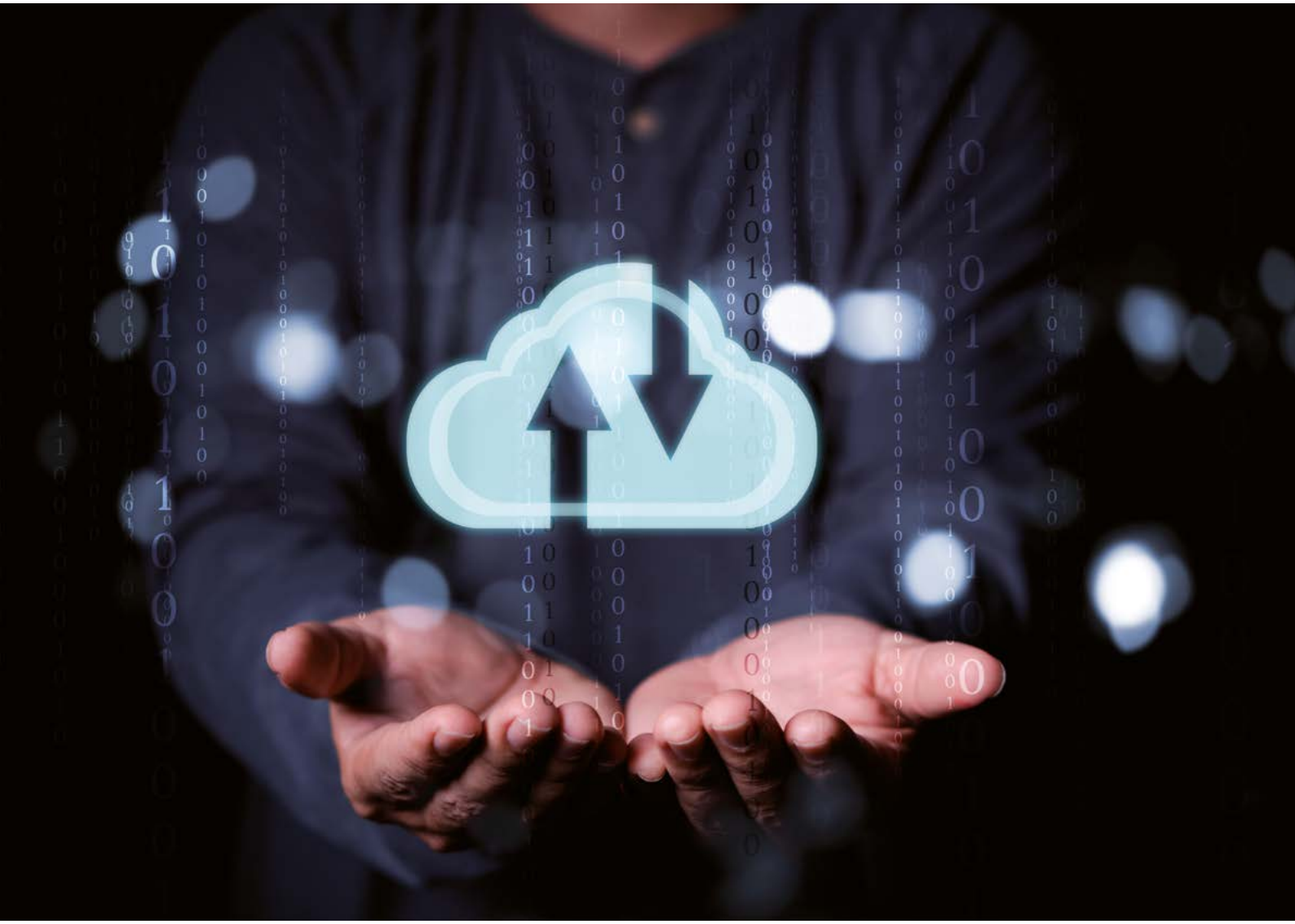
Der Einzug der CSBW in das neue Dienstgebäude in Bad Cannstatt, gemeinsam mit dem Landeskriminalamt und dem Präsidium Technik, Logistik, Service der Polizei des Landes Baden-Württemberg, wird nach derzeitigem Planungsstand zur Jahresmitte 2024 realisiert werden können.

Bis dahin sind die Mitarbeitenden der CSBW in Interimsräumlichkeiten des Umweltministeriums Baden-Württemberg untergebracht. Diese Räumlichkeiten ermöglichen bereits jetzt, in Vorbereitung auf das geplante moderne Bürokonzept in den neuen Räumen, eine flexible Nutzung der Arbeitsplätze durch die Umsetzung eines Desk-Sharing-Konzeptes. Ergänzend dazu wird die Möglichkeit des Homeoffice genutzt und flexibel umgesetzt.

Die effiziente Umsetzung aller Anforderungen an den neuen, finalen Standort der CSBW wird durch eine dafür ins Leben gerufene Projektorganisation gewährleistet. Insgesamt besteht die Projektorganisation aus sechs Teilprojekten und einer Geschäftsstelle. Die Teilprojekte umfassen die Themen Büroorganisation, IT-Infrastruktur und technische Ausstattung, Mobiliar und Standardausstattung in Büros und Besprechungsräumen, Software und Kollaborationstools, Finanzen und Haushalt sowie das Thema New Work[10].

[10] Unter **New Work** versteht man die Gesamtheit der modernen und flexiblen Formen der Arbeit beziehungsweise der Arbeitsorganisation.





5.0
Resümee und Ausblick

Das Jahr 2022 war sowohl hinsichtlich der Entwicklungen im Bereich der Cybersicherheit wie auch für die Cybersicherheitsagentur Baden-Württemberg (CSBW) als neu gegründete Behörde herausfordernd. Für das kommende Jahr erwartet die CSBW einen weiteren, deutlichen Fortschritt bei der Umsetzung von Maßnahmen in den geplanten Handlungsfeldern. Außerdem soll eine kontinuierliche Fortentwicklung der Organisation erfolgen, um den Herausforderungen noch besser begegnen zu können.

Rückblickend hat das Land Baden-Württemberg mit der CSBW einen wichtigen neuen Akteur gewonnen. Bereits im ersten Jahr wurde einiges bewegt! Eine Dynamik, die wir als CSBW-Team auch in das kommende Jahr mitnehmen wollen.

Mit dem Ende des Jahres 2022 ging auch das erste Jahr der CSBW als eigenständige, operativ tätige Landesoberbehörde zu Ende. Neben der noch zu bewältigenden Aufbauarbeit und der kontinuierlichen Einstellung und Integration der neuen Mitarbeitenden in die bestehenden Teams und Strukturen, waren der Angriffskrieg Russlands in der Ukraine sowie die Ausläufer der Pandemie die wesentlichen Herausforderungen für die CSBW.

Die bereits zuvor angespannte Cybersicherheitslage in Deutschland spitzte sich, wie auch der im Oktober 2022 veröffentlichte BSI-Bericht zur „Lage der IT-Sicherheit in Deutschland" darlegt, in Folge des Kriegs in der Ukraine weiter zu – der russische Angriffskrieg gegen die Ukraine wird auch im Cyberraum geführt. Die Cyberbedrohungslage für Deutschland war und ist insgesamt unverändert hoch. Nach Einschätzung der CSBW gilt dies auch für Baden-Württemberg. Hier wurden insbesondere im Bereich des Landesverwaltungsnetzes die Sicherheitsmaßnahmen deutlich verstärkt.

Jede dieser Herausforderungen hat gezeigt, dass das Modell einer modernen und agil arbeitenden Behörde unumgänglich ist, wenn man sich auf den schnelllebigen und komplexen Feldern der Cybersicherheit erfolgreich bewegen und einen aktiven Beitrag zu einem sichereren Cyberraum leisten möchte. Somit ist es nicht minder der Anspruch der CSBW auch im Jahr 2023 ihr Angebot den Anforderungen entsprechend weiter auszubauen, um steigenden Risiken adäquat zu begegnen.

Die Cyberangriffe auf Unternehmen, Behörden, Hochschulen, aber beispielsweise auch auf Krankenhäuser und Einrichtungen der kritischen Infrastruktur werden sicherlich nicht weniger werden – im Gegenteil. Gleichzeitig werden nach Ansicht der Cybersicherheitsexpertinnen und -experten aus den Bereichen Detektion und Reaktion insbesondere immer weiter verfeinerte Angriffsarten und professionalisierte Gruppierungen im Bereich Ransomware-as-a-service die Teams in der CSBW weiterhin fordern.

Gleichzeitig wird die CSBW im Bereich der Prävention mit weiteren Elementen aus der Sensibilisierungskampagne, dem Roll-out der Lernplattform und dem Beratungskonzept für Kommunen konkrete Angebote bereitstellen, um auf die Risiken im Cyberraum aufmerksam zu machen und das Bewusstsein für diese weiter zu schärfen. Zudem wird die CSBW zur Sicherung der Innovationskraft das Feld der Hochschulkooperationen weiter ausbauen.

Nicht zuletzt plant die CSBW ihre Sichtbarkeit weiter zu erhöhen und ihre Rolle als wichtiger Akteur im Bereich der Cybersicherheit zu festigen. Ein wichtiger Meilenstein wird hierbei der Launch der CSBW-Website im ersten Halbjahr 2023 sein. Darüber hinaus baut die CSBW den Austausch mit ihren **Stakeholdern**[11] und Kunden auf Kommunal-, Landes- und Bundesebene stetig aus und forciert gemeinsam mit dem Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg auch den Austausch auf internationaler Ebene.

Die folgenden Zitate vermitteln einen Eindruck über die Wirkung der CSBW, die wir statt eines Schlussworts für sich sprechen lassen wollen.

[11] Mit **Stakeholder** werden alle Anspruchsgruppen oder Personen bezeichnet, für die es aufgrund ihrer Interessenlage von Belang ist, wie eine bestimmte Organisation sich verhält.

Stefan Krebs, CIO/CDO – Beauftragter der Landesregierung für Informationstechnologie:

Mit der Cybersicherheitsagentur Baden-Württemberg ergänzen wir unsere Cybersicherheitsarchitektur passgenau. Wir spüren tagtäglich, dass wir uns gegen die Gefahren im Cyberraum schützen und wappnen müssen, und genau das tun wir mit unserer CSBW. Ich bin stolz auf die bundesweite Vorreiterrolle, die wir schon jetzt einnehmen und auch in Zukunft weiter einnehmen wollen. Mit der CSBW als Herzstück der Cybersicherheitsarchitektur im Land leisten wir weiterhin Pionierarbeit, um auf die starke Zunahme von Cyberangriffen zu reagieren. Mein Dank gilt den Kolleginnen und Kollegen, die sich seit Anbeginn für dieses wichtige Projekt engagieren.

Jochen Wellhäußer, Informationssicherheitsbeauftragter (CISO) der Landesverwaltung BW:

Es gilt zunächst, die von der CSBW geschaffenen, präventiven Angebote wie Lageinformationen, Handlungsempfehlungen sowie Schulungs- und Sensibilisierungsangebote so weit wie möglich Dritten nutzbar zu machen und darüber hinaus Angriffen und Vorfällen mit technischen Analysen und Schwachstellenscans zuvor zu kommen. Im Falle eines Falles – also bei der Bewältigung von Angriffen und ihren Folgen – unterstützt die CSBW maßgeblich die betroffenen Institutionen, um möglichst schnell und zuverlässig wieder in einen „Normalbetrieb“ zu kommen.

Davide Licht, Bürgermeister Stadt Burladingen:

Leider wurde auch die Stadt Burladingen Ziel eines Cyber-Angriffs. In dieser unbekannten Situation konnten meine Mitarbeitenden und ich uns von Beginn an auf die fachkundige und tatkräftige Unterstützung durch die CSBW verlassen. Direkt nach dem Erstkontakt wurden wir mit hilfreichen Tipps und Handlungsempfehlungen unterstützt, sodass wir anhand eines klaren Leitfadens wussten, was zu tun ist und die Mitarbeitenden der EDV-Abteilung sich zielführend der Wiederherstellung unserer Systeme widmen konnten. Schnell, freundlich und vor allem unbürokratisch – einfach unkompliziert – stand uns die CSBW im Team mit Rat und Tat zur Seite. Ein mehr als angenehmer Kontakt und ein absolut vorbildliches Vorgehen einer Landesbehörde, das beispielgebend für modernes, pragmatisches Verwaltungshandeln und die Stabsarbeit steht!

Mein erster Eindruck von der CSBW:

Ich wurde bei der CSBW von allen herzlichst willkommen geheißen, wie noch nie zuvor, und fühle mich hier endlich angekommen.
(Mete, seit Mitte August 2022 bei der CSBW)

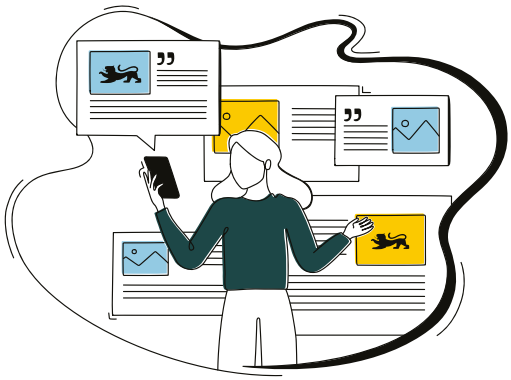
Ich war erstaunt, wie gut der erste Tag vorbereitet war.
Nachdem organisatorische Themen erledigt waren, wurde ich mit Offenheit und Herzlichkeit in meiner neuen Abteilung begrüßt.
(Nadine, seit September 2022 bei der CSBW)

Das zeichnet die CSBW aus:

Da ich bereits eine gewisse Behördenerfahrung habe, zeichnet sich die CSBW aus meiner Sicht besonders durch äußerst motivierte Mitarbeitende aus, welche auch stets bereit sind, sich über das übliche Maß hinaus zu engagieren.
(Martin, seit September 2021 bei der CSBW)

Abwechslungsreiche und verantwortungsvolle Aufgaben in einem interdisziplinären Team!
(Rolf, seit Oktober 2021 bei der CSBW)

Ein Fokus auf fachlicher Weiterentwicklung, New Work-Ansätze und die Herausforderung, das Land gegen Bedrohungen aus dem Cyberraum zu schützen – das zeichnet die CSBW aus.
(Simon, seit August 2022 bei der CSBW)



In den letzten beiden Jahren hat sich in der CSBW viel getan.

Wir arbeiten nicht mehr an abstrakten Prozessen, sondern entwickeln Prozesse weiter. Vorfälle werden reflektiert und die Erkenntnisse fließen in die Weiterentwicklung ein.
(Jasmin, seit März 2021 bei der CSBW)

Die Entwicklung ist zum einen natürlich in der reinen Anzahl an Personen, die mittlerweile für die CSBW arbeiten, zu erkennen. Ohne das gesamte Team wäre die CSBW nicht da, wo sie heute steht. Zum anderen aber auch an den mittlerweile vielen erfolgreich abgeschlossenen kleinen und großen Projekten, den geknüpften Kontakten, den fertiggestellten Produkten und den bereits erfolgreich gemeisterten Vorfällen. Die CSBW an sich wird dadurch immer greifbarer. (Nadine, seit Dezember 2020 bei der CSBW)

Die aktuelle Cyber-Sicherheitslage zeigt, dass es gut, richtig und wichtig war, die CSBW zu gründen. Mit einem ausgezeichneten Team haben wir dieses Jahr bereits über 50 Cybersicherheitsvorfälle bearbeitet, hierunter auch Wesentliche wie das Klinikum Friedrichshafen, die Stadtverwaltungen Schriesheim sowie Burladingen, die Hochschulen Heilbronn sowie Ulm. Ohne die CSBW wären alle Betroffenen auf sich gestellt gewesen und es wären für den Steuerzahler jeweils hohe Summen für externe Dienstleister entstanden. Durch die Bündelung der Expertise in der CSBW kann ad hoc jedem Betroffenen kostenneutral weitergeholfen werden.
(Björn, seit Ende September 2021 bei der CSBW)

An der CSBW gefällt mir besonders ...

Ich arbeite besonders gerne bei der CSBW, da wir hier einen super Zusammenhalt haben und hier moderne Behörde gelebt wird.
(Lisa-Marie, seit Juni 2022 bei der CSBW)

Dabei sein zu dürfen, wie etwas Neues entsteht, war für mich schon immer etwas ganz Besonderes. Zu einem vorwärts gehört auch immer wieder ein Innehalten, um zu überprüfen und um nachjustieren zu können.
Genau diesen offenen Prozess üben wir jeden Tag in unserem Team aus.
Das macht Spaß und es entstehen tolle Produkte. Ich bin sehr gerne dabei!
(Heidrun, seit April 2021 bei der CSBW)

IMPRESSUM

Herausgegeben von der
Cybersicherheitsagentur Baden-Württemberg
Willy-Brandt-Straße 41
70173 Stuttgart

Grafische Umsetzung
büro punkt. für visuelle Gestaltung
Hauptstraße 46
73098 Rechberghausen

Druck
Bader Druck GmbH
Daimlerstraße 15a
73037 Göppingen

Bildnachweise:
Wenn nicht anders angegeben, liegt das Copyright der verwendeten Grafiken und Fotografien bei der Cybersicherheitsagentur Baden-Württemberg

S. 1 + 44 Servers data center room ... © sdecoret - stock.adobe.com
S. 2 ai technology ... © issaronow - stock.adobe.com
S. 11 Office teamwork situation ... © Alex from the Rock - stock.adobe.com
S. 12 Micro CPU generates plasma curves © klss777 - stock.adobe.com
S. 14 Integrated circuit ... Fingerprint login ... © Shuo - stock.adobe.com
S. 18 Girl ... hiding behind her laptop notebook ... © EdNurg - stock.adobe.com
S. 21 Username and password ... © calypso77 - stock.adobe.com
S. 23 Neural network 3D illustration ... © vegefox.com - stock.adobe.com
S. 24 Trainer makes presentation ... © fizkes - stock.adobe.com
S. 26 A computer popup box screen warning ... © James Thew - stock.adobe.com
S. 29 Concept of virtual environment ... © makstorm - stock.adobe.com
S. 31 Office woman ... cyber security mockup ... © peopleimages.com - stock.adobe.com
S. 32 Concept of cyber security ... © Thapana_Studio - stock.adobe.com
S. 33 Young handsome male technical support agent ... © Bojan - stock.adobe.com
S. 34 Programmers cooperating brainstorming ... © NDABCREATIVITY - stock.adobe.com
S. 36 Student girl system administrator ... © deagreez - stock.adobe.com
S. 37 Stuttgart ... © Manuel Schönfeld - stock.adobe.com
S. 38 male hand holding cloud technology ... © kwanchaift - stock.adobe.com

Redaktionsschluss: 31. Dezember 2022

MIT UNS. MIT SICHERHEIT.

www.cybersicherheit-bw.de