Baden-Württemberg

Jahresbericht 2024

DER CYBERSICHERHEITSAGENTUR BADEN-WÜRTTEMBERG

CSBW

CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG

Jahresbericht 2024

DER CYBERSICHERHEITSAGENTUR
BADEN-WÜRTTEMBERG

CSBW
CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

CYBERSICHERHEIT-BW.DE

Vorwort

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

an jedem Ort und zu jeder Uhrzeit miteinander vernetzt zu sein, das zeichnet unsere heutige Welt aus. Ein Leben ohne das Internet können wir uns heute gar nicht mehr vorstellen. Sei es das Austauschen von Nachrichten, die schnelle Überweisung per Online-Banking, das Steuern wichtiger Anlagen aus der Ferne oder das Anmelden eines Autos bei der Zulassungsstelle: Bei all dem erleichtert das Internet unser Leben.

Diese Möglichkeiten gehen freilich auch mit erheblichen Risiken und Gefahren einher. Allein in Deutschland entsteht durch Cyberangriffe, Spionage, Sabotage und deren Folgen pro Jahr ein Schaden im deutlichen dreistelligen Milliardenbereich.

Als Land haben wir deshalb schon sehr frühzeitig das Thema Cybersicherheit scharf in den Blick genommen und ganz gezielt Pionierarbeit geleistet. Bereits 2021 haben wir mit dem Aufbau unserer Cybersicherheitsagentur Baden-Württemberg, der CSBW, Maßstäbe gesetzt und bereits zuvor die digitale Sicherheitsarchitektur im Land vollkommen neu aufgestellt. Denn die Sicherheit des 21. Jahrhunderts, das ist insbesondere auch die Sicherheit im digitalen Raum.

Dafür hat die CSBW auch im vergangenen Jahr mit ihrer sehr wertvollen Arbeit jede Menge geleistet. Sie hat bei mehr als 500 Verdachtsfällen und Cybersicherheitsvorfällen in unterschiedlichen Fallkonstellationen und Schweregraden beraten oder unterstützt. Von der Untersuchung von Anomalien und merkwürdigem Systemverhalten über die Prüfung von verdächtigen E-Mails und Identitätsdiebstählen bis hin zur Bewältigung von Angriffen mit Verschlüsselungs-Software – die Arbeit der CSBW ist so vielfältig wie die Mitarbeiterinnen und Mitarbeiter, die hier wirken. In insgesamt drei Fällen unterstützte die CSBW darüber hinaus auch vor Ort mit ihrem mobilen Krisenreaktionsteam, dem Mobile Incident Response Team. Damit gewährleistete die CSBW Unterstützung in den Momenten, in denen sie am meisten gebraucht wurde.

Dabei bergen die Top 3 der durch die CSBW im Jahr 2024 erfassten Angriffsarten keine Überraschungen, wenngleich die Cyberkriminellen ihre Vorgehensweisen stetig weiter verfeinern und erkennbar professionalisieren. So sind Passwort-Kompromittierungen, Phishingversuche und E-Mail-Betrug erneut unter den häufigsten Angriffsarten. Flankierend setzt hier auch das ganzheitliche Präventionskonzept der CSBW an: Mit über 120 Schulungen wurden im vergangenen Jahr mehr als 4.250 Personen, insbesondere aus der Landesverwaltung und den Kommunen, für die vielfältigsten Gefahren des Cyberraums sensibilisiert.

Bei all dem wird klar: Sicherheit gibt es nicht zum Nulltarif. Die CSBW ist unsere Investition in die digitale Sicherheit unseres Landes. Sie wirkt aus Baden-Württemberg, für Baden-Württemberg und ist dabei auch in Zukunft unser Angebot für die öffentliche Verwaltung aller Ebenen im Land, für die Bürgerinnen und Bürger – und den Mittelstand, das Handwerk und Familienbetriebe.

Den Mitarbeiterinnen und Mitarbeitern der CSBW gilt hierfür mein herzlichster Dank. Mit ihrer Expertise, ihrer großen Einsatzbereitschaft und engagierten Arbeit tragen sie entscheidend zur Absicherung des Cyberraums bei.

Herzliche Grüße
Ihr

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

Grußwort

Liebe Leserinnen und Leser,

die Cybersicherheitsagentur Baden-Württemberg (CSBW) hat in ihrem dritten Jahr als Landesoberbehörde erneut Meilensteine gesetzt. Dieser Jahresbericht gibt Auskunft über die CSBW und die vielfältige Arbeit unserer Mitarbeiterinnen und Mitarbeiter. Ich freue mich, dass ich Sie in diesem Jahr zum ersten Mal als neue Präsidentin der CSBW über die geleistete Arbeit informieren darf.

Für 2024 haben wir eine erneute Zunahme der abstrakten wie auch der konkreten Gefahren im Cyberraum registriert. Ein Lagebild, das sich mit den Erkenntnissen anderer Cybersicherheitsbehörden deckt. Neben der steigenden Professionalisierung von Cyberkriminellen sehen die zuständigen Sicherheitsbehörden zunehmend auch staatliche Akteure, die offensiv im Cyberraum agieren. Lesen Sie dazu gerne unser ausführliches Lagebild.

Als CSBW denken wir Cybersicherheit ganzheitlich und bereichsübergreifend. Das bedeutet, dass wir das Themenspektrum aus Prävention, Detektion und Reaktion miteinander verknüpfen. Denn nur so kann Cybersicherheit gelingen und in einem dynamischen Umfeld bestehen. Das zeigt sich in unseren Angeboten und in unserer Organisationsstruktur, aber auch in unserer Vernetzung mit anderen Akteurinnen und Akteuren. Was uns alle verbindet, das ist die Motivation, unseren Beitrag zur Cybersicherheit im Land zu leisten – gemeinsam.

Mit dem Ausbau unserer Präventions- und Sensibilisierungsangebote folgten wir auch 2024 dem Motto, dass Wachsamkeit und das Wissen um die Gefahren der beste Schutz sind. Daneben konnten wir auch in unserem Detektionsbereich die Angebote des Warn- und Informationsdiensts sowie des Computer Emergency Response Teams (CERT) des Landes verstetigen und erweitern. Sollte es doch zu einem Cybersicherheitsvorfall kommen, stehen wir auch reaktiv verlässlich an der Seite der Betroffenen. Dafür halten wir Expertise und Kapazitäten im Bereich des Vorfallmanagements, der Krisenkommunikation sowie der Vorfallbehandlung vor, insbesondere auch mit unserem Mobile Incident Response Team (MIRT).

Ein Cybersicherheitsvorfall kann jederzeit geschehen. Umso wichtiger ist es, möglichst gut vorbereitet zu sein. Dafür steht die CSBW der Landesverwaltung, den Behörden und Kommunen in Baden-Württemberg mit einem Rundum-sorglos-Paket zur Seite. Aber auch Bürgerinnen und Bürger sowie die Unternehmen im Land unterstützen wir mit Angeboten im Präventionsbereich und unserer Cyber-Ersthilfe BW, die rund um die Uhr erreichbar und für jeden kostenlos ist.

Für uns steht fest: Cybersicherheit ist kein Alleingang und kommt nicht von alleine. Auch in Zukunft werden wir uns kontinuierlich an die aktuellen Bedrohungslagen anpassen und Hand in Hand mit unseren Partnerinnen und Partnern für die Sicherheit im Cyberraum einstehen müssen. Dafür bauen auch wir weiterhin ganz gezielt unser Angebotsportfolio aus. Gemeinsam machen wir Baden-Württemberg so – jeden Tag aufs Neue – noch ein Stückchen sicherer. Das ist unser Auftrag, das ist unsere Motivation, das ist unser Versprechen.

In diesem Sinne wünsche ich Ihnen für die Lektüre des Jahresberichtes 2024 spannende Eindrücke und bereichernde Erkenntnisse. Lassen Sie uns auch in den kommenden Jahren an diese Erfolgsgeschichte anknüpfen.

Herzliche Grüße
Ihre

Nicole Matthöfer
Präsidentin der Cybersicherheitsagentur Baden-Württemberg

Inhalt

1. Die Cybersicherheitsagentur Baden-Württemberg in 2024

1.1 Behördenaufbau und Handlungsfelder der CSBW

Zum 31. März 2024 verabschiedete sich der Präsident Ralf Rosanowski nach einer über 40-jährigen Tätigkeit für das Land Baden-Württemberg bei der Polizei, in der Innenverwaltung und zuletzt bei der CSBW in den Ruhestand. Frau Dr. Warken hat zu Beginn des Jahres 2024 ihren Dienst bei der CSBW ebenfalls beendet.

Zum 28. Mai 2024 trat Nicole Matthöfer die Nachfolge an der Spitze der CSBW an und führt seitdem die Dienststelle als Präsidentin. Aktuell bildet die Präsidentin gemeinsam mit den Abteilungsleitungen sowie der Stabsleitung die Leitungsrunde der CSBW.

An die Präsidentin eng angebunden ist der Stab der CSBW, der für die Themenbereiche Grundsatz und Strategie, die politische Koordination sowie Kommunikation und Öffentlichkeitsarbeit verantwortlich ist.

Die CSBW gliedert sich in drei Abteilungen: Prävention, Detektion und Reaktion sowie Querschnitt.

Das Sachgebiet Sensibilisierung & Schulung der Abteilung Prävention befasst sich mit der Entwicklung und Umsetzung von Schulungs- und Sensibilisierungsangeboten sowie der CSBW-Lernplattform. Das Sachgebiet Beratung & Innovationsmanagement hat in 2024 überwiegend Kommunen und Hochschulen beraten und setzte sich mit technologischen Innovationen auseinander. Das Sachgebiet Informationssicherheit ist für das Informationssicherheitsmanagementsystem der CSBW zuständig.

Im Lagezentrum der Abteilung Detektion & Reaktion laufen die Fäden zusammen, hier werden Warnmeldungen und Sicherheitshinweise erstellt sowie Lageberichte verfasst. Außerdem ist hier die Vorfallsteuerung angesiedelt. Die Vorfallbehandlung untersucht bei Cybersicherheitsvorfällen die betroffenen Systeme und unterstützt mit forensischen Analysen, falls nötig mit einem MIRT*. Das Sachgebiet Operative Sicherheitsanalyse befasst sich unter anderem mit Schwachstellenscans. Das Sachgebiet Cyber-Ersthilfe betreibt die 24/7-Hotline der CSBW sowie die weiteren Melde-Kanäle. Das Sachgebiet Steuerungsgruppe ist für die abteilungsinterne Steuerung, die Fachadministration sowie die Entwicklung von Fachanwendungen zuständig.

Das Sachgebiet Personal der Abteilung Querschnitt ist für die Personalgewinnung, Personalentwicklung und die Personalverwaltung zuständig. Dem Sachgebiet Haushalt obliegt die Verantwortung für den Haushalt, das Rechnungswesen sowie Vergaben und Beschaffung. Im Sachgebiet Recht & Organisation sind das Justiziariat, die Registratur, die Servicestelle und die IT-Administration der CSBW angesiedelt.

Informationssicherheitsbeauftragter sowie Geheim- und Sabotageschutzbeauftragter berichten direkt an die Präsidentin.

Für die Cybersicherheit in Baden-Württemberg ist ein umfassender Ansatz erforderlich, der alle Aspekte – von der Prävention über die Detektion bis hin zur Reaktion – behandelt und entsprechende Angebote bereitstellt. Die daraus entstandenen Fachabteilungen decken die operativen Handlungsfelder ab. Die CSBW erfüllt mit ihrem Angebot einerseits die ihr übertragenen gesetzlichen Aufgaben und bietet andererseits ihren Zielgruppen maßgeschneiderte Lösungen für deren Bedarfe. Dies können Standardprodukte oder individuelle Angebote sein, präventive Ansätze oder Leistungen aus dem Spektrum Detektion und Reaktion. Allen gemeinsam ist, dass die Angebote auf die jeweiligen Zielgruppen zugeschnitten sind und eine Nachfrage bedienen. So unterstützt die CSBW andere Organisationen dabei, ihre Cybersicherheit zu verbessern.

*** Das MIRT ist das mobile Einsatzteam, das zur Vorfallbehandlung und -steuerung vor Ort mit Rat und Tat zur Seite steht.**

Organigramm der CSBW

Handlungsfelder der CSBW

[1] CyberSicherheitsGame BW, Web-Based-Trainings
[2] CSBW-Website, Factsheets, Erklärvideos

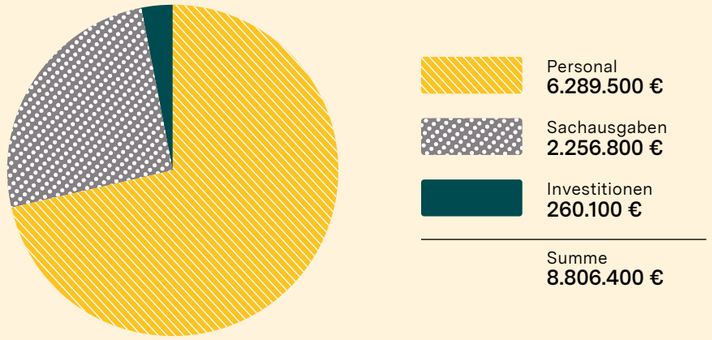
**** Das CERT ist ein Teil der CSBW und die zentrale Stelle für Cybersicherheit in der Landesverwaltung Baden-Württemberg sowie für alle weiteren öffentlichen Stellen im Land.**

1.2 Rahmeninformationen zur CSBW

Haushalt

Im Haushaltsjahr 2024 stand der CSBW im Kapitel 0308 des Staatshaushaltsplans ein Gesamtbudget in Höhe von 8.806.400,00 € (2024) zur Verfügung. Diese finanzielle Ausstattung erlaubte in gewissem Rahmen Planungssicherheit und Spielraum bei der weiteren strategischen Ausrichtung. Der weitaus größte Anteil mit ca. 70 Prozent entfiel dabei weiterhin auf die Kosten für das Personal. Die geplanten Maßnahmen überstiegen die zur Verfügung stehenden Sachmittel, so dass nicht alle geplanten Maßnahmen unmittelbar umgesetzt werden konnten und eine Priorisierung erfolgen musste.

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



Personal

Der CSBW sind im Staatshaushaltsplan 88,5 Stellen zugeordnet. Die Zahl der besetzten Stellen konnte stabil gehalten werden. Zum Jahresende 2024 sind rund 80 Prozent der Stellen besetzt.

Die Anzahl der Beschäftigten mit Schwerbehinderung beziehungsweise anerkannter Gleichstellung erhöhte sich auf zwei Personen.

Der Anteil weiblicher Beschäftigter lag zum Jahresende 2024 bei 44 Prozent und damit auf ähnlichem Niveau wie im Vorjahr.

Der Altersdurchschnitt liegt bei 45 Jahren. Fast 38 Prozent der Beschäftigten sind zwischen 26 und 35 Jahre alt. Dies unterstreicht das Interesse jüngerer Menschen am Thema Cybersicherheit und die Attraktivität der CSBW.

Seit Mitte des Jahres können die Beschäftigten der CSBW auf die ersten Maßnahmen des betrieblichen Gesundheitsmanagements (BGM) zugreifen, u. a. auf ein Employee-Assistance-Programm (EAP).

In Zusammenarbeit mit der Dualen Hochschule Baden-Württemberg Heilbronn (DHBW) bietet die CSBW jährlich zwei Studienplätze im Bereich Wirtschaftsinformatik mit dem Schwerpunkt Software Engineering an. Im Verlauf des Studiums erhalten die Studierenden eine umfassende Ausbildung in allen Bereichen der Cybersicherheit. Zudem absolvieren sie im Rahmen der Kooperation mit dem Landeskriminalamt Baden-Württemberg und der EnBW AG jeweils eine Praxisphase. Das Ziel dieser Partnerschaft ist es, die nächste Generation von Fachkräften im Bereich Cybersicherheit zu fördern und auszubilden.

Dienststandort

Für den April 2025 ist ein Umzug zum finalen Dienststandort nach Bad Cannstatt geplant. Das Dienstgebäude dort teilt sich die CSBW zukünftig mit einem Teil des Landeskriminalamts (LKA) und einem Teil des Präsidiums Technik, Logistik, Service der Polizei in Baden-Württemberg (PTLS Pol).

1.3 Die CSBW im Jahr 2024

2024 war weltpolitisch erneut ein herausforderndes Jahr mit kriegerischen Auseinandersetzungen, Wechseln von Amtsinhaberinnen und Amtsinhabern sowie – auf europäischer Ebene – einer Neujustierung der Cybersicherheitslandschaft durch das Inkrafttreten der NIS2-Richtlinie.

Die Cybersicherheitslage entspannte sich bei genauerer Analyse nicht und die Bedrohungssituation ist unverändert. Auch wenn sich kurzfristig keine neue Spitze im Hinblick auf die Schwere der durch die CSBW bearbeiteten Fälle ergab, knüpft die weiterhin hohe Fallzahl an das Jahr 2023 an. Ständig neue Schwachstellen führen zu einer unverändert kritischen Bedrohungslage. Wünschenswert wäre natürlich, dass die Vielzahl der Fälle der letzten Jahre und die breite Berichterstattung der Medien Wirkung zeigten und entsprechende Sensibilisierungs- und technische Präventionsmaßnahmen umgesetzt werden würden. Insbesondere die international sehr wirkungsvollen Schläge gegen große Gruppierungen, die sowohl die Infrastruktur als auch die Cyberkriminellen selbst sehr schwächten, sind ein wichtiger Erfolg der Ermittlungsbehörden. Erfahrungsgemäß bringt das lukrative Cybercrime-Umfeld jedoch schnell wieder neue Angriffsgruppierungen hervor.

Ende Mai trat die neue Präsidentin der CSBW, Nicole Matthöfer, ihr Amt an. Dies bot eine gute Gelegenheit, nach knapp zweieinhalb Jahren als eigenständige Behörde einen prüfenden Blick auf Prozesse, Strukturen und Angebote zu richten und zu überlegen, ob die erfolgten Weichenstellungen weiterhin Bestand haben sollen. Während in den vergangenen beiden Jahren die Konzeption und Umsetzung von Projekten und Angeboten den meisten Raum einnahm, erfolgten nun einige Verbesserungsprozesse und eine Schärfung des Portfolios. Zielgruppenorientierung und Skalierbarkeit sind dabei wichtige Schlagworte, die mit Leben gefüllt werden sollen. Diese kontinuierliche Prüfung und Anpassung der strategischen und organisatorischen Ausrichtung ist im dynamischen Cybersicherheits-Umfeld unumgänglich und wird die CSBW auch in Zukunft begleiten.

Was sich 2024 erneut deutlich zeigte: Die Vernetzung relevanter Akteure im Themenfeld der Cybersicherheit ist von äußerster Bedeutung. Ob LKA, Landesamt für Verfassungsschutz (LfV) oder die zuständigen Stellen anderer Länder und des Bundes wie das Bundesamt für Sicherheit in der Informationstechnik (BSI), das bayerische Landesamt für Sicherheit in der Informationstechnik (LSI) oder das hessische Hessen CyberCompetence-Center (Hessen3C) – die CSBW nahm Fäden auf, tauschte sich aus und wurde auch hier ihrer Rolle als zentrale Koordinierungs- und Meldestelle gerecht. Denn auch wenn es mittlerweile abgedroschen klingt: Cyberangriffe machen nicht an Ländergrenzen halt, und Erkenntnisse und Erfahrungen aus anderen Bereichen können die eigene Arbeit und deren Ergebnisse bereichern und im besten Falle zur Nutzung von Synergien beitragen.

Eine gute Möglichkeit zum Austausch und zur Vernetzung bieten immer wieder Veranstaltungen und Vorträge, die wir als CSBW wahrnehmen. Auch 2024 waren viele Kolleginnen und Kollegen regelmäßig im Land und andernorts unterwegs, um die Expertise der CSBW zu teilen und aktuelle Entwicklungen in der Cybersicherheit zu diskutieren. Dabei wurden Vorträge auf verschiedenen Fachveranstaltungen gehalten, die das Thema IT-Sicherheit noch stärker in den Fokus rückten. International war die CSBW an einem Panel auf dem „Cybersecurity Congress“ in Barcelona beteiligt und diskutierte mit italienischen und spanischen Fachleuten darüber, wie Menschen erfolgreich und langfristig sensibilisiert werden können und wie die Gewinnung von IT-Fachkräften erfolgreich sein kann. Zudem fand ein weiterer Austausch mit Kalifornien, Israel, Finnland und den Niederlanden statt.

Ein besonderes Highlight war außerdem die aktive Mitgestaltung des diesjährigen Cybersicherheitsforums. Neben der Moderation von verschiedenen Panels wurde ein Vortrag zum Thema „Erfahrungen mit KI-unterstützten Cybersicherheitslösungen in Kommunen“ organisiert und moderiert, bei dem zwei Kommunen über ihre praktischen Erfahrungen berichteten. Er stieß auf großes Interesse bei den Teilnehmerinnen und Teilnehmern. Auch darüber hinaus war das Thema KI häufig Inhalt von Gesprächen und die CSBW wird die Entwicklungen weiter beobachten. Denn disruptive Technologien in der Informationstechnik eröffnen seit jeher vielfältige Chancen, bringen jedoch auch erhebliche Risiken mit sich. Die Aufgabe besteht nicht nur darin, diese Risiken sorgfältig zu bewerten und zu analysieren, sondern auch die Entwicklung technischer Lösungen zu begleiten, sofern sie aktuelle und zukünftige Bedrohungen der Cybersicherheit adressieren. Dabei legt die CSBW besonderen Wert darauf, innovative Ansätze zu identifizieren und in ihre Arbeit und ihr Angebot zu integrieren, um potenziellen Gefahren proaktiv entgegenzuwirken und gleichzeitig die Chancen neuer Technologien optimal zu nutzen.

Zu guter Letzt beschäftigte die Vorbereitung auf die Umsetzung der NIS2-Richtlinie natürlich auch die CSBW. Als eine für die Cybersicherheit zuständige Stelle kamen alle betroffenen Prozesse auf den Prüfstand. Baden-Württemberg hatte mit der Verabschiedung des „Gesetzes zur Verbesserung der Cybersicherheit“ bereits 2021 die Weichen gestellt und mit der Gründung der CSBW schon früh eine zentrale Anforderung der NIS2 erfüllt. Auch eine 24-Stunden-Erreichbarkeit für Meldungen und die Fallerfassung nach bestimmten Kriterien muss das Land nicht komplett neu aufsetzen, sondern kann mit der CSBW auf bewährte Prozesse setzen und diese lediglich in geringem Umfang anpassen. Insofern ist die CSBW gut vorbereitet auf die Umsetzung der NIS2-Richtlinie, wenngleich natürlich bis zur finalen Umsetzung in deutsches Recht noch Unwägbarkeiten bleiben.

1.4 Wechsel in der Behördenleitung: Interview mit der CSBW-Präsidentin Nicole Matthöfer

Frau Matthöfer, wieso haben Sie sich für die Stelle als Präsidentin der CSBW beworben?

Das Themenfeld ist einfach unheimlich spannend. Und aktuell außerdem meiner Meinung nach eines der wichtigsten Politikfelder. Es vergeht doch vor allem im Arbeitsleben kaum eine Minute, in der wir nicht in irgendeiner Weise digitale Dienste nutzen. Und alles, was digital ist, ist auch angreifbar. Dabei muss man den Teufel nicht an die Wand malen, aber wir müssen uns der Verletzbarkeit bewusst sein. Außerdem haben wir als öffentliche Verwaltung ganz klar die Aufgabe, bestimmte Dienste für das Land zu erfüllen und das Vertrauen in die staatlichen Institutionen zu bewahren und wieder zu stärken. Daran in einer neuen Rolle mitzuwirken, hat mich sehr gereizt.

Sie blicken inzwischen auf ein gutes halbes Jahr bei der CSBW zurück. Wie würden Sie diese Monate beschreiben?

Unheimlich intensiv, lehrreich und arbeitsreich. Die Kolleginnen und Kollegen der CSBW sind allesamt sehr engagiert und motiviert und haben eine enorm große Expertise in ihren jeweiligen Tätigkeitsfeldern. Außerdem ist die CSBW als junge Behörde in vielem sehr aufgeschlossen, das macht sich auch im Miteinander bemerkbar. Ich habe mich vom ersten Tag an sehr willkommen gefühlt und die Unterstützung aus der Belegschaft war und ist sehr groß. Ansonsten war es, glaube ich, ein klassischer Start mit viel Zuhören, Hinschauen und Herausfinden,

Nicole Matthöfer wurde 1975 geboren und kommt ursprünglich aus Nordrhein-Westfalen. Sie schätzt bis heute die direkte Kommunikation, die man dem Ruhrgebiet nachsagt. Nach dem Studium der Rechtswissenschaften und dem Rechtsreferendariat startete Nicole Matthöfer ihre berufliche Laufbahn 2004 bei der Finanzverwaltung des Landes Nordrhein-Westfalen. Schon ihre zweite berufliche Station führte sie nach Baden-Württemberg, als stellvertretende Abteilungsleiterin und Leiterin für das Referat Personal und Recht beim LKA Baden-Württemberg. Sie war ab 2011 als Referentin im Innenministerium unter anderem für das Thema Verfassungsschutz tätig, bevor sie 2013 als parlamentarische Beraterin für Innenpolitik zur SPD-Landtagsfraktion wechselte. 2015 kehrte sie ins Innenministerium zurück und war dort u. a. stv. Zentralstellenleiterin, stv. Leiterin des Stabes Flüchtlingsunterbringung sowie Leiterin des Referats Krisenmanagement in der Abteilung Bevölkerungsschutz. Zuletzt arbeitete Nicole Matthöfer als Fraktionsgeschäftsführerin für die SPD-Fraktion im Landtag von Baden-Württemberg.

was gut läuft und beibehalten werden sollte, und gleichzeitig zu schauen, wo ich eigene Akzente setzen möchte und wo Prozesse oder Angebote vielleicht optimiert werden können.

Mit welchen Herausforderungen müssen sich die CSBW und ihre Zielgruppen aus Ihrer Sicht in nächster Zeit auseinandersetzen?

Die Gefahr, Opfer eines Cyberangriffs zu werden, ist unverändert hoch. Das zeigt auch unser Bericht zur Cybersicherheitslage. Insofern stehen wir alle – Landesverwaltung, Kommunen, Unternehmen und Privatpersonen – vor der Herausforderung, dass wir uns gut gegen Angriffe absichern müssen. Und zwar sowohl technisch als auch in Hinblick auf die Prävention bei Mitarbeiterinnen und Mitarbeitern. Denn ein Cyberangriff kann uns jederzeit treffen. Insofern kann man nie genug für Cybersicherheit werben und ich kann allen unsere Angebote nur ans Herz legen. Für die CSBW im Speziellen sehe ich die Herausforderung, dass wir unser vielfältiges Angebot bedarfs- und zielgruppengerecht ausbauen – bei gleichzeitig begrenzten Ressourcen. Leider sind wir in den aktuellen Haushaltsberatungen mit unseren Vorhaben nicht zum Zuge gekommen, obwohl die Anforderungen durch die Umsetzung der NIS2-Richtlinie und die Wünsche aus unseren Zielgruppen stetig steigen. Insofern müssen die Bedarfe der CSBW weiterhin mit Nachdruck vertreten werden.

Gibt es konkrete Vorhaben auf Ihrer Agenda, die Sie anstoßen wollen?

In den ersten Wochen und Monaten standen verschiedene strukturelle und strategische Themen und Entscheidungen im Fokus, beispielsweise Personalgewinnung, Organisationsstruktur und Überlegungen zur strategischen Weiterentwicklung der CSBW und ihres Angebots. Ganz oben auf meiner Liste steht für die nächste Zeit das Thema Prävention. Denn jeder verhinderte Cyberangriff reduziert einerseits die Zahl der Vorfälle, die wir bearbeiten müssen, und anderseits die Auswirkungen und Schäden bei den Betroffenen selbst natürlich enorm. Zudem wollen wir unser Produktportfolio auf den Prüfstand stellen und dynamisch weiterentwickeln.

2. Die Cybersicherheitslage in Baden-Württemberg

Auch im Jahr 2024 schätzten das Bundesamt für Sicherheit in der Informationstechnik, das Bundeskriminalamt, die Landeskriminalämter und die Verfassungsschutz-Behörden die Cyberbedrohungslage in Deutschland unverändert hoch ein. Die CSBW bestätigt diese Einschätzung für Baden-Württemberg. Sie registrierte 2024 insgesamt eine etwas höhere Zahl an Sicherheitsvorfällen und stellte in Teilbereichen eine deutlichere Steigerung fest. Dies ist auch auf ein verfeinertes Cyber-Monitoring zurückzuführen. Die Zahl der erfassten Kompromittierungen von Passwörtern und damit verbundenen Accounts nahm daher im Vergleich zu 2023 erheblich zu.

Eine Meldepflicht an die CSBW besteht bisher nur für die Landesverwaltung. Deshalb ist davon auszugehen, dass die tatsächliche Zahl der Fälle höher ist als in der statistischen Erfassung. Dies gilt insbesondere im privatwirtschaftlichen Bereich, aber auch für das kommunale Umfeld. Dies ist bei den folgenden Zahlen zu beachten.

Die zunehmende Bekanntheit der CSBW als zentrale Koordinierungs- und Meldestelle in Baden-Württemberg trägt aber sicherlich zu einer höheren Meldebereitschaft bei.

2.1 IT-Sicherheitsvorfälle und sicherheitsrelevante Ereignisse[3]

Alle 2024 an die CSBW gemeldeten IT-Sicherheitsvorfälle und sicherheitsrelevanten Ereignisse[4]:

- **Sicherheitsvorfälle: 237 (179)**
  Davon Fälle mit MIRT-Einsatz der CSBW zur Unterstützung vor Ort: 5 (8)[5]

- **Sicherheitsrelevante Ereignisse: 280 (214)**

Im Vergleich zum Vorjahreszeitraum steigerten sich die durch die CSBW erfassten Fälle um gut 30 Prozent. Ein Teil des Anstiegs ist auf ein verändertes Cyber-Monitoring zurückzuführen. Seit April 2024 findet das Cyber-Monitoring toolgestützt statt. Daher sind verfeinerte Feststellungen möglich, was sich insbesondere in der angewachsenen Zahl der sicherheitsrelevanten Ergebnisse zeigt. Die Software findet geleakte Zugangsdaten, die in der überwiegenden Mehrzahl als sicherheitsrelevantes Ereignis zu kategorisieren sind. Bei den sicherheitsrelevanten Ereignissen nehmen verdächtig erscheinende E-Mails oder maliziöse Dateien, Verdachtsfälle kompromittierter Accounts oder verdächtiges Verhalten von IT-Systemen den größten Anteil ein.

Es ist davon auszugehen, dass durch die neuen Analysemethoden die Fallzahl im Jahr 2025 weiter anwachsen und dadurch das Dunkelfeld noch besser ausgeleuchtet wird.

Im Berichtszeitraum wurde bei der CSBW ein einziger schwerwiegender IT-Sicherheitsvorfall bei öffentlichen Stellen erfasst: In der Verwaltung einer Kommune war die IT verschlüsselt. Das MIRT der CSBW rückte kurz nach Bekanntwerden des Falles aus, um Daten zu sichern und die Kommunalverwaltung zu unterstützen. Das MIRT stattete die Verwaltung mit der CSBW-IT-Notfallausrüstung aus und gab praktische Hinweise, so dass die Verwaltung bereits nach sehr kurzer Zeit wieder weitgehend arbeitsfähig war.

Die weiteren registrierten Fälle hatten keine so schwerwiegenden Folgen oder größere Auswirkungen bei den Betroffenen. In den Fallzahlen sind auch kurzzeitige Störungen, Systemausfälle oder Benutzungsfehler enthalten, weil sie die Verfügbarkeit beeinträchtigen.

IT-Sicherheitsvorfälle und sicherheitsrelevante Ereignisse (inkl. Verdachtsfälle) nach Zielgruppen:

Die CSBW hat **Landkreise, Städte und Gemeinden sowie Unternehmen in kommunaler Trägerschaft** in 49 (54) Fällen beraten und unterstützt.

- 3 (5) Fälle erforderten einen Einsatz des MIRT der CSBW zur Unterstützung vor Ort, einschließlich Unterstützung beim Krisenmanagement und der Krisenkommunikation.

- In 44 weiteren Fällen erfolgten die jeweils erforderliche Unterstützung und Beratung beispielsweise in Form der Untersuchung einzelner maliziöser Daten oder E-Mails, Verdachtsfälle kompromittierter Accounts oder verdächtigen Verhaltens von IT-Systemen.

Die CSBW stellt einen leichten Rückgang von Sicherheitsvorfällen und sicherheitsrelevanten Ereignissen bei Kommunen fest. Erfreulich ist, dass die Zahl der schweren Vorfälle 2024 deutlich geringer war als im Vorjahr. Einen Beitrag zu dieser positiven Entwicklung leistete sicherlich die laufende Präventionsarbeit der CSBW bei den Kommunen. Um Vorfälle und Ereignisse zu erkennen und das Dunkelfeld besser auszuleuchten, arbeitet die CSBW mit einem toolgestützten Monitoring. Ohne die mithilfe dieses Tools erlangten Erkenntnisse wäre der Rückgang deutlich stärker ausgefallen (knapp 25 Prozent). Das würde jedoch nur einen vermeintlichen Rückgang der Fälle bedeuten, da an dieser Stelle lediglich das Dunkelfeld anwachsen würde.

[3] Nach der VwV InfoSic gliedern sich Fälle in sicherheitsrelevante Ereignisse oder Sicherheitsvorfälle. Verdachtsfälle sind zunächst sicherheitsrelevante Ereignisse, können sich aber zum Sicherheitsvorfall entwickeln. Sie werden nur in der jeweiligen End-Kategorie gezählt.

[4] Die Zahlen in Klammern beziehen sich jeweils auf den Vorjahreswert, sofern dieser erfasst wurde. Die statistische Erfassung wurde von 2023 zu 2024 auf eine detailliertere und teilweise veränderte Erfassung umgestellt. Eine 1:1-Vergleichbarkeit zum Vorjahreszeitraum ist nicht bei allen Zahlen gegeben.

[5] Die Anzahl der Vorfälle mit MIRT-Einsatz hat sich geringfügig reduziert, aufgrund der geringen Fallzahl ist diese Schwankung allerdings nicht aussagekräftig in Hinblick auf einen langfristigen Trend. Ein MIRT-Einsatz ist außerdem nicht alleiniges Kriterium für eine besondere Schwere eines Falles, da er vor allem erforderlich ist, wenn bspw. eine Datensicherung nur vor Ort möglich ist.

Die CSBW unterstützte und beriet in der **Landesverwaltung** (inkl. aller nachgeordneten Bereiche) in 183 (170) Fällen[6].

- Ein Fall erforderte einen MIRT-Einsatz der CSBW zur Unterstützung vor Ort.
- In den 175 weiteren Fällen erfolgten die jeweils erforderliche Unterstützung und Beratung beispielsweise in Form der Untersuchung einzelner maliziöser Daten oder E-Mails, Verdachtsfälle kompromittierter Accounts oder verdächtigen Verhaltens von IT-Systemen.

Die CSBW hat **Hochschulen, Universitäten und vergleichbare Einrichtungen** in 110 (38) Fällen beraten oder unterstützt.[7]

- 1 Fall erforderte einen MIRT-Einsatz der CSBW zur Unterstützung vor Ort, einschließlich Unterstützung beim Krisenmanagement.
- In den 109 weiteren Fällen erfolgten die jeweils erforderliche Unterstützung und Beratung beispielsweise in Form der Untersuchung einzelner maliziöser Daten oder E-Mails, Verdachtsfälle kompromittierter Accounts oder verdächtigen Verhaltens von IT-Systemen.

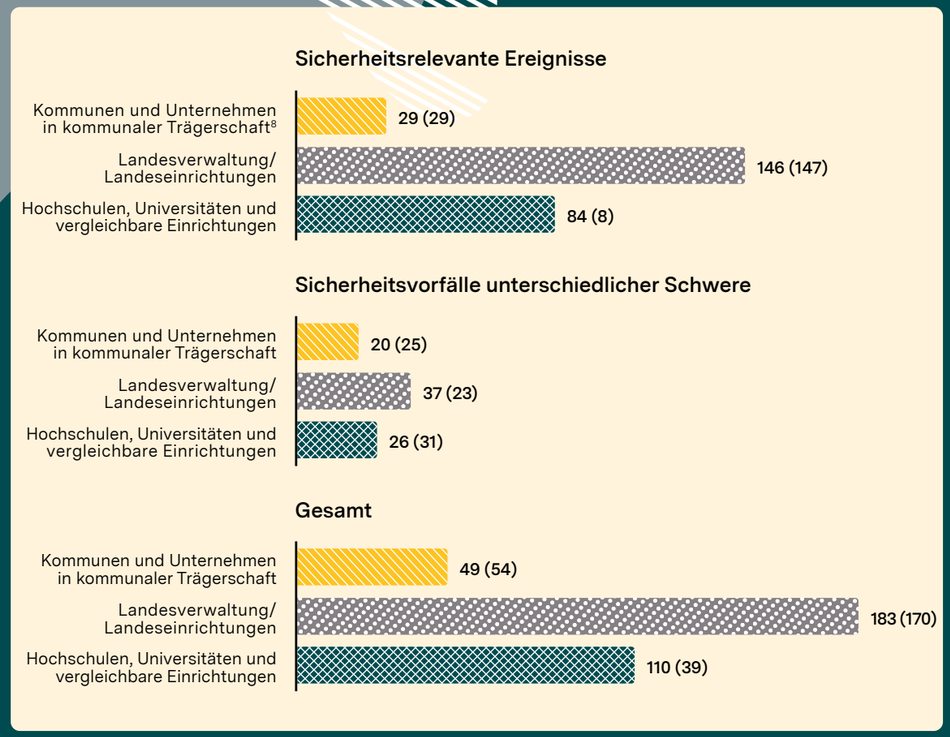
Vorfallsarten

Die Bandbreite der an die CSBW gemeldeten Fälle ist groß: Von False-Positive-Meldungen durch Virenscanner und vermeintlichen Phishing-Mails über tatsächliche Phishing-Mails, Passwort-Kompromittierungen, nicht gepatchte Sicherheitslücken sowie Malware bis hin zu Vollverschlüsselungen mit Ransomware kam das ganze Spektrum vor.

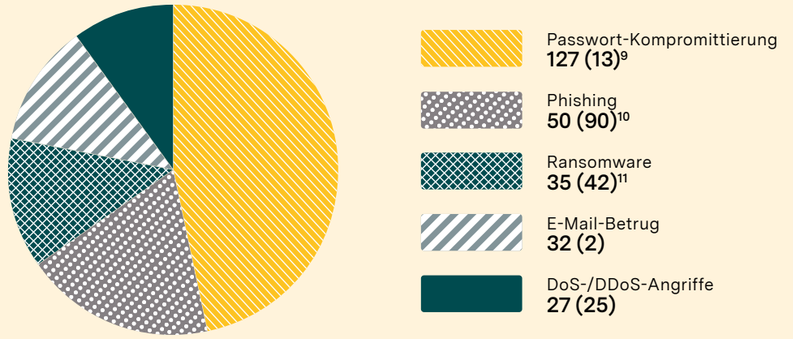
Die CSBW erfasste dabei sowohl zielgerichtete Angriffe, d. h., die Angreifer suchten sich ganz konkret ein Opfer aus, als auch breit gestreute Massenangriffe, die bekannte Schwachstellen ausnutzen oder als Einfallstor beispielsweise Phishing-Mails verwenden.

[6] Im Bereich der Landesverwaltung ist trotz der toolgestützten Security-Analyse nur eine geringfügige Steigerung der Fallzahlen ersichtlich.

[7] Die erhebliche Steigerung im Hochschulbereich ist ebenfalls durch den Einsatz des toolgestützten Monitorings zu erklären. Ohne diese Erkenntnisse wäre die Zahl im Vergleich zum Vorjahr nahezu unverändert.



Die Top 5 der erfassten Angriffsarten:



Fehlkonfiguration/-bedienung und ausgenutzte Schwachstellen sind aus den Top 5 der Angriffsarten herausgefallen, was auf eine zunehmende Sensibilisierung zurückzuführen sein könnte.

[8] Da es bisher keine Meldepflicht von Cybersicherheitsvorfällen in Kommunen an die CSBW gibt, kann die Zahl der Fälle größer sein.

[9] Die sehr starke Zunahme bei der Passwort-Kompromittierung im Vergleich zum Vorjahr ist auf einen erhöhten Tool-Einsatz bei der CSBW zurückzuführen. Dadurch erkennt die CSBW mehr Fälle.

[10] Bei Phishing- und E-Mail-Betrugsversuchen zusammengenommen entwickelte sich die Zahl geringfügig nach unten und liegt damit im Rahmen der statistischen Schwankung.

[11] Die hohe, wenn auch leicht rückläufige Zahl bei Ransomware-Angriffen ist auf ein ausgeweitetes Monitoring durch die CSBW zurückzuführen. Auch in diesem Bereich dehnte die Behörde ihr Sichtfeld aus.

Cyber-Monitoring

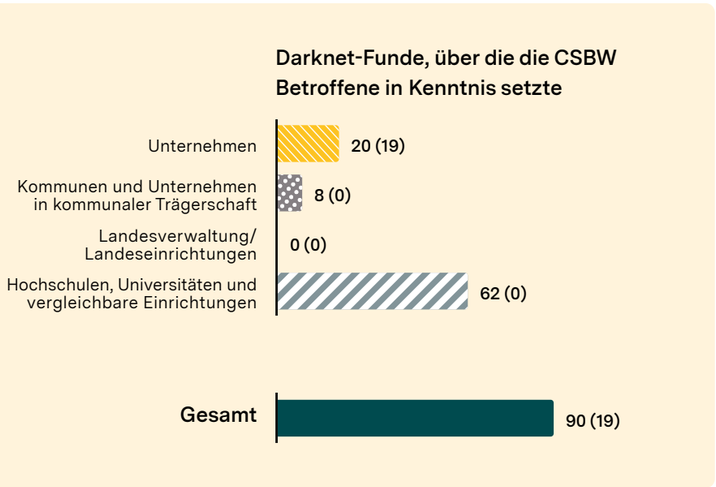
Die CSBW überwacht den Cyberraum auf:

- durchgeführte Ransomware-Angriffe und geleakte Daten
- Credential Leaks
- durchgeführte und angekündigte DDos-Angriffe

Hierfür nutzt die CSBW Cyber-Threat-Intelligence-Plattformen, die Ergebnisse automatisiert liefern können. So können mehr Fälle erkannt und durch das rechtzeitige Erkennen der Schweregrad eines Ereignisses oder Vorfalls verringert oder sogar komplett verhindert werden.

Daher trägt die CSBW mit diesem Cyber-Monitoring deutlich zur Verbesserung der Cybersicherheit bei. Auf Grundlage des Monitorings ergriffene Maßnahmen verringern das Schadenspotenzial sowohl in der Wirtschaft als auch in der Verwaltung. Aufgedeckte Credential Leaks können beispielsweise Kompromittierungen und damit verbundenen Schaden verhindern. Dies verringert die Angriffsfläche und damit das allgemeine Gefährdungspotenzial.

Die CSBW informiert betroffene Behörden, Institutionen und Unternehmen, wenn deren Daten im Cyber-Monitoring auftauchen. So können diese eventuell noch bestehende Sicherheitslücken schließen. Zudem können sich Betroffene durch die Meldung der CSBW, dass Daten zum Verkauf angeboten werden, auf die Kontaktaufnahme mit den Erpressern vorbereiten.



3. Handlungsfeld „Prävention“

Das oberste Ziel der Prävention ist es, Angriffe bestenfalls zu verhindern oder potenzielle Schäden zu minimieren. Ein gestärktes Vertrauen in digitale Systeme verbessert zudem die allgemeine Resilienz von Organisationen. Prävention ist somit der Schlüssel, um Cyberangriffe frühzeitig abzuwehren und langfristig erfolgreich zu bleiben. Das Angebot umfasst digitale und analoge Schulungen, Sensibilisierungsmaßnahmen sowie Beratungsangebote und IT-Sicherheitschecks.

Im Jahr 2024 hat sich die Abteilung Prävention strategisch auf die national und international wachsende, immer komplexere Bedrohungslage ausgerichtet. Im Mittelpunkt des Produktportfolios stehen dabei die Menschen. Außerdem beleuchtet es auch technische Aspekte. Von grundlegender Bedeutung waren der Ausbau der Reichweite sowie die Stärkung der Resilienz. Dabei versteht die CSBW ihr Angebot auch als Gegengewicht zu zentralen Bedrohungen für das demokratische Gemeinwesen und einen Vertrauensverlust in staatliche Institutionen. Das Team hat sich das Ziel gesetzt, innovative Formate zu entwickeln, um diesen Herausforderungen gezielt zu begegnen und unsere Gesellschaft nachhaltig zu schützen. Mit zahlreichen Produkten, die in Form von Factsheets, Web-Based-Trainings, Erklärvideos und Sensibilisierungsaktionen angeboten werden, richtet sich das Angebot mit leicht zugänglichen Informationen an eine breite Zielgruppe. Zusätzlich sind spezialisierte Trainings im Angebot, wie z. B. die Ausbildung zum IT-Grundschutz-Praktiker sowie individuelle Beratungen. Besonders beliebt ist weiterhin der Leitfaden zur Cybersicherheit. Das CyberSicherheitsGame BW der CSBW wurde sukzessive über eine Lernplattform zur Verfügung gestellt. Außerdem bietet die CSBW über die Abteilung Prävention diverse Schulungen online und in Präsenz an. Dabei sind die Themen „Cybersicherheit als Führungsaufgabe“ und „Grundlagen der Cybersicherheit“ besonders gefragt. Im Bereich Beratung ermöglicht der modulare Stufenplan Mindestsicherheitsniveau seit 2023 einen strukturierten und schrittweisen Einstieg in die Informationssicherheit – insbesondere für kleinere Verwaltungseinheiten. Im Umfeld der Hochschulen und des Innovationsmanagements blieb die Vernetzung der Akteure von zentraler Bedeutung. Außerdem beschäftigte sich der Arbeitsbereich beispielsweise mit den Auswirkungen von Themen wie Künstliche Intelligenz auf die Cybersicherheit, evaluierte diese und ermittelte Formate zur Vermittlung dieser Themen an diverse Zielgruppen.

Das Team der Informationssicherheit legt die notwendigen Grundlagen für eine Zertifizierung auf der Basis des BSI-IT-Grundschutzes. Dabei gilt: Die CSBW will hier als gutes Beispiel vorangehen und die Landes- und Kommunalverwaltung sowie weitere öffentliche Stellen dazu motivieren, diesen Schritt ebenfalls zu gehen.

3.1 Schulungen der CSBW

Ein wesentlicher Bestandteil der Präventionsarbeit ist die Wissensvermittlung durch Schulungen. Durchdachte, innovative und zielgruppenorientierte Schulungen dienen dazu, komplexes Cybersicherheits-Wissen verständlich aufzubereiten und zu vermitteln.

Mit dem Fokus auf die Zielgruppe der Landes- und Kommunalverwaltung baut die CSBW aktuell ihr vielfältiges Angebot an Schulungen, Trainings und Präventionsangeboten aus. Hierbei sind insbesondere die Mitarbeitenden der Landes- und Kommunalverwaltungen die Zielgruppe. Die Schulungen der CSBW sind allesamt kostenlos und können in Präsenz oder als Online-Angebot genutzt werden.

Aktuell umfasst das Angebot vier verschiedene Schulungen, wovon im Jahr 2024 zwei Schulungsangebote neu konzipiert und pilotiert wurden. Die momentan am häufigsten durchgeführte Schulung ist die „Grundlagenschulung Cybersicherheit“. Im Jahr 2024 fand die Schulung insgesamt 80-mal mit insgesamt 3.422 Teilnehmenden aus Kommunen, der Landesverwaltung und Institutionen in kommunaler Trägerschaft statt. Nach der Grundlagenschulung ist das am zweithäufigsten durchgeführte Angebot „Cybersicherheit als Führungsaufgabe“, das sich speziell an die Führungskräfte in der Landes- und den Kommunalverwaltungen richtet. Dieses Angebot wurde im Jahr 2024 an 23 Terminen mit insgesamt rund 460 Teilnehmenden durchgeführt.

> **Die Schulungen bieten einen guten Überblick über die unterschiedlichen Angriffsszenarien. Die Inhalte werden kurzweilig und gut verständlich erklärt.**
> Schulungsteilnehmerin

Neu hinzu kamen in diesem Jahr die beiden Angebote „Anwendung von Offline-Passwortmanagern“ und die Aufbauschulung „Prävention im Arbeitsalltag“.

Anwendung von Offline-Passwortmanagern

Was ist ein sicheres Passwort? Um was handelt es sich bei einem Offline-Passwortmanager und wie setze ich diesen richtig ein? Diese und viele weitere Fragen thematisiert das Schulungsangebot „Anwendung von Offline-Passwortmanagern – am Beispiel von „KeePass2“, das in der Landesverwaltung im Einsatz ist.

Das Schulungsangebot ist seit dem zweiten Quartal 2024 verfügbar und wurde im Jahr 2024 bereits 8-mal durchgeführt für insgesamt rund 140 Teilnehmende aus der Landes- und Kommunalverwaltung.

Aufbauschulung Cybersicherheit – Prävention im Arbeitsalltag

Die Schulung „Cybersicherheit – Prävention im Arbeitsalltag“ baut auf die „Grundlagenschulung Cybersicherheit“ auf. Ziel ist es, Mitarbeiterinnen und Mitarbeitern der Landesverwaltung und der Kommunen wirksame und praktisch einfach umsetzbare Präventionsmaßnahmen für den (Berufs-)Alltag an die Hand zu geben.

Das Schulungsangebot ist seit dem zweiten Quartal 2024 verfügbar und wurde im Jahr 2024 bereits 10-mal durchgeführt für insgesamt rund 230 Teilnehmende aus der Landes- und Kommunalverwaltung.

3.2 Digital und zentral: die Lernplattform der CSBW für Landes- und Kommunalverwaltungen

Um den Mitarbeitenden der Landes- und Kommunalverwaltungen die vielfältigen Weiterbildungsangebote der CSBW an einer Anlaufstelle zugänglich zu machen, wurde ein auf Moodle basierendes Learning-Management-System (LMS) aufgebaut: die Lernplattform der CSBW. Sie steht der gesamten Landes- und Kommunalverwaltung unter https://moodle.cybersicherheit.bwl.de kostenlos zur Verfügung. Der Zugriff ist aus dem Landesverwaltungsnetz (LVN) und dem kommunalen Verwaltungsnetz (KVN) möglich.

Auf der Lernplattform können die Nutzerinnen und Nutzer auf E-Learning-Angebote (Web-Based-Trainings, videobasierte Schulungen), Schulungsmaterialien und das Serious Game „CyberSicherheitsGame BW“ zugreifen, Lernerfolge detailliert nachverfolgen und sich in Foren zu spezifischen Themen austauschen. Als Nachweis für die Teilnahme an einer Schulungsmaßnahme erhalten die Teilnehmenden personengebundene Zertifikate.

Nach dem stufenweisen Rollout Ende 2023 ist die Plattform seit dem 1. Februar 2024 für die Landes- und Kommunalverwaltungen zugänglich. Das Angebot auf der Lernplattform wird sukzessive erweitert.

Seit dem Start des Rollouts kann die CSBW positive Zugriffs- und Nutzungszahlen verzeichnen. So haben sich in 2024 über 1369 Nutzerinnen und Nutzer auf der Lernplattform der CSBW registriert und es wurden insgesamt 3091 Teilnahmezertifikate ausgestellt.

CyberSicherheitsGame BW

In Kooperation mit dem Ministerium des Inneren, für Digitalisierung und Kommunen entstand unter Federführung der CSBW das „CyberSicherheits-Game BW“. Dieses sogenannte „Serious Game“ vermittelt Lerninhalte in Gestalt eines Videospiels.

Ergänzend zum bestehenden Schulungsangebot werden hierbei cybersicherheitsbezogene Lerninhalte in die Spiellogik übersetzt. 14 Levels laden dazu ein, sich spielerisch mit Themen wie „Social Engineering“, „Phishing-E-Mails“ oder „Passwortsicherheit“ auseinanderzusetzen.

Mit dem „CyberSicherheitsGame BW“ sollen die Beschäftigten des Landes und der Kommunen für das Thema Cybersicherheit anwenderorientiert und nachhaltig sensibilisiert werden. Das langfristige Ziel ist, den Transfer zwischen theoretischem Lernen und praktischer Anwendung zu ermöglichen und damit eine anhaltende Verhaltensänderung zu erreichen. Das Spiel kombiniert die Vorteile von Präsenzschulungen und E-Learning-Angeboten und animiert dazu, durch Interaktion selbst aktiv zu werden.

Das Produkt steht seit dem ersten Quartal 2024 als Teil des E-Learning-Angebots der CSBW auf der Lernplattform zur Verfügung. Der Rollout inklusive der dazugehörigen Umsetzungsstrategie und verschiedener Begleitmaterialien erfolgte im Oktober 2024.

Web-Based-Trainings

Im Frühjahr 2024 stellte die CSBW zwei neue Web-Based-Training-Schulungseinheiten für die Mitarbeiterinnen und Mitarbeiter von Land und Kommunen zur Verfügung.

Unter Web-Based-Trainings versteht man multimedial aufbereitete Inhalte, die interaktive Elemente beinhalten und als selbstgesteuertes E-Learning-Angebot in individueller Lerngeschwindigkeit absolviert werden können.

Thematisch orientieren sich die neuen Web-Based-Trainings an typischen Abläufen des Arbeitsalltags. Das Modul „Passwort, Social Media und IoT“ beschäftigt sich mit der Erstellung von sicheren Passwörtern, aber auch mit den Vorteilen der Nutzung einer Zwei-Faktor-Authentifizierung als zusätzliche Schutzmaßnahme für Passwörter und Accounts. Ergänzend weist es auf die sichere Nutzung von Social-Media-Plattformen im beruflichen Kontext sowie auf die Gefahren einer unsicheren Konfiguration von IoT-Geräten hin. Das zweite Modul „Das Informationssicherheitsmanagementsystem (ISMS)“ erklärt anschaulich die Aufgaben und Ziele eines Informationssicherheitsmanagementsystems (kurz ISMS). Zusätzlich bietet das Modul einen Überblick über den BSI-IT-Grundschutz und die DIN EN ISO 27001.

3.3 Cybersicherheit einfach, kompakt und zugänglich: Erklärvideos, Leitfaden und Sensibilisierungsaktionen

Erklärvideos

Mit ihren Erklärvideos greift die CSBW eine Vielzahl an Cybersicherheitsthemen auf. Ziel ist es, Cybersicherheit zu erklären und für alle verständlicher zu machen. Darüber hinaus geben hilfreiche Tipps Orientierung, um sich besser vor Angriffen zu schützen. Die Erklärvideos sind auf der Webseite der CSBW für alle Interessierten zugänglich.

Im Video „Phishing, Smishing und Vishing“ werden die typischen Merkmale dieser Angriffsarten dargestellt und erklärt, welche Schutzmaßnahmen ergriffen werden können. Das Video „Social Engineering“ stellt die typischen Methoden bei Social-Engineering-Angriffen dar und gibt den Nutzerinnen und Nutzern Tipps, wie sich diese enttarnen lassen und welche Schutzmaßnahmen getroffen werden können. Im Video zu „Ransomware“ erfahren die Nutzenden, welcher Angriffsvektor sich hinter der Begrifflichkeit verbirgt und welche leicht umzusetzenden Maßnahmen es zum Schutz vor digitalen Erpressungsversuchen gibt. Darüber hinaus wird die Thematik „Sichere Passwörter“ in einem Video aufgegriffen. Insbesondere der sorgsame Umgang mit Passwörtern und die Gestaltung und die Merkmale von sicheren Passwörtern stehen hier im Vordergrund. Zur Ergänzung der Angriffsvektoren wird das Thema „Malware“ ebenfalls thematisiert. Das hierzu passende Video widmet sich den Fragen, was genau eine Schadsoftware eigentlich ist und welche Vorkehrungen zum Schutz zu treffen sind? Um das Angebot abzurunden, wird das Thema „Öffentliche WLAN-Netzwerke“ als ein verlockendes, aber möglicherweise gefährliches Angebot erläutert. Das Erklärvideo thematisiert die Gefahren bei der sorglosen Nutzung von unverschlüsselten WLAN-Netzwerken, aber auch entsprechende Schutzmaßnahmen.

Guide to cybersecurity

Die Broschüre „CSBW-Leitfaden zur Cybersicherheit“ informiert sowohl digital als auch in gedruckter Form darüber, wie man Cybersicherheit schaffen und erhalten kann.

Um Menschen aus anderen Ländern für die vielfältigen Themen der Cybersicherheit sensibilisieren zu können, wurde diese Broschüre im Jahr 2024 zusätzlich in englischer Sprache erstellt. Die CSBW ging damit einem Wunsch von Forschungseinrichtungen nach, die auch ihre Kolleginnen und Kollegen aus anderen Ländern mit Cybersicherheits-Hinweisen versorgt sehen möchten. Mit dem „Guide to cybersecurity“ kann sichergestellt werden, dass die Cybersicherheit nicht durch fehlende Deutschkenntnisse gefährdet ist. Für Kontakte zu internationalen Partnerinstitutionen oder bei internationalen Veranstaltungen kann der englische „Guide to cybersecurity“ der CSBW ebenfalls Verwendung finden.

CSBW-Factsheet-Aktion 2024

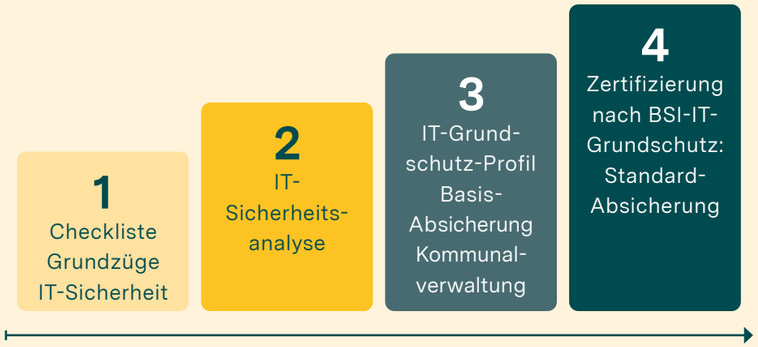
Mit einer sechsteiligen Factsheet-Aktion stellte die CSBW im April 2024 kompaktes Wissen in Form von Factsheets zur Verfügung, die sich grundlegenden Themen rund um die Cyber- und Informationssicherheit widmen.

Die CSBW-Factsheets wurden zu sechs spezifischen Themenschwerpunkten gebündelt. Die Aktionen waren mit thematisch passenden Illustrationen versehen und enthielten eine kurze Beschreibung des Inhalts sowie Verlinkungsbuttons zu den jeweiligen Factsheets.

Bestückt mit wertvollen Informationen und Handlungsempfehlungen ermöglichte die Aktion eine umfängliche Sensibilisierung von Mitarbeitenden des Landes und der Kommunalverwaltungen zu Themen wie „Sicheres Arbeiten“, „Sichere Netzwerke“, „Cybersicherheitsvorfall erkennen“, „Angriffsarten“ und „Präventive Sicherheitsmaßnahmen“.

3.4 Beratung und Innovationsmanagement

In einer unverändert angespannten Sicherheitslage sind es nicht nur die Beschäftigten und Bürgerinnen und Bürger, die im Sinne der Cybersicherheit befähigt werden müssen. Die Beratung von Cybersicherheits-Professionals und Entscheiderinnen und Entscheidern ist ein zentraler Bestandteil der Präventionsstrategie der Cybersicherheitsagentur. Ob in Kommunen oder Landesverwaltung: Verantwortliche sehen sich einer stetig wachsenden Flut an Angriffen ausgesetzt. Daher unterstützt die CSBW auf dem Weg zu einem Mindestsicherheitsniveau.



Empfehlung: Informationssicherheit abhängig vom aktuellen Sicherheitsniveau auf die jeweils folgenden Stufen heben.

Das Stufenmodell befindet sich in der kontinuierlichen Weiterentwicklung. Für 2025 sind bspw. Notfallübungen geplant.

Der stufenweise Weg zum Mindestsicherheitsniveau nach BSI-IT-Grundschutz

- **Stufe 0: Cybersicherheit initiieren**
  Mit einer Beratung von Führungs- und Fachkräften sowie Workshops werden Cybersicherheitsverantwortliche für die Thematik sensibilisiert und auf den Stufenplan Mindestsicherheitsniveau vorbereitet.

- **Stufe 1: Checkliste Grundzüge IT-Sicherheit**
  Durch eine Checkliste mit 92 Fragen, basierend auf dem BSI-IT-Grundschutz, erfolgt eine erste Einschätzung des Sicherheitsniveaus. Die Kunden erhalten eine systematische Auswertung mit praktischen Verbesserungshinweisen zur IT-Sicherheit.

- **Stufe 2: IT-Sicherheitsanalyse**
  Angebot einer detaillierten IT-Sicherheitsanalyse, die gezielte und individuell angepasste Empfehlungen zur Optimierung der IT-Sicherheit bereitstellt.

- **Stufe 3: IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“**
  Die Umsetzung des Profils bietet eine grundlegende Absicherung nach dem BSI-IT-Grundschutz.

- **Stufe 4: Zertifizierung nach BSI-IT-Grundschutz: Standard-Absicherung**
  Die vollständige Umsetzung des BSI-IT-Grundschutzes bietet eine umfassende Absicherung nach dem BSI-IT-Grundschutz.

CSBW **Die CSBW unterstützt die Kommunen bei diesem Prozess mit Schulungen und Beratungsangeboten.**

Die IT-Sicherheitsanalysen waren 2024 ein zentraler Bestandteil der Beratungsangebote. Insgesamt wurden 38 IT-Sicherheitsanalysen bei baden-württembergischen Kommunen durchgeführt. Das Feedback der teilnehmenden Kommunen war durchweg positiv.

Neben den IT-Sicherheitsanalysen wurden zahlreiche Einzelberatungen mit Kommunen und Hochschulen durchgeführt, um spezifische Fragestellungen und Herausforderungen im Bereich der Cybersicherheit zu adressieren. In enger Zusammenarbeit mit dem Ministerium des Inneren, für Digitalisierung und Kommunen bot die CSBW viermal eine fünftägige Online-Zertifizierung zum „BSI-IT-Grundschutz-Praktiker“ an. Diese Schulung beinhaltet eine umfassende Einführung in Inhalte und Umsetzung der IT-Grundschutz-Methodik des BSI. Durch dieses Angebot konnten im Jahr 2024 103 Personen zu BSI-IT-Grundschutz-Praktikern und -Praktikerinnen zertifiziert werden, davon 41 aus der Landesverwaltung und 62 aus den Kommunen.

Die CSBW entwickelt zudem fortlaufend ausgewählte Mustervorlagen auf Basis des BSI-IT-Grundschutzes, die auf der Webseite der CSBW angefordert werden können. Die Mustervorlagen dienen als Basis für die Erarbeitung eigener Sicherheitsdokumente, bieten strukturelle Anleitungen und Formulierungsempfehlungen für spezifische Dokumente und verweisen auf die entsprechenden IT-Grundschutz-Anforderungen bzw. -Bausteine.

Die CSBW-IT-Notfallübung hat uns spielerisch in die Situation eines Cyberangriffs hineinversetzt und uns die Fragen gestellt, die wir uns im Ernstfall stellen würden. Es wurde abteilungsübergreifend geübt, Schwachstellen ermittelt und eine Aufgabenliste für die notwendigen nächsten Schritte festgelegt. Wir sagen Danke für die Möglichkeit, dass wir an diesem tollen Pilotprojekt der CSBW teilnehmen durften.

Adam Bartolf, Leiter IT, Stadt Eppingen

Um die Cybersicherheit von der Theorie in die Praxis zu überführen, hat die CSBW im letzten Halbjahr ein Pilotprojekt mit 5 Kommunen zu IT-Notfallübungen erfolgreich durchgeführt. Ziel war es, einen IT-Cybernotfall zu simulieren, um bestehende Vorkehrungen zu testen. Das Angebot soll 2025 vertieft werden und schließt bedarfs- und zielgruppenorientiert eine Lücke, die in den Beratungen und IT-Sicherheitsanalysen identifiziert wurde.

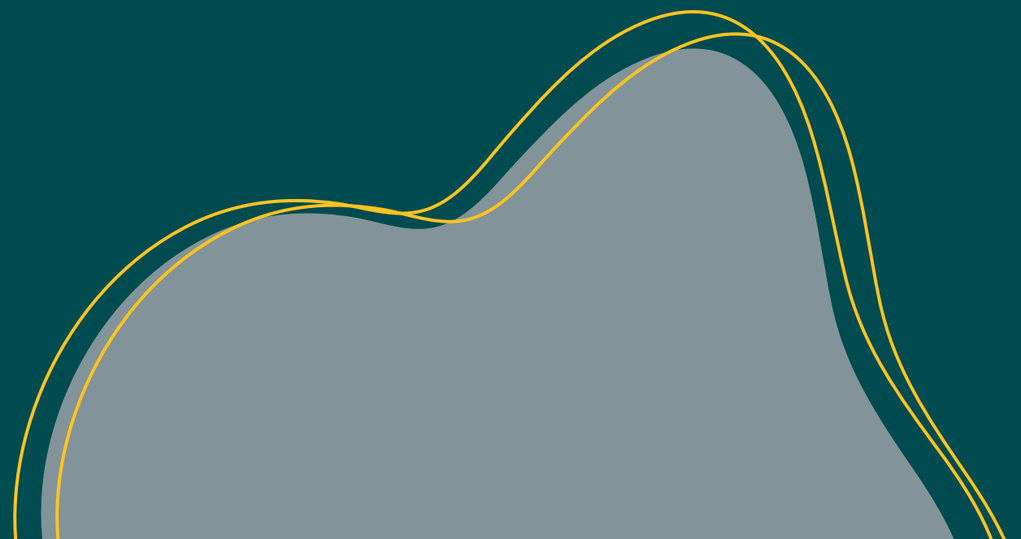
3.5 Informationssicherheit in der CSBW

Als CSBW befassen wir uns mit dem Aufbau, dem Betrieb und der Weiterentwicklung eines nach ISO 27001 zertifizierungsfähigen Informationssicherheitsmanagementsystems (ISMS). Dies ist eine ganzheitliche Vorgehensweise, um für Institutionen aller Arten und Größen eine angemessene Informationssicherheit umzusetzen. Daraus entsteht ein verbindliches behördenspezifisches Sicherheitskonzept zur Informationssicherheit gemäß § 16 E-Government-Gesetz Baden-Württemberg, das sich wiederum an der BSI-IT-Grundschutz-Methodik orientiert.

Das ISMS-Team arbeitete im Jahr 2024 am weiteren Aufbau des ISMS der CSBW, entwickelte Prozesse und Strukturen weiter, erarbeitete notwendige interne Regelungen und beriet intern zu Informationssicherheitskonzepten für Fachverfahren.

4. Handlungsfeld „Detektion und Reaktion“

Das Team Detektion und Reaktion beobachtet und analysiert die Cybersicherheitslage mit einem besonderen Fokus auf das Land Baden-Württemberg und deckt ein breites Angebotsspektrum zur Verbesserung der Cybersicherheit ab. Zur Abteilung gehören die Sachgebiete Lagezentrum, Vorfallbehandlung, Operative Sicherheitsanalyse und Cyber-Ersthilfe BW sowie eine Steuerungsgruppe. Neu im Angebot sind Schwachstellenscans, die seit Ende 2024 öffentlichen Stellen angeboten werden. Das Jahr 2024 war von einem weiterhin hohen Fallaufkommen geprägt, auch wenn die Zahl schwerwiegender Vorfälle rückläufig war.

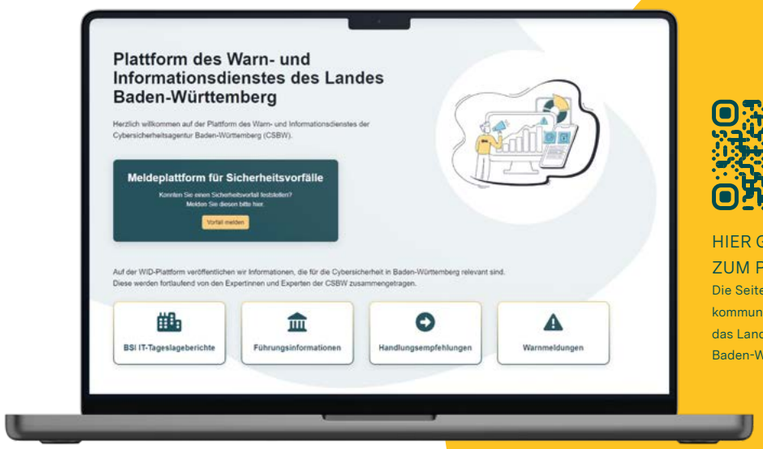


Das Jahr 2024 war für die Abteilung Detektion und Reaktion hinsichtlich schwerwiegender Vorfälle ein relativ ruhiges Jahr. Trotz einer Steigerung der Fallzahlen bei bestimmten Cyberangriffsarten gab es nur einen herausragenden Fall. Sicherlich haben die Angebote und Unterstützungsleistungen der CSBW hierfür einen erheblichen Beitrag geleistet. Denn je mehr Personen und Einrichtungen für die Gefahren sensibilisiert sind, die aus dem Cyberraum kommen können, desto geringer wird die Angriffsfläche für Cyberkriminelle.

Trotzdem war das Jahr 2024 für die Abteilung Detektion und Reaktion ein sehr intensives Jahr. Es bot sich die Gelegenheit, die Weiterentwicklung der Abteilung und damit der gesamten Behörde weiter voranzutreiben. Einige größere Projekte konnten die verschiedenen Sachgebiete nach monatelanger intensiver Vorbereitung und Probeläufen abschließen.

Die CSBW bietet seit Ende 2024 Schwachstellenscans für öffentliche Stellen an. Diese Scans verringern die Angriffsflächen auf den verschiedenen Verwaltungsebenen. Das Portfolio befindet sich weiter im Aufbau und soll im Jahr 2025 um weitere Dienstleistungen ergänzt werden. Der Warn- und Informationsdienst (WID) schuf eine Web-Plattform, auf der er die verschiedenen Meldungen zielgruppenspezifisch veröffentlicht. Alle Meldungen sind damit auf einen Blick verfügbar und nicht mehr in einzelnen E-Mails verteilt. Der WID ist Teil des Lagezentrums der CSBW. Die Cyber-Ersthilfe BW hatte schon frühzeitig die Weichen richtig gestellt, so dass für die Umsetzung der NIS2-Richtlinie im Jahr 2024 nur noch Anpassungen erforderlich waren. Die Kontakte zu den CERTs der anderen Bundesländer wurden weiter gepflegt und teilweise intensiviert. So vereinbarte beispielsweise Präsidentin Nicole Matthöfer im Rahmen ihres Antrittsbesuchs bei der bayerischen Partnerbehörde Hospitationen zwischen den beiden Behörden.

Dass aus der operativen Arbeit der Abteilung auch präventive Angebote erwachsen können, zeigt eindrucksvoll die „Best Practice“ aus einem Vorfall in Mössingen. Der Bericht demonstriert nicht nur die sehr gute Zusammenarbeit der Beteiligten, sondern auch den nahtlosen Übergang innerhalb der CSBW von der Reaktions- an die Präventionsabteilung sowie die Zusammenarbeit mit dem Bereich Krisenkommunikation des Stabs. Diese Fachleute stellen Betroffenen eines Vorfalls umfangreiche Beratungs-, Unterstützungs- und Schulungsangebote zur Verfügung.



HIER GEHT ES DIREKT ZUM PORTAL.
Die Seite ist nur über das kommunale Verwaltungsnetz und das Landesverwaltungsnetz Baden-Württemberg erreichbar.

4.1 Das neue Portal des Warn- und Informationsdienstes (WID-Portal)

Der Warn- und Informationsdienst (WID) der CSBW verteilt aktuelle, sicherheitsrelevante Informationen zu Cybersicherheitsthemen schnell und zielgruppengerecht. Der WID richtet sich primär an die Landesverwaltung, Kommunen und weitere öffentliche Einrichtungen des Landes Baden-Württemberg. Bis Ende 2024 wurden relevante Informationen als Push-Dienst per E-Mail an die Empfänger gesendet.

Um das Angebot zu ergänzen, wurde Ende 2024 das WID-Portal eingeführt. Auf dieses Webportal können berechtigte Nutzerinnen und Nutzer über das Landesverwaltungsnetz (LVN) zugreifen und die für sie relevanten Berichte lesen. Ein Nutzungsrollenkonzept stellt sicher, dass die einzelnen Zielgruppen nur die für sie bestimmten Berichte sehen können.

Auch Nutzerinnen und Nutzer ohne Zugriff auf das LVN können sich für den Push-Dienst registrieren. Nach einer Überprüfung erhalten diese Personen die Berichte automatisch als PDF-Datei per E-Mail. Diese PDF-Dateien werden systemseitig generiert und stellen sicher, dass auch externe Nutzerinnen und Nutzer mit aktuellen Informationen zur Cybersicherheit versorgt werden.

Neben der Möglichkeit, die Berichte im Portal zu lesen, bietet das WID-Portal für Nutzerinnen und Nutzer eine zusätzliche Komfortfunktion. Auf Wunsch erfolgt automatisch eine Benachrichtigung über neu veröffentlichte oder aktualisierte Berichte. Für den Direktzugriff enthält diese einen Link zum jeweiligen Bericht. Die Benachrichtigungen gehen weiterhin per E-Mail ein, so dass man das Portal nicht ständig im Blick haben muss.

Die Ergänzung des WID um das Portal sorgt für eine deutliche Effizienzsteigerung und höhere Flexibilität in der Informationsverteilung, da der WID die Informationen nun gezielter und schneller bereitstellen kann. Auch Nutzerinnen und Nutzer außerhalb des LVN kann der WID durch die PDF-Benachrichtigungen weiterhin zuverlässig an den Informationsfluss anbinden.

4.2 Die Cyber-Ersthilfe BW: bereit für die NIS2-Richtlinie

Im Jahr 2024 war die Arbeit der Cyber-Ersthilfe BW vor allem von der Umsetzung der NIS2-Richtlinie geprägt. Diese Richtlinie bringt nicht nur neue Anforderungen zur Stärkung der Cybersicherheit der kritischen Infrastruktur (KRITIS), sondern auch neue Verpflichtungen für die zuständigen Cybersicherheitsbehörden. Dank des schon vorhandenen Dienstleistungsangebots der Cyber-Ersthilfe BW ist die CSBW gut darauf vorbereitet, diesen neuen Verpflichtungen gerecht zu werden:

24/7-Erreichbarkeit
Die Cyber-Ersthilfe BW ist Tag und Nacht an 365 Tagen im Jahr erreichbar. Dadurch können betroffene Einrichtungen Vorfälle sofort melden und Erste Hilfe in Form von gezielter Beratung erhalten. Dies entspricht der NIS2-Anforderung, Cybersicherheitsvorfälle schnell und wirksam melden zu können.

0711-137 99999

cybererstehilfe@cybersicherheit.bwl.de

https://www.cybersicherheit-bw.de/meldeformular-cyber-ersthilfe-bw

> **Vielen herzlichen Dank für die freundliche, schnelle und kompetente Reaktion und Analyse … Wir hier im Klinikum Esslingen sind sehr froh, einen solchen Partner zur Seite zu haben, auf den wir im Bedarfsfall zurückgreifen können.**
> Teamleiter IT-Infrastruktur & stellv. Geschäftsbereichsleiter

Unterstützung von Kommunen und wesentlichen Einrichtungen
Die Cyber-Ersthilfe BW richtet sich an staatliche und kommunale Einrichtungen, Bürgerinnen und Bürger sowie an Unternehmen. Das schließt kritische Infrastruktur ein, die im Fokus der NIS2-Richtlinie steht. Auf Bitte der betroffenen öffentlichen Stelle eskaliert die Cyber-Ersthilfe BW herausgehobene Fälle umgehend an das CERT BWL. Das Vorfallmanagement, die IT-Forensik und die Krisenkommunikation können so bei Bedarf unmittelbar ihre Arbeit beginnen.

Detektion und Reaktion auf Vorfälle
Die Cyber-Ersthilfe BW analysiert die eingehenden Meldungen auf Häufungen und Muster für eine präzise und aktuelle Ersthilfe. Die CSBW nutzt die daraus gewonnenen Erkenntnisse zu einer Verbesserung des Lagebilds, für Warnmeldungen oder zur Weiterentwicklung ihres präventiven Angebots. Dies erfüllt den Aspekt der proaktiven Maßnahmen und der Risikobewertung, die die NIS2-Richtlinie fordert. Die Möglichkeit zur Analyse von Vorfällen gehört zu den Stärken der Cyber-Ersthilfe BW.

Durch die reaktive Unterstützung, die Präventionsarbeit und die Verbindung zu relevanten Behörden wie der Zentralen Ansprechstelle Cybercrime (ZAC) beim LKA, dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) und dem LfV kann die Cyber-Ersthilfe BW die neuen Vorgaben zur Stärkung der Cybersicherheit auf Landesebene optimal umsetzen.

4.3 Schwachstellenscans erfolgreich gestartet

Die CSBW entwickelte 2024 ein umfassendes Konzept zur Durchführung von Schwachstellen- und Web-Applikationsscans und setzte dieses Konzept um. Dies verbessert die IT-Sicherheit öffentlicher Stellen in Baden-Württemberg durch einen erhöhten Schutz der IT-Infrastruktur vor Sicherheitsrisiken.

Schwachstellenscans dienen dazu, Sicherheitslücken in Computersystemen, Netzwerken und Anwendungen zu identifizieren und geeignete Gegenmaßnahmen zu ergreifen. Solche Scans sind ein wesentliches Werkzeug im Kampf gegen Cyberangriffe und tragen präventiv dazu bei, Daten und Systeme zu schützen.

Damit kann die CSBW seit Ende des Jahres 2024 allen öffentlichen Stellen regelmäßige und systematische Scans als Dienstleistung anbieten, um Schwachstellen frühzeitig zu erkennen. Für diesen Zweck beschaffte die CSBW sowohl die benötigte Hardware als auch spezialisierte Softwarelösungen. Diese Werkzeuge ermöglichen eine präzise Analyse und Bewertung von Sicherheitslücken in den Systemen, was gezielte Maßnahmen zum Schutz der IT-Infrastruktur erlaubt. Die Schwachstellenscans lassen sich in bestehende Sicherheitsprozesse integrieren.

Die Umsetzung dieses Projekts ist ein weiterer Meilenstein der CSBW, die IT-Sicherheit kontinuierlich zu verbessern und die öffentlichen Stellen in Baden-Württemberg vor Bedrohungen aus dem Cyberraum zu schützen.

4.4 Gemeinsam sicherer: Vernetzung der Cybersicherheitsakteure

Cyberkriminelle machen weder vor Staats- und Ländergrenzen Halt noch vor Institutionsgrenzen. Deshalb ist eine Vernetzung der Cybersicherheitsakteure sowohl auf nationaler Ebene als auch zwischen verschiedenen Institutionen elementar. Ein schneller und unbürokratischer Austausch über die neuesten Erkenntnisse zu Cybersicherheitsrisiken, Angriffsvektoren oder aktuell auftretenden Phänomenen ist essenziell für eine bessere Absicherung von IT-Systemen gegen neue und bestehende Gefährdungen.

Verwaltungs-CERT-Verbund

Der Verwaltungs-CERT-Verbund (VCV) ist ein Zusammenschluss der Länder-CERTs und des CERT-Bund im operativen Bereich. Die VCV-Mitglieder tauschen im sogenannten VCV-Chat[12] schnell und formlos technische Informationen aus, um effektiv und schnell auf Cyberangriffe reagieren zu können und besser darauf vorbereitet zu sein.

[12] Gehostet vom Bundesamt für Sicherheit in der Informationstechnik

Zweimal im Jahr treffen sich die VCV-Vertretungen zu einer Präsenzveranstaltung auf operativer Ebene. Die Expertinnen und Experten halten Vorträge zu aktuellen Themen. Die entstandenen Kontakte erwiesen sich schon mehrfach als sehr wertvoll bei akuten Vorfällen.

Im Jahr 2024 präsentierten sich erstmalig die drei Cybersicherheits-Partnerbehörden aus Hessen[13], Bayern[14] und Baden-Württemberg mit einem gemeinsamen Stand auf der IT-Sicherheitsmesse it-sa in Nürnberg. Dort stellten sie ihre Angebote vor und informierten zu den Themen IT- und Cybersicherheit. Bereits in den beiden Jahren zuvor teilten sich Bayern und Baden-Württemberg partnerschaftlich einen Stand.

bwInfoSec

bwInfoSec[15] ist ein Zusammenschluss baden-württembergischer Hochschulen und Universitäten. Ziel ist es, die Informationssicherheit in den teilnehmenden Institutionen zu verbessern. Der Verbund versteht sich als Beratungs- und Austauschplattform für seine Mitglieder.

Einmal pro Monat treffen sich bwInfoSec und CSBW zu einer Sitzung auf operativer Ebene. Die Teilnehmerinnen und Teilnehmer tauschen sich dabei über aktuelle Themen aus.

Perspektivisch sind eine Kooperation und vertiefende gegenseitige Unterstützung geplant.

Darüber hinaus steht die CSBW zu unterschiedlichen Themen in Kontakt und Austausch mit der Wissenschaft und unterstützt beispielsweise Studierende durch die Übernahme der Zweitbetreuung von Masterarbeiten zu relevanten Themen.

4.5 Gemeinsam bewältigt: „Best Practice“ aus dem Fall Mössingen

An der Bewältigung eines Cyberangriffs sind in der Regel verschiedene Rollen beteiligt: die betroffene Stelle, ein oder mehrere IT-Dienstleister, die Polizei, die CSBW. Der Angriff auf die Stadtverwaltung Mössingen demonstriert eine ideale Kooperation.

[13] Hessen CyberCompetenceCenter (H3C)
[14] Landesamt für Sicherheit in der Informationstechnik (LSI)
[15] https://bwinfosec.de/

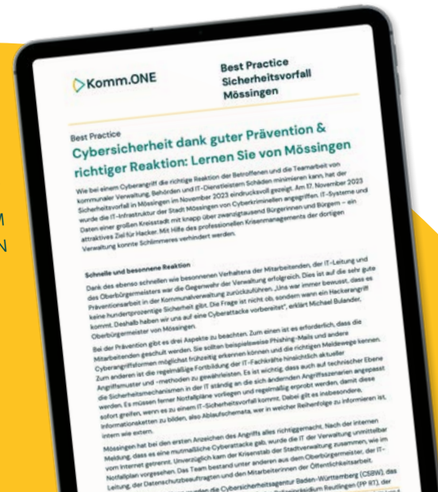
Im November 2023 meldete die Stadtverwaltung Mössingen einen Cybersicherheitsvorfall. Die CSBW entsandte das MIRT, das umgehend vor Ort die Arbeit aufnahm. Das Vorfallmanagement der CSBW übernahm die Koordination des Vorfalls und sorgte für einen reibungslosen Informationsaustausch zwischen den Beteiligten. Diese professionelle und kollegiale Zusammenarbeit ermöglichte eine schnelle und gezielte Vorgehensweise.

Die IT-Forensiker der CSBW analysierten die IT-Systeme. Die Zusammenarbeit mit den IT-Verantwortlichen der Stadt bewirkte die schnelle Identifizierung der betroffenen Systeme, was den Schaden begrenzte. Diese effiziente Nutzung von Ressourcen und Fachwissen war ein Schlüssel zur erfolgreichen Bewältigung des Vorfalls. Neben den technischen Aspekten spielt bei einem Cybersicherheitsvorfall die Krisenkommunikation eine zentrale Rolle. Das erfahrene CSBW-Kommunikationsteam arbeitete eng mit der Stadtverwaltung Mössingen, der kommunalen IT-Dienstleisterin Komm.ONE und dem LKA zusammen, um die Öffentlichkeit angemessen über den aktuellen Stand zu informieren. Denn eine transparente und konsistente Kommunikation trägt erheblich dazu bei, das Vertrauen der Bürgerinnen und Bürger in die Verwaltung zu stärken.

Nach der akuten Phase der Angriffsbewältigung begann der Wiederaufbau der IT-Infrastruktur. In Abstimmung mit dem IT-Dienstleister setzte die Stadt neue, verbesserte Sicherheitsmaßnahmen um, so dass sie den Verwaltungsbetrieb schnell und resilienter wieder aufnehmen konnte. Auch hier war die gute Zusammenarbeit zwischen den Beteiligten von großer Bedeutung. Parallel dazu schaltete das CSBW-Vorfallmanagement die Präventionsabteilung der CSBW ein. Diese Fachleute bieten Sensibilisierungsmaßnahmen und Schulungsangebote für Verwaltungen an.

Aus dem Cybersicherheitsvorfall Mössingen erwuchs in 2024 ein abteilungs- und institutionenübergreifender Best-Practice-Bericht. Er beschreibt die mustergültige Kooperation der Beteiligten.

BEST-PRACTICE-BERICHT ZUM CYBERANGRIFF AUF MÖSSINGEN



5. Resümee und Ausblick

Die CSBW ist nach viel Aufbauarbeit in der Sicherheitsarchitektur des Landes verankert – wenngleich sie sich als junge Behörde stetig weiterentwickelt und ihr Angebotsportfolio ausbaut.

Die weiterhin stark angespannte Cybersicherheitslage Deutschlands sorgte für weiterhin genug Arbeit bei der CSBW, sowohl in den detektiven und reaktiven Bereichen als auch im präventiven Bereich. Die CSBW unterstützte und beriet zahlreiche Behörden und weitere öffentliche Einrichtungen des Landes und der Kommunalebene daher sowohl präventiv als auch reaktiv. Ein Schwerpunkt lag auf dem Ausbau der Angebote, zum Beispiel wurden neue Lerninhalte auf der CSBW-Lernplattform bereitgestellt und die Schwachstellenscans für öffentliche Stellen konzipiert und realisiert. Über allem steht das Ziel, die Cybersicherheit im Land weiter zu fördern.

Ein wichtiger Meilenstein war natürlich der Wechsel in der Behördenleitung und zugleich war dieser die Chance, Bestehendes zu evaluieren und Bewährtes beizubehalten, aber auch notwendige Nachjustierungen vorzunehmen. Das sechste CyberSicherheitsForum, die Teilnahme an der IT-Sicherheitsmesse it-sa in Nürnberg, der Launch des CyberSicherheitsGames auf der Lernplattform sowie der Ausbau der Cyber-Monitorings waren weitere wichtige Meilensteine.

Der Dreiklang aus Prävention, Detektion und Reaktion sorgt weiterhin für ein breites Angebotsportfolio, das im Jahr 2025 geschärft werden soll. Mit neuen Schulungsterminen und -themen, Erklärvideos und neuen an der Bedrohungslage orientierten Angeboten für die Zielgruppen wird die CSBW auch weiterhin auf Risiken im Cyberraum aufmerksam machen und Lösungs- und Hilfsangebote liefern. Auf politischer und regulatorischer Ebene wird sicherlich die Umsetzung der NIS2-Richtlinie weiterhin ein wichtiges Thema sein.

IMPRESSUM

Herausgeber
Cybersicherheitsagentur Baden-Württemberg
Hauptstätter Straße 67
70178 Stuttgart
V. i. s. d. P.: Susanne Krieg

Grafische Umsetzung
orelunited Werbeagentur GmbH
Fritz-Reuter-Straße 18
70193 Stuttgart

Druck
FLYERALARM GmbH
Alfred-Nobel-Str. 18
97080 Würzburg

Naturpapier creme FSC®

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

Redaktionsschluss: 31. Dezember 2024

Mit uns.
Mit Sicherheit.

CSBW

CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG