Baden-Württemberg



JAHRESBERICHT 2025

DER CYBERSICHERHEITSAGENTUR BADEN-WÜRTTEMBERG

CSBW

CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG



www.cybersicherheit-bw.de

JAHRESBERICHT 2025

DER CYBERSICHERHEITSAGENTUR BADEN-WÜRTTEMBERG

CSBW
CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG

Inhalt

S. 6 **Vorwort des Ministers**

S. 8 **Vorwort der Präsidentin**

S. 10 **Einblick in die CSBW – Interview mit Abteilungs- und Stabsleitung**

S. 12 **1. Zahlen, Daten, Fakten 2025**

S. 13 1.1 Allgemeine Zahlen zur CSBW

S. 16 1.2 Zahlen zur Cybersicherheit im Land

S. 18 **2. Die Cybersicherheitslage in Baden-Württemberg**

S. 24 **3. Angebote und Projekte der CSBW 2025**

S. 26 3.1 CyberSicherheitsCheck für kleine und mittlere Unternehmen (CSC KMU)

S. 27 3.2 Notfallübungen nun Teil des Stufenplans Mindestsicherheitsniveau

S. 28 3.3 Neue Schulungs- und E-Learning-Angebote

S. 30 3.4 Neue Sensibilisierungs- und Informationsmaterialien

S. 31 3.5 CSBW-Cybermonitoring

S. 32 3.6 Cybersicherheitsportal Baden-Württemberg

S. 33 3.7 Bund-Länder-Zusammenarbeit verstärkt: Vorsitz der UAG Lagebild bei der CSBW

S. 34 3.8 Unterstützung der Bundestagswahl 2025

S. 35 3.9 Umsetzung der NIS2-Richtlinie und Verabschiedung der CSVO

S. 36 **4. Fazit und Ausblick**

S. 38 **Impressum**



Sehr geehrte Damen und Herren,

das Jahr 2025 war ein herausforderndes Jahr für die Cybersicherheit. Wir erleben immer komplexere und gefährlichere Angriffe, mit dem Ziel, Systeme und Daten von Bürgerinnen und Bürgern, Unternehmen und Behörden zu kompromittieren. Die Cybersicherheit nimmt damit in unserer Sicherheitspolitik eine immer größere Rolle ein.

In Baden-Württemberg unterstützte und beriet die Cybersicherheitsagentur bei 979 Cybersicherheitsvorfällen – die Dunkelziffer der tatsächlichen Fälle dürfte jedoch weitaus höher liegen. Die CSBW unterstützte die Betroffenen bei der Bewältigung dieser Vorfälle und war damit Helferin in der Not. Daher sind die Cybersicherheitsagentur und ihre geleistete Unterstützung nicht mehr aus der Cybersicherheitsarchitektur des Landes – und darüber hinaus – wegzudenken. Durch ihre hervorragende Arbeit haben wir es geschafft, zahlreiche Cyberangriffe zu verhindern, die Auswirkungen von erfolgreichen

Angriffen einzugrenzen und damit dem Land, den Kommunen und der Privatwirtschaft viel Geld, Ärger und „Know-how-Abfluss“ zu sparen. Allein das gezielte CSBW-Cybermonitoring verhindert durch reduzierte Reaktionszeiten und Schadensvermeidung Schäden in Höhe von mehr als 20 Millionen Euro pro Jahr.

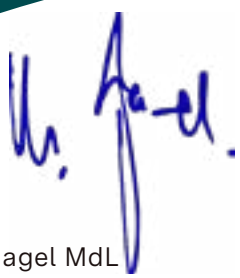
Auch im Vorfeld unterstützte die Cybersicherheitsagentur, damit Schäden proaktiv verhindert werden: Durch ihre zahlreichen Präventionsangebote hat sie dazu beigetragen, dass Angriffe von Kriminellen ins Leere laufen und keine Wirkung erzielen. Jede nach der rund 120 CSBW-Schulungen erkannte Phishing-E-Mail ist ein potenzielles Datenleck weniger.

Ein weiterer wichtiger Schwerpunkt der Arbeit der Cybersicherheitsagentur im Jahr 2025 war außerdem die Förderung der Zusammenarbeit zwischen den verschiedenen Akteuren in der Cybersicherheitslandschaft. Durch die enge Kooperation mit anderen Landesbehörden, den anderen Ländern sowie internationalen Partnern haben wir es geschafft, Kräfte zu bündeln und Anstrengungen zu koordinieren, um die Cybersicherheit in Baden-Württemberg dauerhaft zu stärken.

Die Landesregierung hat in den letzten Jahren durch die Gründung der Cybersicherheitsagentur im Jahr 2021 und den konsequenten, durchdachten Aufbau einer Cybersicherheitsarchitektur die Weichen gestellt und damit die enorme Bedeutung der Cybersicherheit für die Unternehmen, Bürgerinnen und Bürger und die Verwaltung hervorgehoben. Als Innenminister ist es mir ein besonderes Anliegen, die Sicherheit und Integrität unserer digitalen Infrastruktur zu gewährleisten. Deshalb bin ich stolz auf unsere Cybersicherheitsagentur und danke ausdrücklich allen ihren Mitarbeiterinnen und Mitarbeitern für ihre hervorragende Arbeit, ihre fachliche Expertise und ihr persönliches Engagement.

Der vorliegende Jahresbericht gibt einen guten Einblick in die Arbeit der Cybersicherheitsagentur. Allen Leserinnen und Lesern wünsche ich auf den folgenden Seiten eine interessante Lektüre.

Ihr



Manuel Hagel MdL
Minister des Inneren, für Digitalisierung und Europa



Sehr geehrte Damen und Herren,

in einer Zeit, in der sich die politische Weltlage so fragil zeigt wie seit Langem nicht mehr, ist Cybersicherheit aus unserer Sicherheitspolitik nicht mehr wegzudenken. Die Bedrohungslage im Cyberraum hat sich auch 2025 weiter verschärft und es ist notwendiger denn je, dass wir die Anstrengungen zur Sicherheit und Verteidigung im digitalen Raum intensivieren.

Die Gründe dafür sind vielfältig. Cyberangriffe gefährden unsere staatlichen Institutionen, unsere Wirtschaft und unsere kritischen Infrastrukturen wie Energieversorgung, Verkehr und Gesundheitswesen. Erfolgreiche Angriffe können schwerwiegende Auswirkungen auf unser Gemeinwesen und die wirtschaftliche Stabilität haben. Wie verwundbar unsere Gesellschaft ist, zeigte bereits der Stromausfall Anfang des Jahres in Berlin. Ursache war zwar kein Cyberangriff, dies hätte aber genauso gut der Fall sein können. Jedenfalls wurde klar, wie schnell eine Krisenlage entstehen kann.

Cyberangriffe, insbesondere solche auf staatliche Institutionen, und der Umgang damit können zudem das Vertrauen in staatliches Handeln untergraben und letztlich unsere Demokratie gefährden. Die Manipulation von Informationen und die Verbreitung von Fehlinformationen können die öffentliche Meinung beeinflussen und beispielsweise die Integrität unserer Wahlen gefährden. Die Verbreitungswege und technischen Mittel hierfür waren nie besser.

Darum plädiere ich dafür, Cybersicherheit als originäres Thema der Sicherheitspolitik zu betrachten und zu behandeln. Sie ist nicht nur ein Nebenaspekt der Digitalisierung. Wir brauchen ein umfassendes Verständnis, das nicht nur die technische Sicherheit von Systemen und Netzen umfasst, sondern auch die politische und strategische Dimension von Cyberangriffen in den Blick nimmt. In Baden-Württemberg sind wir dafür die ersten Schritte gegangen. Nun gilt es, diesen Weg konsequent weiterzugehen und Cybersicherheit als integralen Bestandteil unserer Sicherheitsarchitektur zu verankern und entsprechende Maßnahmen zu ergreifen, um unsere Sicherheit und Stabilität im digitalen Raum zu gewährleisten.

Als CSBW tragen wir dazu jeden Tag aufs Neue bei. Dieser Jahresbericht gibt Ihnen einen Überblick über unsere Arbeit und die Herausforderungen, denen wir gegenüberstehen. Wir werden alles tun, um eine sichere digitale Zukunft für Baden-Württemberg zu gestalten. Um diese Herausforderungen erfolgreich zu meistern, benötigen wir eine nachhaltige und zukunftsorientierte Ausstattung. Wir müssen als Land in die Weiterentwicklung unserer Kompetenzen und Kapazitäten investieren, um den immer komplexeren Bedrohungen im Cyberraum weiter gerecht zu werden. Es ist von entscheidender Bedeutung, dass wir dranbleiben und die notwendigen Weichen stellen, um die damit verbundenen Gefahren präventiv und detektiv, aber auch reaktiv zu bekämpfen.

Ihre



Nicole Matthöfer
Präsidentin der Cybersicherheitsagentur Baden-Württemberg

Einblick in die CSBW – Woran wir arbeiten und was uns antreibt

Wie würdet ihr das vergangene Jahr bei der CSBW in drei Worten zusammenfassen?
Björn Schemberger: Kurz gesagt: fokussierend, effizienzsteigernd und identitätsstiftend.
Susanne Krieg: Da kann ich mich anschließen und ergänzen: spannend, herausfordernd und wegweisend.

Was sind die prägendsten Entwicklungen oder Trends, die eure Arbeit aktuell am meisten beeinflussen?
Krieg: Das sind natürlich Fragen rund um KI. Wir stellen aber auch fest, dass Cybersicherheit zunehmend flächendeckend als wichtig erkannt wird – und das ist gut so. Das merken wir vor allem an den stark gestiegenen Anfragen zum Angebot der CSBW. Cybersicherheit ist kein Thema mehr nur für Eingeweihte, sondern in der Breite angekommen.
Schemberger: Das kann ich nur bestätigen. Wir nehmen bei uns im Bereich Detektion und Reaktion eine stark wachsende Nachfrage wahr. Immer mehr Organisationen erkennen den Mehrwert der CSBW und wollen unsere Leistungen nutzen. Der Bedarf wächst, daher ist es sehr wichtig, dass wir mitwachsen. Teilweise stoßen wir bereits an Belastungsgrenzen.

Welche Themen bestimmen die inhaltliche und organisatorische Weiterentwicklung der Behörde?
Krieg: Um an die vorherige Frage anzuknüpfen: Der Umgang mit unseren Ressourcen ist ein großes Thema. Wie können wir mit begrenztem Personal möglichst viel erreichen? Wir sind eine kleine Behörde – das hat Vorteile, etwa kurze Wege. Aber auch Nachteile, weil die Aufgaben auf wenige Schultern verteilt sind.
Schemberger: Zudem entwickeln wir die CSBW ständig weiter. Die Cybersicherheit ist ein schnelllebiges Thema, Anforderungen verändern sich oft. Daher ist es wichtig, Aufgaben konsequent dort zu verankern, wo sie fachlich hingehören, und die Strukturen entsprechend zu stärken. Nur so aufgestellt, können wir kurzfristig auf neue Anforderungen reagieren. Das bedeutet auch, Bedarfe klar zu benennen und personell zu unterlegen.

Was zeichnet die CSBW als Arbeitsplatz aus?
Schemberger: Die Mitarbeitenden der CSBW verbindet ein starkes gemeinsames Interesse an der Sache und an den Zielen der CSBW. Die Motivation der Beschäftigten ist sehr hoch.
Krieg: Kein Tag ist wie der andere. Wir haben ein sehr gutes Miteinander und viele hochqualifizierte Kolleginnen und Kollegen mit unterschiedlichsten Hintergründen. Diese Vielfalt empfinde ich als sehr bereichernd.

Wo liegen aktuell die größten Herausforderungen in euren Bereichen?
Schemberger: Cybersicherheit ist ein extrem dynamisches Feld, entsprechend schnelllebig ist auch unser Arbeitsalltag. Wir müssen immer auf dem neuesten Stand bleiben. Die IT-Welt verändert sich rasant. Sei es zum Beispiel der zunehmende Weg in die Cloud oder KI-gestützte Angriffe. Die Komplexität und Anzahl der Vorfälle nehmen zu. Gleichzeitig wächst die Nachfrage nach unseren Leistungen stark.
Krieg: In der Stabsarbeit ist eine zentrale Herausforderung die Vermittlung eines komplexen, oft abstrakten Themas an unterschiedliche Zielgruppen. Wir übernehmen eine verbindende Rolle – intern zwischen Leitung und Fachbereichen sowie extern gegenüber Politik, Verwaltung und Öffentlichkeit.

Welche Botschaften sind im Austausch mit den Kunden und Betroffenen besonders wichtig?
Krieg: Ein Cyberangriff ist kein Makel, sondern eine Straftat. Um ein realistisches Lagebild zu erhalten und andere zu schützen, sollten Vorfälle unbedingt gemeldet werden. Ein offener Umgang damit ist entscheidend.
Schemberger: Insbesondere Führungskräften möchte ich zudem mitgeben: Das abstrakte Bedrohungsrisiko wächst seit Jahren. Die bisherigen Sicherheitsmaßnahmen reichen oft nicht mehr aus. Organisationen müssen IT-Sicherheit noch ernster nehmen und stärker in technische Schutzmaßnahmen investieren. IT-Sicherheit muss mit der Digitalisierung skalieren. Nur wenn IT-Sicherheit beim Design der Digitalisierung mitgedacht wird, kann eine sichere Umgebung gestaltet werden.

Welche Rolle soll die CSBW künftig in Baden-Württemberg einnehmen?
Krieg: Wir werden weiterhin die zentrale Behörde für Cybersicherheit im Land sein und unsere Rolle als Dreh- und Angelpunkt weiter ausbauen…
Schemberger: … Mit zusätzlichem Personal wollen wir unser Angebot erweitern und weitere Zielgruppen erreichen, um das Cybersicherheitsniveau insgesamt zu erhöhen.

Wenn ihr euch etwas für die Zukunft der CSBW wünschen dürft – was wäre das?
Krieg: Ein gesundes, kontinuierliches Wachstum – und dass allen in Baden-Württemberg klar ist: Bei Cybersicherheitsvorfällen hilft die CSBW.
Schemberger: Genau! Wir leisten bereits heute hochwertige Arbeit und unterstützen die Menschen und Organisationen in Baden-Württemberg effektiv. Das zeigt sich auch in dem Willen der neuen Regierung, die CSBW zu stärken und weiter auszubauen. Durch Wachstum wollen wir noch mehr Schlagkraft entwickeln. Nur so kann die CSBW ihre Aufgaben umfassend wahrnehmen und die Cybersicherheit in Baden-Württemberg nachhaltig stärken.



Björn Schemberger ist Vizepräsident der Cybersicherheitsagentur sowie Abteilungsleiter Detektion und Reaktion. In seinem Verantwortungsbereich liegen die Cyber-Ersthilfe, das Lagezentrum, die Vorfallbehandlung, die operative Sicherheitsanalyse sowie die Steuerungsgruppe der Abteilung. Mit seinem Team behält er die aktuelle Bedrohungslage im Blick, berät und unterstützt Betroffene kompetent bei der Bewältigung von Cybersicherheitsvorfällen und macht das Land Schritt für Schritt sicherer im Cyberraum.



Susanne Krieg ist Leiterin des Stabs der CSBW. In ihrem Verantwortungsbereich werden zentrale strategische und organisatorische Themen gebündelt. Dazu zählen insbesondere die Kommunikation und Öffentlichkeitsarbeit, die Arbeit in Gremien und mit Kooperationspartnern sowie die Bearbeitung von politischen und strategischen Fragestellungen und Grundsatzthemen. Der Stab verbindet, koordiniert und vermittelt – intern zwischen allen Ebenen und Bereichen sowie extern gegenüber Politik, Verwaltung und Öffentlichkeit.



1. Zahlen, Daten, Fakten 2025

In CSBW-Sichtweite:



MHP Arena | **Mercedes-Benz-Museum** | **Gaskessel**

1.1 Zahlen zur CSBW

Der Standort der CSBW

3 **S-Bahn-Linien zur CSBW**

8 **Regionalbahnstrecken zur CSBW**

5 **U-Bahn-Linien zur CSBW**

Entfernung zum Stuttgarter Hauptbahnhof (Luftlinie)

3,67 km

Sichtweite aus dem CSBW-Büro bei klarem Wetter vom Wasen bis zur Schwäbischen Alb

40 km

0 **Faxgeräte**

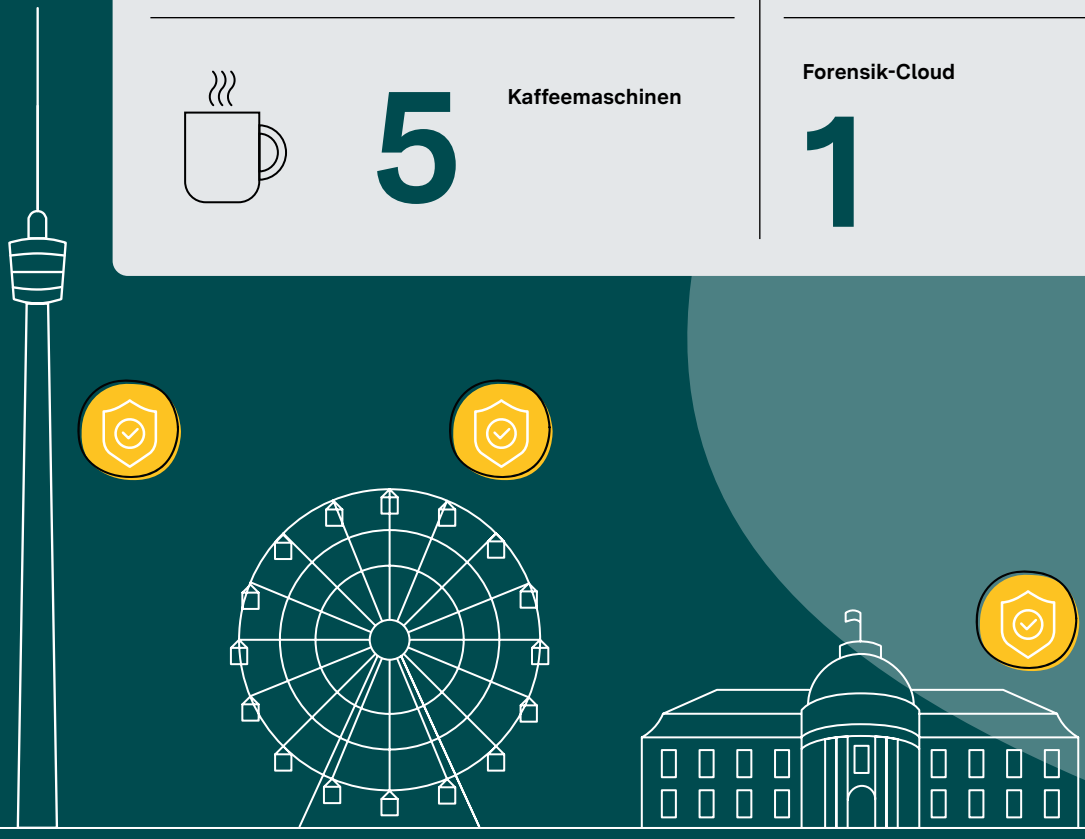
5 **Kaffeemaschinen**

Möglicher Remote-Anteil

60%>

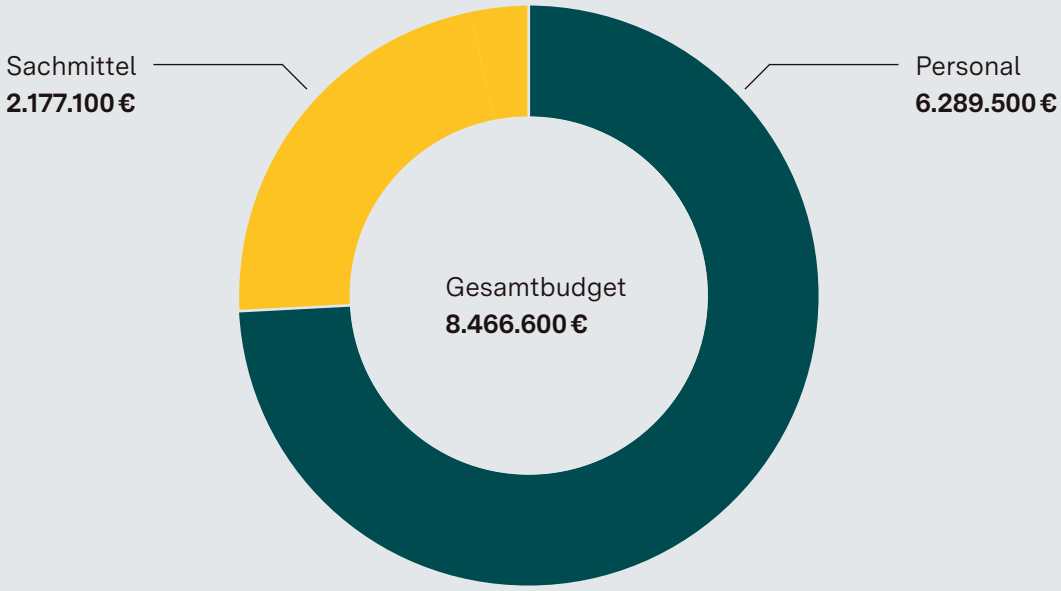
Forensik-Cloud

1



Fernsehturm **Cannstatter Wasen** **Villa Reitzenstein**

Haushalt



Social-Media-Aktivitäten der CSBW auf LinkedIn

Followerwachstum 2025

161 %

Ø Posting-Frequenz

2,3

Beiträge pro Woche

Personal

Stellen im Staatshaushaltsplan: 88,5

Tarifbeschäftigte: 48 %

Beschäftigte im Beamtenstatus: 52 %

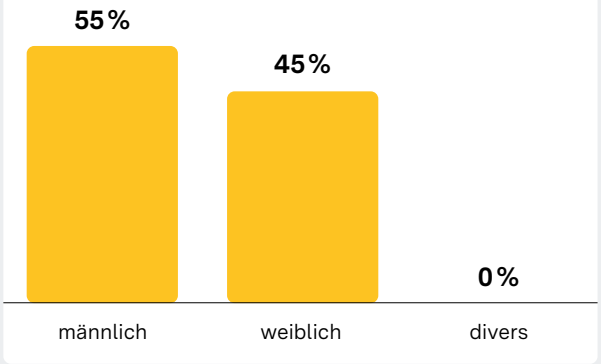
Beschäftigte in Teilzeit[1]: 12

Beschäftigte mit Schwerbehinderung: 3

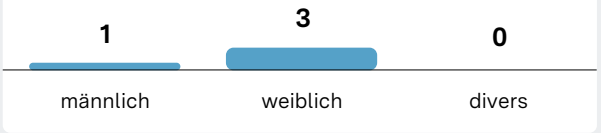
Befristete Beschäftigungsverhältnisse: 0

Leitungspositionen: 5

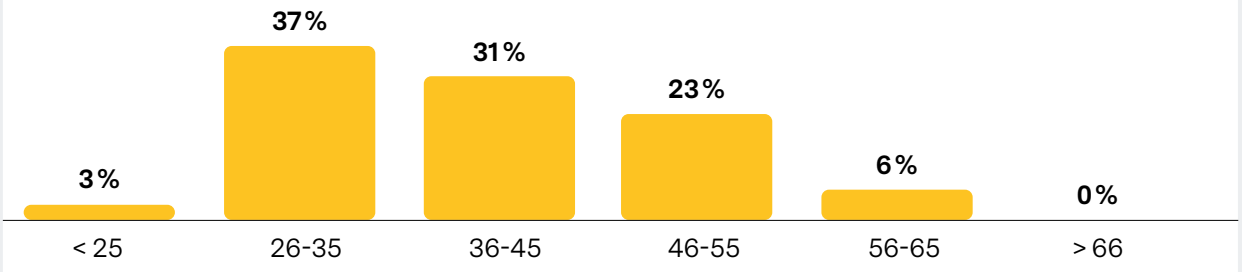
Anteil Beschäftigte nach Geschlecht



Leitungspositionen nach Geschlecht[2]



Altersdurchschnitt: 39,8 Jahre



[1] Beschäftigungsgrade zwischen 50 % und 90 %
[2] Eine Leitungsposition ist bei Redaktionsschluss vakant.

1.2 Zahlen zur Cybersicherheit im Land

() Zahlen in Klammern geben die Vorjahreswerte an.

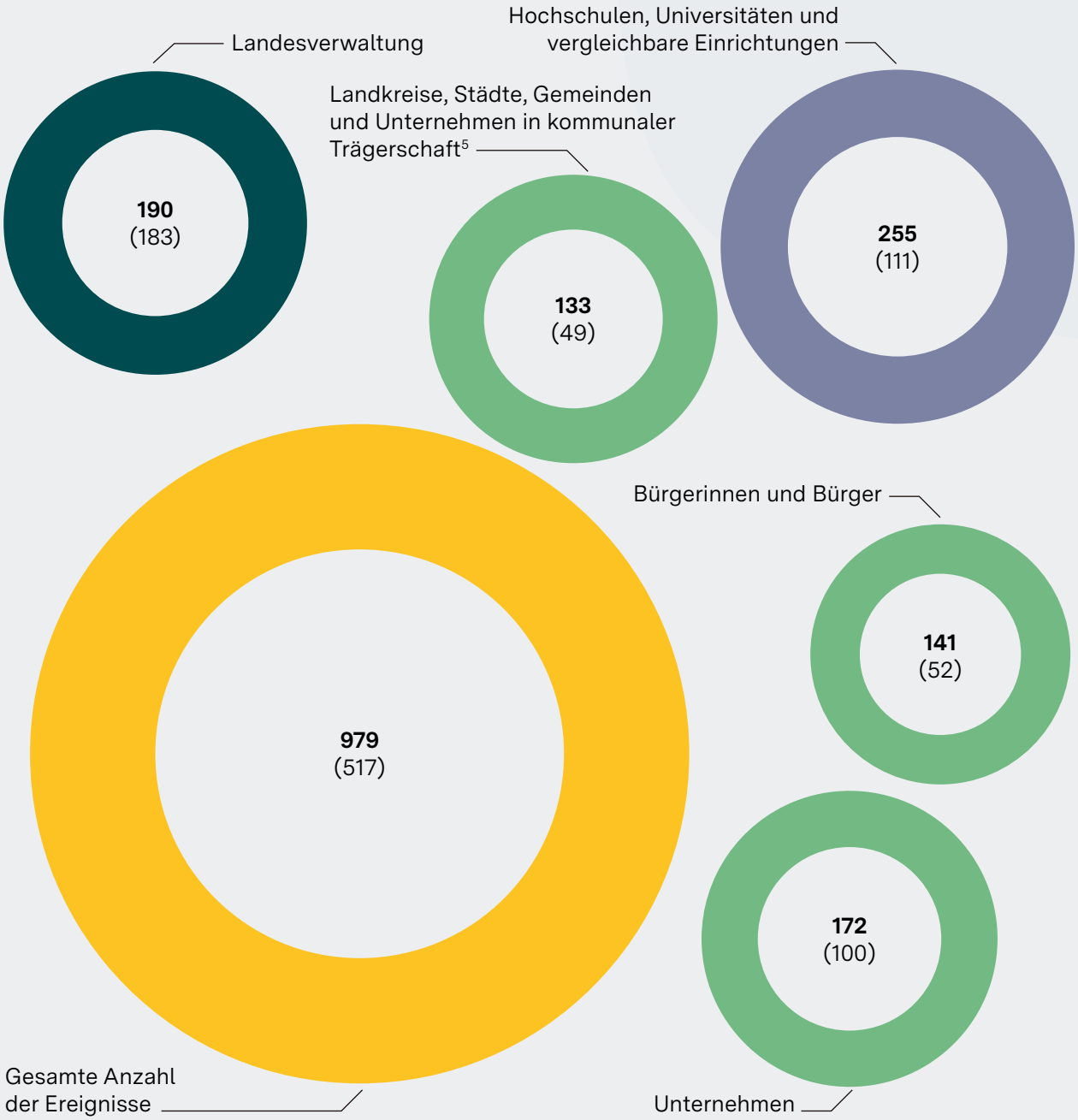
Detektion und Reaktion

IT-Sicherheitsvorfälle und sicherheitsrelevante Ereignisse[3]

979 **Fälle**[4] (517)

89 % **Steigerung im Vergleich zum Vorjahr**

Sicherheitsvorfälle und sicherheitsrelevante Ereignisse (inkl. MIRT[5]-Einsätze) nach Zielgruppen[6]:



[3] Bei der CSBW registrierte und bearbeitete Fälle bei öffentlichen Stellen, Unternehmen und Privatpersonen, in denen die CSBW mit Betroffenen im Austausch war und bei Bedarf beriet und unterstützte.

[4] Da es keine Meldepflicht von Cybersicherheitsvorfällen in Kommunen und der Privatwirtschaft an die CSBW gibt, kann die tatsächliche Zahl der Fälle jeweils größer sein.

[5] Mobile Incident Response Team = mobiles Einsatzteam

[6] Die Lücke von 88 (22) Fällen zur Gesamtzahl entfällt auf die Kategorie „Sonstige“, zu denen Anstalten, Körperschaften und Stiftungen des öffentlichen Rechts; Unternehmen mit Landesbeteiligung; Schulen; Vereine und Verbände gehören.

() Zahlen in Klammern geben die Vorjahreswerte an.

Warnmeldungen und Meldungen bei der Cyber-Ersthilfe BW

Von der CSBW gesendete Warnmeldungen und Informationen über die Plattform des Warn- und Informationsdienstes (WID)

11,3 pro Woche

Eingegangene Meldungen in der Cyber-Ersthilfe BW (per Telefon, E-Mail oder Kontaktformular)

327 mehr als doppelt so viele Fälle wie im Vorjahr (159)

Stunden pro Tag, in denen die CSBW erreichbar ist

24 (24)

Cyber-Monitoring

Über Darknetfunde durch CSBW informierte Betroffene aus Landesverwaltung, Kommunen und Unternehmen in kommunaler Trägerschaft, Hochschulen, Universitäten und vergleichbaren Einrichtungen sowie Unternehmen

249 (90)

Steigerung im Vergeich zum Vorjahr

280 %

Verhinderte Schadenssumme

24 Mio. €

Steigerung der Funde: im öffentlichen Sektor

350 %

in Unternehmen

150 %

an Hochschulen, Universitäten und vergleichbaren Einrichtungen

310 %

Nutzung Präventionsangebote der CSBW

Durchgeführte Schwachstellenscans

38

Reichweite durch IT-Sicherheitsanalysen in Kommunen und Landkreisen in Einwohnern

3.595.170

Schulungen:

Ø Schulungen pro Woche

> 2

Kommunen, die ein Schulungsangebot der CSBW wahrgenommen haben

237



2. Die Cybersicherheitslage in Baden-Württemberg

Ronja Kemmer –
Chief Digital Officer der Landesregierung im Ministerium des Inneren, für Digitalisierung und Europa

„Cybersicherheit ist ein absolutes Top-Thema. Digitale Verwundbarkeit ist ein reales Risiko für Gesellschaft, Wirtschaft und Staat. Entscheidend ist deshalb, dass wir uns gegen Cyberangriffe abhärten. Dabei unterstützt die CSBW mit hoher Expertise und trägt so dazu bei, den digitalen Raum sicherer zu machen.“

Die Cybersicherheitsagentur schätzt die Cyberbedrohungslage in Baden-Württemberg unverändert hoch ein. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) kommt für Deutschland zu ähnlichen Erkenntnissen. Die CSBW registrierte 2025 insgesamt eine deutlich höhere Fallzahl und insbesondere einen großen Anstieg der Anzahl sicherheitsrelevanter Ereignisse.

Registrierte Fälle: IT-Sicherheitsvorfälle und sicherheitsrelevante Ereignisse

Die Verwaltungsvorschrift zur Informationssicherheit, erlassen vom baden-württembergischen Innenministerium, unterscheidet zwischen **Sicherheitsvorfällen** und **sicherheitsrelevanten Ereignissen**. Sicherheitsrelevante Ereignisse können sich zum Sicherheitsvorfall entwickeln und werden nur in der jeweiligen End-Kategorie gezählt.

Im Vergleich zum Vorjahreszeitraum stieg die Zahl der von der CSBW erfassten Sicherheitsvorfälle nur unwesentlich, die der registrierten sicherheitsrelevanten Ereignisse jedoch um knapp 140 %. Hierbei liegt der größte Anteil bei potenziell kompromittierten Zugangsdaten, Phishing-Versuchen und verdächtig erscheinenden E-Mails sowie ausnutzbaren Schwachstellen in IT-Systemen. Die Zahl der erfassten Kompromittierungen von Passwörtern und damit verbundenen Accounts hat sich im Vergleich zu 2024 mehr als verdoppelt. Dies ist auch auf ein deutlich verbessertes und ausgeweitetes Monitoring zurückzuführen, wodurch mehr Vorfälle erkannt werden konnten.

Im Berichtszeitraum kam es zu Fällen ganz unterschiedlicher Schwere. Von großer Bedeutung und mit schwerwiegenden Folgen bei den Betroffenen waren beispielsweise der erfolgreiche Angriff auf den Online-Shop einer Landesinstitution, die zum Teil erfolgreiche Netzwerkkompromittierung einer Hochschule und eine schwerwiegende Fehlkonfiguration der Website einer Kommune. Außerdem erfasste die CSBW erfolgreiche Ransomware-Angriffe auf drei Schulen und zwei Kommunen. Das MIRT (Mobile Incident Response Team) der CSBW rückte in drei dieser Fälle aus, um den Betroffenen vor Ort zu helfen. Durch die Bereitstellung der für solche Fälle von der CSBW vorgehaltenen Notfallausrüstung, konnte die Arbeitsfähigkeit vor Ort rasch wiederhergestellt werden.

Die anderen registrierten Fälle hatten keine so schwerwiegenden Folgen oder größere Auswirkungen bei den Betroffenen. In den Fallzahlen sind auch kurzzeitige Störungen, Systemausfälle oder Benutzungsfehler berücksichtigt, sofern diese die Verfügbarkeit beeinträchtigten.

Eine Meldepflicht für Sicherheitsvorfälle 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 sowohl im privatwirtschaftlichen als auch im kommunalen Bereich und sollte bei den folgenden Zahlen und Einordnungen berücksichtigt werden.

Cyber-Monitoring

Ergänzend zu den bei der CSBW eingehenden Meldungen vervollständigt das Cyber-Monitoring der CSBW das Lagebild. Die CSBW überwacht mit ihrem Cyber-Monitoring den Cyberraum auf:

- Angekündigte und durchgeführte Ransomware-Angriffe sowie geleakte Daten
- Credential Leaks
- Schwachstellen in IT-Systemen und Software
- Kompromittierte IT-Systeme und Netzwerke
- Angekündigte und durchgeführte DDos-Angriffe (Distributed Denial of Service)

Über etwaige Funde informiert die CSBW betroffene Behörden, Institutionen und Unternehmen. So können Betroffene bestehende Sicherheitslücken schließen und sich auf mögliche Auswirkungen gezielt vorbereiten. Durch die Nutzung von Cyber-Threat-Intelligence-Plattformen kann die CSBW mehr Fälle häufiger und früher erkennen. Dies mildert die Auswirkungen eines Angriffs oder verhindert ihn sogar komplett. Dadurch trägt die CSBW deutlich zur Verbesserung der Cybersicherheit bei. Die frühzeitige Aufdeckung von geplanten DDoS-Angriffen ermöglicht beispielsweise ein wertvolles Zeitfenster, um Abwehrmaßnahmen gezielt zu härten.

Doch nicht nur Zeit, sondern auch Geld kann so gewonnen werden: Durch das Cyber-Monitoring der CSBW konnten 2025 potenzielle Schadenssummen in Höhe von 24 Millionen Euro verhindert werden. Insofern ist die CSBW eine gute Investition in die Cybersicherheit des Landes.

IT-Sicherheitsvorfälle und sicherheitsrelevante Ereignisse nach Zielgruppen

Die Anzahl der Sicherheitsvorfälle in **Landkreisen**, **Städten und Gemeinden** sowie bei **Unternehmen in kommunaler Trägerschaft** stieg um fast 50 % im Vergleich zum Vorjahr. Die Anzahl der sicherheitsrelevanten Ereignisse stieg um mehr als 170 %.

Die Anzahl der Sicherheitsvorfälle in der **Landesverwaltung** halbierte sich im Jahr 2025. Die Anzahl der sicherheitsrelevanten Ereignisse stieg um knapp 4 % im Vergleich zum Vorjahr.

Die Anzahl der Sicherheitsvorfälle an **Hochschulen**, **Universitäten und vergleichbaren Einrichtungen** stieg nur leicht an. Die Anzahl der sicherheitsrelevanten Ereignisse verzeichnete jedoch einen Anstieg um mehr als 130 % im Vergleich zum Vorjahr.

Unabhängig von der Zielgruppe umfassten die Unterstützung und Beratung der CSBW die Untersuchung verdächtiger Dateien oder E-Mails und die Prüfung von E-Mail-Konten auf Kompromittierung. Außerdem wurde verdächtiges Verhalten von IT-Systemen untersucht und IT-Systeme oder Netzwerksegmente wurden umfassend forensisch analysiert. Schließlich leistete die CSBW Unterstützung bei der Vorfallbewältigung und beriet bei der Krisenkommunikation.

Der Aufwand für die Unterstützungsleistungen der CSBW variierte erheblich, von wenigen Stunden bis hin zu mehreren Wochen. Unabhängig von der Zielgruppe konnten die betroffenen Einrichtungen den Vorfall nur in wenigen Fällen selbstständig bearbeiten. Das Ausrücken des mobilen Einsatz-Teams war glücklicherweise nur in wenigen Fällen notwendig.

Vorfall - und Angriffsarten

Prozentuale Entwicklung im Vergleich zum Vorjahr,
() Zahlen in Klammern geben die absolute Fallzahl für 2025/2024 an.

	Kommunen und Unternehmen in kommunaler Trägerschaft[7]	Landesverwaltung / Landeseinrichtungen	Hochschulen, Universitäten und vergleichbare Einrichtungen
Sicherheitsrelevante Ereignisse	+ 171 % (133/49)	+ 4 % (190/183)	+ 130 % (255/111)
Sicherheitsvorfälle unterschiedlicher Schwere	+ 45 % (29/20)	- 54 % (17/37)	+ 12 % (29/26)

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

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

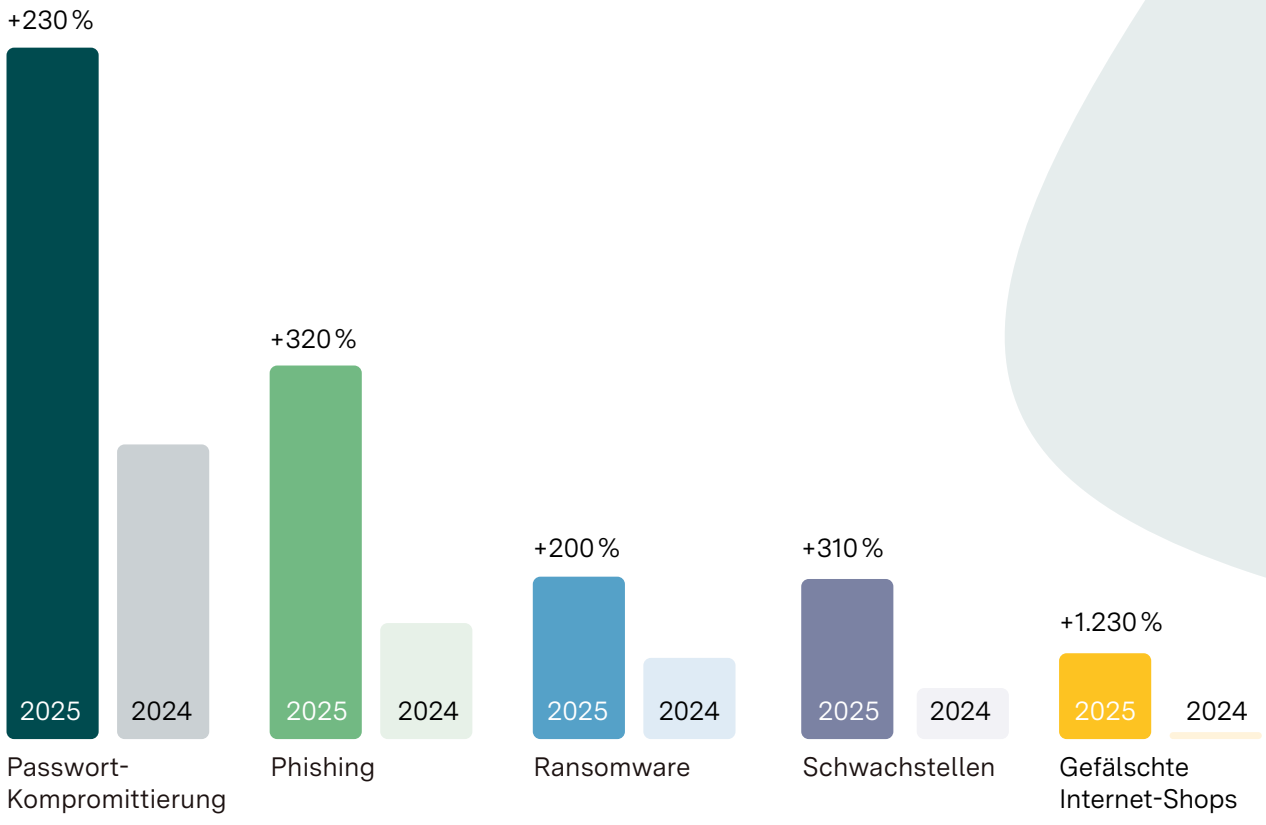
Die CSBW erfasste dabei sowohl zielgerichtete Angriffe, bei denen sich Angreifer ganz konkret ein Opfer aussuchen, als auch breit gestreute Massenangriffe, bei denen Angreifer bekannte Schwachstellen ausnutzen oder Phishing-Mails als Einfallstor verwenden.

Hinsichtlich der Angriffszahlen und Angriffsarten ergibt sich ein klares Bild: Die CSBW konnte ihre Reichweite und Bekanntheit deutlich erhöhen, die Meldebereitschaft ist gestiegen und die Aktivität zahlreicher Cybercrime-Gruppierungen ist angestiegen.

Die sehr starke Zunahme im Vergleich zum Vorjahr von mehr als doppelt so vielen Fällen bei der Passwort-Kompromittierung ist auf einen erhöhten Tool-Einsatz bei der CSBW zurückzuführen. So erkennt die CSBW wesentlich mehr Fälle. Die Zahl der Phishing-E-Mails verdreifachte sich aufgrund einer erhöhten Meldebereitschaft. Die Verdoppelung bei der Erfassung von Ransomware-Angriffen ist einerseits auf ein ausgeweitetes Monitoring durch die CSBW zurückzuführen, durch das mehr Fälle erkannt werden. Andererseits hat die wieder deutlich erhöhte Aktivität von Ransomware-Gruppierungen hierzu beigetragen.

Die Verdreifachung erfasster Schwachstellen geht ebenfalls auf ein verstärktes Monitoring zurück und deckt sich mit den Erkenntnissen des BSI, dass die Zahl der entdeckten Schwachstellen stetig wächst. Neu in den Top 5 der Angriffsarten ist 2025 der Betrug mit Internetshops. Hier stiegen die erfassten Fälle um den Faktor 12 an. Dies liegt vor allem in der größeren Bekanntheit der CSBW bei Unternehmen und Privatpersonen begründet und der inzwischen höheren Meldebereitschaft dieser Zielgruppen.

Top 5 der bei der CSBW erfassten Angriffsarten
Prozentuale Steigerung zum Vorjahr



Einschätzung der Cybersicherheitslage in Baden-Württemberg

Die Bedrohungslage durch Cyberangriffe bleibt in Baden-Württemberg unverändert kritisch. Die bei der CSBW registrierten Fälle haben sich nahezu verdoppelt, was unter anderem auf ein weiter verbessertes Monitoring, aber auch eine erhöhte Meldebereitschaft zurückzuführen ist. Der Rückgang der Fallzahlen des vergangenen Jahres im kommunalen Umfeld hat sich nicht fortgesetzt. Die Zahlen sind sowohl bei minderschweren Ereignissen als auch bei schwereren Vorfällen wieder angestiegen. Eine enorme Zunahme an sicherheitsrelevanten Ereignissen stellte die CSBW im Hochschulbereich fest. Doch auch in den anderen Zielgruppen stieg diese Zahl deutlich an.

Grund hierfür ist einerseits das toolgestützte Cyber-Monitoring, das wir kontinuierlich weiter ausbauen. Die im Monitoring eingesetzte Software findet geleakte Zugangsdaten, durchsucht automatisiert das Darknet sowie das Clearnet und ermöglicht so eine umfassende Betrachtung des Cyberraums. Dadurch kann die CSBW das Dunkelfeld besser ausleuchten, das allerdings weiterhin groß bleibt.

Weitere Gründe für die gestiegene Fallzahl sind zum einen das personelle Wachstum der CSBW im Jahr 2025, wodurch weitere Aufgaben und Services ausgebaut werden konnten. Zum anderen ist der Bekanntheitsgrad der CSBW gestiegen, was zu einer höheren Zahl an Meldungen durch Betroffene führt. Hier ist für die Zukunft ein weiterer Anstieg zu erwarten, wenngleich es für viele Betroffene weiterhin eine gewisse Hemmschwelle gibt, einen Vorfall zu melden. Sei es aus Scham oder aus Angst vor Imageverlust und Rufschädigung. Die CSBW arbeitet jedoch vertraulich und gibt keine Informationen ohne Zustimmung der Betroffenen an die Öffentlichkeit weiter.

Die CSBW beobachtet, dass es infolge technischer Entwicklungen immer einfacher wird, einen Cyberangriff durchzuführen. Mit Künstlicher Intelligenz (KI) erstellte Phishing-Mails werden beispielsweise immer häufiger und immer besser – und lassen die Erfolgsquote der Kriminellen steigen. Wenn eine Cyber-Gruppierung eine solche E-Mail an 1 Million Empfänger sendet und nur 1 Promille darauf hereinfällt, bleiben immer noch 1.000 Opfer, die die Gruppierung ausbeuten kann.

Ein weiterhin großes Thema sind Ransomware-as-a-Service-Modelle. Dies sind illegale Geschäftsmodelle, die es ermöglichen, Ransomware-Angriffe durchzuführen, ohne dafür technisches Wissen zu benötigen. Man kauft die Ransomware und die notwendige Expertise einfach als Dienstleistung ein.

Barbara Kluge –
Ständige Vertreterin der Abteilungsleitung für Cyber- und Informationssicherheit im Bundesministerium des Innern

„Die Cybersicherheitsagentur Baden-Württemberg ist ein hervorragendes Beispiel dafür, wie sich alle beteiligten Akteure im Cybersicherheitsbereich unkompliziert koordinieren und wie sie zusammenarbeiten. Denn Cybersicherheit ist eine gesamtstaatliche Aufgabe. Aus dem „Ländle“ stammend erfüllt es mich mit besonderem Stolz zu sehen, wie Baden-Württemberg neue Maßstäbe bei der Bündelung von Kräften für mehr Cybersicherheit setzt.“

Dass die Zahlen nicht noch viel deutlicher angestiegen sind, führt die CSBW auf ein großes Dunkelfeld, aber auch die Präventionsarbeit der CSBW sowie anderer Einrichtungen und die damit verbundene erhöhte Wachsamkeit der Mitarbeiterinnen und Mitarbeiter auf den verschiedenen Verwaltungsebenen in Baden-Württemberg zurück.

Die Zunahme entdeckter Software-Schwachstellen, über die sich Angreifende unberechtigten Zugang zu IT-System verschaffen können, vergrößert die Angriffsfläche und damit die Wahrscheinlichkeit, Opfer eines Cyberangriffs zu werden. Deshalb ist es so wichtig, Software zu aktualisieren, sobald ein Patch zur Verfügung steht.

Eine nicht unwesentliche Rolle im Cyberraum spielt die geopolitische Situation. Der seit Februar 2022 andauernde Ukraine-Krieg und der weiter ungelöste Gaza-Konflikt rufen vermehrt staatliche Cyberakteure auf den Plan. Diese sind vor allem im Spionagebereich aktiv und hinterlassen in der Cyberwelt ihre Spuren. Die politischen Spannungen zwischen den USA und China sowie zwischen den USA und dem Iran tragen ebenfalls zu einer verschärften Lage im Cyberraum bei.



Bernd Geisler –

Präsident des Landesamtes für Sicherheit in der Informationstechnik

„Mit der CSBW verbindet uns eine mehrjährige vertrauensvolle Zusammenarbeit. Der gegenseitige Austausch von Informationen und Know-how kommt den Landesverwaltungen und vor allem den Kommunen in Baden-Württemberg und Bayern zugute.“



3. Angebote und Projekte der CSBW 2025

Cybersicherheit ist ein hochdynamisches Feld. Für uns als CSBW bedeutet das, dass wir die Risiken und Trends in der Cybersicherheit stets beobachten und unsere Angebote entsprechend überprüfen und anpassen. Um unseren Kundinnen und Kunden einen Überblick unserer Services zu geben, nutzen wir unsere Portfolioübersicht.

Das gesamte CSBW-Produktportfolio

WEITERBILDUNG

Schulungen / Webinare

- Grundlagen- und Aufbauschulung
- Cybersicherheit
- Cybersicherheit als Führungsaufgabe[8]
- BSI IT-Grundschutz: Einführung und Übersicht
- BSI IT-Grundschutz Praktiker (Zertifizierung)
- BSI BCM-Praktiker (Zertifizierung)
- Krisenkommunikation
- Künstliche Intelligenz
- Anwendung von Offline-Passwortmanagern
- IoT & Cybersicherheit

Web-Based-Trainings

- Grundlagen der Cybersicherheit
- Cybersicherheit im Büro / im Homeoffice
- Informationssicherheit unterwegs
- Spam, Phishing, Smishing
- Sichere Passwörter, Social Media und IoT
- Informationssicherheitsmanagement (ISMS)
- KeePass2

Serious Game

- CyberSicherheitsGame BW

ERSTHILFE & REAKTION

Cyber-Ersthilfe BW

- 24/7-Meldemöglichkeit per Telefon, E-Mail oder Formular
- Kontaktierung Betroffener bei Clear- und Darknetfunden sowie Schwachstellen
- Eskalationsmanagement

Vorfallbehandlung

- Analyse von Sicherheitsvorfällen und Verdachtsfällen
- Technische Unterstützung und Beratung zur IT-Sicherheit
- Mobile Incident Response
- Vorfallmanagement
- Unterstützung des Kunden beim Krisenmanagement
- Notfall-Equipment
- Krisenkommunikation

WISSEN

Factsheets zu diversen Themengebieten

- Sicheres Arbeiten: Homeoffice und Arbeitsplatz
- Künstliche Intelligenz
- Cybersicherheitsvorfall erkennen
- u.v.m.

Erklärvideos

- Phishing, Smishing und Vishing
- Sichere Passwörter
- Fake-Webseiten, Fake News und DeepFake
- u.v.m.

„Kurz erklärt“

- Die häufigsten Cyberbedrohungen
- Hackergruppen
- Künstliche Intelligenz

IT-BETRIEB

Unterstützung Rechenzentren

- Cyber- und Darknet-Monitoring
- Information zu SW-Schwachstellen
- Malware Information Sharing Platform (MISP)
- Operative Vernetzung mit Partnern (u.a. VCV-Austausch) Sektor
- Beratung zu Sicherheitsarchitekturen (Prüfdokument)
- Vernetzung und Unterstützung der Rechenzentren

SENSIBILISIERUNG

Sensibilisierungsaktionen zur Cybersicherheit

- Saisonale oder anlassbezogene Aktionen (z.B. Cybersicherheit in der Weihnachtszeit, Wahlen)

Handlungsempfehlungen Cybersicherheit

- Leitfaden in Deutsch und Englisch
- CSBW-Notfallkarte

Phishing-Simulation

(Abrufmöglichkeit für Ressorts)

CSBW-Passwortrechner

STANDORTBESTIMMUNG

Beratung für KMU

- CyberSicherheitsCheck für KMU (CSC KMU)

Operative Sicherheitsanalyse

- Schwachstellenscan
- Web-Applikations-Scan
- Beratung zu Sicherheitsarchitekturen (Prüfdokument)

Beratung für die Landesverwaltung und Kommunen / Stufenplan Mindestsicherheitsniveau

- Checkliste Grundzüge IT-Sicherheit
- IT-Sicherheitsanalyse
- IT-Notfallübungen
- ISMS-Vorlagen

DETEKTION & REPORTING

Warn- und Informationsdienst

- Lagebild zur Cybersicherheit
- Bewertung der Lageentwicklung
- Warnmeldungen und Handlungsempfehlungen
- Cyber- und Darknet-Monitoring
- Information zu SW-Schwachstellen
- Operative Vernetzung mit Partnern im öffentlichen Sektor (u.a. VCV-Austausch)

AUSTAUSCH

Operative Vernetzung

- Vernetzung und Unterstützung der Rechenzentren
- Austausch mit weiteren fachlich zuständigen Stellen
- Vernetzung mit relevanten Akteuren (auch Sicherheitsbehörden)
- Incident-Onboarding (Kennenlernen des Kunden vor dem Krisenfall)
- Weitere Austausche u.a. mit internationalen Partnern
- Fachliche Hospitationen

Bitte beachten:
Der Zugriff auf die WID- und CSBW-Lernplattform ist nur über das Netz der Landes- und Kommunalverwaltung möglich.

[8] Erfüllt die Anforderungen der verpflichtenden Führungskräfteschulung nach NIS2.

3.1 CyberSicherheitsCheck für kleine und mittlere Unternehmen (CSC KMU)

- **60-minütige Einstiegsberatung**
- **Unternehmensleitung im Fokus**
- **8 Themenschwerpunkte**

Der CyberSicherheitsCheck für KMU ist eine Einstiegsberatung zum Thema Cybersicherheit für kleine und mittelständische Unternehmen. Geschulte Beraterinnen und Berater sensibilisieren in circa einstündigen Gesprächen die Unternehmensleitung für die grundlegenden Themen der Cybersicherheit, ihre Verantwortung in der Führungsrolle sowie für die Umsetzung konkreter Maßnahmen. Mit einer Checkliste wird der Ist-Zustand erhoben und daraus werden konkrete Handlungsempfehlungen für mehr Cybersicherheit im Betrieb identifiziert. Das Beratungsangebot erfolgt unter Koordinierung und Anleitung der CSBW über Multiplikatoren, die den Unternehmen geschulte Beraterinnen und Berater für den CSC KMU zur Seite stellen.

Ursprünglich als Forschungsprojekt gestartet, übernahm 2025 die CSBW die Bearbeitung dieses wichtigen Bausteins in der Cybersicherheitsarchitektur des Landes Baden-Württemberg.

Die CSBW entwickelt den CSC KMU seither fort. Nach einer ersten Bedarfserhebung wurde der Lenkungsausschuss gegründet. In diesem tauschen sich das Innenministerium BW, das Wirtschaftsministerium BW, das Landesamt für Verfassungsschutz BW, das Landeskriminalamt BW sowie der Baden-Württembergische Industrie- und Handelskammertag (BWIHK) und der Baden-Württembergische Handwerkstag (HandwerkBW) regelmäßig zu strategischen und organisatorischen Themen der Weiterentwicklung aus.

Gleichzeitig findet der Aufbau einer eigenen Community für die zahlreichen Beraterinnen und Berater mit Hilfe einer eigenen Veranstaltung statt, dem sogenannten Netzwerktreffen, welches bereits zweimal mit großem Erfolg durchgeführt wurde.

Bei Interesse am CSC KMU können sich Unternehmen aus Baden-Württemberg direkt an die IHKen, HWKen sowie die Wirtschaftsförderung Nordschwarzwald wenden.

Das erfolgreiche Konzept des CSC KMU, das schon mehrere hundert Male durchgeführt wurde, stößt auch bundesweit auf Interesse. So schloss die CSBW eine Kooperation mit der Deutschen Industrie- und Handelskammer sowie mit der Digital Agentur Berlin und macht den CSC KMU somit bundesweit verfügbar. Erste Betriebe außerhalb von Baden-Württemberg wurden anhand des CyberSicherheitsChecks beraten und haben dadurch ihr Cybersicherheitsniveau verbessert.

Ein Ausbau hinsichtlich weiterer Multiplikatoren wird angestrebt.

CSBW CYBER SICHERHEITS CHECK BADEN-WÜRTTEMBERG

3.2 Notfallübungen nun Teil des Stufenplans Mindestsicherheitsniveau

Der Stufenplan Mindestsicherheitsniveau hat das Ziel, gemeinsam das Sicherheitsniveau in Baden-Württemberg zu erhöhen und eine Hilfestellung für den Einstieg in den BSI-IT-Grundschutz zu geben. Stufe 1 bezieht sich auf die Checkliste Grundzüge IT-Sicherheit und Stufe 2 auf die IT-Sicherheitsanalysen.

Nach rund zwei Jahren praktischem Einsatz des Stufenplans Mindestsicherheitsniveau in Stadt- und Gemeindeverwaltungen wurde dieser auf alle öffentlichen Zielgruppen der CSBW ausgeweitet. Das heißt, auch die Landesverwaltung sowie Landkreise können ihn nun nutzen und damit die Cybersicherheit in ihren Behörden verbessern.

Neben der Ausweitung auf weitere Zielgruppen wurde der Stufenplan Mindestsicherheitsniveau auch fachlich weiterentwickelt. Die Ergebnisse der abgeschlossenen IT-Sicherheitsanalysen zeigten einen großen Bedarf an Grundlagen wie Leitlinien oder Nutzungsrichtlinien. Die CSBW hat hierfür Muster entwickelt und stellt diese auf Anfrage allen öffentlichen Stellen in Baden-Württemberg zur Verfügung.

- Leitlinie zur Informationssicherheit
- IT-Nutzungsrichtlinie
- Bestellungsurkunde einer oder eines Informationssicherheitsbeauftragten
- IT-Betriebshandbuch
- Berechtigungskonzept
- Checkliste IT-Notfallmanagement bei Cyberangriffen

Außerdem wurde der Stufenplan um IT-Notfallübungen erweitert, deren Ziel die Sensibilisierung der gesamten Organisation ist, um frühzeitig präventive Maßnahmen zu ergreifen und so bei einem tatsächlichen Cyberangriff den Schaden so gering wie möglich zu halten. Zu den zentralen Aspekten gehören unter anderem die Zusammensetzung eines Krisenstabs, interne und externe Krisenkommunikation sowie die richtige Anwendung eines IT-Notfallhandbuchs.



Dr. Frank Mentrup –
Präsident des Städtetags BW

„Die Cybersicherheitsagentur Baden-Württemberg ist ein verlässlicher Partner der Kommunen – sowohl in der Prävention als auch im akuten Fall eines Cyberangriffs. Sie stärkt das Bewusstsein für Cybersicherheit und unterstützt Kommunen dabei, digitalen Risiken souverän zu begegnen.“

3.3 Neue Schulungs- und E-Learning-Angebote

Ein besonders wichtiger Baustein der Prävention vor Cyberangriffen liegt im Bewusstsein für die Risiken sowie für die Möglichkeiten, sich bestmöglich vor ihnen zu schützen. Mit den Schulungen und E-Learning-Angeboten bietet die CSBW den Mitarbeitenden der Landesverwaltung und Kommunen im Land ein vielseitiges Angebot zur Weiterbildung an. Ob in Präsenz, als Web-Based-Training oder als Webinar: Die CSBW hat auch 2025 neue attraktive Schulungsangebote zu Grundlagen und speziellen sowie aktuellen Themen entwickelt.

Web-Based-Training-Reihe: „Grundlagen der Cybersicherheit“

In der dreiteiligen Web-Based-Training-Reihe „Grundlagen der Cybersicherheit“ lernen Teilnehmende zentrale Begrifflichkeiten und die Grundwerte der Informationssicherheit kennen, erhalten Einblicke in reale Angriffsmethoden und erfahren, wie sie Bedrohungen frühzeitig erkennen und angemessen reagieren.

Das erste Modul legt die theoretischen Grundlagen, skizziert die relevantesten Zertifizierungen (BSI IT-Grundschutz und DIN EN ISO 27001) und zeigt, wie Cyberangriffe in der Realität ablaufen können. Im zweiten Modul wechselt die Perspektive: In der Rolle einer bzw. eines Cyberkriminellen planen die Nutzerinnen und Nutzer einen Angriff und erstellen eine Fake-Website. So wird ersichtlich, wie Angreifende in der Praxis vorgehen. Den Abschluss bildet das dritte Modul, das den Fokus auf das Erkennen eines Cyberangriffs und die richtige Reaktion legt.

Das E-Learning-Angebot ist seit dem zweiten Quartal 2025 verfügbar und wurde im Jahr 2025 insgesamt 18.736-mal von Teilnehmenden aus der Landes- und Kommunalverwaltung abgerufen.

Schulungsangebot zur Cyber-Krisenkommunikation

Welche Kommunikationsschritte werden im Cyber-Krisenfall notwendig? Was kann schon vor einem Cyber-Krisenfall vorbereitet werden? Diese und weitere Fragen thematisiert das Schulungsangebot „Einführung in die Grundlagen der Cyber-Krisenkommunikation“. Ziel der 90-minütigen Schulung ist es, Mitarbeitende aus Presse- und Öffentlichkeitsarbeit der Landes- und Kommunalverwaltungen für eine gut vorbereitete Krisenkommunikation zu sensibilisieren.

Inhaltlich bietet die Schulung einen leicht verständlichen Überblick zu den notwendigen Kommunikationsschritten im Cyber-Krisenfall und zeigt anhand realer Beispiele Tipps zur kommunikativen Vorbereitung auf einen Krisenfall auf. Auch die Grundsätze und Kernbotschaften einer gelungenen Cyber-Krisenkommunikation sind Themen der Schulung.

„IoT und Cybersicherheit – Tipps zum Schutz von IoT-Geräten“

Die Digitalisierung unterschiedlichster Arbeitsaufgaben wird häufig durch den Einsatz von IoT-Geräten (Internet of Things) unterstützt. Cyberkriminelle nutzen diese jedoch auch als Angriffsvektor aus. Ziel der 90-minütigen Schulung ist es, die Teilnehmenden für die Gefährdungen von ungeschützten IoT-Geräten zu sensibilisieren.

Inhaltlich lernen die Teilnehmenden leicht verständlich die Funktionsweise von IoT-Geräten beispielhaft anhand eines Sprachassistenzsystems kennen. Darüber hinaus wird mit Hilfe realer Beispiele auf die Cybersicherheits-Gefährdungen durch IoT-Geräte eingegangen. Außerdem werden wichtige Tipps zum Schutz von IoT-Geräten gegeben, wie z. B. die Absicherung der Geräte durch einen Passwortschutz und eine sichere Konfiguration des Home-Routers.

Schulung zum aktuellen Thema Künstliche Intelligenz

Die 90-minütige Schulung „Künstliche Intelligenz – Tipps zur sicheren Nutzung“ liefert eine Übersicht über die Funktionsweise Künstlicher Intelligenz sowie deren typische Einsatzzwecke im öffentlichen Bereich. Ziel der Schulung ist es, die Aufmerksamkeit für Chancen und Risiken von KI-Anwendungen zu wecken und leicht umsetzbare Tipps zur sicheren Nutzung aufzuzeigen.

Die Schulung richtet sich an Mitarbeitende aus Landes- und Kommunalverwaltungen. Inhaltlich wird neben der Funktionsweise von KI auf die Gefahren eingegangen, insbesondere bei generativen KI-Modellen. Die Schulung fokussiert sich hierbei auf die Cybersicherheits-Gefährdungen beispielsweise durch Large-Language-Models. Zahlreiche Tipps zur sicheren Nutzung von KI und zur Erkennung von sogenannten Deepfakes runden die Inhalte ab.

Das Schulungsangebot wurde schnell stark nachgefragt. Noch im Jahr 2025 fand es insgesamt 10-mal statt.

Webinar: „BSI IT-Grundschutz-Praktiker“

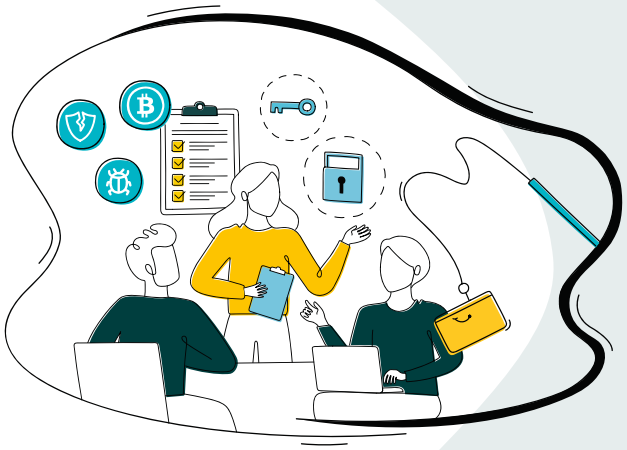
Ergänzend zur Zertifizierung zum BSI IT-Grundschutz-Praktiker hat die CSBW ein niederschwelliges und kompaktes dreistündiges Webinar zum BSI IT-Grundschutz entwickelt. Es greift u. a. die wichtigsten Begriffe, Standards und Vorgehensweisen auf.

Business-Continuity-Management als Grundlage einer resilienten Struktur: Zertifizierung zum BCM-Praktiker

Zum Schutz vor Cybersicherheitsvorfällen müssen technische und organisatorische Maßnahmen sowie die Fachkompetenz der Beschäftigten gewährleistet sein. Die Aus- und Weiterbildung der verantwortlichen Personen ist dabei ein entscheidender Faktor. Für eine höhere Resilienz müssen sich Organisationen mit dem Thema Business Continuity Management (BCM) auseinandersetzen.

BCM ist dabei ein systematischer Ansatz, um sicherzustellen, dass die eigene Organisation auch bei Störungen wie Cybersicherheitsvorfällen handlungsfähig bleibt. Der Ansatz umfasst die Identifikation kritischer Fachverfahren bzw. Geschäftsprozesse, die Bewertung von Risiken und die Sicherstellung von Maßnahmen zur Aufrechterhaltung oder schnellen Wiederherstellung dieser Prozesse. So sollen Ausfallzeiten minimiert und die Resilienz gestärkt werden.

Zur Ausbildung von Fachleuten hat die CSBW im vierten Quartal 2025 die Zertifizierung zum BCM-Praktiker erfolgreich pilotiert. Auch 2026 soll Mitarbeitenden von öffentlichen Stellen diese Zertifizierung angeboten werden.



3.4 Neue Sensibilisierungs- und Informationsmaterialien

Der Faktor Mensch ist bei Abwehr von Gefahren im Cyberraum entscheidend. Mit Hilfe unterschiedlicher neuer Formate sollen u. a. die Mitarbeitenden der Landesverwaltung sowie der Städte, Gemeinden und Landkreise für aktuelle Themen, wie beispielsweise Künstliche Intelligenz, sensibilisiert werden. Einige Produkte stehen auch als Print-Version zur Verfügung und kommen bei Veranstaltungen und Schulungen zum Einsatz. Ein großer Teil der Sensibilisierungsmaterialien, wie z. B. die Erklärvideos und Factsheets, ist öffentlich über die Website der CSBW zugänglich und steht somit auch KMU und Bürgerinnen und Bürgern zur Verfügung. Im Jahr 2025 sind zur Prävention die nachfolgenden Sensibilisierungs- und Informationsmaterialien entstanden.

Erklärvideos und Factsheets

Die Erklärvideos sind auf der Webseite der CSBW zu finden. Ziel ist es, Cybersicherheit zu erklären und für alle verständlicher zu machen. Im Jahr 2025 sind Erklärvideos zu den Themen Künstliche Intelligenz, Fake-Webseiten, Fake-News und Deepfakes, sichere Cloud-Nutzung und IoT veröffentlicht worden.[9]

Zudem veröffentlichte die CSBW insgesamt sieben neue CSBW-Factsheets auf der Website.[10] Sie informieren niederschwellig zu den Themen Künstliche Intelligenz, Passkeys, Täuschungsversuche und Fake-Shops, Identitätsdiebstahl im Internet sowie zu Cloud und sicherer Cloud-Nutzung.

Guide to cybersecurity

Ob bei Veranstaltungen und Schulungen oder in digitaler Anwendung, die Broschüre „Leitfaden zur Cybersicherheit“ ist ein bewährtes und beliebtes Sensibilisierungsprodukt, das niedrigschwellig darüber informiert, wie man Cybersicherheit schaffen und erhalten kann. Seit 2025 ist sie in digitaler Version auch als englischsprachiger „Guide to cybersecurity“ über die Website verfügbar und sorgt so für mehr Awareness bei fremdsprachigen Menschen, bei internationalen Partnerinstitutionen oder bei internationalen Veranstaltungen.[11]

KI „Kurz erklärt“

Im Bereich „Kurz erklärt“ auf der Website liefert die CSBW hilfreiche Informationen zu verschiedenen Aspekten der Cybersicherheit. Neu hinzugekommen ist das Thema Künstliche Intelligenz. Die Seiten erklären leicht verständlich, was Künstliche Intelligenz ist, wie diese funktioniert und welche Chancen und Gefahren hinsichtlich der Cybersicherheit damit einhergehen. Leitfragen vor dem Einsatz von KI-Anwendungen und Tipps zur sicheren Nutzung ergänzen das Angebot.

Notfallkarte für Cybersicherheitsvorfälle

Die CSBW hat eine Notfallkarte für Cybersicherheitsvorfälle konzipiert, die alle wichtigen Schritte aufführt, die bei Meldung eines Sicherheitsvorfalls wichtig sind.[12]

Die Kontaktdaten der internen Meldestellen können individuell eingetragen werden. So ist bei einem Notfall die Nummer schnell zur Hand und die Einleitung unverzüglicher Maßnahmen ist möglich.

Passwortrechner

Auf der CSBW-Lernplattform wurde das Angebot um einen CSBW-Passwortrechner ergänzt. Mit diesem lässt sich die Stärke eines Passworts einschätzen. Der Passwortrechner gibt an, wie lange Angreifende in etwa benötigen, um das eingegebene Passwort zu knacken.

[9] Erklärvideos:

[11] Guide to cybersecurity:

[10] CSBW-Factsheets:

[12] Notfallkarte für Cybersicherheitsvorfälle:

3.5 CSBW-Cybermonitoring

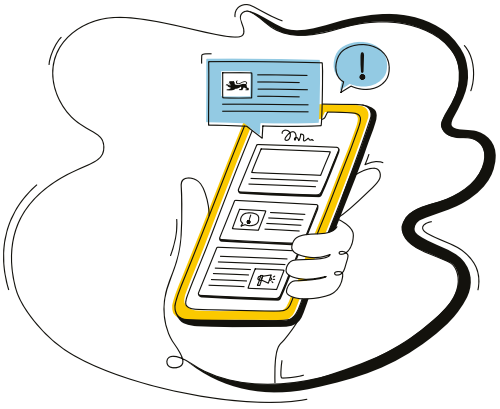
Das Cybermonitoring der CSBW dient der proaktiven Erkennung und Bewertung digitaler Bedrohungen. Zielgruppe sind IT-Verantwortliche, CERTs (Computer Emergency Response Team) und strategische Entscheiderinnen und Entscheider, die auf belastbare Informationen zur Gefahrenlage angewiesen sind. Die Kombination verschiedener Datenquellen und Analysemethoden erlaubt eine frühzeitige Identifizierung potenzieller Risiken, woraus sich Handlungsempfehlungen ableiten lassen.

Der Ansatz umfasst mehrere Ebenen:

- Credential Leaks: Erkennung kompromittierter Zugangsdaten in offenen, kriminellen und geschlossenen Quellen
- Domain- und IP-basierte Überwachung: Laufende Kontrolle der Domains und IP-Ranges von Landesverwaltung, Kommunen und Hochschulsektor auf Missbrauch, Spoofing und technische Schwachstellen. Auf Wunsch nimmt die CSBW weitere berechtigte Einrichtungen in ihr Monitoring auf.
- Akteurüberwachung: Beobachtung relevanter Bedrohungsakteure und ihrer Aktivitäten in einschlägigen Foren
- Ransomware- und Darknet-Monitoring: Identifikation von Leaks, Datenverkäufen oder Erpressungsversuchen
- Telegram: Analyse entsprechender Kanäle zur Früherkennung von DDoS-Aktivitäten
- Schwachstellenüberprüfung: Abgleich bekannter Schwachstellen mit eigenen Systemen

Eingesetzte Tools sind u. a. OSINT (Open Source Intelligence), kommerzielle CTI (Cyber Threat Intelligence)-Feeds und Tools zur Analyse der öffentlichen Angriffsfläche. Durch die Zusammenführung und Auswertung dieser Informationen entsteht ein weitreichendes Lagebild bestehender oder bevorstehender Bedrohungen. Sicherheitsvorfälle können dadurch oft verhindert oder schneller eingegrenzt werden. Das Monitoring verhinderte im Jahr 2025 kalkulatorische finanzielle Schäden durch reduzierte Reaktionszeiten und verminderte Schadenshöhen von 24 Millionen Euro.

Im Betrachtungszeitraum konnten bereits zahlreiche Leaks frühzeitig erkannt, fehlerhafte DNS (Domain Name System)-Einträge korrigiert und missbräuchliche Domain-Verwendungen beendet werden. Das Cybermonitoring der CSBW hat sich damit als effektives Frühwarnsystem und wertvolle Entscheidungsgrundlage etabliert.



Steffen Jäger –
Präsident des Gemeindetags BW

„Auch im vergangenen Jahr war die CSBW wieder ein sehr wertvoller Partner für den Gemeindetag. Gemeinsam arbeiten wir vertrauensvoll und intensiv daran, die Informationssicherheit in den Verwaltungen unserer Gemeinden und Städte weiter zu steigern.“

3.6 Cybersicherheitsportal Baden-Württemberg

Seit ihrer Gründung im Jahr 2021 entwickelte die CSBW kontinuierlich Produkte und Dienstleistungen, um unterschiedliche Zielgruppen bei der Verbesserung ihres Cybersicherheitsniveaus zu unterstützen. Viele dieser Angebote waren jedoch zunächst nur für die Hauptzielgruppen der CSBW über das Landes- und Kommunalverwaltungsnetz verfügbar. So auch die WID-Plattform, die bereits seit Ende 2023 innerhalb der Landes- und der Kommunalverwaltung etabliert ist. Mit der Schaffung eines Cybersicherheitsportals BW[13] erfolgt die Bündelung dieser Angebote an zentraler Stelle auf der Website und wird damit für weitere Zielgruppen zugänglich.

Mit diesem Schritt ist der Warn- und Informationsdienst (WID) der CSBW auch für nicht-öffentliche Einrichtungen verfügbar. Dazu zählen alle Unternehmen, insbesondere die etwa 500.000 kleinen und mittleren Unternehmen in Baden-Württemberg sowie die Bürgerinnen und Bürger des Landes. Das Lagezentrum der CSBW veröffentlicht hierüber aktuelle Meldungen und Empfehlungen rund um das Thema Cybersicherheit. Für Teile davon ist eine einmalige Registrierung der Interessenten erforderlich. Diese Informationsprodukte können sich Interessenten ergänzend per E-Mail zusenden lassen (Push-Service).

Darüber hinaus enthält das neue Webportal das gesamte Beratungsmaterial für den CyberSicherheitsCheck für KMU (CSC KMU). Es ist damit die zentrale Anlaufstelle für alle CSC-KMU-Beraterinnen und -Berater. Diesen Bereich möchte die CSBW schrittweise weiterentwickeln, um die Beraterinnen und Berater durch Fortbildungsangebote, fachliche Handreichungen sowie Handlungsempfehlungen weiter in der Umsetzung des CSC KMU zu unterstützen. Auch die Durchführung der CyberSicherheitsChecks soll dann über ein Online-Tool innerhalb des Cybersicherheitsportals Baden-Württemberg möglich sein.

Das Portal ist so konzipiert, dass der Leistungsumfang in vorab definierten Entwicklungszyklen stetig erweitert werden kann. Die CSBW ergänzt nach und nach zusätzliche Funktionalitäten auf Modulebene. Beispielsweise:

- HPI Identity Leak Checker[14]
- Konfigurationstool für die Planung von Backup-Strategien und zur Durchführung von Pentests
- Architekturkonzepte für Bausteine einer IT-Infrastruktur: z. B. zunächst Ransomware-resilientes Backup, Patch-Management sowie Passwort-Verwaltung und später weitere Inhalte

Somit ist das neue Cybersicherheitsportal auf der Website der zentrale Ort zur Veröffentlichung von Werkzeugen zur Detektion, Reaktion und Prävention von Cybersicherheitsvorfällen für alle Zielgruppen in Baden-Württemberg.

[13] https://portal.cybersicherheit-bw.de/
[14] Mit dem Identity Leak Checker des Hasso-Plattner-Instituts können Sie mit Ihrer E-Mail-Adresse prüfen, ob Ihre Zugangsdaten im Internet veröffentlicht wurden.

3.7 Bund-Länder-Zusammenarbeit verstärkt: Vorsitz der UAG Lagebild bei der CSBW

Seit Anfang 2025 arbeitet die CSBW in der Unterarbeitsgruppe Lagebild (UAG Lagebild) der Länderarbeitsgruppe Cybersicherheit im Rahmen der Innenministerkonferenz mit. Diese bundesländerübergreifende Arbeitsgruppe widmet sich zentralen Themen der Cybersicherheit. In der UAG Lagebild steht der gemeinsame Überblick über die Cybersicherheitslage in Deutschland im Fokus. Ziel dieser UAG ist es, Informationen aus den Bundesländern und dem Bund zur Cybersicherheitslage systematisch zu bündeln und auszuwerten. Dies soll eine fundierte Grundlage für politische und operative Entscheidungen schaffen.

Derzeit beteiligen sich zehn Bundesländer und der Bund an der UAG. Sie versteht sich als Forum der Zusammenarbeit, in dem Expertise, Erfahrungen und Perspektiven aus verschiedenen Ländern und dem Bund zusammentreffen. Die Ergebnisse der gemeinsamen Arbeit fließen über die Länderarbeitsgruppe Cybersicherheit in die Innenministerkonferenz ein. Dort können sie einen wichtigen Beitrag zur strategischen Ausrichtung der Innenpolitik leisten.

Ein besonderer Meilenstein im Engagement der CSBW: Im August 2025 hat die CSBW den Vorsitz der UAG Lagebild übernommen. Mit dieser verantwortungsvollen Aufgabe koordiniert die Behörde die inhaltliche Ausrichtung, organisiert die monatlichen Treffen und begleitet die Umsetzung der gemeinsam definierten Arbeitsschritte maßgeblich.

Dabei legt die CSBW großen Wert auf eine konstruktive und lösungsorientierte Zusammenarbeit der Beteiligten. Sie sieht ihre Rolle in dieser Arbeitsgruppe als wichtigen Beitrag zur Stärkung der Cybersicherheit nicht nur in Baden-Württemberg, sondern in der ganzen Bundesrepublik. Die Übernahme des Vorsitzes zeigt, dass die CSBW bereits als starke Partnerin des Bundes, des Bundesamtes für Informationssicherheit sowie der anderen Bundesländer etabliert ist. Die CSBW freut sich, gemeinsam mit den Partnern aus den Bundesländern und dem Bund neue Wege zur Verbesserung der Sicherheitslage in Deutschland zu entwickeln.

> **Dr. Achim Brötel –**
> **Präsident des Landkreistags Baden-Württemberg**
>
> **„Mit der CSBW haben wir einen verlässlichen Partner an unserer Seite, der die Kommunen durch Beratung und Schulungen im Bereich der Cybersicherheit wirksam unterstützt. Die enge Zusammenarbeit im Land erhöht unsere Resilienz bei Cyberangriffen und sollte durch den beabsichtigten Cybersicherheitspakt noch weiter gestärkt werden.“**

3.8 Unterstützung der Bundestagswahl 2025

Der Schutz gesellschaftlich relevanter Prozesse im Cyberraum gehört, nach Vorgabe des Cybersicherheitsgesetzes Baden-Württemberg, zu den vielfältigen Aufgaben der CSBW. Die CSBW hat daher die Landeswahlleitung vor und während der Bundestagswahl beraten und operativ unterstützt.

Die CSBW richtete ein themenbezogenes Cybermonitoring ein, um einschlägige Quellen auf Hinweise nach Angriffen oder Manipulationen zu durchforsten. Am Wahltag waren Kolleginnen und Kollegen der CSBW bis spät in die Nacht begleitend vor Ort. Der Warn- und Informationsdienst des Lagezentrums lieferte fortlaufend Analysen und Lageberichte und hätte vor Ort im Falle eines Falles direkt aktiv werden können.

Um auch die Kandidierenden der Bundestagswahl 2025 für die häufigsten Gefahrenquellen im Bereich Cybersicherheit zu sensibilisieren und einen Überblick empfohlener Schutzmaßnahmen anzubieten, stellte die CSBW im Vorfeld einen Leitfaden[15] zur Verfügung. Dieser thematisiert u. a. die Sensibilisierung des Wahlkampfteams sowie die Nutzung sicherer Passwörter. Insbesondere die Übersichtsseiten zu den häufigsten Einfallstoren und den wichtigsten Schutzmaßnahmen stießen auf sehr positive Resonanz.

Ebenfalls im Vorfeld der Bundestagswahl beteiligte sich die CSBW an einer gemeinsamen Online-Veranstaltung „Sicher im Wahlkampf“, mit dem Landeskriminalamt Baden-Württemberg (LKA) und dem Landesamt für Verfassungsschutz Baden-Württemberg (LfV). Amts- und Mandatstragende, die in der Politik aktiv sind, sowie Kandidierende wurden damit über die Gefahren im digitalen und analogen Raum informiert und mit Handlungsempfehlungen ausgestattet. Zur Landtagswahl 2026 setzte die CSBW ein ähnliches Angebot um.

> **Andreas Stenger –**
> **Präsident des Landeskriminalamts Baden-Württemberg**
>
> **„Cyberkriminalität ist eine der größten Herausforderungen unserer Zeit. Wer heute in Cybersicherheit investiert, schützt morgen Handlungsfähigkeit, Wohlstand und Vertrauen.“**

[15] Leitfaden zur Cybersicherheit für die Kandidierenden der Bundestagswahl:

3.9 Umsetzung der NIS2-Richtlinie und Verabschiedung der CSVO

Am 13. November 2025 hat der Bundestag das Gesetz zur Umsetzung der europäischen NIS-2-Richtlinie verabschiedet. Für Baden-Württemberg setzt die im April 2025 verabschiedete Cybersicherheitsverordnung (CSVO) die Anforderungen der NIS-2-Richtlinie auf Länderebene, insbesondere für Landesbehörden, um. Zugleich konkretisiert die CSVO das Cybersicherheitsgesetz aus dem Jahr 2021.

Mit der CSVO rückt insbesondere der Aspekt der Cybersicherheit als Führungsaufgabe in den Fokus. Nicht erst als Reaktion auf diese Verantwortlichkeit bietet die CSBW das Schulungsangebot „Cybersicherheit als Führungsaufgabe“ an, um Führungskräfte in ihrer Verantwortungsrolle für die Cybersicherheit zu unterstützen.

Bereits mit der Gründung der CSBW antizipierte Baden-Württemberg die voraussichtlichen zentralen Anforderungen der NIS-2-Richtlinie. Die CSBW ist die zentrale Meldestelle für die obersten Landesbehörden, also vor allem die Ministerien im Land. Alle sogenannten „wichtigen Stellen“ des Landes müssen bei der CSBW registriert werden. Kommt es bei einer wichtigen Stelle zu einem erheblichen Sicherheitsvorfall, so bearbeitet die CSBW diesen priorisiert.

Für die kritischen Infrastrukturen (KRITIS), die im Fokus der NIS-2-Richtlinie stehen, ist die CSBW die zentrale Kontaktstelle (ZKL) für das Bundesamt für Sicherheit in der Informationstechnik (BSI). Die CSBW ist in diesem Sinne Anlaufstelle für den Informationsaustausch. KRITIS-Unternehmen sind verpflichtet, Cybersicherheitsvorfälle dem BSI zu melden. Dieses wiederum kann die Expertise der ZKL des jeweiligen Bundeslandes erbitten. Nach Rücksprache unterstützt die CSBW dann in diesen einzelnen Fällen.

Mit der Cyber-Ersthilfe BW setzt die CSBW weitere Verpflichtungen der NIS-2-Richtlinie bereits seit Längerem um. Sie ist rund um die Uhr erreichbar und ermöglicht es, betroffenen Einrichtungen, wie von NIS-2 gefordert, Cybersicherheitsvorfälle schnell und wirksam zu melden. Außerdem analysiert die Cyber-Ersthilfe BW die eingehenden Meldungen für eine präzise Ersthilfe. Die CSBW nutzt die daraus gewonnenen Erkenntnisse für eine Verbesserung des Lagebilds, für Warnmeldungen oder zur Weiterentwicklung ihres präventiven Angebots und erfüllt somit die Anforderungen nach proaktiven Maßnahmen und einer Risikobewertung.

Kurzum: Baden-Württemberg und die CSBW haben die Weichen für die Umsetzung der NIS-2-Richtlinie frühzeitig richtig gestellt. Die CSBW war somit trotz der unklaren Situation auf Bundesebene bereits gut vorbereitet.

Reiner Möller –
Polizeipräsident Aalen

„Die Zusammenarbeit mit der CSBW war sehr produktiv. Die betroffenen Kommunen waren schnell wieder kommunikations- und arbeitsfähig. Die digital-forensische Arbeit konnte wesentlich gestrafft werden, sodass kein doppelter Aufwand bei verschiedenen Behörden erforderlich war. Dabei ist der Kontakt mit der CSBW immer freundlich, sehr professionell und pragmatisch. Sehr gut ist, dass die Incident-Response-Maßnahmen auch die Begleitung der Kommunikation nach innen und außen, auch zu anderen Behörden, abdecken.“



4. Fazit und Ausblick

Thomas Berger –
Präsident des Präsidiums Technik, Logistik, Service der Polizei Baden-Württemberg

„CSBW – wenn man sie nicht hätte, müsste man sie erfinden! Wir brauchen diese staatliche Kompetenz außerhalb der originären Strafverfolgung. Gemeinsam mit unterschiedlichen Aufgaben, die Menschen zu beschützen – was wäre noch verbindender?!“

Die Zukunft der Cybersicherheit in Baden-Württemberg

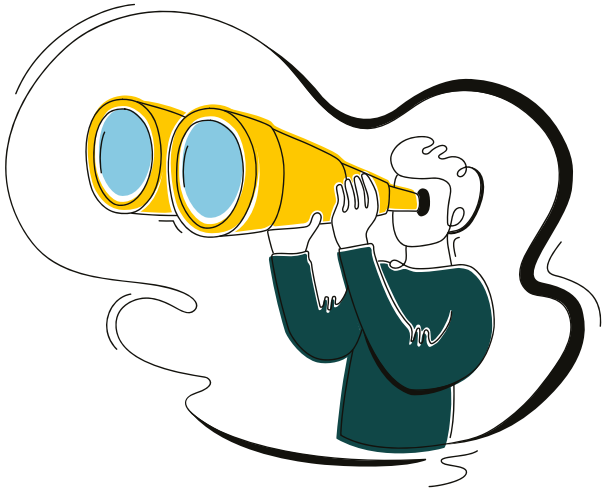
Die Cybersicherheitslage in Baden-Württemberg bleibt kontinuierlich herausfordernd, da die Cyberwelt in einem ständigen Wandel begriffen ist. Neue technische Entwicklungen eröffnen sowohl Chancen als auch Risiken, und die kriminellen Akteure im Cyberraum werden immer vielfältiger und gerissener. Angesichts dieser Dynamik ist es entscheidend, dass die Cybersicherheitsarchitektur ebenso dynamisch wächst und alle Akteure gemeinsam an einem Strang ziehen. Wie bei so vielem gilt: Cybersicherheit ist kein Sprint, sondern ein Marathon. Erforderlich sind eine strategische und nachhaltige Herangehensweise, die präventive Maßnahmen, bundesweite sowie internationale Zusammenarbeit und kontinuierliche Anpassung und Verbesserung umfasst – bei gleichzeitiger operativer Schlagkraft.

Die CSBW hat 2025 ihr Angebot auf den Prüfstein gestellt und eine noch konkretere Zielgruppenpassung und Bedarfsorientierung in den Mittelpunkt gestellt. Für 2026 gilt es, die Ergebnisse der Koalitionsverhandlungen nach der Landtagswahl zu bewerten und in neue Konzepte und Angebote zu gießen. Dabei ist aus unserer Sicht eine personelle und finanzielle Stärkung der CSBW unerlässlich, um den großen Bedarf an weiteren Angeboten zu decken. Für uns stehen dabei eine Ausweitung der Präventionsarbeit, der Aufbau von Angeboten zu Schwachstellenscans und Penetrationstests, die Ermöglichung von ISMS-Beratung für unsere Zielgruppen sowie das Setzen und Überprüfen von Standards ganz oben auf der Agenda. Zudem prüfen wir, wie wir noch mehr skalierungsfähige Unterstützungsangebote bereitstellen können. Die Vernetzung mit Partnern und Kunden treiben wir weiter voran und nehmen verstärkt das Thema „Sicherheit und Verteidigung“ sowie eine Erweiterung unserer Zielgruppen in den Blick.

Generell gilt: Die Sensibilisierung für die Bedeutung von Cybersicherheit muss auf allen Ebenen, vom Sekretariat bis zur Hauspitze, vom Hausdienst bis zur IT-Abteilung, von der Pforte bis zur Leitungsebene, stattfinden. Unsere vielfältigen Präventionsangebote werden daher weiter an Bedeutung gewinnen, da der beste Vorfall immer noch der ist, der gar nicht erst eintritt.

Noch völlig unkalkulierbar ist, wie schnell und weitgehend die Veränderungen durch KI-Modelle voranschreiten werden. 2026 wird diesbezüglich sicherlich ein Jahr der Weichenstellung sein und auch die CSBW wird ihr Angebotsportfolio darauf ausrichten müssen.

Die CSBW wird auf alle neuen Bedrohungen und Herausforderungen flexibel und anpassungsfähig reagieren müssen. Schon heute leistet sie einen wichtigen Beitrag zur Sicherheit von Baden-Württemberg und ist als dritte Säule der Sicherheitsarchitektur des Landes unerlässlich für das Land. Mit großer Motivation, langfristigem Engagement und einer strategischen Herangehensweise kann Baden-Württemberg weiterhin die Vorreiterrolle beim Thema Cybersicherheit einnehmen und somit die Bevölkerung, Unternehmen und Institutionen sowie öffentliche Einrichtungen des Landes vor den Risiken des Cyberraums schützen.



Impressum

Herausgegeben von der
Cybersicherheitsagentur Baden-Württemberg
Deckerstraße 41
70372 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 + 40	Diverse businesspeople smiling ... © Flamingo Images - stock.adobe.com
S. 6	Portrait Manuel Hagel © Marcel Ditrich
S. 8	Portrait Nicole Matthöfer © CSBW, Pascal Seez
S. 11	Portrait Björn Schemberger © CSBW, Arne Claußen; Portrait Susanne Krieg © CSBW, Daniela Vey
S. 12	Ausblick über Stuttgart © CSBW, Kristina Stelzig
S. 18	Trainer makes presentation ... © fizkes - stock.adobe.com
S. 24	Business and entrepreneurship symposium. ... © kasto - stock.adobe.com
S. 36	Servers data center room ... © sdecoret - stock.adobe.com

Redaktionsschluss: 31. Dezember 2025

© Cybersicherheitsagentur Baden-Württemberg, Stuttgart 2026

Vervielfältigung und Verbreitung, auch auszugsweise, mit Quellenangabe gestattet. Bei einer auszugsweisen Verwendung dürfen die urheber- und lizenzrechtlich geschützten Abbildungen nicht weiterverwendet werden.



Mit uns. Mit Sicherheit.

www.cybersicherheit-bw.de