Landesamt für Sicherheit in
der Informationstechnik

LSI-PANORAMA 2025

IT-Sicherheit für den Freistaat Bayern

VORWORT

Liebe Leserinnen und Leser,

die fortschreitende Digitalisierung prägt unsere Gesellschaft in einem bisher ungekannten Ausmaß.
Mit den Chancen, die die digitale Transformation bietet, gehen jedoch ebenso erhebliche Herausforderungen im Bereich der IT-Sicherheit einher. Der Schutz unserer digitalen Infrastruktur ist zu einer zentralen Aufgabe geworden, die nur durch eine enge Zusammenarbeit aller Akteure erfolgreich bewältigt werden kann.

In einer Zeit, in der Cyberangriffe immer raffinierter und vielfältiger werden, ist es unsere Aufgabe, den Schutz unserer digitalen Infrastruktur kontinuierlich zu verbessern und das Bewusstsein für IT-Sicherheit zu stärken.

Das Landesamt für Sicherheit in der Informationstechnik (LSI) nimmt hierbei eine Schlüsselrolle ein. Unsere Arbeit ist geprägt von kontinuierlicher Innovation, strategischer Weitsicht und einem unermüdlichen Einsatz, um die Sicherheit der Bayerischen IT-Systeme zu gewährleisten. Dabei setzen wir auf modernste Technologien, präventive Maßnahmen und eine enge Vernetzung mit Partnern aus Wirtschaft, Wissenschaft und Verwaltung. Es ist unser Anspruch, auch in Zukunft eine sichere digitale Infrastruktur zu schaffen, die Innovation fördert und das Vertrauen aller Bürgerinnen und Bürger in die digitale Gesellschaft festigt.

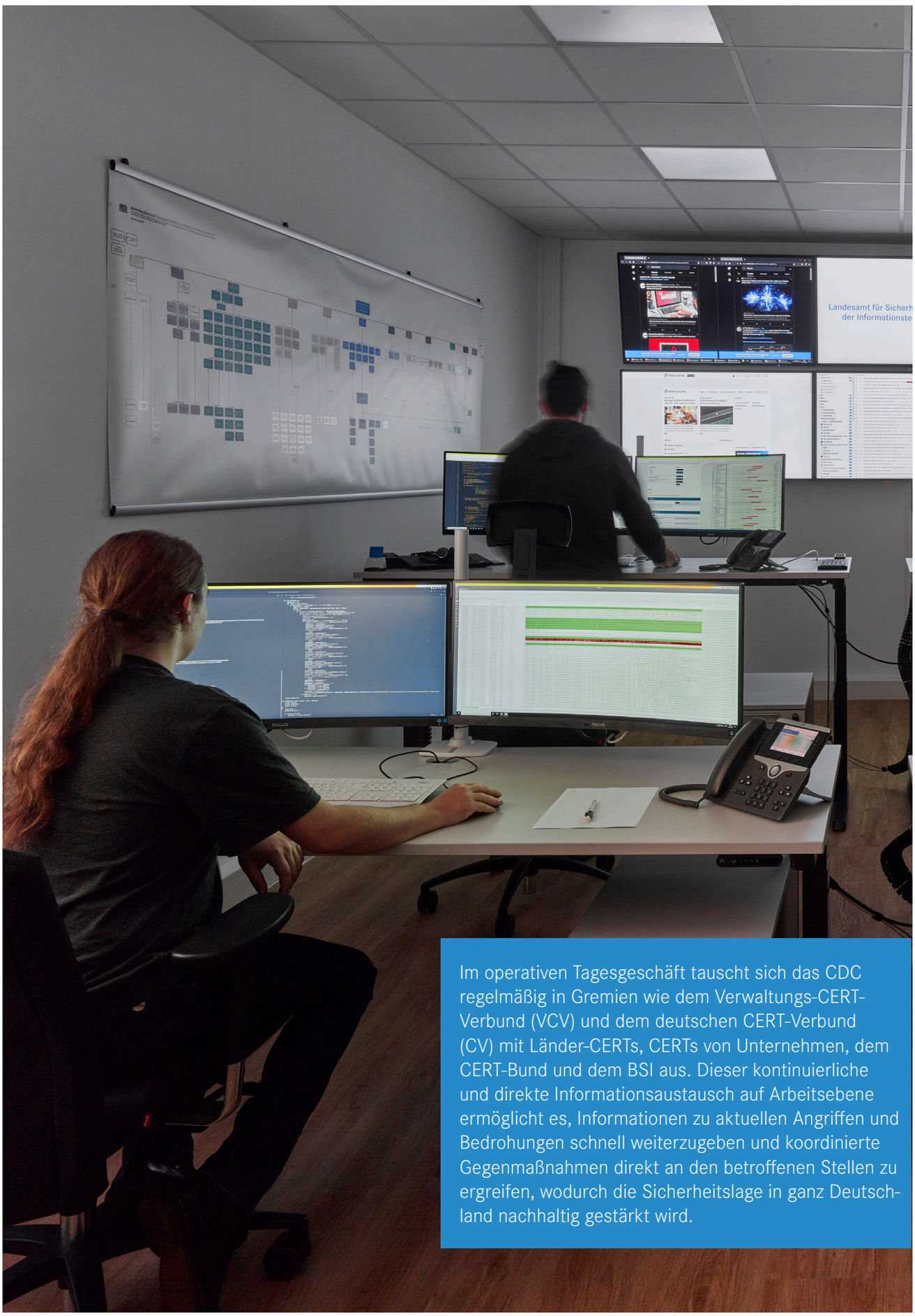
Das LSI Panorama 2025 zeigt die aktuellen Entwicklungen, Herausforderungen und Chancen im Bereich der IT-Sicherheit auf, sowie unser Unterstützungsangebot für unsere Zielgruppen. Es ist ein Wegweiser für die Zukunft, der uns inspiriert, weiterhin mutig voranzuschreiten und die digitale Souveränität Bayerns zu stärken.
Gemeinsam können wir eine sichere digitale Zukunft gestalten.

Ich lade Sie ein, die vielfältigen Beiträge und Erkenntnisse dieses Berichts zu entdecken und sich aktiv an der Gestaltung einer sicheren digitalen Welt zu beteiligen.

Vielen Dank für Ihr Interesse.

Bernd Geisler
Präsident des Landesamtes
für Sicherheit in der Informationstechnik

INHALTSVERZEICHNIS



Im operativen Tagesgeschäft tauscht sich das CDC regelmäßig in Gremien wie dem Verwaltungs-CERT-Verbund (VCV) und dem deutschen CERT-Verbund (CV) mit Länder-CERTs, CERTs von Unternehmen, dem CERT-Bund und dem BSI aus. Dieser kontinuierliche und direkte Informationsaustausch auf Arbeitsebene ermöglicht es, Informationen zu aktuellen Angriffen und Bedrohungen schnell weiterzugeben und koordinierte Gegenmaßnahmen direkt an den betroffenen Stellen zu ergreifen, wodurch die Sicherheitslage in ganz Deutschland nachhaltig gestärkt wird.

1. Das CYBER DEFENCE CENTER (CDC)

Das Cyber Defence Center (CDC) im Landesamt für Sicherheit in der Informationstechnik (LSI) ist die zentrale Anlaufstelle für alle IT-Sicherheitsvorfälle, Verdachtsfälle und Auffälligkeiten im Bereich der bayerischen Staatsverwaltung, für Kommunen sowie für Betreiber kritischer Infrastrukturen in Bayern. Seine Wurzeln reichen zurück bis ins Jahr 2003, als das Bayern-CERT als erste Instanz entstand und später im LSI zum Lagezentrum ausgebaut wurde. Im Zuge der stetigen Weiterentwicklung erfolgte die offizielle Umbenennung von „Lagezentrum“ in „Cyber Defence Center“ (CDC), um den proaktiven Charakter hervorzuheben. Von Anfang an war es das Ziel, aus einer reaktiven Alarmanalyse ein proaktives Cyber Defence Center zu formen.

IT-Sicherheit im Freistaat

Zur Umsetzung der NIS-2-Richtlinie ergänzt das LSI sein CDC durch den Digitalen Ersthelfer: Eine 24/7-Rufbereitschaft für akute IT-Vorfälle außerhalb der regulären Dienstzeiten. Dies ermöglicht eine schnelle Erstbewertung, gezielte Eskalation und unterstützt damit in kritischen Lagen rund um die Uhr.

Im CDC werden täglich rund 2,7 Milliarden Datensätze automatisiert ausgewertet. Dabei greift es auf verschiedenste Quellen, wie beispielsweise Netzwerk-Sensoren im Bayerischen Behördennetz, sowie Open Source Intelligence (OSINT) und Informationen aus nationalen und internationalen CERT-Partnerschaften zurück. Verdächtige Aktivitäten werden von spezialisierten Analysten untersucht, um Angriffsvektoren genau zu identifizieren und Bedrohungen abzuwenden.

Auf Basis der Analyseergebnisse ergreift das CDC aktive Gegenmaßnahmen von Warnmeldungen über automatisches Blocken schädlicher Netzwerkaktivität bis hin zur Koordination mit der unmittelbar betroffenen Einrichtung und der direkten Vorfallsbearbeitung.

Die Leistungsfähigkeit des CDC zeigt sich in den Zahlen für das Jahr 2024: Monatlich wurden etwa 456 Millionen potenziell schädliche Internetaufrufe abgewehrt, von 42 Millionen eingehenden E-Mails wurden rund 30 Millionen als schadhaft bzw. auffällig erkannt und ihre Zustellung geblockt. Mehr als 140.000 Nutzer im Bayerischen Behördennetz profitieren somit täglich vom Schutz des CDC.

2. Warn- und Informationsdienst (WID) & Malware Information Sharing Platform (MISP)

Angesichts der ständig neuen Sicherheitslücken stellt das LSI mit dem Warn- und Informationsdienst (WID) sowie der Malware Information Sharing Platform (MISP) zentrale Dienste zur Stärkung der Cyberresilienz zur Verfügung. Mit dem Warn- und Informationsdienst offeriert das LSI seinen Zielgruppen – Bayerns Staatsverwaltung, Kommunen und öffentlichen Unternehmen im KRITIS Bereich – ein zentrales Frühwarnsystem. Das Portal informiert täglich über sicherheitsrelevante Schwachstellen und bietet passgenaue Handlungsempfehlungen.

Prävention und Reaktion in der Informationssicherheit

Über individuell konfigurierbare Abonnements und automatische E-Mail-Benachrichtigungen erhalten die Nutzerinnen und Nutzer bedarfsgerechte Informationen zu mehr als 1.500 Softwareprodukten. Seit November 2023 ist auch ein Abruf über eine REST-API möglich.

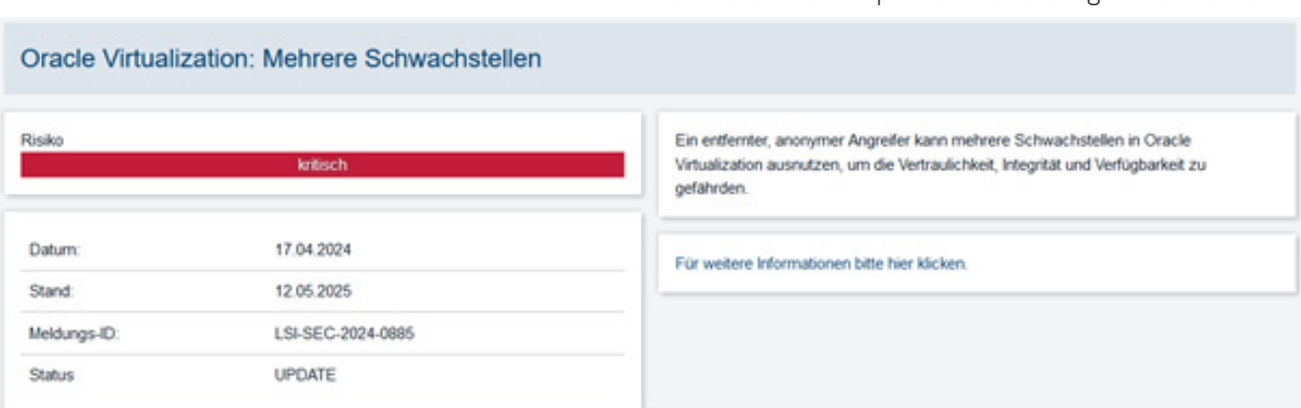
Ergänzt wird dieses Angebot durch die MISP-Platform, die strukturierte Daten zu Schadsoftware und Angriffskampagnen bereitstellt. Diese Informationen stammen unter anderem aus dem Cyber Defence Center (CDC) des LSI. Sie helfen dabei, Angriffe zu erkennen und abzuwehren, bevor sie Schaden anrichten.

Im Fall eines sicherheitsrelevanten Vorfalls sind schnelle Reaktionszeiten entscheidend. Das LSI stellt mit seinem MISP eine Plattform bereit, über die sich Informationen zu aktuellen Malware-Bedrohungen, sogenannte Indikatoren für Kompromittierungen (IoCs) strukturiert sammeln, verwalten und vor allem mit anderen Akteuren im Cybersecurity-Umfeld austauschen lassen. Diese Indikatoren stammen sowohl aus externen als auch internen Quellen, wie zum Beispiel den Analysen und Auswertungen des Cyber Defence Centers.

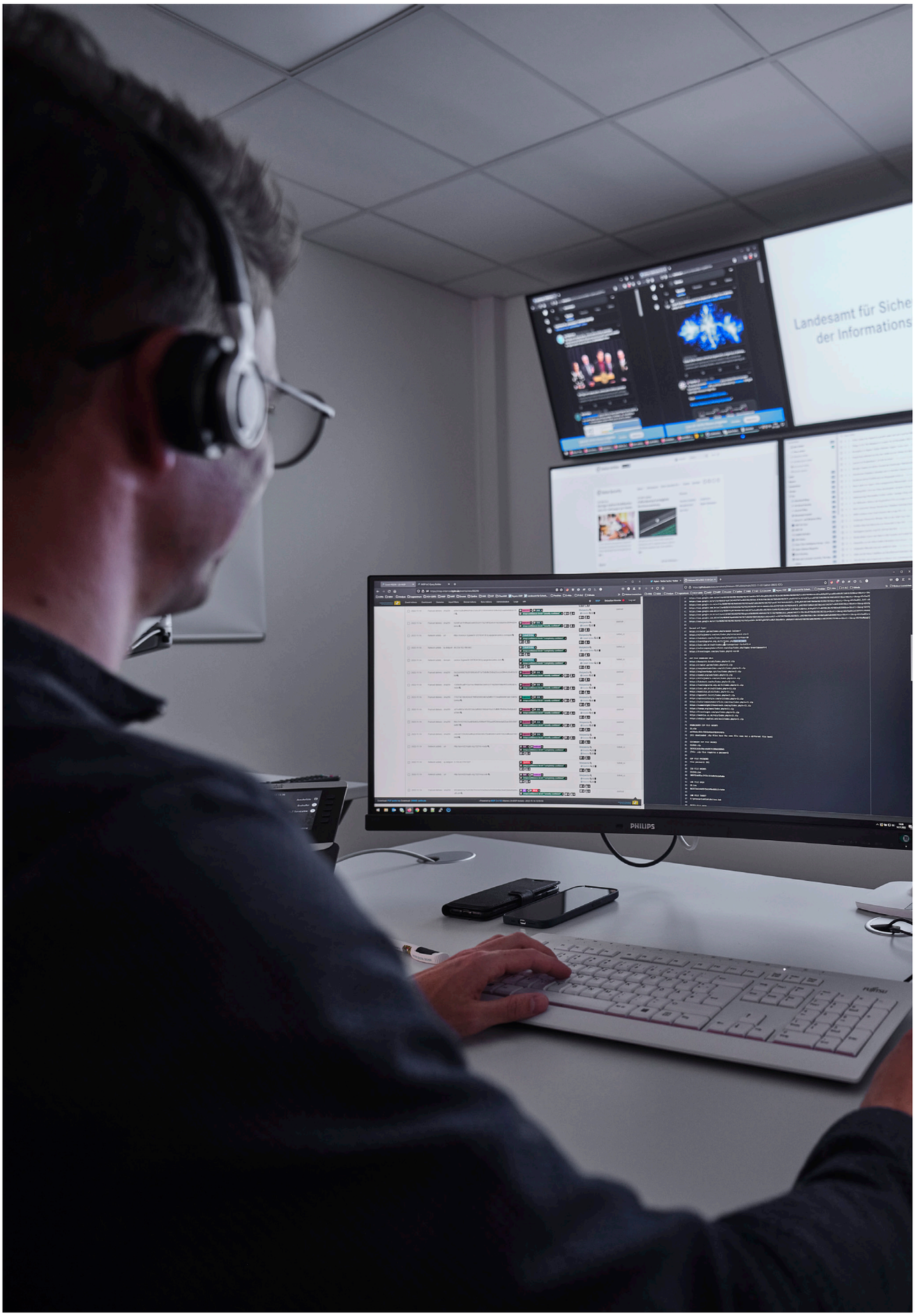
Das LSI setzt die eigene MISP-Instanz aktiv in automatisierten Prozessen ein, um Sicherheitsinstanzen kontinuierlich mit aktuellen IoCs zu versorgen und somit Angriffe mit bekannten Angriffsvektoren präventiv zu unterbinden.

Das MISP ermöglicht es dem LSI und allen weiteren Nutzern, Informationen zur Abwehr von Cyberangriffen zu teilen und sich mit anderen Akteuren im Cybersecurity-Umfeld zu vernetzen. Durch den gemeinsamen Wissens- und Ressourcenaustausch werden neue Gefahren frühzeitig erkennbar, sodass passende Schutzmaßnahmen schnell eingeleitet werden können. So werden das Bayerische Behördennetz und die Netzwerke angeschlossener MISP-Teilnehmer effektiver abgesichert.

Das LSI stellt basierend auf der etablierten Infrastruktur MISP auch allen bayerischen Kommunen, unabhängig von ihrer Größe oder technischen Ausstattung, sowie sämtlichen Behörden und der Staatsverwaltung als zentrale IoC-Austauschplattform zur Verfügung. Der Betrieb erfolgt vollständig über das LSI, sodass für die teilnehmenden Stellen keine zusätzlichen Aufwände oder Kosten entstehen. Darüber hinaus unterstützt das LSI bei der Einführung und Anwendung der Plattform, um eine effektive und praxisnahe Nutzung sicherzustellen.



Darstellung einer Warnmeldung über das Warn- und Informationsportal des LSI

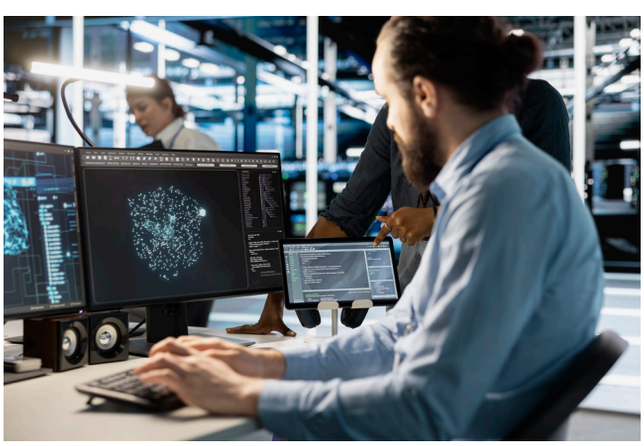

Landesamt für Siche
der Informations
PHILIPS

3. Digitale Spurensuche – IT-Forensik im Cyber Defence Center

Die Welt der Forensik ist vielen aus dem Kriminalfilm oder der Strafverfolgung bekannt: Tatorte werden akribisch untersucht, Spuren gesichert und Beweise gesammelt, um Täter zu überführen. In einer zunehmend digitalisierten Welt ist ein vergleichbares Vorgehen auch in der Informationssicherheit erforderlich – nur dass sich „Tatorte“ nicht auf Straßen, Gebäude oder physische Objekte beschränken, sondern sich auch auf Server, Netzwerke und IT-Systeme erstrecken. Genau hier setzt die IT-Forensik an – ein hochspezialisiertes Fachgebiet, das digitale Spuren sichert, analysiert und in einen beweisfähigen Zusammenhang bringt.

IT-Forensik im Cyber Defence Center

Im Landesamt für Sicherheit in der Informationstechnik (LSI) spielen IT-forensische Analysen eine zentrale Rolle bei der Abwehr und Aufklärung von Cyberangriffen auf das Bayerische Behördennetz. Die Expertinnen und Experten im Bereich IT-Forensik sind dabei so etwas wie digitale Ermittlerinnen und Ermittler. Ihr Auftrag beginnt meist dann, wenn Hinweise auf einen sicherheitsrelevanten Vorfall auftauchen – etwa durch ungewöhnliche Netzaktivitäten, verdächtige Dateien oder Anomalien, die das Cyber Defence Center (CDC) registriert.



Zu Beginn einer forensischen Untersuchung steht die Sicherung des digitalen Tatorts. Dabei ist besondere Sorgfalt erforderlich, denn die Integrität der Daten muss gewährleistet sein, damit Beweise verwertbar bleiben. Festplatten, virtuelle Maschinen oder ganze Systeme werden forensisch gesichert, in der Regel durch exakte Kopien (Images), die eine lückenlose Beweiskette sicherstellen. Ziel ist es, Veränderungen am Original zu vermeiden und gleichzeitig eine vollumfängliche Analyse zu ermöglichen.

Die anschließende Auswertung erfolgt systematisch. Je nach Art und Betriebssystem des betroffenen Systems – sei es Windows, Linux oder andere – unterscheiden sich die sogenannten digitalen Artefakte, also die Spuren, die Nutzeraktivitäten oder Angriffe hinterlassen. Ähnlich wie bei einer klassischen Spurensuche nach Fingerabdrücken oder DNA identifizieren IT-Forensiker beispielsweise Logdateien, Zeitstempel, Dateiänderungen oder untypisches Nutzerverhalten. Die größte Herausforderung dabei besteht häufig darin, harmlose Aktivitäten im Rahmen des normalen Betriebs von tatsächlichen Angriffsaktionen zu unterscheiden – eine Aufgabe, die ein hohes Maß an Erfahrung, technisches Verständnis und analytisches Denken erfordert.

Bedrohungslage immer im Blick

Ein zentrales Ziel der forensischen Arbeit ist es, den Tathergang zu rekonstruieren. Dazu werden die gesammelten Informationen in einen chronologischen Zusammenhang gebracht, der idealerweise Rückschlüsse auf Angriffsweg, Zeitpunkt und Methodik zulässt. Diese Analyse ist nicht nur Grundlage für die Behebung der Sicherheitslücke, sondern liefert auch wertvolle Erkenntnisse für die zukünftige Verteidigung. So können aus der Untersuchung eines konkreten Vorfalls neue

Indikatoren für das Sicherheitsmonitoring im Behördennetz abgeleitet werden – ein entscheidender Mehrwert für die kontinuierliche Verbesserung der IT-Sicherheit.

Klarer Fokus auf dem Schutz staatl. IT-Infrastrukturen

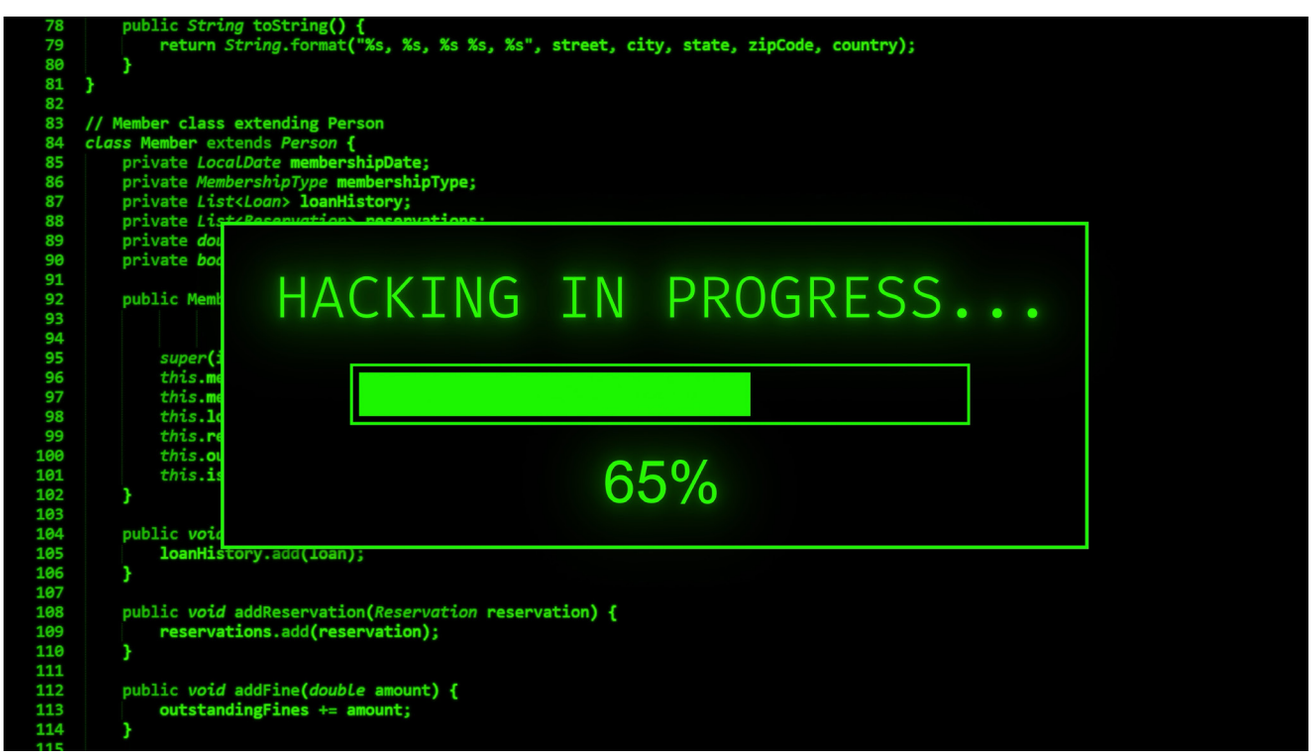
Im Unterschied zur klassischen IT-Forensik im Strafverfahren liegt der Fokus des LSI nicht auf der strafrechtlichen Verfolgung, sondern auf dem Schutz staatlicher IT-Infrastrukturen. Aus diesem Grund kommt die forensische Expertise des LSI in der Regel nicht im Nachhinein zur Anwendung, sondern möglichst frühzeitig im Rahmen präventiver oder begleitender Maßnahmen. Hierfür wurde eigens ein Verfahren zur sogenannten Triage-Analyse entwickelt, das eine schnelle Ersteinschätzung ermöglicht. Anhand weniger Artefakte und der Netzwerküberwachung kann festgestellt werden, ob überhaupt ein IT-Sicherheitsvorfall vorliegt – und falls ja, wie groß dessen Ausmaß ist.
Reicht diese Vorab-Analyse nicht aus, fordern die Spezialistinnen und Spezialisten umfassendere Daten zur weiteren Untersuchung an.

Dabei behalten sie nicht nur die unmittelbare Bedrohungslage im Blick, sondern auch die übergreifenden sicherheitsstrategischen Aspekte: Wie kann ein ähnlicher Vorfall künftig verhindert werden? Welche Lehren lassen sich aus der Analyse ziehen?
Wie lassen sich daraus Schutzmaßnahmen erhöhen?

Die Qualität und Wirksamkeit dieser Arbeit basiert maßgeblich auf kontinuierlicher Weiterbildung und Spezialisierung. Die IT-Forensik unterliegt einem ständigen Wandel – neue Betriebssysteme, neue Angriffstechniken und neue digitale Spuren erfordern ein stetes Lernen. Das LSI investiert daher gezielt in die Qualifikation seines Fachpersonals. Interne Fortbildungen, Schulungen zu Windows- und Linux-Forensik sowie praxisnahe Capture-the-Flag-Formate sorgen dafür, dass die Mitarbeitenden des Forensikteams stets auf dem neuesten Stand sind und auch weiterhin komplexe Angriffszenarien erkennen und analysieren können.

Jede Minute zählt

Gerade in der Abwehr moderner Cyberbedrohungen zählt jede Minute. Die Forensikexpertinnen und -experten des LSI leisten mit ihrer Arbeit einen unsichtbaren, aber essenziellen Beitrag zur digitalen Souveränität Bayerns. Ihre Arbeit fängt dort an, wo die digitale Spur beginnt – und endet nicht selten mit einem Erkenntnisgewinn, der weit über den einzelnen Vorfall hinausreicht.



4. Penetrationstests – IT-Systeme unter kontrolliertem Beschuss

Penetrationstests zählen zu den wirkungsvollsten Mitteln, um Schwachstellen in IT-Systemen vor deren Ausnutzung durch Dritte zu identifizieren. Ein Penetrationstest, auch als „Pentest“ bekannt, ist ein Verfahren zur Identifizierung von Sicherheitslücken in IT-Systemen, Netzwerken oder Anwendungen.

Es werden strukturierte Angriffs- und Belastungstests durchgeführt, bei denen reale Bedrohungsszenarien simuliert werden. Auf diese Weise werden potenzielle Schwachstellen aufgedeckt, bevor sie von Cyberkriminellen ausgenutzt werden können.

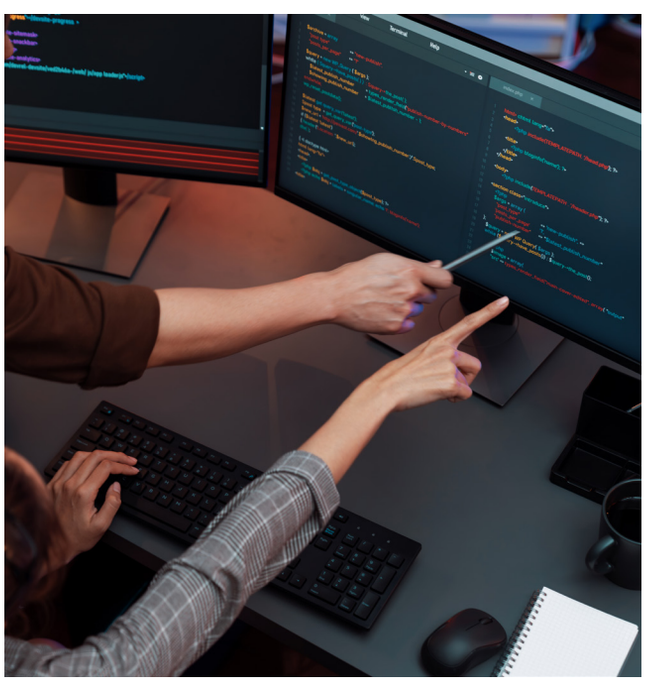
Angreifen, um zu schützen

Im Fokus stehen insbesondere Web- und Mobile-Anwendungen, bei denen gängige Angriffsmuster wie SQL-Injection und Cross-Site Scripting (XSS) geprüft oder unsichere Konfigurationen identifiziert werden. App-Penetrationstests haben spezifische Ziele und Methoden, die auf die jeweilige Technologie und die damit verbundenen Risiken abgestimmt sind. Aus den Testergebnissen werden gezielte Maßnahmen abgeleitet, um die Sicherheit der Anwendungen zu verbessern.

Ein Penetrationstest besteht grundlegend aus mehreren Phasen: Planung, Durchführung, Auswertung und Nachbereitung. In der Planungsphase werden die Ziele und der Umfang des Tests definiert. Anschließend erfolgt die Durchführung, in der verschiedene Angriffsvektoren ausprobiert werden. Nach Abschluss der Tests wird eine detaillierte Auswertung erstellt, die die gefundenen Schwachstellen dokumentiert und Empfehlungen zur Behebung gibt. Die Nachbereitung umfasst auch die Unterstützung bei der Umsetzung der empfohlenen Maßnahmen.

Sicherheitslücken erkennen, bevor es andere tun

Penetrationstests sind ein unverzichtbares Instrument zur Gewährleistung der IT-Sicherheit in Behörden und ermöglichen es, die Sicherheitsarchitektur öffentlicher Stellen gezielt zu optimieren. Sie tragen dazu bei, die Resilienz gegenüber Cyberangriffen zu erhöhen und das Vertrauen der Bürger in die digitalen Dienstleistungen zu stärken. In einer Zeit, in der Cyberbedrohungen allgegenwärtig sind, ist es unerlässlich, proaktiv zu handeln und die Sicherheit der Systeme kontinuierlich zu überprüfen und zu verbessern.



5. Post-Quanten-Kryptografie – Schutz für die Welt von morgen

Quantencomputer stellen eine potenzielle Bedrohung für die IT-Sicherheit dar, da sie aufgrund ihrer Rechenleistung in der Lage sind, komplexe Verschlüsselungsalgorithmen zu brechen, die derzeit als sicher gelten. Die meisten aktuellen asymmetrischen Verschlüsselungssysteme basieren auf der Schwierigkeit bestimmter mathematischer Probleme, wie der Faktorisierung großer Zahlen. Ein leistungsfähiger Quantencomputer könnte diese Probleme jedoch in einer praktikablen Zeitspanne lösen und so die Verschlüsselung brechen. Wenn Verschlüsselungssysteme gebrochen werden können, sind persönliche Daten, Bankinformationen und staatliche Geheimnisse potenziell gefährdet. Dies könnte zu einem massiven Verlust von Privatsphäre und Sicherheit führen.

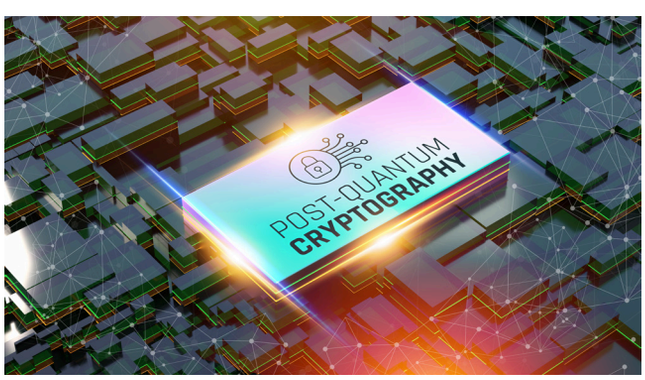
Sicherheit gegen Quantenangriffe

Post-Quanten-Kryptografie bezieht sich auf kryptografische Algorithmen (d.h. Verschlüsselungsmethoden), die auch gegen Angriffe durch Quantencomputer sicher sind. Während viele gängige Verschlüsselungsmethoden auf Problemen basieren, die für klassische Computer schwierig, aber für Quantencomputer lösbar sind, basiert die Post-Quanten-Kryptografie (PQK) auf mathematischen Problemen, die auch für Quantencomputer als schwierig gelten.

Durch die Verwendung dieser und anderer post-quantenkryptografischer Methoden kann die Sicherheit von Daten auch in einer Ära von Quantencomputern gewährleistet werden. Es ist jedoch wichtig zu beachten, dass diese Methoden noch intensiv erforscht und getestet werden, um ihre Sicherheit und Praktikabilität zu gewährleisten.

In mehreren Projekten hat sich das LSI mit der Frage auseinandergesetzt, wie diese, teilweise noch in der Erforschung und Entwicklung befindlichen Verfahren im Freistaat eingesetzt werden können.

So wurde in einem Projekt zusammen mit den Fraunhofer AISEC erforscht, wie im Bayerischen Behördennetz eine Verschlüsselung implementiert werden kann, die auch zukünftigen Generationen von Quantencomputer standhält. Es wurden konkrete Schritte und Maßnahmen abgeleitet, die bereits jetzt als Vorbereitung für neue PQK-Verfahren umgesetzt werden können.
Ein aktuelles Projekt wird in enger Zusammenarbeit vom Landesamt für Sicherheit in der Informationstechnik (LSI), der Ostbayerischen Technischen Hochschule Regensburg (OTH) und dem Zweckverband der Wasserversorgungsgruppe Laber-Naab (ZVLN) durchgeführt. Das Projekt „KRITIS³M“ (https://kritis3m.de) entwickelt und erprobt zukunftsweisende Lösungen für kritische Infrastrukturen und Security-Module auf Basis von Post-Quanten-Kryptografie. Damit wird Grundlagenforschung konkret für den Einsatz vor Ort nutzbar gemacht. Die Technologie verhindert, dass Angreifer falsche Steuerbefehle in Systemen zur Wassergewinnung und Verteilung über Pumpen und Hochbehälter einspeisen können. Solche Angriffe könnten in kritischen Infrastrukturen massiven Schaden anrichten. Insbesondere vor dem Hintergrund der Entwicklungen im Bereich Quantencomputing ist es von enormer Bedeutung, derartige Szenarien in künftige IT-Sicherheitskonzepte einzubeziehen. Es ist entscheidend, bereits im Voraus Verschlüsselungsmethoden zu entwickeln und diese umfangreich zu testen.



Im Zweckverband der Wasserversorgungsgruppe Laber-Naab sind aktuell 13 Kommunen zusammengeschlossen. Mit über 1.000 Wasserleitungskilometern werden rund 12.500 Haushalte mit Trinkwasser versorgt. Seit mehreren Jahren hat der Zweckverband auch ein besonderes Augenmerk auf den Schutz der Steuerungssysteme und der IT-Systeme sowie seiner Kundendaten in der Verwaltung gelegt.

© 2025 Bayerisches Staatsministerium der Finanzen und für Heimat/Christian Blaschka

Mit dem Startschuss des neuen Forschungsprojekts „HeCKI“ setzen das LSI und die OTH Amberg-Weiden ein starkes Zeichen für den Schulterschluss zwischen Wissenschaft und Praxis Die gemeinsame Initiative zeigt, dass eine frühzeitige und interdisziplinäre Auseinandersetzung mit den Auswirkungen Künstlicher Intelligenz auf die Cybersicherheit unerlässlich ist, um den Schutz kritischer digitaler Infrastrukturen wirksam zu gewährleisten.


© Ostbayerische Technische Hochschule (OTH) Amberg-Weiden

6. Projekt HeCKI – Informationssicherheit im Zeitalter der Künstlichen Intelligenz

Die rasante Entwicklung von Künstlicher Intelligenz (KI) zählt zu den bedeutendsten Fortschritten der vergangenen Jahre. Seit der breiten Verfügbarkeit generativer KI-Systeme wie ChatGPT hat sich das gesellschaftliche, wirtschaftliche und sicherheitspolitische Umfeld grundlegend verändert. Neben vielfältigen Chancen zur Effizienzsteigerung, Prozessoptimierung und Automatisierung eröffnet der Einsatz von KI auch neue Angriffsflächen, die bestehende Schutzmechanismen herausfordern. Besonders im Bereich der IT-Sicherheit wird deutlich, dass KI nicht nur Werkzeuge für Innovation und Fortschritt liefert, sondern auch ein Bedrohungspotenzial für IT-Infrastrukturen entfaltet.

Um den daraus resultierenden Herausforderungen systematisch zu begegnen, wurde am 16. Januar 2025 das Forschungsprojekt „HeCKI – Herausforderungen für die Cybersicherheit durch KI“ offiziell gestartet. Träger dieses Projekts sind das Landesamt für Sicherheit in der Informationstechnik (LSI) und die Ostbayerische Technische Hochschule (OTH) Amberg-Weiden, die in enger Kooperation an der Schnittstelle zwischen wissenschaftlicher Forschung und praxisnaher Anwendung agieren. Das auf zwei Jahre angelegte Projekt verfolgt das Ziel, die sicherheitsrelevanten Implikationen von KI umfassend zu sammeln, zu analysieren und geeignete Schutzmaßnahmen daraus abzuleiten.

Forschungsprojekt HeCKI

Das Projekt HeCKI setzt genau hier an: Es identifiziert neuartige Bedrohungslagen, analysiert deren Wirkmechanismen und entwickelt auf dieser Grundlage praxisorientierte Handlungsempfehlungen. Im Fokus stehen dabei die für das LSI relevanten Zielgruppen, darunter Bayerische Behörden, kommunale Einrichtungen und Betreiber kritischer Infrastrukturen. Für diese Akteure sollen didaktisch aufbereitete Informations- und Schulungsformate entwickelt werden, die sowohl zur Sensibilisierung als auch zur operativen Risikoabwehr beitragen. Hierzu zählen etwa digitale Lernmodule, Beratungsunterlagen und gezielte Fortbildungsangebote für Entscheidungsträgerinnen und Entscheidungsträger im öffentlichen Bereich.
Eine besondere Stärke des Projekts liegt in der engen Verzahnung von Forschung, Lehre und behördlicher Praxis. Die OTH Amberg-Weiden bringt ihre langjährige Expertise in den Bereichen KI-Forschung, Informationssicherheit und E-Learning ein. Über das hauseigene E-Learning-Medienlabor, das 2017 im Rahmen des Lernlabors Cybersicherheit gegründet wurde, verfügt die Hochschule über die notwendige Infrastruktur, um komplexe Forschungsergebnisse in verständliche und interaktive Lernformate zu übertragen. Diese werden im Projektverlauf gezielt für die Umsetzung beim LSI aufbereitet, wodurch eine direkte Verwertung im sicherheitsrelevanten Kontext gewährleistet ist.

Enge Kooperation für gemeinsamen Erfolg

Für das LSI stellt HeCKI ein zentrales Vorhaben dar, um die eigene Strategie zur proaktiven Gefahrenabwehr weiter auszubauen. Das LSI – bundesweit eine der ersten eigenständigen Fachbehörden für IT-Sicherheit – ist unter anderem für den Schutz des bayerischen Behördennetzes sowie für die Beratung von Kommunen und kritischen Infrastrukturen zuständig. Mit dem Projekt HeCKI soll dieses Mandat weiter gestärkt werden, indem neuartige Angriffsvektoren frühzeitig erkannt und geeignete Reaktionen darauf entwickelt werden. Ziel ist es, nicht nur defensiv auf Sicherheitsvorfälle zu reagieren, sondern die Schutzmechanismen systematisch zu erweitern und den Sicherheitsstandard im Freistaat nachhaltig zu erhöhen.
Ein weiterer Aspekt des Projekts betrifft die Förderung eines gesamtheitlichen Sicherheitsbewusstseins im öffentlichen Sektor. Durch die gezielte Aufklärung über KI-gestützte Manipulationstechniken – etwa bei Sprach- oder Video-Fälschungen – werden insbesondere jene Angriffsszenarien adressiert, die auf psychologische Täuschung und Social Engineering abzielen. Klassische Betrugsmaschen wie der sogenannte „Enkeltrick“ erfahren durch KI eine neue, besorgniserregende Qualität: Stimmen lassen sich täuschend echt imitieren, Videos manipulieren und Nachrichten massenhaft verbreiten. Die Fähigkeit, solche Täuschungen zu erkennen und abzuwehren, erfordert neue Kompetenzen auf Seiten der Beschäftigten in Verwaltung und öffentlichen Einrichtungen.

Nicht zuletzt verfolgt das Projekt auch das Ziel, die digitale Souveränität öffentlicher Stellen zu stärken. Durch die fundierte Auseinandersetzung mit KI-Risiken und der Entwicklung praxisnaher Schutzkonzepte leistet HeCKI einen wichtigen Beitrag zur sicheren digitalen Transformation in Bayern. Das Projekt hebt dabei nicht nur die Relevanz technischer Maßnahmen hervor, sondern auch die Notwendigkeit vorausschauenden, verantwortungsvollen Handelns im Umgang mit einer Technologie, die das Potenzial hat, nahezu alle Lebensbereiche zu beeinflussen.

7. Tabletop-Übungen – Die Feuerwehrübungen für die Kommunalverwaltung

Was passiert eigentlich, wenn plötzlich alle Computer in der Verwaltung ausfallen? Wenn E-Mails nicht mehr ankommen, Daten nicht mehr abrufbar sind oder keine Programme mehr starten? Solche Szenarien sind längst keine Science-Fiction mehr – und genau deshalb muss man sich gezielt auf diese IT-Notfälle vorbereiten.

Schwachstellen erkennen, um Abläufe zu verbessern

Ein besonders nützliches und zugleich unkompliziertes Mittel dafür sind sogenannte Tabletop-Übungen.
In einer solchen Übung kommen Mitarbeitende zusammen, um gemeinsam durchzuspielen, wie sie im Ernstfall handeln würden. Das heißt, es wird zusammen diskutiert, wie die Verwaltung im Ernstfall auf verschiedene Vorfälle reagieren würde.

Ein erfahrener Moderator führt durch das Szenario:
Was passiert, wenn plötzlich alle Systeme ausfallen?
Wer macht was?
Wo gibt es Lücken, und wie kann man diese schließen?

Das Ziel der Übung ist es, Schwachstellen zu erkennen, Abläufe zu verbessern und Sicherheit zu gewinnen, um im Notfall nicht überrascht zu werden.

Das LSI hat mit dem Tabletop-Paket einen einfachen Leitfaden mit unterschiedlichen Notfallszenarien zur Durchführung dieser Übungen erarbeitet.
Darin werden alle notwendigen Unterlagen zur Verfügung gestellt:

- Einführungsschreiben
- Infoblatt
- Situationshandbücher
- Feedbackbefragung Übungsteilnehmer
- Feedbackbefragung TTX-Paket

Jedes vom LSI entwickelte Szenario basiert auf fiktiven, aber realitätsnahen Bedrohungen. Die Übungen sind außerdem so gestaltet, dass sie individuell an die spezifischen Bedürfnisse verschiedener Organisationen angepasst werden können.

“Die gemeinsame Organisation des IT-Grundschutz-Tags zeigt eindrucksvoll, wie wichtig die enge und vertrauensvolle Zusammenarbeit von Bund und Ländern für die Sicherheit unserer digitalen Verwaltung ist“, betont Bernd Geisler, Präsident des LSI. „Nur gemeinsam können wir den wachsenden Herausforderungen der IT-Sicherheit wirkungsvoll begegnen.“

8. IT-Grundschutz-Tag 2025 – Erfolgreiche Kooperation von LSI und BSI

Das LSI beteiligt sich regelmäßig an Fachveranstaltungen rund um Informationssicherheit, sowohl als aktiver Mitgestalter als auch als Veranstalter. Ziel ist es, aktuelle Entwicklungen, bewährte Methoden und zukunftsweisende Themen in die Breite zu tragen und den fachlichen Austausch zwischen Verwaltung, Wirtschaft und Wissenschaft zu fördern. In diesem Rahmen war der diesjährige IT-Grundschutz-Tag ein Highlight.

Klares Zeichen für vertrauensvolle Zusammenarbeit

Am 07. Juli 2025 war das Staatsministerium der Finanzen und für Heimat in Nürnberg Gastgeber eines besonderen Ereignisses: Erstmals wurde der IT-Grundschutz-Tag gemeinsam vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem LSI organisiert. Für das LSI war dies nicht nur ein organisatorischer Meilenstein, sondern auch ein klares Zeichen für die vertrauensvolle Zusammenarbeit zwischen dem Bund und dem Freistaat Bayern im Bereich der Informationssicherheit.

Die etablierte Veranstaltungsreihe zur Informationssicherheit des BSI stand in diesem Jahr unter dem Leitthema „IT-Grundschutz mit Weitblick – Synergien mit übergreifenden Themen“.

Stärkung der Informationssicherheit

In einem vielseitigen Fachprogramm wurden sowohl aktuelle Herausforderungen als auch künftige Entwicklungen im Bereich der Informationssicherheit adressiert. Mehr als 140 Teilnehmer waren vor Ort in Nürnberg dabei, über 1.000 weitere verfolgten die Veranstaltung digital. Der breite Teilnehmerkreis aus Verwaltung, Wirtschaft und Wissenschaft unterstreicht das große Interesse an praxisnaher Informationssicherheit.

Im Mittelpunkt standen neben der Weiterentwicklung des IT-Grundschutzes vor allem Querschnittsthemen - von Datenschutz über Risikomanagement bis hin zu Fragen der Cyberresilienz. Zahlreiche Fachvorträge, praxisnahe Impulse und der gezielte Austausch zwischen den Teilnehmern machten den Tag zu einer wertvollen Plattform für Vernetzung und Wissenstransfer. Der IT-Grundschutz-Tag hat eindrucksvoll gezeigt, wie durch enge Kooperation und gemeinsame Verantwortung über föderale Ebenen hinweg ein wirksamer Beitrag zur Informationssicherheit geleistet werden kann. Die Vortragsfolien sowie die Aufzeichnungen der einzelnen Beiträge stehen auf der Webseite des BSI zur Verfügung.

Auch künftig wird sich das LSI regelmäßig an zentralen Veranstaltungen zur Cybersicherheit beteiligen. So stärken wir gemeinsam die digitale Sicherheit in Bayern - und darüber hinaus.


Herzlich Willkommen
Thementag „Kommunale IT-Sicherheit"
IT-Sicherheit
Trinkwasserversorgung
Abwasserentsorgung

9. Thementagsreihe „Kommunale IT-Sicherheit“

Das Landesamt für Sicherheit in der Informationstechnik (LSI) bietet jährlich in allen sieben Regierungsbezirken Thementage für Kommunen und Betreiber kritischer Infrastrukturen mit unterschiedlichen Schwerpunkten zur Informationssicherheit an.
Dabei darf das Landesamt die Teilnehmer vor Ort bei staatlichen und kommunalen Behörden begrüßen.
Durch die Präsenzveranstaltungen steht neben den inhaltlichen LSI-Beiträgen vor allem auch der Austausch zwischen den Teilnehmern und dem LSI im Vordergrund.

Persönlicher Austausch im Vordergrund

LSI-Präsident Bernd Geisler eröffnet die Veranstaltungen und stimmt auf das Kernthema ein, worauf die Referenten des LSI mit Fachvorträgen zur aktuellen IT-Sicherheitslage und den Angeboten des LSI durch den Tag führen. Neben dem neuen Produkt des LSI „Weg in das IT-Risikomanagement“ wird auch in einem Beitrag auf den Einsatz der künstlichen Intelligenz in der öffentlichen Verwaltung eingegangen.

Erstmalig findet dieses Jahr auch eine Kooperation mit dem Landeskriminalamt (LKA) statt, in dem die Kollegen Beispiele aus der Cyberkriminalität aufzeigen. Auch für die Teilnehmer der Betreiber kritischer Infrastrukturen werden in einem Beitrag die aktuellen Angebote des LSI aufgezeigt.

Bereits vergangenes Jahr konnte das LSI insgesamt rund 900 Teilnehmer zur Thementagsreihe willkommen heißen. Dabei lag der Schwerpunkt beim Thema „kommunale IT-Notfallprävention“. Die IT-Experten aus der kommunalen IT-Sicherheitsberatung des LSI stellten Neuerungen in den Sensibilisierungsmöglichkeiten in Form von Online-Schulungen und Phishing-Simulationen vor. Außerdem wurde eindrucksvoll in einem Live-Hacking-Vortrag auf gängige Angriffsvektoren und möglichen Gegenmaßnahmen hingewiesen.
Abschließend wurden die neuen LSI Table-Top-Übungen und die neue Version des LSI IT-Notfallmanagements vorgestellt.

Orientierungs- und Arbeitshilfen stark gefragt

2024 wurden erstmals auch Betreiber kritischer Infrastrukturen (KRITIS-Betreiber) zur Thementagsreihe „Kommunale IT-Sicherheit“ eingeladen, für deren Beratung es im LSI ebenfalls ein eigenes IT-Expertenteam gibt. Diesen wurden bei der Veranstaltung die verschiedenen Orientierungs- und Arbeitshilfen des LSI für Krankenhäuser, Wasserversorger, Wasser- und Siedlungsabfallentsorger präsentiert.
Besonders erfreulich war die Bereitschaft einiger kommunaler Teilnehmer, ihre Erfahrungen im Bereich der IT-Sicherheit durch Gastbeiträge bei der Veranstaltung zu teilen.


LSI – eine bayerische Besonderheit
Landesamt für Sicherhe

10. BITS & bites 2025

Die Fachtagung „BITS & bites“ wurde letztes Jahr ins Leben gerufen und richtet sich primär an Informationssicherheitsbeauftragte (ISBs) und IT-Verantwortliche von Behörden, die zur unmittelbaren Staatsverwaltung gehören. Der Fokus der Veranstaltung liegt auf der Vernetzung und dem Austausch der IT-Sicherheitsbeauftragten und dem LSI.

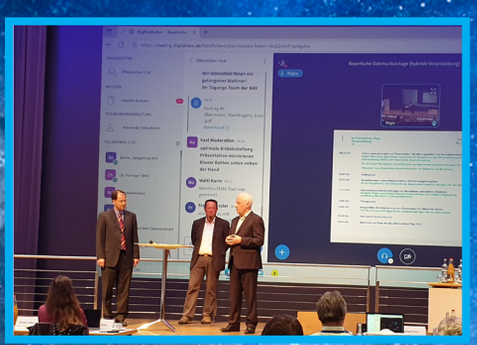
Veranstaltungreihe bayernweit ausgedehnt

Nach den überaus positiven Rückmeldungen im ersten Jahr der Veranstaltungsreihe wurde sie für 2025 erneut aufgelegt. Um möglichst vielen Interessierten die Möglichkeit zur Teilnahme zu geben, wurde die Veranstaltung dieses Jahr in Nürnberg, München, Regensburg und Würzburg durchgeführt.

Aufgrund der auch in diesem Jahr sehr hohen Resonanz bei den Informationssicherheitsbeauftragten und zum ersten Mal auch einiger IT-Leiter wurde noch ein weiterer Zusatztermin in München angeboten. Die Veranstaltungsreihe fand Mitte dieses Jahres statt. Während der Tagung wurden digitale Herausforderungen und Problemstellungen im Kontext der IT-Sicherheit beleuchtet.

Auf der diesjährigen Agenda standen aktuelle Themen und Problematiken, die durch das LSI aufbereitet und anschließend mit den Teilnehmern diskutiert wurden. Dabei konnten Gastdozenten aus dem Wasserwirtschaftsamt und bei der Regierung von Mittelfranken angesiedelten Landesstelle OT gewonnen werden. Einige Themenvorschläge, wie beispielsweise die Absicherung von Webanwendungen unter Berücksichtigung der aktuellen Bedrohungslage, standen ebenso wie der Umgang mit verschiedenen Cloudumgebungen auf der Tagesordnung. Neben den fachlichen Vorträgen fand auch die Versorgung mit Häppchen und Getränken großen Zuspruch.


Schutzbedarf
Eigene Struktur
Bausteine / Anforderungen
jährlich aktualisiert
Maßgeschneidertes Regelwerke für jede Behörde
ISMS-Tool
To Do
To Do
To Do
Audit
Überprüfung und Unterstützung
Umsetzung der Maßnahmen



11. Datenschutz und IT-Grundschutz sind bislang nahezu berührungsfreie Paralleluniversen

Am 22. Mai fanden in Amberg die Datenschutztage statt, bei der ein Fachvortrag die Bedeutung der Zusammenarbeit zwischen Datenschutz und IT-Grundschutz hervorhob. Dr. Wambsganz vom Bayerischen Landesbeauftragten für den Datenschutz, Stefan Obermeier vom Landesamt für Sicherheit in der Informationstechnik, sowie Alexander Lutz vom Bayerischen Finanz- und Heimatministerium präsentierten ein innovatives Projekt, das die bislang getrennten Disziplinen zusammenbringen soll.

Synergien schaffen

Das Ziel der Kooperation ist es, Synergien zu schaffen, um Ressourcen effizienter zu nutzen und Doppelarbeit zu vermeiden. Obwohl Datenschutzbeauftragte und Informationssicherheitsbeauftragte teilweise eine ähnliche Zielsetzung haben, arbeiten beide Bereiche unabhängig.

Der Fachvortrag analysierte die Gemeinsamkeiten und Unterschiede fundiert und zeigte, wo sich Schnittstellen für eine bessere Zusammenarbeit ergeben. Diese wurden beschrieben und bereits erfolgreich am Bayerischen Staatsministerium der Finanzen und für Heimat erprobt. Alexander Lutz stellte die Ergebnisse anhand eines konkreten Fachverfahrens vor. Im nächsten Schritt soll das Konzept in einem weiteren Fachverfahren getestet werde.

Abschließend ist geplant, einen Leitfaden zu entwickeln, der die gewonnenen Erkenntnisse einem breiten Fachpublikum zugänglich macht.

Praxisnahe Vorträge und Diskussionen

Im Juli reisten die Dozenten in das „andere Universum“ und präsentierten den Vortrag auf dem IT-Grundschutz-Tag dem interessierten Fachpublikum. Das Thema stieß dort über Bayern hinaus auf großes Interesse und zeigt, wie wichtig die Vernetzung der beiden Disziplinen für eine sichere digitale Zukunft ist. Mit diesem Ansatz setzt Bayern ein Zeichen für eine stärkere Zusammenarbeit zwischen Datenschutz und Informationssicherheit, um die Effizienz und den Schutz in der digitalen Verwaltung nachhaltig zu verbessern.

© Paul Schmidt Kunstmühle Vach KG

12. Neues Unterstützungsangebot für Betreiber von Wasserkraftanlagen

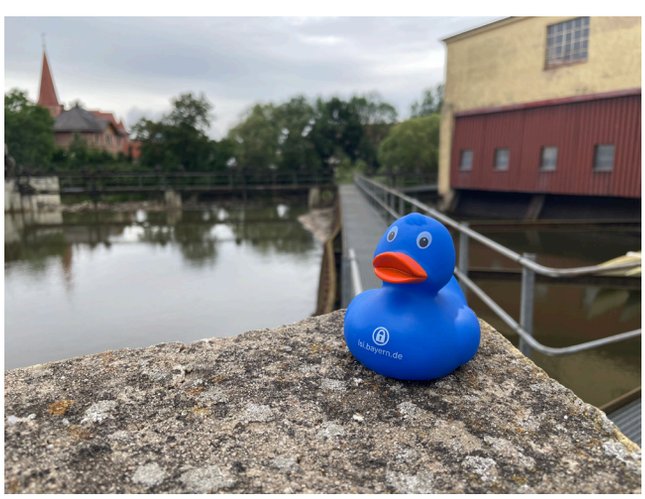
Das Referat „IT-Sicherheit öffentlicher KRITIS-Betreiber“ des LSI hat in Zusammenarbeit mit Branchenvertretern Beratungsunterlagen für Betreiber von Wasserkraftanlagen im KRITIS-Sektor Energie entwickelt.

In Bayern trägt die Wasserkraft mit etwa 19 % zur Bruttostromerzeugung bei. Darunter sind rund 3.400 kleine Anlagen (bis 100kW). Diese Anlagen stellen eine wichtige Zielgruppe dar, die das LSI gezielt mit niederschwelligen Beratungsunterlagen anspricht. So sollen auch kleinere Betreiber bestmöglich bei der schwierigen Aufgabe der Absicherung ihrer IT-Systeme und Leittechnik unterstützt werden.
Die große Bedeutung der Funktionsfähigkeit der Stromversorgung wird durch den massiven Stromausfall in Spanien und Portugal im April 2025 deutlich. Die Berichterstattung zeigt, dass viele Bereiche des öffentlichen Lebens, wie das Telefonnetz und der öffentliche Verkehr, erheblich beeinträchtigt wurden. Dies unterstreicht die Notwendigkeit, auch kleine Anlagen unter den bayerischen Wasserkraftwerken abzusichern.

Orientierungshilfen für kritische Infrastrukturen

Das LSI hat bereits Orientierungshilfen für die kritischen Infrastrukturen der Branchen Wasser (Trinkwasserversorger und Abwasserentsorger), Siedlungsabfallentsorgung sowie für Krankenhäuser erstellt und pressewirksam veröffentlicht. Für den Sektor Energie wurde nun speziell für Betreiber von Wasserkraftanlagen eine Checkliste erstellt, welche gemeinsam mit einem Arbeitskreis entwickelt wurde und die speziellen Gegebenheiten der Wasserkraftanlagen berücksichtigt. Diese dient als Leitfaden zur Verbesserung der IT-Sicherheit, wurde mit Partnern aus der Praxis erprobt und wird, wie die anderen Beratungsunterlagen, ebenfalls kostenfrei zugänglich sein.

Die Checkliste für Wasserkraftwerke setzt sich aus zwei Teilen zusammen: Die 10 Fragen zur IT-Sicherheit, welche die wichtigsten abzusichernden Aspekte in Kürze abfragen. Damit wird es den Betreibern ermöglicht, eine schnelle Ersteinschätzung ihres Standes der IT-Sicherheit zu treffen. Im zweiten Teil werden die einzelnen Themengebiete näher erläutert und deren Umsetzungsgrad anhand von Fragen ermittelt. Die Checkliste dient dabei als „roter Faden“, der die empfohlenen Maßnahmen in eine strukturierte Abfolge bringt. Anwender werden bei der Arbeit mit der Checkliste schrittweise dabei unterstützt, die Resilienz ihrer IT-Infrastruktur auszubauen. Die Checkliste dient als heranführendes Einstiegsdokument. Die bereits veröffentlichten Beratungsunterlagen des LSI können in einem nächsten Schritt zur weiteren Erhöhung des IT-Sicherheitsniveau genutzt werden.



13. NIS-2: Neue Anforderungen für Betreiber kritischer Infrastrukturen

Jährlich entsteht alleine in Deutschland ein Schaden in Höhe des Jahresumsatzes von DAX-Konzernen durch Cyberkriminelle. Dies ist eine ernst zu nehmende Bedrohung für den Wirtschaftsstandort Deutschland beziehungsweise Europa, weshalb die Europäische Union Ende 2022 die NIS-2-Richtlinie erlassen hat. Diese Richtlinie soll das Cybersicherheitsniveau der von NIS-2 betroffenen Organisationen in der gesamten EU unter anderem in Sektoren wie Gesundheit, Energie-, Wasserversorgung und Verkehr erhöhen und europaweit harmonisieren.

Erhöhung des Cybersicherheitsniveaus

Aber nicht nur Betreiber kritischer Infrastrukturen werden zukünftig reguliert: Auch die Bundesverwaltung und manches verarbeitende Gewerbe sowie Hersteller bestimmter Waren sind betroffen, sofern sie über definierten Schwellenwerten liegen. Einrichtungen der bayerischen Landesverwaltung werden ebenfalls durch NIS-2 reguliert. Details zu diesen „Einrichtungen mit Bedeutung für den Binnenmarkt“ werden in einem eigenen Artikel der Richtlinie beschrieben.

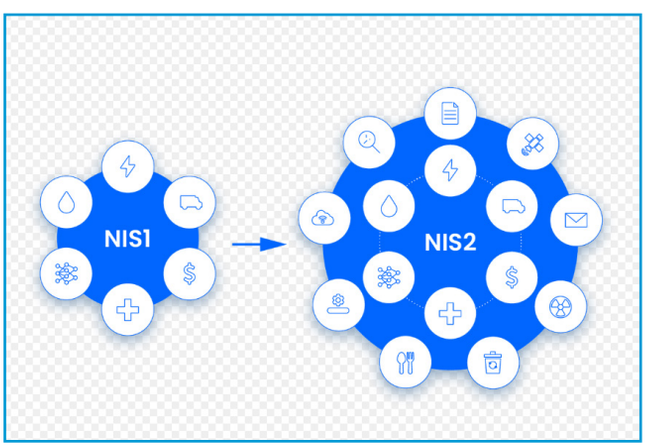
Die NIS-2-Richtlinie wurde von der Bundesregierung noch nicht in nationales Recht umgesetzt (Stand September 2025). Die veröffentlichten letzten Regierungsentwürfe unterscheiden zwischen wichtigen und besonders wichtigen Einrichtungen sowie Betreibern kritischer Anlagen. Die Einrichtungsart, in die ein Unternehmen fällt, bestimmt sich einerseits durch den Sektor, in dem das Unternehmen tätig ist, und andererseits durch Schwellenwerte wie beispielsweise Mitarbeiterzahl und Jahresumsatz. Prognosen gehen davon aus, dass alleine in Deutschland über 30.000 Einrichtungen von der Regulierung betroffen sind.

Nur von wenigen Staaten wurde die NIS-2-Richtlinie fristgerecht bis Ende letzten Jahres in nationales Recht umgesetzt. Viele Anforderungen an Unternehmen lassen sich aber heute schon aus der EU NIS-2-Richtlinie ableiten. Das LSI empfiehlt betroffenen Unternehmen, sich am besten bereits jetzt auf die kommenden Anforderungen vorzubereiten.

Checkliste kostenfrei im Downloadcenter

Als Hilfestellung hat das LSI eine „Checkliste nach NIS-2-Kriterien“ entwickelt, die zentrale Anforderungen und Pflichten der NIS-2-Richtlinie für wichtige und besonders wichtige Einrichtungen sowie Betreiber kritischer Anlagen, die den besonders wichtigen Einrichtungen zuzurechnen sind, aufzeigt.
Darüber hinaus wurde für Betreiber kritischer Infrastrukturen eine Handlungsempfehlung mit konkreten Maßnahmen entwickelt, die als Einstieg in die Absicherung dient.

Die Checkliste sowie die Handlungsempfehlung („Handlungsempfehlung KMU“) kann auf der Website des LSI kostenfrei heruntergeladen werden.



14. Maßnahmen am LSI zur EU-Richtlinie 2022/2555 (NIS-2-Richtlinie)

Mit der Änderung des Bayerischen Digitalgesetzes (BayDiG) vom 17.10.2024 wurden die Regelungen der EU-Richtlinie 2022/2555 (NIS-2-Richtlinie) fristgerecht in Landesrecht überführt. Hierdurch wurde das LSI als die in Bayern zuständige Stelle benannt.
Damit einhergehend nimmt das Bayern-CERT die Rolle eines CSIRT im Sinne der EU-Richtlinie war. In diesem Zuge ist das Bayern-CERT im Cyber Defence Center nun auch rund um die Uhr erreichbar.

Erreichbarkeit 24 Stunden an 7 Tagen in der Woche

Ferner hat das LSI sein Beratungsportfolio für Behörden der Staatsverwaltung um ein zielgruppenorientiertes Schulungsangebot für Behördenleitungen erweitert. Dieses Angebot ermöglicht es den obersten Dienstbehörden, die in der EU-Richtlinie geforderten Kenntnisse und Fähigkeiten der Leitungsebene im Bereich der Cybersicherheit sicherzustellen, ohne auf externe Schulungsmaßnahmen zurückgreifen zu müssen. Überdies stellt das LSI bereits seit mehreren Jahren durch spezielle Onlinekurse allen Beschäftigten des Freistaats ein Sensibilisierungs- und Schulungsangebot zur Verfügung.
Zur Wahrung der Pflichten, die sich im Zusammenhang mit wichtigen Einrichtungen gemäß der EU-Richtlinie innerhalb der Staatsverwaltung ergeben, wurde am LSI die sogenannte EBB-Stelle Bayern als eigenständige, direkt dem Präsidenten unterstellte Organisationseinheit geschaffen.

Einrichtungen mit Bedeutung für den Binnenmarkt

Bei „EBB“, der Abkürzung für den im BayDiG geschaffenen Begriff „Einrichtungen mit Bedeutung für den Binnenmarkt“ (EBB), handelt es sich um eben solche wichtigen Einrichtungen, welche spezifische Funktionen in der Staatsverwaltung wahrnehmen. Die EBB-Stelle stellt den Prozess zur Identifizierung dieser Behörden unter Einbeziehung der obersten Dienstbehörden sicher. Ferner steht sie den EBB zu NIS-2-spezifischen Fragestellungen zur Seite und tauscht sich hierzu auf Arbeitsebene auch mit den Verwaltungen von Bund und Ländern aus. Zusätzlich unterstützt die EBB-Stelle jene Referate innerhalb des LSI, welche Berührungspunkte zu den auf die Staatsverwaltung entfallenden Regelungen aus NIS-2 aufweisen, so zum Beispiel zur Einhaltung der Meldepflichten bei erheblichen Sicherheitsvorfällen. Im Kontext der NIS-2 Richtlinie übernimmt die EBB-Stelle auch die dem LSI durch das BayDiG auferlegten Aufsichtspflichten und verfolgt die gegebenenfalls notwendige Durchsetzung weiterer Maßnahmen.


Landesamt für Sicherheit in der Informationstechnik
LSI – eine bayerische Besonderheit
• Bayern seit 01.12.2017 erstes Bundesland mit eigenem Landesamt als Cybersicherheitsbehörde
• Aktuell rund 160 (geplant: 200)
• Rechtsgrundlage BayDiG
• Aufgaben: Schutz bayerisches Behördennetz + Beratung Staat, Kommunen KRITIS-Betreiber
• Standorte: Nürnberg, Bad Neustadt a.d. Saale, Würzburg
m k
MÜNCHEN
KLINIK

15. Thementage Informationssicherheit in Kliniken

Aktuelle IT-Sicherheitsvorfälle zeigen, dass Krankenhäuser gegen Cyberangriffe gut gerüstet sein müssen, um die Patientensicherheit zu gewährleisten. Zur Unterstützung der Klinikleitungen, IT-Sicherheitsverantwortlichen und IT-Leitungen der bayerischen Kliniken bietet das Landesamt für Sicherheit in der Informationstechnik (LSI) eine jährliche Informationsveranstaltungsreihe zum Thema „Informationssicherheit in Kliniken“ an. Die Veranstaltungen dieser Reihe fanden sowohl online als auch in Präsenz statt.

Gewährleistung der Patientensicherheit

Referentinnen und Referenten aus unterschiedlichen Bereichen berichteten aus ihrem Arbeitsgebiet „Informationssicherheit“, stellten Unterstützungsmöglichkeiten bei Sicherheitsvorfällen sowie zur Stärkung der Informationssicherheit vor, sprachen über finanzielle Förderungsmöglichkeiten von Krankenhäusern, beleuchteten Hintergründe und berichteten von ihren Praxiserfahrungen.

Rund 60 Teilnehmer wurden am 30.07.2025 in der München Klinik Bogenhausen begrüßt. Zu Gast waren Klinikleitungen, IT-Leiter und Informationssicherheitsbeauftragte von Kliniken aus dem südbayerischen Raum.

Zum Auftakt der Veranstaltung begrüßten LSI-Präsident Bernd Geisler und der kaufmännische Geschäftsführer der München Klinik gGmbH, Herr Dr. med. Guderjahn, die Teilnehmer. Anschließend präsentierten Gastredner und Experten des LSI die aktuelle Sicherheitslage und zahlreiche Fachvorträge.

Das Experten-Team des LSI stellte dabei die Unterstützungsmöglichkeiten im Rahmen von IT-Sicherheitsvorfällen durch das Cyber Defence Center des LSI vor, sowie Themen wie Multifaktor-Authentisierung, Beratungsangebote des LSI für die bayerischen Kliniken und Table-Top-Übungen.

Die Bayerische Krankenhausgesellschaft und das Bayerische Staatsministerium für Gesundheit, Pflege und Prävention informierten die Teilnehmer über aktuelle Themen wie „Sicherheitsanforderungen der ePA und Telematikinfrastruktur“ sowie „Transformationsfonds und Cybersicherheit“. Die Klinik München stellte ihr physikalisches Sicherheitskonzept vor und gab dadurch einen wertvollen Einblick in die praktische Umsetzung der Informationssicherheit. Abschließend präsentierte die Zentrale Ansprechstelle Cybercrime (ZAC) des Bayerischen Landeskriminalamts (BLKA) Phänomene und Schwachstellen im Bereich Cybercrime aus Sicht der Polizei.

Während der Veranstaltung entstand ein konstruktiver Diskurs zu unterschiedlichen Themen der Informationssicherheit in Kliniken. Das LSI freut sich auf den Austausch mit weiteren Teilnehmern in künftigen Veranstaltungen.

16. IP-basierte Alarmierung – ein kostenfreier Service sorgt für Sicherheit im Fall der Fälle

Das Landesamt für Sicherheit in der Informationstechnik (LSI) bietet allen interessierten Kommunen, Unternehmen mit staatlicher Beteiligung sowie Betreibern kritischer Infrastruktur unterhalb der Schwellenwerte der BSI-Kritis Verordnung (BSI-KritisV) die Möglichkeit zur Teilnahme am kostenfreien Service der IP-basierten Alarmierung.
Ziel der IP-basierten Alarmierung ist es, Schwachstellen und Gefährdungen von Systemen, die anhand der öffentlichen IP-Adressen für jedermann ansprechbar sind, schnellstmöglich zu detektieren und die Eigentümer diesbezüglich zu alarmieren. So können die Betroffenen zügig Maßnahmen zur Gefahrenabwehr ergreifen, um einen potentiellen Schaden durch kriminelle Akteure zu reduzieren oder im besten Fall ganz zu vermeiden.

Alarmierungssysteme verkürzen Reaktionszeiten immens

Dieser Service basiert zu großem Teil auf der Arbeit im Cyber Defence Center des LSI, welches die aktuelle Sicherheits- und Bedrohungslage mit Fokus auf das Bayerische Behördennetz im Blick behält. Dabei werden beständig aktuelle IT-Sicherheitsvorfälle, laufende Angriffskampagnen und die aktuelle Bedrohungslage ausgewertet und Gegenmaßnahmen abgeleitet. Das LSI gewinnt hierzu Erkenntnisse aus eigenen Analysen sowie dem Austausch mit anderen IT-Sicherheitsbehörden, u.a. mit dem BSI.

Um das volle Potential dieses Service auszuschöpfen, können neben den öffentlichen IP-Adressen noch weiterführende Informationen zu den betriebenen Diensten sowie entsprechende Produktinformationen an das LSI gemeldet werden. Durch deren Auswertung lässt sich die Qualität der Alarmierungen zusätzlich erhöhen. Somit können spezifischere Maßnahmenempfehlungen bereitgestellt und Fehlalarme vermieden werden.

Die aktuellen Nutzerzahlen der IP-basierten Alarmierung betragen:
Kommunen: 581 Kommunen meldeten dem LSI zuletzt 2064 Netzbereiche.
Unternehmen mit staatlicher Beteiligung und Betreiber kritischer Infrastruktur (unabhängig von ihrer Größe): 121 Anmeldungen und 332 unterschiedliche Adressbereiche.

Kontakt direkt und kostenfrei

Für weitere Informationen zu unserem kostenfreien Service wenden sich interessierte Kommunen, Unternehmen mit staatlicher Beteiligung sowie Betreiber kritischer Infrastruktur bitte an die jeweils zuständigen Beratungsreferate des LSI:

Kommunal:
0911/21549-523
beratung-kommunen@lsi.bayern.de

Betreiber kritischer Infrastruktur unabhängig von deren Größe und Unternehmen mit staatlicher Beteiligung:
0911/21549-525
beratung-kritis@lsi.bayern.de
beratung-beteiligungen@lsi.bayern.de


Landesamt für Sicherheit in der Informationstechnik
BW
CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

17. Starke Allianzen – der Gemeinschaftsstand auf der it-sa 2024

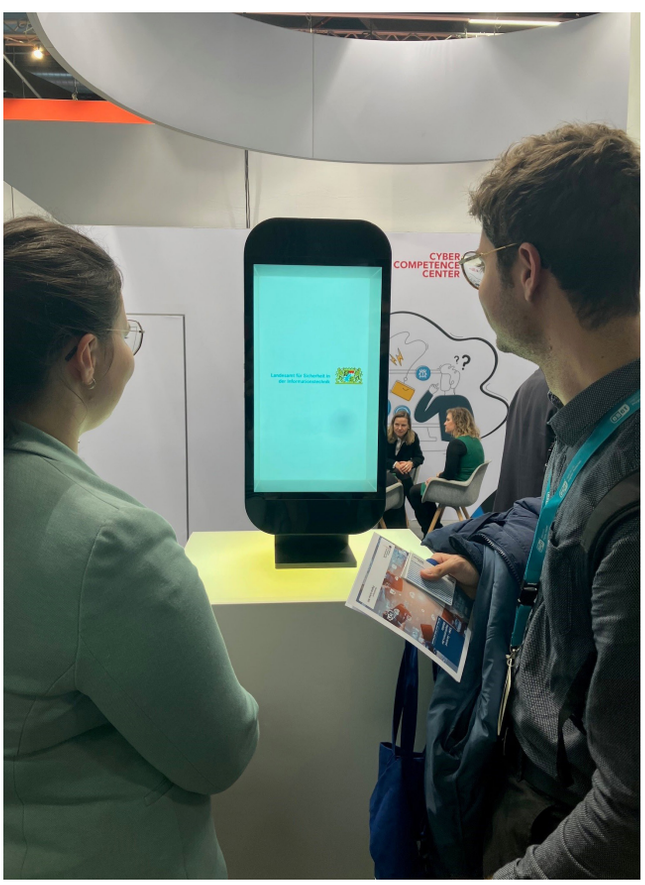
Die it-sa ist eine der führenden Fachmessen für IT-Sicherheit in Europa und findet jährlich in Nürnberg statt. Sie bietet eine Plattform für Unternehmen, Fachleute und Experten aus der IT-Sicherheitsbranche, um sich über aktuelle Trends, Technologien und Lösungen im Bereich der Informationssicherheit auszutauschen.

Kooperationen über Grenzen hinweg

Seit 2022 präsentieren sich das LSI und die Cybersicherheitsagentur Baden-Württemberg (CSBW) mit einem gemeinsamen Stand auf der it-sa. Im Jahr 2024 beteiligte sich zudem das Hessen CyberCompetence-Center (Hessen3C) am Gemeinschaftsstand.
Die Kooperation zwischen den Bundesländern unterstreicht die Bedeutung des Austauschs und der Zusammenarbeit im Bereich der Informationssicherheit, insbesondere in einer Zeit, in der Cyberbedrohungen immer komplexer und vielfältiger werden.

Der Gemeinschaftsstand soll das Bewusstsein für die Notwendigkeit einer robusten Informationssicherheit schärfen. Durch die zunehmende Bedrohungslage in der IT ist der Austausch zwischen den verschiedenen Akteuren - von staatlichen Institutionen über Unternehmen bis hin zu Forschungseinrichtungen – entscheidend, um effektive Lösungen zu entwickeln und umzusetzen.

Die it-sa 2024 bot eine hervorragende Gelegenheit zum Networking sowie einen Raum für Wissensaustausch und gemeinsame Initiativen. Der Gemeinschaftsstand der Cybersicherheitsbehörden aus Bayern, Baden-Württemberg und Hessen steht exemplarisch für die kollektiven Anstrengungen, die notwendig sind, um die digitale Sicherheit in Deutschland nachhaltig zu verbessern.



Auch im Jahr 2025 wird sich das LSI gemeinsam mit dem Hessen3C vom 7. bis 9. Oktober auf der it-sa präsentieren. Der Stand ist in Halle 9 mit der Standnummer 316 zu finden. Besuchen Sie uns und informieren Sie sich über die Aufgaben des LSI. Wir freuen uns auf den Austausch mit Ihnen.


Skydeck

18. Karriere im digitalen Schutzraum – Perspektiven am LSI

Als erst 2017 gegründete Behörde befindet sich das LSI im stetigen Aufbau und leistet seitdem einen wichtigen Beitrag zur IT-Sicherheit in der Staatsverwaltung sowie bei Kommunen und öffentlichen KRITIS-Unternehmen. Rund 150 engagierte Mitarbeiterinnen und Mitarbeiter arbeiten daran, die digitale Infrastruktur der öffentlichen Verwaltung nachhaltig zu stärken – und die Zahl wächst weiter. In den kommenden Jahren wird unsere Behörde auf rund 200 Mitarbeitende anwachsen, um den Herausforderungen der fortschreitenden Digitalisierung gerecht zu werden.

Als hochmoderne, kompetente IT-Sicherheitsbehörde für den Freistaat Bayern bieten wir attraktive Karrieremöglichkeiten.

Duales Studium – der ideale Start in eine spannende Karriere

Im LSI können verschiedene duale Studiengänge absolviert werden, die praxisnahe Ausbildung und fundierte Theorie miteinander verbinden:

- Verwaltungsinformatik (FH): Ein praxisorientiertes Studium, das sowohl Informatik als auch Verwaltungswissenschaften umfasst. Theoriephasen an der Hochschule für Angewandte Wissenschaften in Hof und an der Hochschule für den öffentlichen Dienst in Bayern in Hof wechseln sich mit Praxisphasen im LSI ab. Bereits zu Beginn des Studiums erfolgt die Verbeamtung.
- Bachelor IT – Duales Studium (BIDS): Das Studium erfolgt in einem Bachelor-Studiengang mit IT-Ausrichtung an einer beliebigen Hochschule innerhalb Bayerns. Die Praxisphasen werden dann im LSI in Nürnberg absolviert.
- Cybersecurity (B.Sc.) in Kooperation mit der TH Ingolstadt: In diesem Studiengang werden fundierte Kenntnisse im Bereich der IT-Sicherheit erworben. Die neu erlangten Kompetenzen können in den Praxisphasen am LSI eingesetzt werden.

Nach erfolgreichem Abschluss des Studiums erfolgt die Übernahme als Tarifbeschäftigter in einem unbefristeten Arbeitsverhältnis bzw. als Beamter – der Einstieg in eine vielversprechende Karriere.

Direkteinstieg – für IT-Talente mit Hochschulabschluss

Das LSI ist regelmäßig auf der Suche nach neuen engagierten Kolleginnen und Kollegen in der 3. und 4. Qualifikationsebene.
Der Direkteinstieg ist daher möglich als:

- IT-Experte/in (3. Qualifikationsebene): Voraussetzung für diesen Einstieg ist ein abgeschlossenes Studium im Bereich IT (Diplom [FH] / Bachelor).
- Referent/in (4. Qualifikationsebene): Für den Einstieg als Referent/in ist ein Studium im Bereich IT mit einem Masterabschluss oder Diplom [Univ.] notwendig.

Für beide Qualifikationsebenen gilt: Bei Vorliegen der persönlichen und laufbahnrechtlichen Voraussetzungen erfolgt in der 3. Qualifikationsebene nach 6 Monaten, in der 4. Qualifikationsebene nach 1,5 Jahren eine Verbeamtung.

Individuelle Entwicklung Fortbildung und Aufstieg

Es bestehen zahlreiche Aufstiegsmöglichkeiten, um die Karriere weiter voranzubringen:

- In der 3. Qualifikationsebene: Beförderungen bis A12 sind auf dem gleichen Dienstposten möglich. Darüber hinaus bietet das LSI eine weitere Beförderungsmöglichkeit bis Besoldungsgruppe A13 auf einem herausgehobenen Dienstposten. Mit einer modularen Qualifizierung können auch Dienstposten ab A14 übernommen werden.
- In der 4. Qualifikationsebene: Hier sind Beförderungen bis A14 auf demselben Dienstposten vorgesehen. Nach einer erfolgreichen Bewerbung auf einen entsprechenden Dienstposten können sogar Ämter ab Besoldungsgruppe A15 bekleidet werden.

Zudem können unsere Mitarbeiterinnen und Mitarbeiter vielfältige Weiterbildungsmöglichkeiten ausgerichtet an den wachsenden Aufgabenstellungen in Anspruch nehmen.

Moderne Arbeitswelt – Flexibilität und Wertschätzung

Darüber hinaus bietet das LSI seinen Mitarbeitenden:

- Spannende Aufgaben mit Verantwortung: Die Arbeit ist geprägt durch ein abwechslungsreiches und innovatives Aufgabengebiet mit sinnvollen, zukunftsweisenden Projekten, die die IT-Sicherheit der öffentlichen Verwaltung maßgeblich stärken.

- Flexibilität und Work-Life-Balance: Wir bieten flexible Arbeitszeiten, teilzeitfähige Stellen und die Möglichkeit zur Wohnraumarbeit mit bis zu 80% im IT-Bereich – damit Beruf und Privatleben gut miteinander vereinbar sind.

- Angenehmes Arbeitsumfeld: Unsere modernen Arbeitsplätze sind bestens ausgestattet. Die Räumlichkeiten bieten ideale Voraussetzungen für den Austausch und den Rückzug.

Bewerbungswege und Perspektiven

- Wertschätzender Umgang: In unserer Behörde wird ein respektvoller und wertschätzender Umgang gepflegt. Die kollegiale Zusammenarbeit erfolgt in hoch motivierten Teams.

Stellen werden mehrmals jährlich ausgeschrieben, Initiativbewerbungen sind ausdrücklich erwünscht. Insgesamt eröffnet das LSI eine moderne, zukunftsgerichtete Laufbahn im öffentlichen Dienst – mit gesellschaftlicher Relevanz und persönlicher Entwicklung.

19. Drachenbootrennen der Bayerischen Finanzgewerkschaft

Seit 2012 führt die Bayerische Finanzsporthilfe (BFSH) jährlich ein großes Bayernturnier für die Beschäftigten der bayerischen Finanzverwaltung durch. Begleitet werden die sportlichen Wettbewerbe mit einem Empfang der Bayerischen Finanzgewerkschaft (BFG). Die BFSH möchte mit den sportlichen Wettbewerben den Sport bei den Beschäftigten – sowohl bei den aktiven als auch ehemaligen – der Finanzverwaltung des Freistaates Bayern fördern. Mit einer großen Siegerehrung wird der Turniertag beendet.
2016 kam das Drachenbootrennen dazu und wurde seither immer an einem separaten Tag auf der Olympiaregattastrecke in Oberschleißheim bei München durchgeführt.

Im Jahr 2024 nahmen die Mitarbeiterinnen und Mitarbeiter des Landesamts für Sicherheit in der Informationstechnik erstmalig und mit großer Begeisterung am Drachenbootrennen der Bayerischen Finanzgewerkschaft in Oberschleißheim teil. Das Team des LSI konnte hierbei (aller Vorurteile gegenüber „Nerds“ zum Trotz) seine sportliche Seite unter Beweis stellen und erreichte Platz 40 von über 100 Teams. Damit ist das LSI für das Drachenbootrennen 2025 sicher qualifiziert.

Teamgeist auf dem Wasser

Mit viel Teamgeist und Einsatzbereitschaft paddelten die Mitarbeiterinnen und Mitarbeiter des LSI im Drachenboot über die Regatta-Strecke. Trotz der starken Konkurrenz bewiesen sie Durchhaltevermögen und Zusammenhalt, was zu der guten Platzierung führte. Das Drachenbootrennen bot dabei nicht nur Gelegenheit, sich sportlich zu betätigen, sondern auch eine Möglichkeit, sich abseits des Arbeitsalltags besser kennenzulernen und als Team enger zusammenzuwachsen.

Durch die Teilnahme an solchen Veranstaltungen wird der Zusammenhalt im Team gestärkt und die Motivation und das Engagement der Mitarbeiter gefördert.
Insgesamt war die Teilnahme des LSI am Drachenbootrennen in Oberschleißheim ein voller Erfolg und zeigt, dass die Mitarbeiterinnen und Mitarbeiter im LSI nicht nur in ihrem beruflichen Umfeld, sondern auch im sportlichen Wettkampf überzeugen können.
Das LSI nutzt auch 2025 die Chance, wieder am Drachenbootrennen teilzunehmen.

20. Erste gemeinsame Übung bayerischer Cybersicherheitsbehörden

Die Bedrohung durch komplexe Cyberangriffe auf die öffentliche Verwaltung, kritische Infrastrukturen, Kommunen und Unternehmen nimmt immer stärker zu. In der Ende 2023 veröffentlichten Cybersicherheitsstrategie 2.0, der strategischen Grundlage für die Cybersicherheitsarchitektur in Bayern, wird das Handeln der bayerischen Behörden mit Cybersicherheitsaufgaben ganzheitlich betrachtet, um ausgehend von vorhandenen Ansätzen Angebote zur Prävention, Abwehr und Unterstützung für mehr Cybersicherheit auszubauen und dabei Synergien nutzbar zu machen.

Angebote zur Prävention, Abwehr und Unterstützung

So sollen behördenübergreifende Cybertrainings der bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben durch Planung und Durchführung von Ressort- und sektorübergreifenden Übungen von Cyberlagen etabliert werden.

Im Januar 2024 wurde deshalb ein Projekt ins Leben gerufen, welches unter Leitung des LSI die Planung und Durchführung einer ersten gemeinsamen Übung von drei bayerischen Sicherheitsbehörden zum Ziel hatte. Das Bayerische Landeskriminalamt (BLKA) mit seiner Zentralen Ansprechstelle Cybercrime (ZAC), das Landesamt für Sicherheit in der Informationstechnik (LSI) und die Zentralstelle Cybercrime Bayern (ZCB) der Generalstaatsanwaltschaft in Bamberg entwickelten im Laufe des Jahres 2024 ein Übungsszenario, welches die behördenübergreifende Kommunikation während der Vorfallsbearbeitung in den Blick nehmen sollte.

Im Visier des fiktiven Angreifers lagen dabei die Daten der Verwaltung von drei mittelgroßen Städten in Bayern, die mittels Ransomware teilweise verschlüsselt wurden. Die Informationen hierzu sollten die an der Übung beteiligten Behörden zu unterschiedlichen Zeiten über unterschiedliche Kanäle oder Meldewege erreichen.

Behördenübergreifende Kommunikation

Auf Behördenseite galt es, die verschiedenen Meldungen unter Berücksichtigung der Vertraulichkeit zu einem Lagebild zusammenzuführen, erkannte Angriffsmuster zu teilen und gegenüber den Betroffenen mit einer Stimme zu sprechen.
Die Übung wurde am 16. Oktober durchgeführt. Durch den an die Partnerbehörden verteilten LSI-Lagebericht war das BLKA schnell über Schwachstellen und Vorfälle informiert und konnte den Anruf der betroffenen Stadt zügig einordnen.
Die Generalstaatsanwaltschaft wurde wie angedacht nach einem fiktiven Zeitsprung zum nächsten Tag einbezogen, als klar war, dass ein Straftatbestand vorlag. Der unterschiedliche Aufgabenschwerpunkt der Sicherheits- und Strafverfolgungsbehörden wurde in der Abstimmungsbesprechung, die vor deren Kommunikation mit den simuliert betroffenen Behörden durchgeführt wurde, deutlich. Für die angegriffenen Städte ergab sich daraus eine durchgängige Begleitung durch die beteiligten Cybersicherheitsbehörden trotz unterschiedlicher Stadien der Angriffsausbreitung. Auch technische Plattformen für Kommunikation und Datenaustausch wurden auf geeignete Einsatzmöglichkeiten geprüft.

Verbesserungspotential erkennen

Das Ziel, anhand konkreter Szenarien einerseits etablierte Prozesse immer wieder einzuüben, andererseits aber auch Verbesserungspotential zu erkennen und Ansätze für die Optimierung von Abläufen zu entwickeln, wurde erreicht. Daneben trägt das wachsende gegenseitige Verständnis für die durch verschiedene Aufgabenschwerpunkte bedingte unterschiedliche Herangehensweise der Behörden zu einem zügigen, bedarfsgerechten Austausch untereinander bei und hilft letztlich Betroffenen bei der Bewältigung ihrer Lage. Die Bayerischen Sicherheitsstrategie 2.0 sieht eine Verstetigung von Übungen vor. In der nachfolgenden Übung sollten die erarbeiteten Maßnahmen verifiziert werden, um nachhaltige Verbesserungen zu erreichen.

Für weitere Informationen steht Ihnen das Beratungsteam des LSI gerne zur Verfügung.

Die Beratung für die Staatsverwaltung erreichen Sie über:

E-Mail: beratung-staatsverwaltung@lsi.bayern.de
Telefon: 0911 21549-521

Die Beratung für Kommunen erreichen Sie über:

E-Mail: beratung-kommunen@lsi.bayern.de
Telefon: 0911 21549-523

Die Beratung für KRITIS-Betreiber erreichen Sie über:

E-Mail: beratung-kritis@lsi.bayern.de
Telefon: 0911 21549-525

Herausgeber Landesamt für Sicherheit in der Informationstechnik
Keßlerstraße 1 | 90489 Nürnberg
pressestelle@lsi.bayern.de
www.lsi.bayern.de
Telefon: 0911 21549-0

Stand Oktober 2025
Druck Bayerisches Staatsministerium
der Finanzen und für Heimat

Wollen Sie mehr über die Arbeit der Bayerischen Staatsregierung wissen?

BAYERN | DIREKT ist Ihr direkter Draht zur Bayerischen Staatsregierung. Unter www.servicestelle.bayern.de im Internet oder unter direkt@bayern.de per E-Mail erhalten Sie Informationsmaterial und Broschüren, Auskunft zu aktuellen Themen und Internetquellen sowie Hinweise zu Behörden, zuständigen Stellen und Ansprechpartnern bei der Bayerischen Staatsregierung.

BAYERN | DIREKT
www.bayern.de Tel. 089 12 22 20