Landesamt für Sicherheit in
der Informationstechnik

LSI-PANORAMA 2024

IT-Sicherheit für den Freistaat Bayern

VORWORT

Liebe Leserinnen und Leser,

es ist mir eine große Freude, Ihnen das Panorama des Landesamts für Sicherheit in der Informationstechnik (LSI) vorzustellen. Als zentrale Behörde zum Schutz staatlicher IT-Systeme stehen wir vor vielfältigen Herausforderungen und Aufgaben, die es zu bewältigen gilt.

Die Bedrohungen im Bereich der IT-Sicherheit nehmen stetig zu und werden immer raffinierter. Cyberkriminelle nutzen fortschrittliche Technologien, um Schwachstellen in Systemen auszunutzen und vertrauliche Informationen zu stehlen oder Schaden anzurichten. Es ist daher unerlässlich, dass wir uns kontinuierlich mit den neuesten Entwicklungen im Bereich der IT-Sicherheit auseinandersetzen und unsere Maßnahmen entsprechend anpassen.

Ich bin stolz darauf, dass die Mitarbeiterinnen und Mitarbeiter des LSI ihr Bestes geben, um die IT-Infrastruktur des Freistaats Bayern zu schützen und bayerische Behörden vor Cyberangriffen zu bewahren. Ihr Engagement und Ihre Expertise sind unverzichtbar für unseren Erfolg im Bereich der IT-Sicherheit.

In diesem Panorama möchten wir Ihnen einen Überblick über die Aufgaben des LSI sowie unser Unterstützungsangebot für unsere Zielgruppen im Bereich der IT-Sicherheit geben. Zudem möchten wir Ihnen einen kleinen Ausblick auf das Kommende geben.

Ich hoffe, dass Ihnen das Panorama einen informativen Einblick in unsere Arbeit gibt und Sie ermutigt, sich aktiv für die Sicherheit im digitalen Raum einzusetzen. Wir sind fest davon überzeugt, dass wir gemeinsam eine sicherere digitale Zukunft gestalten können.

Vielen Dank für Ihr Interesse.

Präsident des Landesamtes
für Sicherheit in der Informationstechnik

INHALTSVERZEICHNIS

LSI Standort Nürnberg

1. DAS LANDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

Bayern reagierte mit der Gründung des LSI im Jahr 2017 als erstes Bundesland auf die wachsenden Gefahren und Bedrohungen im Cyberraum. Hauptstandort des LSI ist Nürnberg. Mit seiner zentralen Lage in Bayern, besten Verkehrsanbindungen, einer vielfältigen Hochschullandschaft in der unmittelbaren Umgebung, zahlreichen Firmen im IT-Sicherheitsumfeld und nicht zuletzt mit der it-sa, Europas größter Messe für IT-Sicherheit, ist Nürnberg idealer Standort für das LSI.

Neben dem Hauptstandort in Nürnberg, hat das LSI zwei Außenstellen, in Würzburg und Bad Neustadt a.d.Saale.

LSI Außenstelle Bad Neustadt a.d.Saale

LSI Außenstelle Würzburg

Aktuell beschäftigt das LSI rund 150 Mitarbeiterinnen und Mitarbeiter. Im Endausbau soll das LSI auf 200 Mitarbeiterinnen und Mitarbeiter wachsen.

Das LSI ist eine zentrale Behörde, die sich mit der IT-Sicherheit der bayerischen Behörden befasst. Als nachgeordnete Behörde des bayerischen Staatsministeriums der Finanzen und für Heimat spielt es eine

LSI Nürnberg Innenbereich

wichtige Rolle bei der Abwehr von Cyberbedrohungen und der Sicherstellung eines hohen Schutzniveaus für die digitale Infrastruktur des bayerischen Behördennetzes im Freistaat.

Die Aufgaben des LSI sind vielfältig und umfassen unter anderem die Analyse von Bedrohungslagen, konkrete Unterstützung bei IT-Sicherheitsvorfällen, die Unterstützung bei der (Weiter-) Entwicklung von Sicherheitskonzepten in staatlichen Behörden, die Beratung von bayerischen Behörden und Betreibern kritischer Infrastrukturen, sowie die Durchführung von Schulungen und Sensibilisierungsmaßnahmen im Bereich der IT-Sicherheit. Darüber hinaus arbeitet das LSI eng mit anderen Sicherheitsbehörden in Bayern, auf nationaler und internationaler Ebene zusammen, um ein ganzheitliches Sicherheitskonzept zu gewährleisten.

Zentrales Anliegen des LSI ist es, staatliche Behörden und Kommunen in Bayern vor den Gefahren im digitalen Raum zu schützen. Dazu gehört die Aufklärung über aktuelle Bedrohungsszenarien, die Sensibilisierung für sicherheitsrelevante Themen sowie die Unterstützung bei der Umsetzung von IT-Sicherheitsmaßnahmen. Durch gezielte Präventionsmaßnahmen soll das Bewusstsein für IT-Sicherheit gestärkt und das Risiko von Cyberangriffen minimiert werden.

Ein weiterer Schwerpunkt der Arbeit des LSI liegt auf der Analyse von Sicherheitsvorfällen und der Entwicklung und Umsetzung von Maßnahmen zur Abwehr von Cyberangriffen. Hierbei arbeitet das LSI eng mit anderen Behörden, Unternehmen und Forschungseinrichtungen zusammen, um schnell auf neue Bedrohungen reagieren zu können und effektive Gegenmaßnahmen zu entwickeln.

Damit leistet das LSI einen wichtigen Beitrag zur IT-Sicherheit in Bayern.

LSI Nürnberg Innenbereich

2. SIEGEL „KOMMUNALE IT-SICHERHEIT“

Kommunen als Teil der öffentlichen Verwaltung sind oftmals die ersten Ansprechpartner für Bürger und die Wirtschaft vor Ort. Die Bedeutung eines sicheren IT-Betriebs in den Kommunen wächst stetig, da sie zunehmend von digitalen Technologien abhängig sind und sensible Daten verwalten. Cyberangriffe auf kommunale Einrichtungen können schwerwiegende Folgen haben und das Vertrauen der Bürgerinnen und Bürger in die Verwaltung erschüttern. Daher ist es entscheidend, dass die Kommunen angemessene Maßnahmen ergreifen, um ihre IT-Systeme vor Angriffen zu schützen.

KOMMUNALE IT-SICHERHEIT

Stadt Musterhausen

vertreten durch

Herrn Ersten Bürgermeister
Dr. Max Mustermann

hat das
Siegel Kommunale IT-Sicherheit
des Landesamtes für Sicherheit in der Informationstechnik erworben.

Die Stadt misst der IT-Sicherheit hohen Stellenwert bei und hat ein Konzept für Informationssicherheit nach dem BayDiG erstellt.

Als Beauftragte für Informationssicherheit (ISB) ist ernannt

Frau Eva Musterfrau

Geltungsbereich: Bacon ipsum dolor sit amet doner meatball jowl short ribs, chicken prosciutto salami frankfurter. Pig drumstick turducken short ribs, brisket meatloaf

Gültig bis: 1. Januar 2025

Nürnberg, Datum

Bernd Geisler, Amtsleitung
Landesamt für Sicherheit in der Informationstechnik

Durch die Vergabe des Siegels „Kommunale IT-Sicherheit“ möchte das LSI dazu beitragen, das Bewusstsein für IT-Sicherheit in den bayerischen Kommunen zu stärken und ihnen dabei helfen, ihre Systeme gegen Cyberangriffe zu schützen.

Das Siegel „Kommunale IT-Sicherheit“ gibt gerade kleineren Kommunen eine sinnvolle Orientierung und Unterstützung bei der gesetzeskonformen Einführung eines Informationssicherheitskonzeptes zur Umsetzung der Mindestanforderungen des bayerischen Digitalgesetzes. Das Siegel wurde auf Grundlage gängiger Informationssicherheitsmanagementsysteme (ISMS) entwickelt. Der Maßnahmenkatalog des Siegels mit ca. 60 Maßnahmen und dazugehörigen Prüffragen ist als eine Art Vorstufe zu einer Zertifizierung auf Basis einer Selbstauskunft zu verstehen. Zu den Maßnahmen gehören unter anderem die Implementierung von Sicherheitsrichtlinien, regelmäßige Schulungen der Mitarbeiterinnen und Mitarbeiter im Umgang mit

IT-Sicherheit, die Durchführung von Sicherheitsaudits sowie die Einrichtung eines Notfallmanagements für den Fall eines Sicherheitsvorfalls. Gleichwohl attestiert das Siegel „Kommunale IT-Sicherheit“ einer Kommune den verantwortungsvollen Umgang mit den anvertrauten Daten seiner Bürgerinnen und Bürgern.

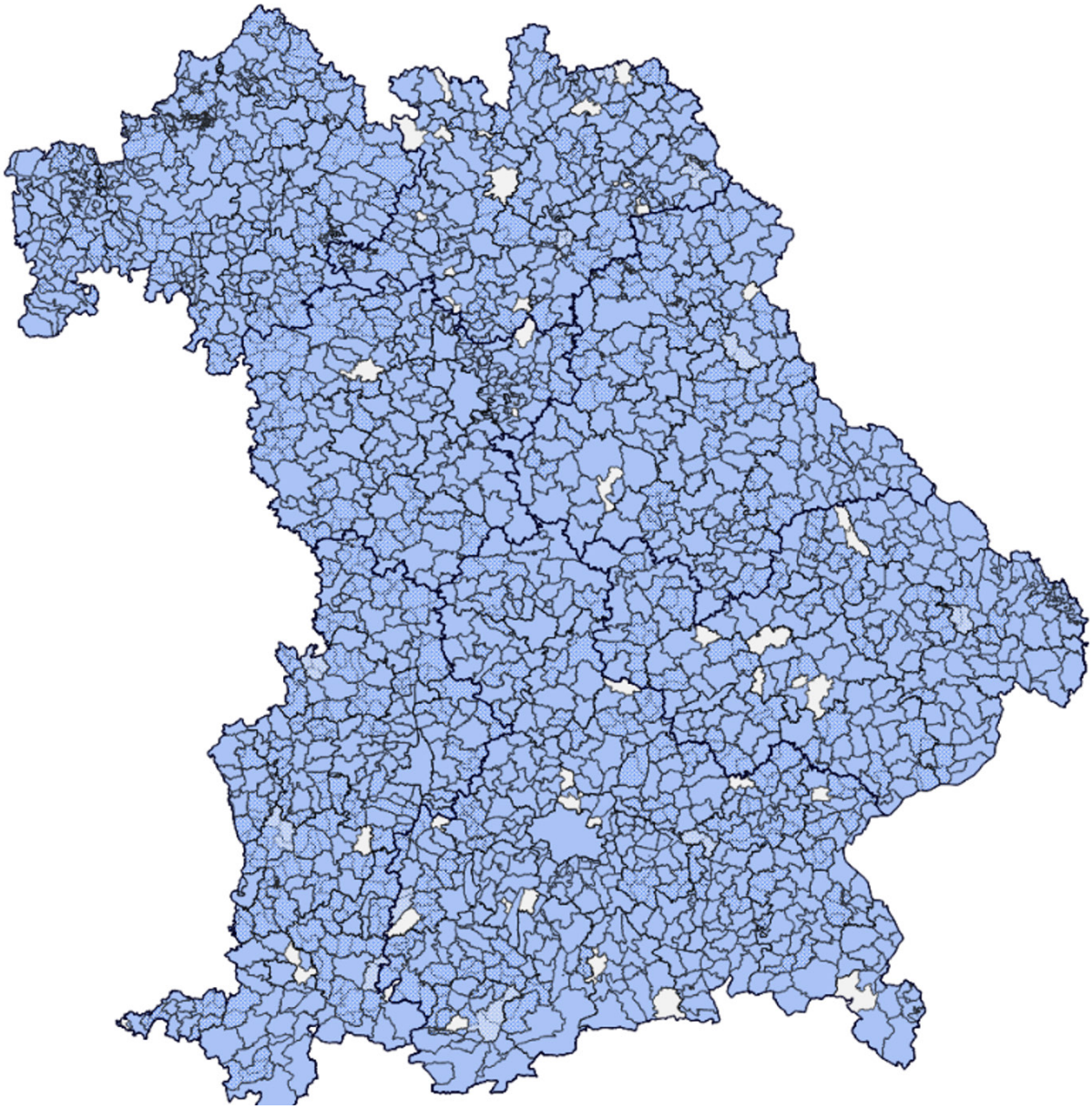
Bisher wurde das LSI-Siegel an über 530 bayerische Kommunen übergeben. Damit ist auch der Nachweis erbracht, dass gesetzeskonforme IT-Sicherheitskonzepte umgesetzt wurden. Durch das Siegel ist ein erster Schritt in Richtung einer zertifizierten IT-Landschaft geebnet.

Obgleich die Zielgruppen des Siegels vor allem kleine bayerische Städte, Märkte und Gemeinden sind, steht es auch größeren Kommunen frei, das Siegel des LSI zu erwerben. Je größer die Kommune, desto mehr wird jedoch das Informationssicherheitskonzept der Organisationsgröße, der komplexeren Netzarchitektur und den arbeitsteiligeren Prozessen Rechnung tragen müssen. Das LSI empfiehlt diesen Kommunen, eine Zertifizierung

nach einem ISMS-Standard, beispielsweise CISIS12 oder IT-Grundschutz, anzustreben. Neben dem LSI Siegel nutzen gerade größere Kommunen auch diese Standards.

Ein vom LSI erteiltes Siegel ist bis zu zwei Jahre gültig. Sollte eine Kommune bereits nach einem gängigen ISMS-Standard zertifiziert sein, kann im Falle einer vergleichbaren Betrachtung die Zertifizierung anerkannt werden, um das Siegel „Kommunale IT-Sicherheit“ des LSI zu erhalten.

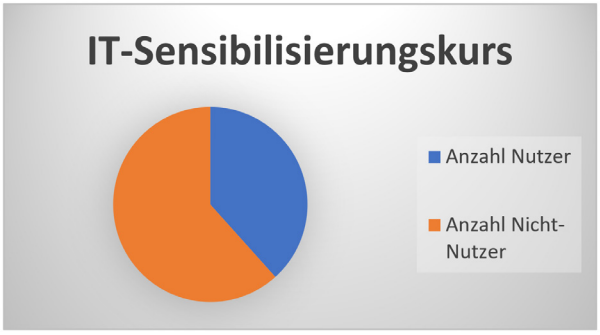
Das Siegel „Kommunale IT-Sicherheit“ ist bereits in der Version 3.0 veröffentlicht. Um der aktuellen Sicherheitslage gerecht zu werden und um die schrittweise Verbesserung der Informationssicherheit in Bayern weiter zu unterstützen, wurden mit der Veröffentlichung der **Version 3.0** einige bestehende Maßnahmen angepasst und andere neu hinzugefügt – neben der Betrachtung von IoT-Geräten / Haus-IT, Vorkehrungen bei exponierten Servern oder SSL-Analyse flossen Erkenntnisse aus dem LSI bekannten kommunalen Sicherheitsvorfällen ein. Hätten die dem LSI bekannten und in der Vergangenheit von IT-Sicherheitsvorfällen betroffenen Kommunen die im Siegel geforderten Maßnahmen umgesetzt, hätten die IT-Sicherheitsvorfälle wahrscheinlich verhindert oder zumindest die Auswirkungen eingedämmt werden können.



Reichweite des LSI: 94% aller bayerischen Kommunen nutzen mit Stand Ende 2023 die vielfältigen Angebote des LSI, wie etwa das Siegel kommunale IT-Sicherheit, Sensibilisierungskurse oder den Warn- und Informationsdienst (blau hinterlegte Kommunen)

3. IT-SENSIBILISIERUNGSKURSE

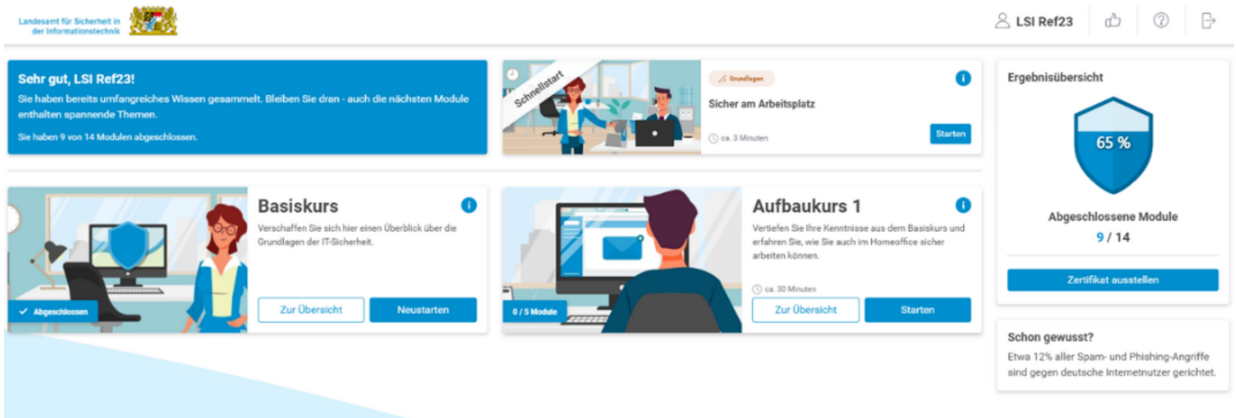
Die Sensibilisierung der eigenen Mitarbeiter ist beim Thema IT-Sicherheit von zentraler Bedeutung, da diese oft die erste Verteidigungslinie gegen Cyberangriffe und Datenverluste darstellen. Mitarbeiter können durch Unachtsamkeit, Unwissenheit oder Fahrlässigkeit Sicherheitsvorfälle in einem Unternehmen verursachen und somit IT-Systeme gefährden.



Übersicht der Nutzer des IT-Sensibilisierungskurses im Vergleich zur Gesamtanzahl der Kommunen

Ein Großteil aller Sicherheitsvorfälle wird von eingehenden E-Mails ausgelöst. Auf Grund dessen stellt die Sensibilisierung von Mitarbeitern eine zentrale Säule in einem IT-Sicherheitskonzept dar. Das LSI bietet neben den staatlichen Behörden auch den bayerischen Kommunen einen kostenlosen Zugang zu Online-Sensibilisierungskursen an. Alle kommunalen Verwaltungen (Gemeinden, Märkte, Städte, Landratsämter und Bezirke) in Bayern können hierzu einen freien Zugang erhalten. Die Kurse werden über den Digital.Campus Bayern angeboten.

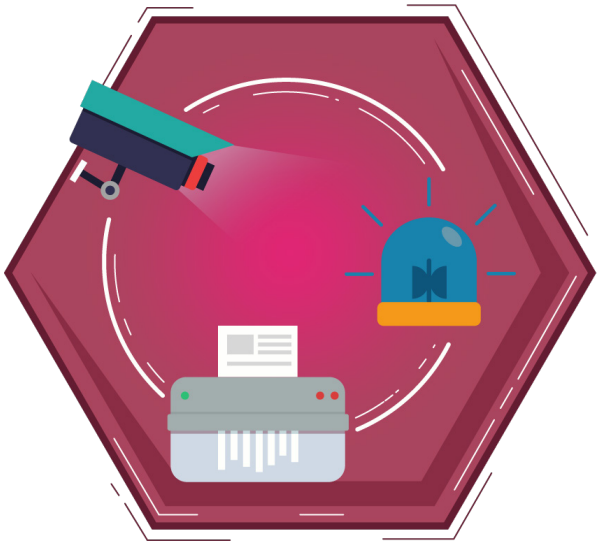
Durch Schulungen und Sensibilisierungsmaßnahmen können Mitarbeiter für potenzielle Bedrohungen sensibilisiert werden und lernen, wie sie sich vor Cyberangriffen schützen können. Sie werden über gängige Betrugsmaschen informiert, lernen den Umgang mit Passwörtern und sensiblen Daten sowie das Erkennen von Phishing-E-Mails.



Darüber hinaus trägt eine gut informierte Belegschaft dazu bei, dass Sicherheitsrichtlinien und Sicherheitsmaßnahmen in den Behörden besser eingehalten werden. Mitarbeiter werden zu aktiven Beteiligten am Schutz der eigenen Daten und tragen somit zur Stärkung der gesamten IT-Sicherheit bei.

Mit den didaktisch hochwertigen Kursen kann das Personal regelmäßig hinsichtlich IT-Awareness geschult werden. Es werden ein Basiskurs und Aufbaukurse zu spezifischen Themen der IT-Sicherheit angeboten. Bisher nutzen rund 800 der 2.056 Kommunen in Bayern die kostenfreien Sensibilisierungskurse des LSI.

4. IT-NOTFALLMANAGEMENT



Mit der Handreichung des LSI zum IT-Notfallmanagement erhalten die bayerischen Gemeinden, Märkte und kleine Städte ein speziell auf ihre Bedürfnisse ausgerichtete Unterstützungsleistung, unabhängig von einem konkreten Informationssicherheitskonzept. Ein IT-Notfallmanagement ist ein wichtiger Baustein für ein Informationssicherheitskonzept, ersetzt aber in dieser Hinsicht keine Zertifizierung.

Die LSI Handreichung orientiert sich am Standard BSI 100-4 und ist eine begleitende Hilfestellung beim Auf- und Ausbau eines IT-Notfallmanagements. Sie stellt für die Bereiche IT-Notfallvorsorge und IT-Notfallbewältigung Grundlagen, verschiedene Vorlagen und Musterdokumente zur Verfügung, um das IT-Notfallmanagement an die individuellen Bedürfnisse von Kommunen anpassen zu können. Kommunen, die bereits ein IT-Notfallmanagement aufgebaut haben, kann die LSI-Handreichung als zusätzliche Anregung und Checkliste dienen.

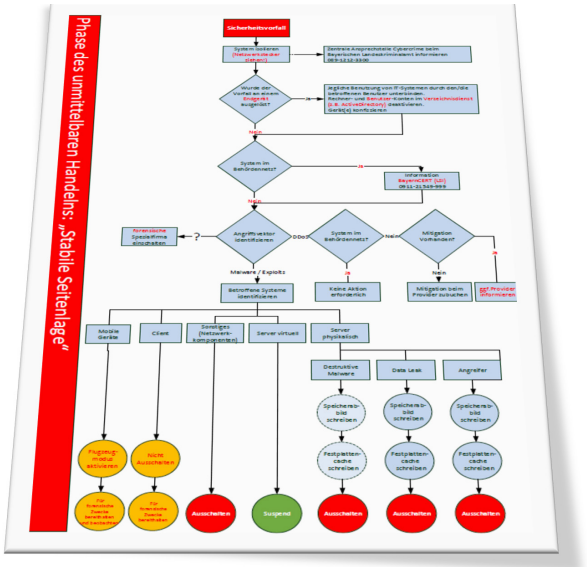
Damit besteht die Möglichkeit:

- erste Maßnahmen schnell umzusetzen,
- Grundlagen für ein IT-Notfallmanagement aufzu bauen,
- die wesentlichen Potentiale zu beleuchten und auszubauen,
- ein IT-Notfallmanagement einzuführen und
- Feedback zu ihrem Notfallkonzept und strukturierte Beratung zu Einzelpositionen einzuholen.

Das zentrale Dokument des LSI Handreichung zum IT-Notfallmanagement, ist eine ToDo-Liste in Form eines Excel-Fragebogens, der „Rote Faden“. Er gliedert sich in die Bereiche Konzeptionierung der Grundlagen, der IT-Notfallvorsorge und der IT-Notfallbewältigung. Er stellt die wesentlichen Fragen zu den einzelnen Maßnahmen, führt als Wegweiser durch die Vorlagen und dokumentiert den zeitlichen Fortschritt.

Das in der LSI-Handreichung beschriebene IT-Notfallmanagement-Konzept orientiert sich an der ISIS12-Struktur und beinhaltet somit eine IT-Notfallmanagementleitlinie, ein IT-Notfallvorsorgekonzept und ein IT-Notfallhandbuch.

Die LSI Handreichung zum IT-Notfallmanagement wurde bisher von über 470 Kommunen angefragt.



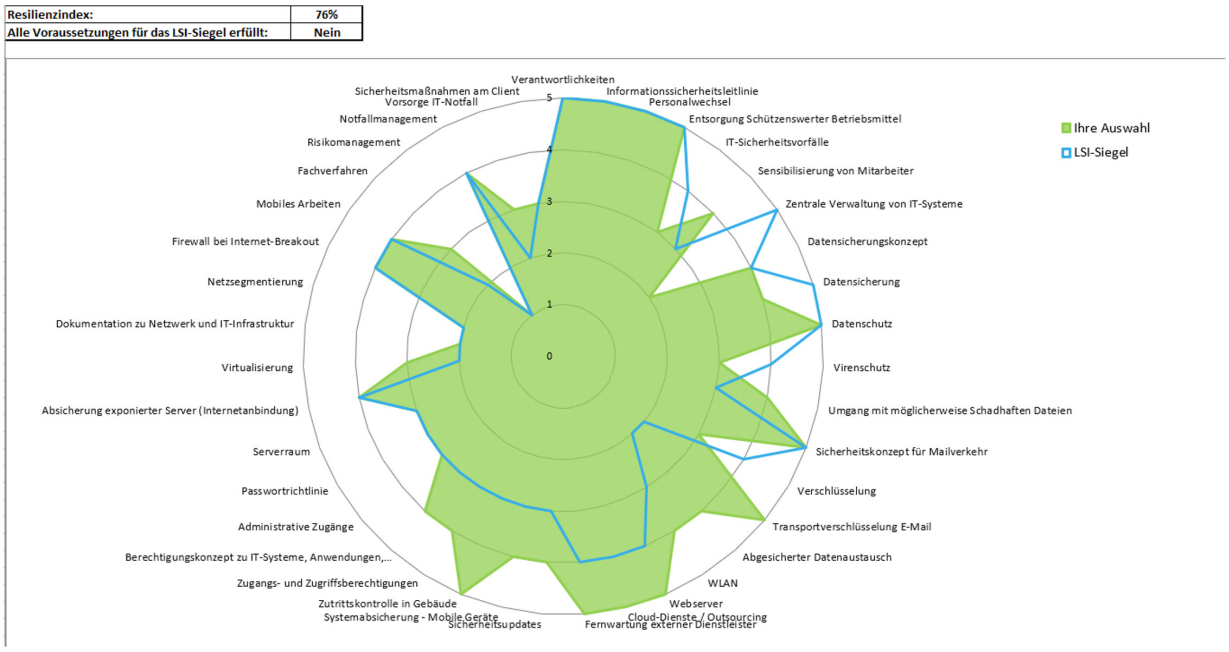
Auszug aus dem LSI IT-Notfallmanagement

5. IT-RESILIENZ

Der Begriff IT-Resilienz beschreibt die Widerstands- und Anpassungsfähigkeit der gesamten IT-Infrastruktur bei Cyberangriffen. Ziel ist es, durch maximale Widerstands- und Anpassungsfähigkeit die IT-Infrastruktur zu schützen und damit ein hohes Sicherheitsniveau zu schaffen. Das LSI Konzept zur IT-Resilienz soll hier ein visuelles Unterstützungswerkzeug sein.

Das LSI hat als ersten Einstieg in die Kommunale IT-Sicherheit die Handreichung IT-Resilienz entwickelt und veröffentlicht.

Mithilfe der Handreichung können ein aktueller Stand der Informationssicherheit der eigenen Organisation ermittelt sowie notwendige Verbesserungen erkannt werden. Hierbei wirken die Entwicklungsschichten als Stufensystem, welche aufeinander aufbauen und bei der Verbesserung in den jeweiligen Bereichen helfen sollen. So wird in kleinen Stufen einfach an das LSI Siegel „Kommunale IT-Sicherheit“ herangeführt. Durch die Auswahl der Entwicklungsstufe wird ein Netzdiagramm und ein IT-Resilienz-Index erstellt, welcher den allgemeinen Stand der Informationssicherheit der Kommune abbildet. Ziel ist es, einen möglichst hohen IT-Resilienz-Index zu erreichen. Die visuelle Darstellung soll den Informationssicherheitsbeauftragten (ISB) auch bei der Berichterstattung zur Informationssicherheit gegenüber den Verantwortlichen (z.B. Bürgermeister) unterstützen.



Beispiel zur Visualisierung des Verbesserungspotentials der IT-Sicherheit aus der LSI IT-Resilienz


ID
50746
50746

6. WARN- UND INFORMATIONSDIENST (WID)

In jedem Softwareprodukt werden mit der Zeit Schwachstellen entdeckt, die ein unmittelbares Risiko für die davon betroffenen IT-Systeme darstellen. Ebenso werden Schadcodekampagnen von Angreifern immer größer und raffinierter angelegt.

Der Warn- und Informationsdienst (WID) des LSI alarmiert tagesaktuell die Staatsverwaltung, Kommunen und öffentliche Unternehmen im KRITIS Bereich über Schwachstellen und neue Gefährdungslagen, um Bedrohungen für die IT-Sicherheit schnellstmöglich abzumildern.

Die IT-Sicherheitsexperten des Bayern-CERT im LSI veröffentlichen täglich Warnmeldungen. Grundlage ist die Sichtung von Informationen aus zahlreichen öffentlich verfügbaren Quellen (OSINT), die anschließende Analyse und Bewertung. Die Experten schlagen Maßnahmen zur Behebung von Sicherheitslücken vor oder sprechen reaktive Handlungsempfehlungen zur Schadensbegrenzung aus. Mithilfe der Warnmeldungen können Risiken für IT-Systeme deutlich reduziert werden.

Der Zugang zu den Warnmeldungen kann über ein Web-Portal mit der Möglichkeit zur Recherche erfolgen. Die Warnmeldungen können aber auch als E-Mail abonniert werden, womit man aus über 1.400 verschiedenen Softwareprodukten einen eigenen individuellen E-Mail-News-Feed erhält.

Bitte melden Sie sich an

Warn- und Informationsdienst

Landesamt für Sicherheit in der Informationstechnik

Startseite | Warnmeldungen

Security Advisories

6136 Datensätze

1 2 3 4 ... 123 50 pro Seite

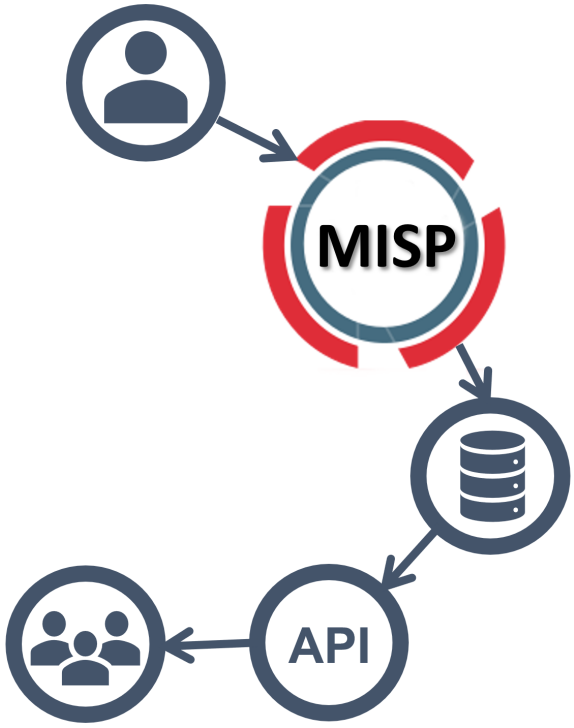
Stand	Risiko	ID	Titel	Status
TT.MM.JJJJ - TT.MM.JJJJ				
20.02.2024, 15:05		LSI-SEC-2024-0398	Paessler PRTG: Mehrere Schwachstellen	UPDATE
20.02.2024, 14:16		LSI-SEC-2024-0429	IBM App Connect Enterprise: Schwachstelle ermöglicht Codeausführung	NEU
20.02.2024, 14:16		LSI-SEC-2024-0428	Liferay Portal und DXP: Mehrere Schwachstellen	NEU
20.02.2024, 14:15		LSI-SEC-2024-0427	Linux Kernel: Schwachstelle ermöglicht Codeausführung	NEU
20.02.2024, 14:15		LSI-SEC-2024-0182	Linux Kernel: Mehrere Schwachstellen	UPDATE
20.02.2024, 14:15		LSI-SEC-2023-2635	Linux Kernel: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff	UPDATE
20.02.2024, 14:15		LSI-SEC-2023-1497	Linux Kernel: Schwachstelle ermöglicht nicht spezifizierten Angriff	UPDATE
20.02.2024, 11:59		LSI-SEC-2024-0425	Rancher: Schwachstelle ermöglicht Privilegieneskalation	NEU
20.02.2024, 11:17		LSI-SEC-2022-1839	Apache Commons Text: Schwachstelle ermöglicht Codeausführung	UPDATE
20.02.2024, 11:10		LSI-SEC-2024-0426	Python: Mehrere Schwachstellen ermöglichen Denial of Service	UPDATE

7. MALWARE INFORMATION SHARING PLATFORM (MISP) FÜR KOMMUNEN

In einer zunehmend digitalisierten Welt sind Kommunen und öffentliche Einrichtungen vermehrt Ziel von Cyberangriffen und Malware-Infektionen. Der Faktor Zeit ist hierbei entscheidend. Sicherheitslücken werden von Cyberkriminellen genauso schnell ausgenutzt wie diese bekannt werden. Ziel muss es daher sein, sich möglichst schnell vor neuesten Bedrohungen zu schützen. Hierfür bietet das LSI ein innovatives Angebot: die Einrichtung einer Malware Information Sharing Platform (MISP).

Das MISP des LSI ermöglicht es, Informationen über aktuelle Malware-Bedrohungen – sogenannte Kompromittierungsindikatoren -. auszutauschen und diese in eigene Sicherheitssysteme automatisch zu übernehmen, bewährte Praktiken zur Abwehr von Cyberangriffen zu teilen und sich mit anderen Akteuren im Bereich der Cybersicherheit zu vernetzen. Durch den gemeinsamen Austausch von Wissen und Ressourcen kann frühzeitig vor neuen Bedrohungen gewarnt werden, damit entsprechende Gegenmaßnahmen ergriffen werden. Dies ermöglicht es, IT-Systeme schneller und besser zu schützen, sowie potenzielle Sicherheitslücken zu schließen, bevor sie von Angreifern ausgenutzt werden können.

Das MISP-Angebot richtet sich an alle Kommunen in Bayern, unabhängig von ihrer Größe oder ihrem technologischen Know -how, sowie alle Behörden der bayerischen Staatsverwaltung.



Visualisierung Austausch von Informationen über MISP

Die Plattform wird vom LSI bereitgestellt und betreut, sodass von den Behörden und Kommunen keine zusätzlichen Kosten oder Ressourcen für den Betrieb aufgebracht werden müssen. Darüber hinaus bietet das LSI Schulungen und Unterstützung bei der Implementierung und Nutzung der Plattform an, um sicherzustellen, dass die Nutzer das volle Potenzial dieser wichtigen Ressource ausschöpfen können.

Durch die Teilnahme am MISP des LSI können nicht nur die eigenen IT-Systeme der Nutzer schneller und besser geschützt werden, jeder Nutzer trägt auch aktiv zur Stärkung der Cybersicherheit in ganz Bayern bei. Indem Nutzer ihr Wissen und ihre Erfahrungen mit anderen teilen, tragen sie dazu bei, dass die Daten aller Bürgerinnen und Bürger in Bayern in den Kommunen sicher sind.

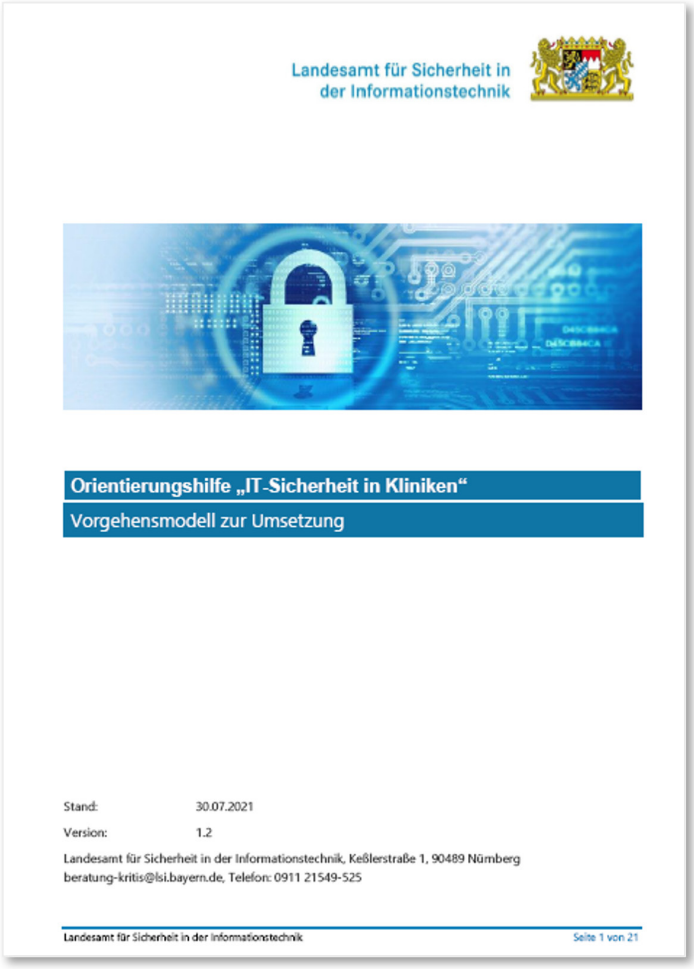
8. KRITIS – KLINIKEN

Die Digitalisierung im Gesundheitswesen hat in den letzten Jahren stark zugenommen und bietet viele Vorteile, wie die effiziente Verwaltung von Patientendaten, die Verbesserung der medizinischen Versorgung und die Möglichkeit der Fernüberwachung von Patienten.

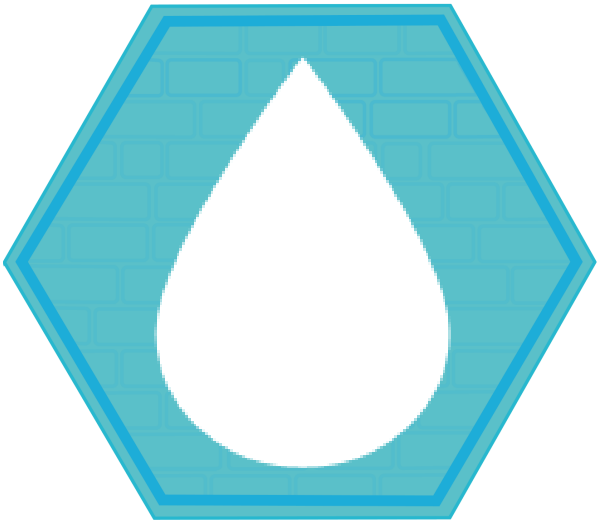
Allerdings bringt die zunehmende Vernetzung und Nutzung von IT-Systemen auch neue Herausforderungen mit sich, insbesondere in Bezug auf die Sicherheit sensibler Gesundheitsdaten von Patienten.

Um Kliniken und medizinische Einrichtungen dabei zu unterstützen, ihre IT-Sicherheit zu stärken und sich vor Cyberangriffen zu schützen, bietet das LSI umfassende Unterstützung an.

Das LSI hat hierfür die „Orientierungshilfe IT-Sicherheit für Kliniken“ entwickelt, um Kliniken bei der Verbesserung ihrer IT-Sicherheit zu unterstützen und sie auf mögliche Bedrohungen vorzubereiten. Die Orientierungshilfe besteht aus einer Liste von Orientierungsfragen mit zugeordneten Maßnahmenempfehlungen, sowie dem dazugehörigen Vorgehensmodell. Das vom LSI bewusst übersichtlich gestaltete Dokument dient als Leitfaden für eine schnell umsetzbare „Best Practice“ Vorgehensweise zur Identifikation von Bedrohungen, entsprechenden Maßnahmen zu deren Vermeidung und klaren organisatorischen Regelungen.



9. KRITIS – WASSER



Wasser ist für jeden so selbstverständlich wie die Luft zum Atmen. Wir sind gewohnt, dass es zu jeder Tages- und Nachtzeit in ausreichender Menge und hoher Qualität zur Verfügung steht. In Bayern gehört die sichere und zuverlässige Trinkwasserversorgung zur kommunalen Daseinsvorsorge für die Menschen vor Ort. Die Trinkwasserversorgung in Bayern wird von über 2.200 meist kleineren kommunalen Trinkwasserversorgern der Städte und Gemeinden, von Zweckverbänden und Fernwasserversorgern gewährleistet.

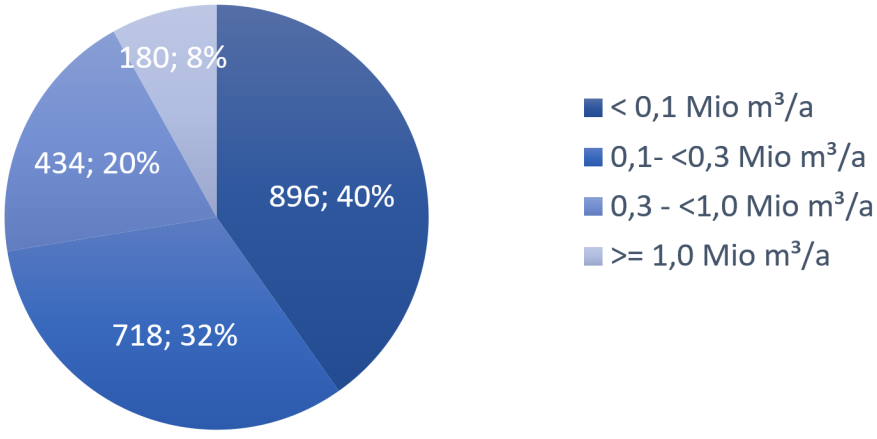
Ein ähnliches Bild zeigt sich bei der Abwasserbeseitigung: Auch diese Aufgabe wird in Bayern von rund 2.300 überwiegend kleineren Abwasserentsorgern der Kommunen oder von Abwasserzweckverbänden gewährleistet. In den Kläranlagen wird in mehreren Schritten das Abwasser gereinigt - bevor es in einem sauberen Zustand dem natürlichen Wasserkreislauf durch Einspeisung in Flüsse wieder zugeführt wird.

Wie in allen Lebensbereichen wächst auch bei Trinkwassergewinnung, -aufbereitung, -verteilung und Abwasserentsorgung der Grad der Technisierung und damit die Anzahl der digital steuerbaren und unter-

Versorgte Einwohner	Anzahl in Bayern, 2016
> 500.000	2
< 500.000	1
< 200.000	4
< 100.000	16
< 50.000	212
< 10.000	1348
< 1.000	417
< 100	198
Keine	34

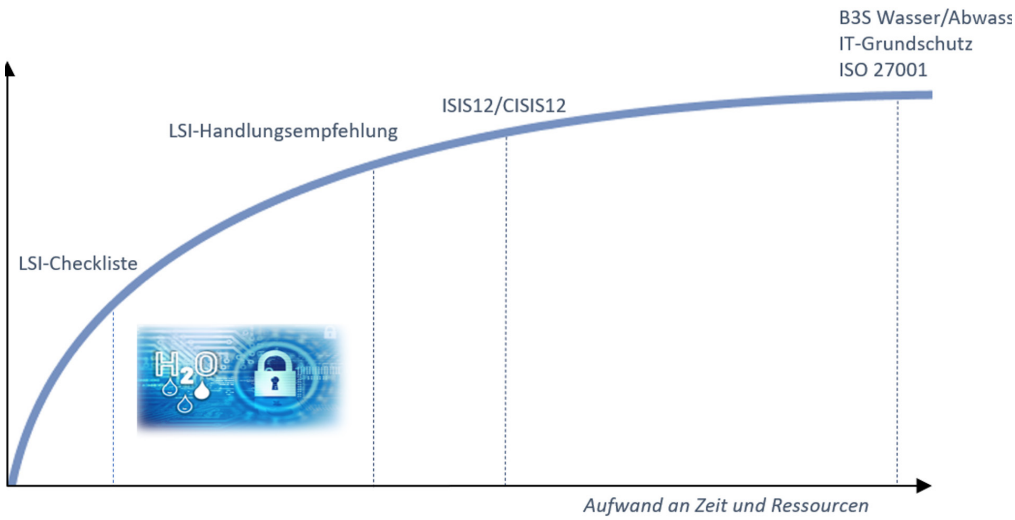
KRITIS nach BSI-KritisV
meldepflichtig beim BSI

Sub-KRITIS
Betreiber einer kritischen Infrastruktur (unter dem Schwellenwert)
-> Zielgruppe des LSI gemäß Art. 42 (2) BayDiG



einander vernetzten Systeme stetig. Die IT-Sicherheit ist zentraler Bestandteil beim Schutz der Infrastruktur vor Ausfällen und Cyberangriffen. Der Stellenwert der IT-Sicherheit steigt mit zunehmender Digitalisierung und jeder neuen Bedrohung. Der Technisierungsgrad, der Aufbau und die Steuerung der technischen Anlagen, die Vernetzungsstrukturen und die Organisationsstrukturen können sich von Wasserversorger zu Wasserversorger stark unterscheiden. Deshalb braucht es individuell angepasste Sicherheitskonzepte.

Das LSI hat in enger Kooperation mit mehreren Trinkwasserversorgern und Abwasserentsorgern als Erprobungspartner ein Unterstützungsangebot entwickelt, welches sich insbesondere an kleinere Organisationen in der Trinkwasserversorgung und Abwasserentsorgung richtet. Ziel ist es, die Einführung eines individuell angepassten IT-Sicherheitskonzepts zu unterstützen und den Weg zu einer abgesicherten (möglicherweise zertifizierten) IT-Landschaft zu ebnen.



Aufwand-Nutzen-Schätzung zur Einordnung der LSI Unterlagen für KRITIS-Betreiber

Teil dieses Unterstützungsangebotes sind folgende Materialen:

- Checkliste zur Mindestabsicherung
- Handlungsempfehlung mit zugehörigem Vorgehensmodell

Die Checkliste zur Mindestabsicherung erleichtert den Einstieg und zielt auf das Erreichen einer grundlegenden Absicherung ab. Sie dient vor allem kleineren Wasserversorgern und Abwasserentsorgern dazu, den aktuellen Stand ihrer Absicherung zu überprüfen und eventuelles Verbesserungspotential zu erkennen. Gleichzeitig schlägt sie entsprechende Maßnahmen vor. Ist ein Aufgabengebiet nach extern ausgelagert, hilft sie, die wichtigsten Anforderungen im Blick zu behalten. Es ist dann empfehlenswert, die Checkliste gemeinsam mit dem Dienstleister zu bearbeiten und die Resultate mit dem verantwortlichen Personal und der technischen Führungskraft sowie der Geschäftsleitung durchzusprechen. Die Checkliste zur Mindestabsicherung ist auf ein optimales Verhältnis zwischen Aufwand und Nutzen ausgelegt.

Die Handlungsempfehlung ist der nächste Schritt auf dem Weg in eine abgesicherte IT-Landschaft. Die Zielgruppe sind mittelgroße Wasserversorger und Abwasserentsorger. Die Handlungsempfehlung befasst sich deutlich tiefer mit der Thematik und ist dementsprechend komplexer und umfangreicher. Sie ermöglicht analog der Checkliste zur Mindestabsicherung, den aktuellen Stand der Absicherung zu prüfen, eventuelles Verbesserungspotential zu erkennen und schlägt entsprechende Maßnahmen vor.

Das Vorgehensmodell ist als Begleitdokument zur Handlungsempfehlung konzipiert und empfiehlt eine zeitliche Reihenfolge für die Umsetzung der Maßnahmen.

Das Unterstützungsangebot für Trinkwasserversorgung wurde um die Abwasserentsorgung erweitert..

Beratungsangebot für Wasserversorger und Abwasserentsorger

10. KRITIS – SIEDLUNGSABFALLENTSORGUNG

Auch vor der Siedlungsabfallentsorgung, einer auf den ersten Blick weniger technologieintensiv erscheinenden Branche, macht die Digitalisierung nicht Halt.

Die Siedlungsabfallentsorgung ist ein wichtiger Bestandteil der öffentlichen Infrastruktur und spielt eine entscheidende Rolle für die Gesundheit und Umwelt in ihrer Umgebung. Von der Sammlung und Sortierung von Abfällen bis hin zu Entsorgung und Recycling –viele Prozesse in diesem Bereich sind mittlerweile digitalisiert und vernetzt. Dies bringt zwar viele Vorteile mit sich, birgt aber auch Risiken, insbesondere im Hinblick auf die Sicherheit sensibler Daten und kritischer Infrastrukturen.

Ein erfolgreicher Cyberangriff auf ein Unternehmen in der Siedlungsabfallentsorgung könnte verheerende Folgen haben. Persönliche Informationen von Kunden, Zahlungsdaten, Betriebsgeheimnisse - all diese sensiblen Daten könnten gestohlen oder manipuliert werden. Dies würde nicht nur zu finanziellen Verlusten führen, sondern auch das Vertrauen der Kunden erschüttern und den Ruf der jeweiligen Organisation nachhaltig schädigen.

Darüber hinaus könnten Angriffe auf die IT-Infrastruktur in der Siedlungsabfallentsorgung auch direkte Auswirkungen auf die öffentliche Gesundheit und Umwelt haben. Wenn beispielsweise Abfallentsorgungsanlagen lahmgelegt oder sensible Umweltdaten manipuliert werden, könnte dies schwerwiegende Konsequenzen nach sich ziehen. Aus nicht abgeholtem Müll können gesundheitliche Gefährdungen wie beispielsweise die Ausbreitung von Krankheiten resultieren. Es ist daher unerlässlich, dass Unternehmen in der Siedlungsabfallentsorgung angemessene Maßnahmen zur IT-Sicherheit ergreifen.

Der Bereich der Siedlungsabfallentsorgung wurde Anfang 2021 im IT-Sicherheitsgesetz 2.0 als neuer KRITIS-Sektor definiert. Aus diesem Anlass hat das LSI für die kommunalen Abfallwirtschaftsbetriebe und die Betreiber von Abfallverwertungsanlagen in Bayern ein Unterstützungsangebot erarbeitet.

Das vom LSI entwickelte Unterstützungsangebot für mehr IT-Sicherheit im Bereich der Siedlungsabfallentsorgung richtet sich insbesondere an kleine und mittlere Organisationen. Ziel ist es, diese bei der Einführung eines individuell angepassten IT-Sicherheitskonzepts zu unterstützen und ihnen den Weg zu einer abgesicherten IT-Landschaft zu ebnen. Durch die Umsetzung zielgerichteter und pragmatischer Maßnahmen kann bereits mit überschaubarem Aufwand eine hohe Widerstandskraft gegenüber Angriffen auf IT-Infrastruktur erreicht werden.

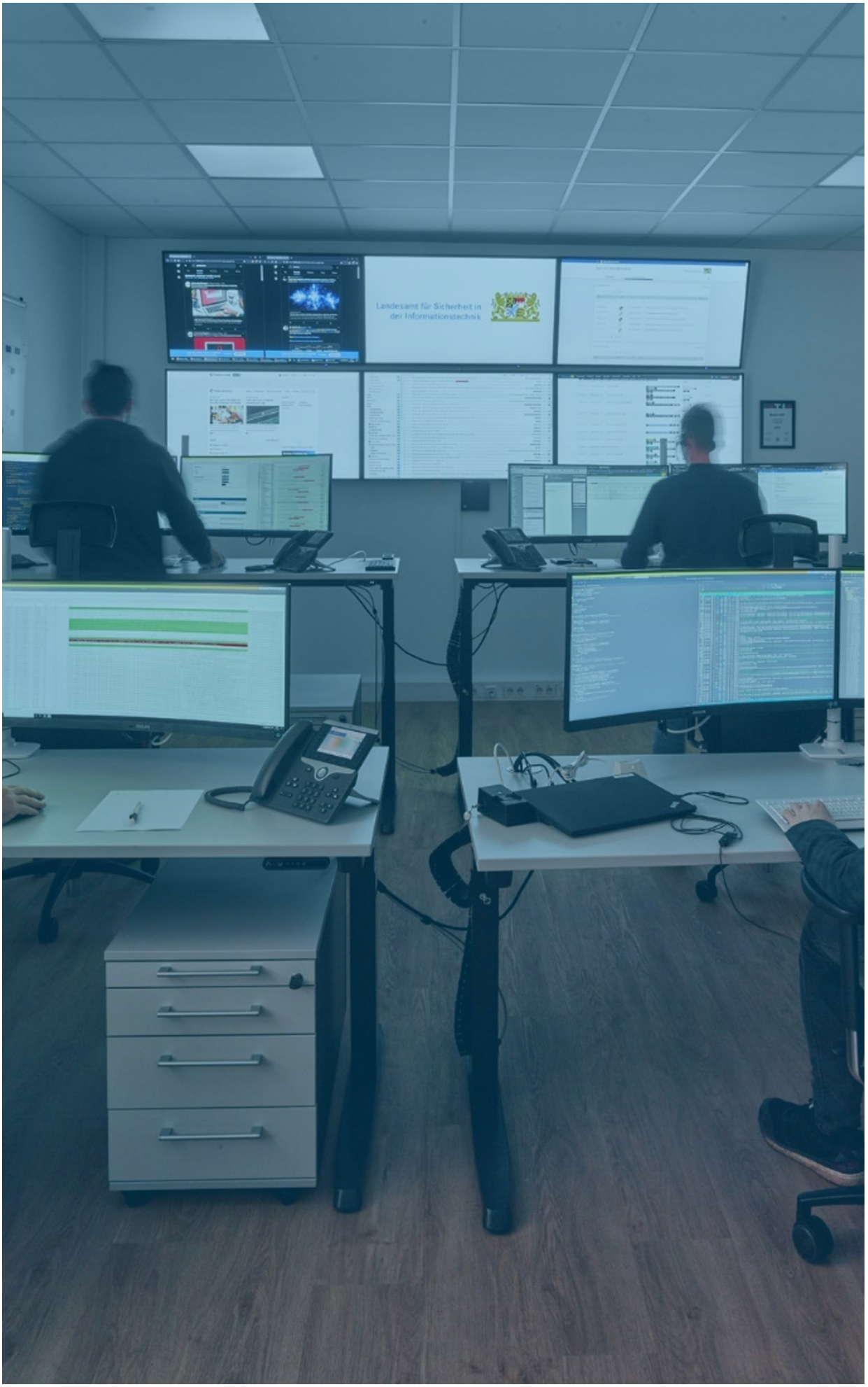
11. BERATUNGSKONZEPT FÜR BAYERISCHE UNTERNEHMEN MIT STAATLICHER BETEILIGUNG

Im Rahmen des Ausbaus der Beratungs- und Unterstützungsleistungen für Unternehmen mit staatlicher Beteiligung wurde eine Handlungsempfehlung (Checkliste mit Maßnahmenempfehlungen) durch das LSI entwickelt.

Die Unterlagen zeigen kleinen und mittelgroßen Unternehmen empfohlene technische und organisatorische Maßnahmen auf. Durch deren korrekte Umsetzung wird eine grundlegende Absicherung der bestehenden IT-Landschaft erzielt.

Durch die pragmatische Auswahl der Maßnahmenempfehlungen mit dem Fokus „Ein Mehr an Informationssicherheitsgewinn“ wird die Größe des Werks überschaubar gehalten. Gleichzeitig unterstützen ausführliche und einfach gehaltene Beschreibungen eine zielgerichtete Umsetzung. Zudem eignen sich die Unterlagen hervorragend dazu, den eigenen Stand der Absicherung zu überprüfen.

Die grafische Auswertung bietet einen kompakten Überblick über den aktuellen Stand der empfohlenen (Mindest-) Absicherungsmaßnahmen.


Landesamt für Sicherheit in
der Informationstechnik

12. LAGEZENTRUM

Herzstück des LSI ist das Lagezentrum. Es hat die Aufgaben Vorfälle zu erkennen, zu erfassen und zu bewerten, über aktuelle Sicherheitsbedrohungen zu informieren, zu warnen, zu alarmieren und bei IT-Sicherheitsvorfällen zu reagieren. Es verfügt dabei jederzeit über ein verlässliches Bild der aktuellen IT-Sicherheitslage und kann somit den Handlungsbedarf und die Handlungsoptionen bei IT-Sicherheitsvorfällen schnell und kompetent einschätzen. Der Leiter des Lagezentrums, Christoph Hofmann, beantwortet im Interview Fragen zum Lagezentrum.

Redaktion: Was macht das Lagezentrum des LSI?

Christoph Hofmann: Wir sammeln, bündeln und bewerten täglich eine Vielzahl von unterschiedlichen Informationen, um damit ein tagesaktuelles IT-Sicherheitslagebild zu ermitteln. Die ausgewerteten Informationen stammen aus verschiedenen Quellen wie beispielsweise Open Source Intelligence (OSINT), von Partnern oder von eigenen Analysen und Sensoren. Dieses Lagebild beinhaltet beispielsweise alle IT-Sicherheitsvorfälle und -verdachtsfälle in unserem Zuständigkeitsbereich. Darüber hinaus beinhaltet es auch Informationen zu aktuellen Bedrohungen verschiedener Cybergruppierungen und Informationen zu Schwachstellen in Softwareprodukten. Das Lagebild wird allen Informationssicherheitsbeauftragten der bayerischen Staatsverwaltung und allen beteiligten Behörden der Cyberabwehr Bayern (CAB) in Form eines Lageberichts täglich zur Verfügung gestellt. Von zentraler Bedeutung ist die sicherheitstechnische Bewertung. Abhängig davon werden zielgerichtete Maßnahmen eingeleitet wie beispielsweise die Erstellung einer Warnmeldung oder direkt die Vorfallsbearbeitung gestartet. Für die Vorfallsbearbeitung ist eine Zusammenarbeit mit der betroffenen Behörde unerlässlich. Die Vorfallsbearbeitung hat ein sehr weites Spektrum. Dies kann beispielsweise die Analyse eines Clients sein, bei dem ein Anfangsverdacht einer Kompromittierung mit Schadcode besteht, andererseits aber auch die komplette forensische Analyse eines verschlüsselten Netzwerks.

Redaktion: Welche Bedrohungen sind derzeit als kritisch anzusehen?

Christoph Hofmann: Die Bedrohung durch Schwachstellen in Softwareprodukten ist weiterhin auf einem hohen Niveau. Kritische Schwachstellen in Produkten wie Firewalls oder VPN-Komponenten sind hier besonders hervorzuheben, da Angreifer diese Schwachstellen aktiv ausnutzen und so Zugriff ins interne Netzwerk erhalten könnten. Außerdem besteht weiterhin eine hohe Bedrohung durch Ransomware-Gruppierungen, welche unter anderem diese Schwachstellen ausnutzen, in Netzwerke eindringen, Daten extrahieren und die lokalen Daten verschlüsseln. Um die Daten zu entschlüsseln, wird ein Lösegeld gefordert und bei fehlender Bereitschaft zur Zahlung wird gedroht, die gestohlenen Daten im Darknet zu veröffentlichen.

Redaktion: Wie reagiert unser Lagezentrum auf solche Bedrohungen?

Christoph Hofmann: Wir sind auf diese Bedrohungen mit unserer stetig wachsenden Fachexpertise vorbereitet. Ansonsten reagieren wir besonnen, zielgerichtet und konsequent.

Redaktion: Welche Rolle spielt die Zusammenarbeit mit anderen Bundesländern und dem BSI bei der Bekämpfung dieser Bedrohungen?

Christoph Hofmann: Im Tagesgeschäft arbeiten wir in verschiedenen Gremien wie beispielsweise dem Verwaltungs-CERT-Verbund (VCV) oder dem deutschen CERT-Verbund (CV) mit anderen Länder-CERTS, CERTs von Unternehmen, CERT-Bund oder anderen Stellen mit dem BSI zusammen. Diese operative Zusammenarbeit ist ein zentrales Element unserer Arbeit im Lagezentrum. So können wir uns sehr schnell und effizient auf Arbeitsebene mit verschiedenen CERTs austauschen und abstimmen. Über diesen Weg werden beispielsweise Informationen zu aktuellen Angriffen oder Bedrohungen ausgetauscht.

Redaktion: Zum Abschluss, was raten Sie staatlichen Behörden und Kommunen, um sich vor Cyberangriffen effektiv zu schützen?

Christoph Hofmann: Staatliche Behörden sollten grundsätzlich das Angebot unseres IT-Dienstleistungszentrums nutzen. Für all diese Dienstleistungen sind die dazugehörigen Systeme gemäß unseren Vorgaben gehärtet und außerdem ist ein aktives Monitoring durch unsere Sensorik gewährleistet. Kommunen sollten vor allem unser vielschichtiges Beratungsangebot nutzen und uns bei Verdachtsfällen umgehend kontaktieren.

13. AUDITS

In einer Zeit, in der Cyberangriffe und Datenlecks immer häufiger vorkommen, ist es für Organisationen unerlässlich, ihre IT-Systeme und -Prozesse regelmäßig auf Sicherheitslücken zu überprüfen. Zur Hilfestellung bietet das LSI ein Audit zur Einführung eines Informationssicherheits-Managementsystems (ISMS) an.
Audits sind systematische Überprüfungen von IT-Systemen, -Prozessen und -Infrastrukturen, um potenzielle Schwachstellen aufzudecken und Sicherheitsrisiken zu identifizieren. Das LSI führt diese Audits im Auftrag von Behörden durch und unterstützt sie dabei, ihre IT-Sicherheit zu steigern und sich besser gegen Cyberbedrohungen zu schützen.
Durch die Teilnahme an einem Audit des LSI können Organisationen nicht nur potenzielle Schwachstellen in ihren IT-Systemen identifizieren, sondern auch Maßnahmen zur Verbesserung ihrer IT-Sicherheit ergreifen. Zudem sind Audits eine Erfolgskontrolle für die Wirksamkeit eines Informationssicherheitsmanagementsystems (ISMS). In Folge von regelmäßigen Überprüfungen erhöht sich zusätzlich das Verantwortungsbewusstsein, das Engagement und die Motivation der Mitarbeiter.
Das Audit-Konzept des LSI bietet drei Level: Bronze, Silber und Gold. In über zehn Ressorts wurde sich für ein LSI-Audit entschieden und das Level Bronze erreicht. Künftig sollen weitere Audits für die Level Bronze und Silber folgen.

Gesprächsrunde

14. IT-SICHERHEITSBERATUNG FÜR DIE STAATSVERWALTUNG

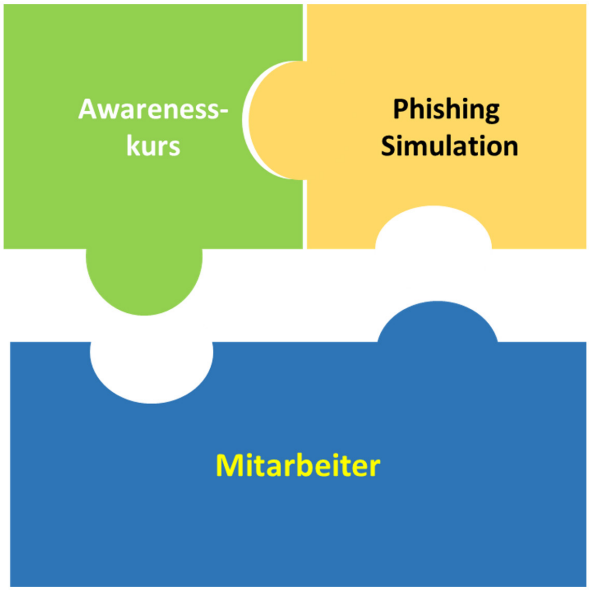
Das LSI führt pro Jahr über 250 zum Teil sehr umfangreiche Einzelberatungen in der Staatsverwaltung durch. Zu der quantitativen Steigerung von zuletzt 25% gegenüber dem Vorjahr kommt eine zunehmende Tiefe der von den Behörden der bayerischen Staatsverwaltung beim Referat „IT-Sicherheitsberatung für die Staatsverwaltung“ angefragten Beratungsleistungen.

Für das von der Regierung von Mittelfranken projektierte Technik-VPN wurde beispielsweise unter Einbeziehung des LSI in Bezug auf IT-Sicherheit der Ansatz „Security by Design“ verwirklicht. So entstand ein Konzept zu sicheren Zugängen für Dienstleister zur Haustechnik und anderen in Behörden des Freistaats verbauten oder aufgestellten Geräten. Verbindungen aus dem Technik-VPN heraus werden zum Zweck der Fernwartung oder zur Überwachung der Betriebszustände benötigt. Das IT-DLZ ist über den Betrieb des Technik-VPN eingebunden. Im Zuge des Projekts entstand ein Technik-VPN-Leitfaden, in den unter intensiver Mitwirkung des LSI die Aspekte der IT-Sicherheit eingeflossen sind. Mit dem nun verfügbaren Technik-VPN werden auch andere Behörden in die Lage versetzt, künftige Anforderungen, die sich beispielsweise aus der Energiewende ergeben, sicher umzusetzen. Das LSI berät auch in diesem speziellen Bereich der IT zu Umsetzungsprojekten und leistet so einen Beitrag zu einem sicheren Betrieb der Gebäudeinfrastruktur.

Für die Mitarbeiter der Staatsverwaltung wurden die Sensibilisierungskurse zur IT-Sicherheit um ein Angebot zur Simulation von Phishing-Emails ergänzt. Die Behörden bekommen einen vom LSI erstellten „Baukasten“ mit allen notwendigen zentralen Komponenten sowie Vorschläge und Vorlagen für Phishing-Emails zur Verfügung gestellt.

Mit diesen Mitteln und einer stets begleitend angebotenen Beratung durch das LSI kann die jeweilige Behörde eigenverantwortlich eine auf ihre Mitarbeiter begrenzte Phishing-Kampagne simulieren und so unter Wahrung der Vertraulichkeit das eigene Personal sensibilisieren.

Das LSI wird darüber hinaus zu zahlreichen Veranstaltungen bayerischer Behörden eingeladen. In Fachvorträgen und Vorführungen geht die Beratung für die Staatsverwaltung auf die gewünschten Themen ein, weist dabei einerseits auf den durch die bayerischen IT-Sicherheitsrichtlinien vorgegebenen Rahmen hin und stellt andererseits Leitfäden und Handlungsempfehlungen sowie sein offenes Beratungsangebot vor. Der Erfolg solcher Veranstaltungen zeigt sich oft schon kurzfristig durch einen Anstieg von Beratungsanfragen. Bei den anschließenden Beratungen werden die Fachbehörden frühzeitig mit Informationen und Methoden zu IT-Sicherheit versorgt, sodass auch dadurch der Grundsatz „Security by Design“ wesentlich unterstützt wird.




Landesamt für Sicherheit in der Informationstechnik
„Kommunale IT-Sicherheit 2023“
Thementag Oberpfalz
Landesamt für Sicherheit in der Informationstechnik

15. THEMENTAGE UND VERANSTALTUNGEN

Das LSI bietet jährlich Thementage mit unterschiedlichen Schwerpunkten für bayerische Kommunen, kommunale Dienstleister und Betreiber kritischer Infrastrukturen an.

Die jährliche Thementagsreihe „Kommunale IT-Sicherheit“ wird vom LSI in allen sieben Regierungsbezirken in Form von Informationsveranstaltungen vor Ort durchgeführt. Die Teilnehmer erhalten einen Überblick über das aktuelle IT-Sicherheitslagebild in Bayern. Zusätzlich wurden die jährlichen Neuerungen des Beratungsangebots des LSI für Kommunen vorgestellt. Dies waren zuletzt die Themen IT-Resilienz, Siegel „Kommunale IT-Sicherheit“ 3.0, der Warn- und Informationsdienst (WID), die Bedeutung der öffentlichen IP-Adressen für Warnmeldungen und die Malware Information Sharing Platform (MISP). In Zusammenarbeit mit der Regierung von Oberfranken wird auch zum Förderprogramm zur Einführung eines Informationssicherheitskonzepts informiert. Mit den Veranstaltungen werden regelmäßig mehrere hundert interessierte Vertreter bayerischer Kommunen auf allen Ebenen erreicht.

Im Themenkomplex KRITIS werden eigene Veranstaltungsreihen, zum Beispiel zur „Informationssicherheit in Kliniken“ durchgeführt. Der Thementag „Informationssicherheit in Kliniken“ beitet den Klinikleitungen, IT-Leitern und Informationssicherheitsbeauftragte bayerischer Kliniken Gelegenheit, sich untereinander zu vernetzen und zu informieren. Neben der aktuellen Bedrohungslage werden die Unterstützungsmöglichkeiten des LSI bei einem IT-Sicherheitsvorfall vorgestellt. Die Teilnehmer erhalten einen Einblick in das Lagezentrum des LSI, die Orientierungshilfe für IT-Sicherheit in Kliniken, die Malware Information Sharing Platform (MISP), sowie den Warn- und Informationsdienst (WID). Referenten berichten aus der Praxis ihres täglichen Arbeitsbereichs, darüber hinaus werden die Themen Informationssicherheit, Unterstützungsmöglichkeiten bei Sicherheitsvorfällen, Stärkung der Informationssicherheit, finanzielle Förderung von Krankenhäusern in Bezug auf Informationssicherheit, Internet of Things, Awareness und Auswirkungen eines Stromausfalls vorgestellt.

Das LSI beteiligt sich regelmäßig an Veranstaltungen bayerischer Kommunen und Verbänden, beispielsweise mit Live-Hacking-Vorführungen bei Tagen der offenen Tür oder Tagen der Cybersicherheit für Kommunen, Fachvorträgen bei Wasserwerksnachbarschaftstreffen und dem ISB-Bootcamp.

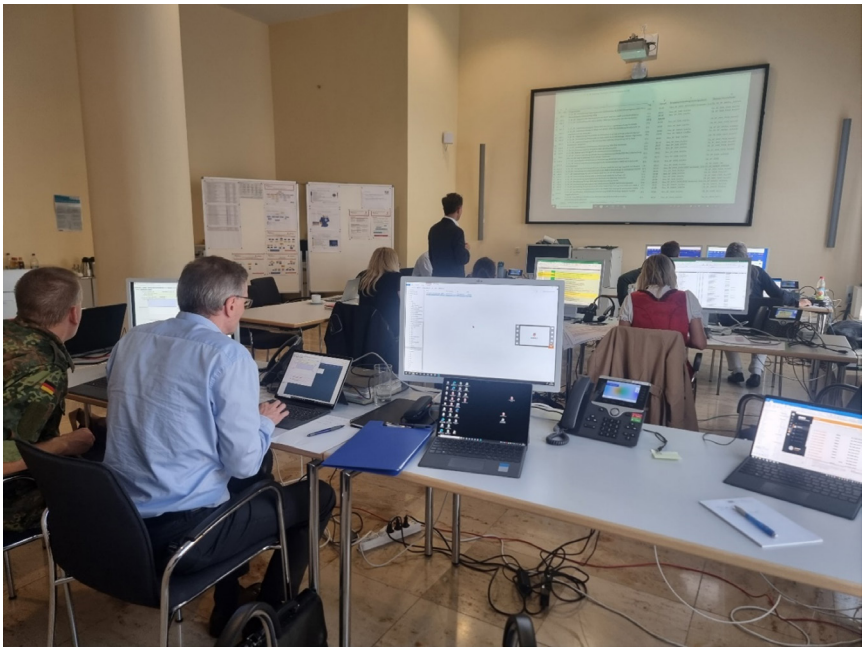
Impressionen der verschiedenen Veranstaltungen

16. BAYERN BEI DER LÜKEX

Bereits seit 2004 werden vom Bund in Abständen von meist zwei Jahren

Länder-
übergreifende
Krisenmanagement-Übungen
(**Ex**ercise) –

LÜKEX - als Stabsrahmenübungen konzipiert. Dabei decken die Themenschwerpunkte ein breites Spektrum ab. Nach der Übung einer Gasmangellage in Süddeutschland im Jahr 2018 mit zwei beteiligten Ressorts in Bayern lag der Schwerpunkt für die aufgrund der Pandemie zweimal verschobenen Übung im Jahr 2023 bei einem Cyberangriff auf das Regierungshandeln. Dieses Thema betrifft heutzutage alle Behörden, deshalb war die Beteiligung bundesweit sehr hoch. Auch in Bayern haben diesmal fünf Ressorts das LÜKEX-Thema aufgegriffen und sich aktiv an der Ausarbeitung eines bayerischen Übungsszenarios beteiligt. Das LSI übernahm als Cybersicherheitsbehörde des Freistaats die Projektleitung für Bayern und die Einbindung in die Übung auf Bundesebene sowie die Abstimmung mit Partnerländern. Im Vorfeld wurde das BSI vom LSI mit einer fiktiven bayerischen Lage versorgt, einem Baustein aus dem bayerischen Szenario für einen realitätsnahen Ausgangszustand auf Bundesebene. Die daraus resultierende Warnmeldung war Teil der Ausgangssituation für die Übungstage am 27. und 28. September 2023. An diesen beiden Tagen versorgte das Lagezentrum des LSI die Übenden mit fiktiven Informationen und Fragestellungen vom BSI oder anderen Länder-CERTs, sowie eigenen Beiträgen. Die im Innenministerium zusammengezogene Steuerungsgruppe setzte sich aus Vertretern aller beteiligten Ressorts zusammen und wurde vom LSI geleitet.



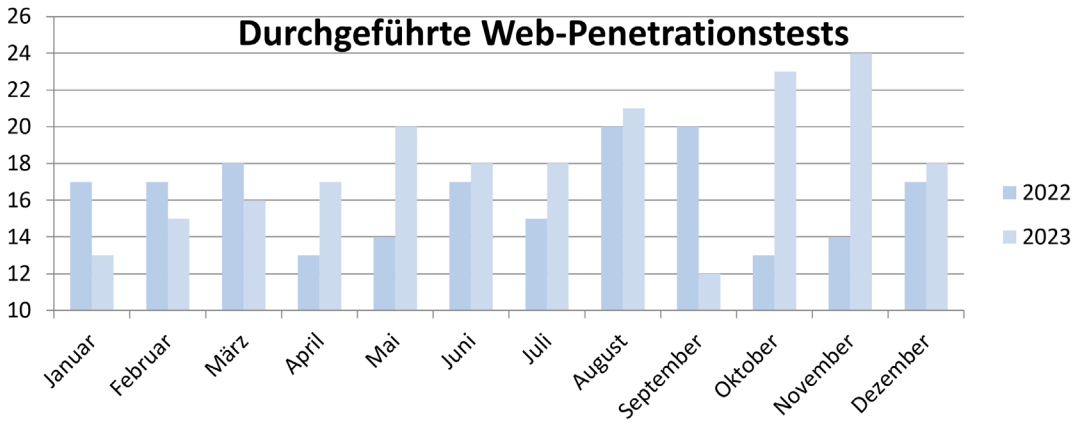
LÜKEX-Übung 2023- Steuerungsgruppe Bayern

Je Ressort wurden aus der Steuerungsgruppe fachspezifische Einlagen eingespielt und im Ablauf nötige, aber nicht aktiv beteiligte Behörden simuliert, um eine realistische Lage zu erzeugen. Die übenden Ressorts waren dadurch veranlasst, sich untereinander abzustimmen und ressortspezifische Meldewege zu nutzen. Im Ergebnis zeigte sich, dass die Krisenstäbe der Ressorts trotz unterschiedlicher Fachaufgaben in einer durch Cyberangriffe begleiteten Lage abgestimmt und koordiniert vorgehen. Es zeigte sich, dass das LSI und der CISO der bayerischen Verwaltung wesentlich zur Einschätzung der Lage und zur Entscheidung über das Ergreifen von wirksamen Maßnahmen beitragen. In den Krisenstäben der Ressorts wurden die jeweiligen Informationssicherheitsbeauftragten in unterschiedlicher Ausprägung eingebunden, um den Informationsfluss zu optimieren.

Nach dem Erfolg der LÜKEX-23 wurde der Gedanke regelmäßiger Übungen in der Bayerischen Cybersicherheitsstrategie 2.0 verankert. Erste Aufgabe hier ist, dass bayerische Cybersicherheitsbehörden mit unterschiedlichen Schwerpunkten miteinander üben und ihre Prozesse in Bezug auf den gegenseitigen Austausch optimieren.

17. REFERAT 13 – PENETRATIONSTEST

Im Bereich der Penetrationstest blickt das Landesamt für Sicherheit in der Informationstechnik auf erfolgreiche Jahre zurück. Zentrale Aufgabe ist, die digitale Infrastruktur des Freistaats Bayern zu schützen, indem Schwachstellen in Webanwendungen, mobilen Apps und IT-Infrastrukturen frühzeitig aufgedeckt und die Betreiber der Anwendungen informiert werden. Dabei zeigt das kontinuierlich hohe Volumen an Tests, sowie die gewonnenen Erkenntnisse daraus, wie dringlich und unerlässlich diese präventive Dienstleistung für die Staatsbehörden im Freistaat ist.



Durchgeführte Web-Penetrationstests der Jahre 2022 und 2023 im Vergleich

Im Jahr 2023 lag der Fokus auf folgenden Kernaufgaben:

Penetrationstests von Webanwendungen: Mit insgesamt 210 geprüften Webanwendungen und Software-Komponenten wurde nicht nur ein hohes Arbeitspensum bewältigt, dass ein hohes Maß an Spezialkenntnissen bedarf, sondern auch insg. deutlich mehr Freigaben erteilt als im Vorjahr. Dies zeigt auch, dass bei Webanwendungen Aspekte der IT-Sicherheit immer besser bereits bei der Entwicklung berücksichtigt werden. Damit wird ein insg. besserer Sicherheitsstandard bei neuen Anwendungen erreicht. Durchschnittlich konnte das LSI rund eine Freigabe pro Arbeitstag erteilen.

Auch für Software- und Infrastruktur-Komponenten führt das LSI gezielte Penetrationstests und Quellcodeanalysen durch, um Schwachstellen frühzeitig zu identifizieren und zu beheben. Diese Prüfungen sind essenziell, um die IT-Infrastruktur des Freistaats sicher und widerstandsfähig gegenüber Cyberangriffen zu halten. Die Einführung einer eigenen Test-Hotline hat 2023 die Erreichbarkeit und die Unterstützung für die LSI Kunden in diesem Bereich erheblich verbessert. Auch künftig wird das LSI den wachsenden Herausforderungen mit modernen Tools, der weiteren Optimierung von Prozessen und einem engagierten Team mit hoher Expertise begegnen können.

Auch in den kommenden Jahren wird das Beratungsangebot des LSI für seine Zielgruppen weiter ausgebaut. Für die Zukunft ist die Weiterentwicklung des Siegels „Kommunale IT-Sicherheit 4.0“, sowie der IT-Resilienz und des IT-Notfallmanagements in Arbeit. Zusätzlich soll das Beratungsangebot um das Thema „Kommunales Risikomanagement“ ergänzt werden. Das Angebot der „Kommunalen TableTop-Übungen“ wurde bereits in den ersten Veranstaltungen der Thementagsreihe 2024 „IT-Notfallprävention“ vorgestellt.

Zudem soll das Beratungsangebot für Betreiber kritischer Infrastrukturen sukzessive ausgebaut werden. Für 2024 ist ein Beratungskonzept „IT-Sicherheit für Wasserkraftanlagen“ in Bearbeitung.

Die Thementagsreihen des LSI werden in 2024 fortgeführt und wurden bereits im März 2024 unter dem Motto „IT-Notfallprävention“ gestartet. Über 900 Vertreterinnen und Vertreter aus dem Kommunalen Bereich haben hierbei teilgenommen.

Im Zuge der Umsetzung der NIS2-Richtlinie werden die Aufgaben des LSI weiter ausgebaut, um verstärkt proaktive Maßnahmen gegen Cyberbedrohungen ergreifen zu können.

Kooperationen mit Hochschulen und anderen Behörden sollen intensiviert werden, damit der Schutz staatlicher IT-Systeme nachhaltig erhöht werden kann.

18. AUSBLICK

Zukünftig wird das Beratungsangebot des LSI soll für seine Zielgruppen ausgebaut. Darunter zählen die Weiterentwicklung des Siegels „Kommunale IT-Sicherheit 4.0“, sowie der IT-Resilienz und des IT-Notfallmanagements. Zusätzlich soll das Beratungsangebot um das Thema „Kommunales Risikomanagement“ ergänzt werden. Das Angebot der „Kommunalen TableTop-Übungen“ wurde bereits in den Veranstaltungen der Thementagsreihe „IT-Notfallprävention“ vorgestellt.

Zudem soll das Beratungsangebot für Betreiber kritischer Infrastrukturen sukzessive ausgebaut werden. Aktuell wird ein Beratungskonzept „IT-Sicherheit für Wasserkraftanlagen“ entwickelt.

Im Zuge der Umsetzung der NIS2-Richtlinie werden die Aufgaben des LSI weiter ausgebaut, um verstärkt proaktive Maßnahmen gegen Cyberbedrohungen ergreifen zu können.

Kooperationen mit Hochschulen und anderen Behörden sollen intensiviert werden, damit der Schutz staatlicher IT-Systeme nachhaltig erhöht werden kann.

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 Dezember 2024
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