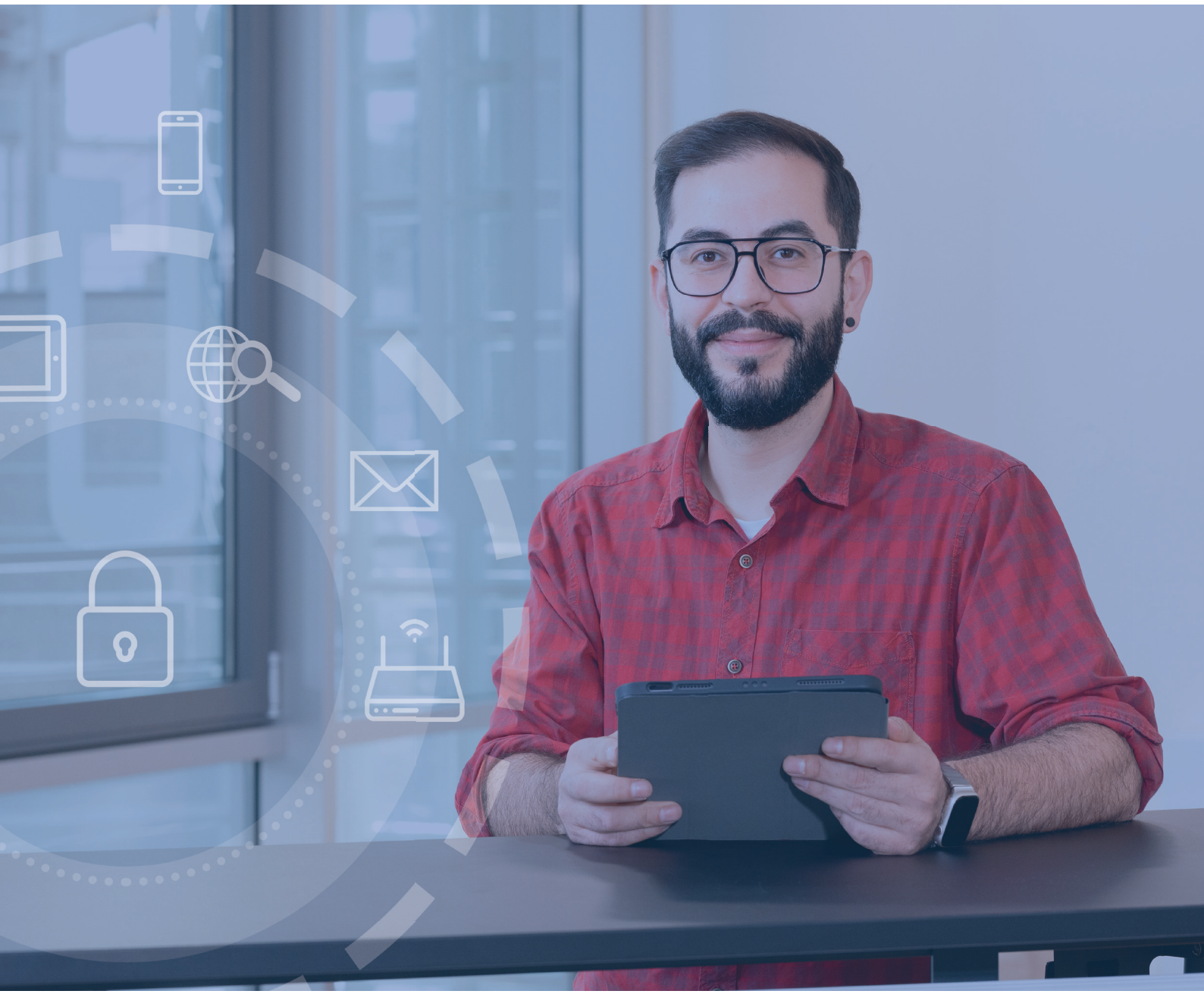
LVR InfoKom
Das Systemhaus

Qualität für Menschen



IT-Sicherheitsbericht 2025

LVR-InfoKom

Wir finden, Software, Computer und Systeme sollten für die Menschen da sein. Und nicht umgekehrt.

Also machen wir sie so: IT-Qualität für Menschen.

Inhalt

Vorwort

Thomas Eichmüller, LVR-Dezernat 6
Leiter des Fachbereichs
IT-Gesamtsteuerung und Informationssicherheits-
beauftragter im LVR

Jan Quatram, LVR-InfoKom
Leiter der Abteilung
Strategie und Projektmanagement und
Leitender Informationssicherheitsbeauftragter
(CISO) bei LVR-InfoKom

Liebe Leser*innen,

das Jahr 2025 hat erneut deutlich gemacht: IT-Sicherheit ist im kommunalen Umfeld nicht nur technische Disziplin, sondern eine zentrale Voraussetzung für Handlungsfähigkeit, Verlässlichkeit und Vertrauen in die öffentliche Verwaltung. Die zunehmende Digitalisierung kommunaler Leistungen erweitert kontinuierlich unsere Angriffsfläche. Gleichzeitig steigen die Erwartungen an Verfügbarkeit, Datenschutz und Resilienz: Bürger*innen, Mitarbeitende, Politik und Partnerorganisationen gehen zu Recht davon aus, dass digitale Dienste genauso zuverlässig funktionieren wie analoge Prozesse – nur schneller, komfortabler und jederzeit erreichbar.

Dabei stehen wir unter besonderen Rahmenbedingungen: begrenzte Ressourcen, heterogene Systemlandschaften, viele organisatorische Schnittstellen und häufig historisch gewachsene IT-Strukturen. Hinzu kommen eine steigende Zahl externer Abhängigkeiten – etwa durch Cloud-Dienste, Betreiber- und Supportmodelle oder Verbundlösungen – sowie die Realität, dass die öffentliche Verwaltung längst Bestandteil kritischer digitaler Lieferketten ist. Diese Gemengelage macht deutlich, warum klassische Schutzmaßnahmen allein nicht ausreichen. Sicherheitsstrategie muss integrierter, proaktiver und konsequent betrieben werden – und sie muss sich an den tatsächlichen Risiken und Prioritäten unserer kommunalen Aufgaben orientieren.

Ein entscheidender Faktor zur Bewältigung dieser Herausforderungen ist die kommunale Vernetzung. IT-Sicherheit kann heute nicht mehr isoliert betrachtet werden: Bedrohungen und Schwachstellen betreffen häufig viele Kommunen gleichzeitig, und Angreifer nutzen standardisierte Muster sowie wiederkehrende Angriffspfade. Umso wichtiger ist es, dass wir gemeinsam lernen, Erfahrungen systematisch austauschen, Standards entwickeln und Synergien konsequent nutzen. Die Vernetzung zwischen den beiden Landschaftsverbänden LVR und LWL in NRW sowie die Vernetzung zu weiteren IT-Dienstleistern im kommunalen Umfeld durch govdigital, KDN und VITAKO ist dabei weit mehr als ein formaler Rahmen – sie ist ein strategischer Hebel, um Expertise zu bündeln, gemeinsame Sicherheitsanforderungen zu definieren, Prioritäten abzustimmen und nachhaltige Kooperationsmodelle zu etablieren.

Gleichzeitig entfaltet diese Vernetzung eine unmittelbare operative Wirkung im Alltag der IT-Sicherheitsarbeit: durch gemeinsame Lagebilder und Frühwarnmechanismen, abgestimmte Vorgehensweisen in Incident- und Krisensituationen, gegenseitige Unterstützung bei personellen Engpässen sowie durch koordiniertes Handeln bei Beschaffung, Betrieb und Weiterentwicklung sicherheitsrelevanter Lösungen. Vor dem Hintergrund des zunehmenden Fachkräftemangels gewinnt diese Zusammenarbeit zusätzlich an strategischer Bedeutung. Nicht alle werden perspektivisch noch in der Lage sein, alle sicherheitsrelevanten Aufgaben qualitativ wie quantitativ eigenständig zu erfüllen, etwa im 24/7-Incident-Response-Betrieb, beim Betrieb spezialisierter Sicherheitswerkzeuge oder beim Vorhalten aktueller Bedrohungs- und Lageexpertise.

Die Ereignisse des Jahres 2025 unterstreichen diese Entwicklung eindrücklich. Der BSI-Lagebericht (siehe Seite 4-5) beschreibt eine weiterhin angespannte und dynamische Bedrohungslage für den öffentlichen Sektor. Konkrete Vorfälle auf kommunaler Ebene – wie die koordinierten DDoS-Angriffe auf zahlreiche kommunale Webangebote in Sachsen-Anhalt oder der Ransomware-Angriff auf die Gemeindeverwaltung Untereisesheim, der einen umfassenden IT-Notbetrieb erforderlich machte – zeigen, dass IT-Sicherheitsereignisse keine theoretischen Szenarien mehr sind, sondern reale Betriebslagen darstellen, auf die sich Kommunen organisatorisch, technisch und personell vorbereiten müssen.

Die in diesem Bericht behandelten Themenfelder Incident Response, Identity & Access Management (IAM), Service Asset & Configuration Management (SACM) sowie Software- und Lifecycle-Management stehen in direktem Zusammenhang mit diesen Ereignissen und bilden gemeinsam einen Teil des Fundaments einer belastbaren Sicherheitsarchitektur. Zusammengenommen zeigen diese Themen, dass IT-Sicherheit nur dann wirksam und nachhaltig umgesetzt werden kann, wenn technische Maßnahmen, organisatorische Strukturen und kommunale Zusammenarbeit im Verbund zusammenspielen.
Der vorliegende Bericht versteht sich daher nicht nur als Rückblick auf das Jahr 2025, sondern als Beitrag zur gemeinsamen Weiterentwicklung von Resilienz, Handlungsfähigkeit und Sicherheit in der kommunalen IT-Landschaft.

Thomas Eichmüller, LVR-Dezernat 6
Leiter des Fachbereichs IT-Gesamtsteuerung und
Informationssicherheitsbeauftragter im LVR

Jan Quatram, LVR-InfoKom
Leiter der Abteilung Strategie und Projektmanagement
und Leitender Informationssicherheitsbeauftragter (CISO)
bei LVR-InfoKom

I. Allgemeine Lage der IT-Sicherheit in Deutschland

Mit seinem Bericht zur Lage der IT-Sicherheit in Deutschland informiert das Bundesamt für Sicherheit in der Informationstechnik (BSI) jährlich über die Bedrohungslage im Cyberraum. Demnach besteht weiterhin kein Grund zur Entwarnung: Viele Behörden, Unternehmen und andere Organisationen machten es Angreifern nach wie vor zu leicht, sodass diese mit vergleichsweise geringem Aufwand und einfachen Mitteln weiterhin großen Schaden anrichten konnten. Denn Angreifer gingen mehr und mehr den Weg des geringsten Widerstandes und suchten sich jene Ziele aus, deren Angriffsflächen das niedrigste Schutzniveau aufwiesen. Das betraf insbesondere kleine und mittlere Unternehmen (KMU) sowie Institutionen des politischen und vorpolitischen Raums, deren Web-Angriffsflächen nicht ausreichend geschützt waren. Nach dem Kosten-Nutzen-Kalkül cyberkrimineller Angreifer gibt es keine uninteressanten Ziele mehr, bei denen vermeintlich „nichts zu holen“ wäre. Jede aus dem Internet erreichbare Institution oder Person ist prinzipiell bedroht, jede und jeder ist ein interessantes Ziel. Im aktuellen Berichtszeitraum führte dies unter anderem dazu, dass Schwachstellen zunehmend ausgenutzt (Exploitation) und mehr Daten exfiltriert und veröffentlicht wurden (Datenleaks). Eine gesamtgesellschaftliche Steigerung der Präventionsfähigkeiten durch ein wirksames Angriffsflächenmanagement aufseiten der Verteidiger ist daher das Gebot der Stunde.

Die Dimensionen der Cybersicherheitslage im BSI-Lagebericht 2025

In der Dimension Bedrohungen sind in diesem Jahr durchaus positive Trends zu beobachten. Im Cybercrime-Bereich führten internationale Strafverfolgungsmaßnahmen zu einer Stabilisierung. Namentlich mit LockBit und Alphv konnten zwei vormals sehr aktive Angreifergruppen nahezu ausgeschaltet werden. Bei den Angriffsinfrastrukturen stachen im Berichtszeitraum insbesondere die Botnetze Badbox und Vo1d als die größten und aktivsten hervor.

Die Angriffsflächen in Deutschland zeigen dagegen nach wie vor einen besorgniserregenden Zustand. Insbesondere Web-Angriffsflächen müssen mehr professionelle Aufmerksamkeit durch wirksames Angriffsflächen-Management erhalten. So werden beispielsweise viel zu oft bekannte Schwachstellen in Perimetersystemen zu spät oder gar nicht gepatcht. Im aktuellen Berichtszeitraum wurden darüber hinaus durchschnittlich täglich 119 neue Schwachstellen in IT-Systemen bekannt, ein Wachstum von rund 24 Prozent im Vergleich zum vergangenen Berichtszeitraum.

Die im Berichtszeitraum beobachteten Gefährdungen, das heißt die Zahl der tatsächlichen Angriffe, Vorfälle und Störungen, gingen damit auch im Jahr 2025 nicht zurück. Erfolge im Bereich der Bedrohungen führen wegen zu vieler zu schlecht geschützter Angriffsflächen noch nicht zu einer Abnahme der Gefährdungen. Dabei setzte sich konkret der Trend weg von großen, aufwendigen Angriffen hin zu vielen kleinen, einfach durchzuführenden fort: Rund 80 Prozent der angezeigten Angriffe, zum Beispiel mit Ransomware, richteten sich gegen kleine und mittlere Unternehmen, denen häufig die Mittel und das Wissen fehlen, um sich selbstständig zu schützen.

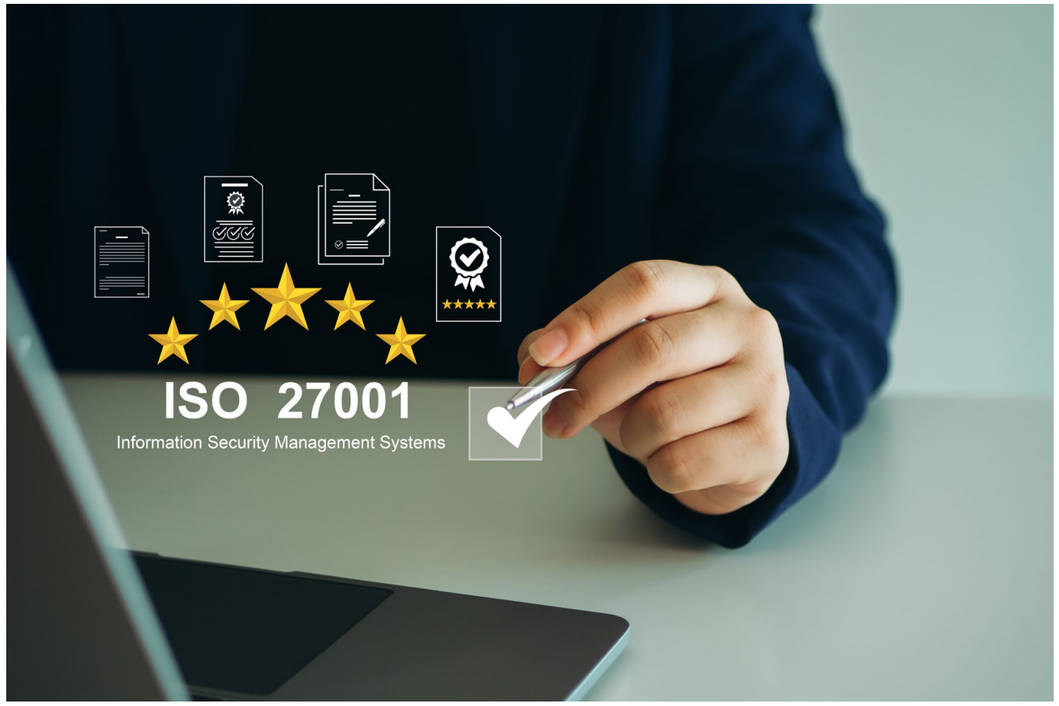
In der Dimension Schadwirkung beobachtete das BSI ebenso weiterhin hohe Werte. Die Anzahl der Leak-Geschädigten nahm zu, ebenso wie Zugangsdatendiebstähle. Während die Bereitschaft zur Zahlung von Lösegeldern im aktuellen Berichtszeitraum weiter sank, wurden im Zuge von Datenleaks nach Exploitation-Angriffen die durchschnittlich höchsten Lösegelder seit Beginn der Aufzeichnungen registriert. Hinzu kommen die Kosten durch entgangene Einnahmen bei angriffsbedingten Systemausfällen sowie Kosten für IT-forensische Untersuchungen oder für die Wiederherstellung von IT-Systemen.

Die dargestellten Gefährdungen und Schadwirkungen im BSI-Lagebericht 2025 zeigen, dass in der Dimension Resilienz noch großer Handlungsbedarf besteht. Die Schlussfolgerung des BSI: Angriffsflächen schützen! Nur, wer sich aktiv schützt, erhöht die Chancen, Gefährdungen zu entgehen oder Schadwirkungen zu minimieren.

II. Aktuelle Bewertung der IT-Sicherheit im LVR

Bezogen auf den Berichtszeitraum 2025 ist die Lage der IT-Sicherheit im LVR insgesamt als positiv zu bewerten. Es gab nur einen nennenswerten IT-Sicherheitsvorfall und dies trotz zunehmend kritischer Bedrohungslage. Im Gegensatz zu 2024 hat der LVR deutlich mehr E-Mails empfangen – so gab es einen Anstieg von 36,5 Millionen auf 47,6 Millionen. Ein Großteil davon – in Höhe von 33 Millionen – waren E-Mails, die potenzielle Bedrohungen enthielten. Auch bei den direkten Angriffen konnte ein enormer Anstieg festgestellt werden. Waren es im Jahr 2024 noch ca. 1,15 Millionen Angriffe monatlich, die durch das Intrusion Prevention System (IPS) entdeckt und verhindert wurden, ist der Wert 2025 um 200.000 gestiegen.

Weiterhin ist zu beobachten, dass die Anzahl gezielter Phishing-Mails im Berichtszeitraum abermals stark zugenommen hat. Die Phishing-Mails haben dabei sehr an Qualität gewonnen, was eine Identifizierung durch die Mitarbeitenden des LVR zunehmend erschwert. Dieser Trend wird durch den Einsatz von KI und Einbindung von Deepfakes voraussichtlich auch immer weiter zunehmen.



Diese positive Bilanz ist im Wesentlichen auf das bestehende Sicherheitskonzept in Form des Handbuches für IT-Sicherheit und Datenschutz und seine konsequente Umsetzung zurückzuführen, insbesondere auch im Hinblick auf die Achtsamkeit der Mitarbeitenden. Die Realisierung erfolgt als laufender Prozess im Rahmen des in LVR-InfoKom etablierten Informationssicherheits-Management-Systems (ISMS), welches nach der international anerkannten Standardnorm ISO 27001 zertifiziert ist. Seit der Erstzertifizierung im Jahr 2012 wird das ISMS regelmäßig durch externe Auditoren geprüft und rezertifiziert. Bestandteile des präventiven Schutzes sind dabei eine Reihe von Systemen:

- LVR-InfoKom betreibt eine mehrstufige und mit unterschiedlichen Virenschutzprogrammen ausgestatte Infrastruktur, die sowohl die PCs, die Server, die Dateien sowie die Verbindungen zum Internet schützt.
- Für die sichere E-Mail-Kommunikation werden Verschlüsselungs-Gateways genutzt. Diese überprüfen alle eingehenden E-Mails und sorgen dafür, dass die meisten davon erst gar nicht ins LVR-Netz gelangen, weil sie eindeutig entweder unerwünschte Werbung oder Schad-Mails sind. E-Mails, die nicht eindeutig klassifiziert werden können, werden mit einer Markierung versehen, damit die LVR-Mitarbeitenden sie mit besonderer Vorsicht behandeln. In diesem Fall erhält man eine entsprechende Nachricht. Über das LVR-Sicherheitspostfach besteht die Möglichkeit, sicher und datenschutzkonform personenbezogene Daten mit externen Kontakten auszutauschen.
- Sämtliche Internetinhalte, die von LVR-Mitarbeitenden aus dem Internet angefordert werden, laufen über einen Proxy. Diese Art Filter verfügt über einen Antivirusschutz und kategorisiert Web-Inhalte nach ihrer Reputation.
- Das LVR-interne Netzwerk ist in viele logische Abschnitte unterteilt, sodass beispielweise die unterschiedlichen LVR-Standorte inklusive der LVR-Rechenzentren voneinander getrennt sind. Der Netzwerkverkehr zwischen diesen Abschnitten, aber auch zwischen dem internen Netzwerk und dem Internet, wird durch sogenannte Next-Generation Firewalls reglementiert und dabei mithilfe einer Deep Packet Inspection überprüft. Werden potenzielle Angriffe oder schädliche Aktionen erkannt, werden diese durch ein Intrusion Prevention System automatisiert verhindert.

IT-Sicherheit in Zahlen 2025

Firewall

ca. 3,01 Petabyte Internet-Traffic
ca. 1,35 Millionen verhinderte Angriffe pro Monat durch das IPS

Mailing

47,6 Millionen **empfangene** E-Mails 2025 …

… davon

- 33,1 Millionen potenziell bedrohliche E-Mails
- 2,6 Millionen Massen-/Newsletter-E-Mails
- 11,9 Millionen schadfreie E-Mails und davon
- 60.000 S/MIME verschlüsselte E-Mails
- 41.000 digital signierte E-Mails

Alle Angaben sind gerundet.

5,8 Millionen **versendete** E-Mails 2025 …

… davon

- 22.500 S/MIME verschlüsselte E-Mails
- 34.000 an das LVR Sicherheitspostfach ausgesteuerte E-Mails
- 7.500 digital signierte E-Mails

Alle Angaben sind gerundet.

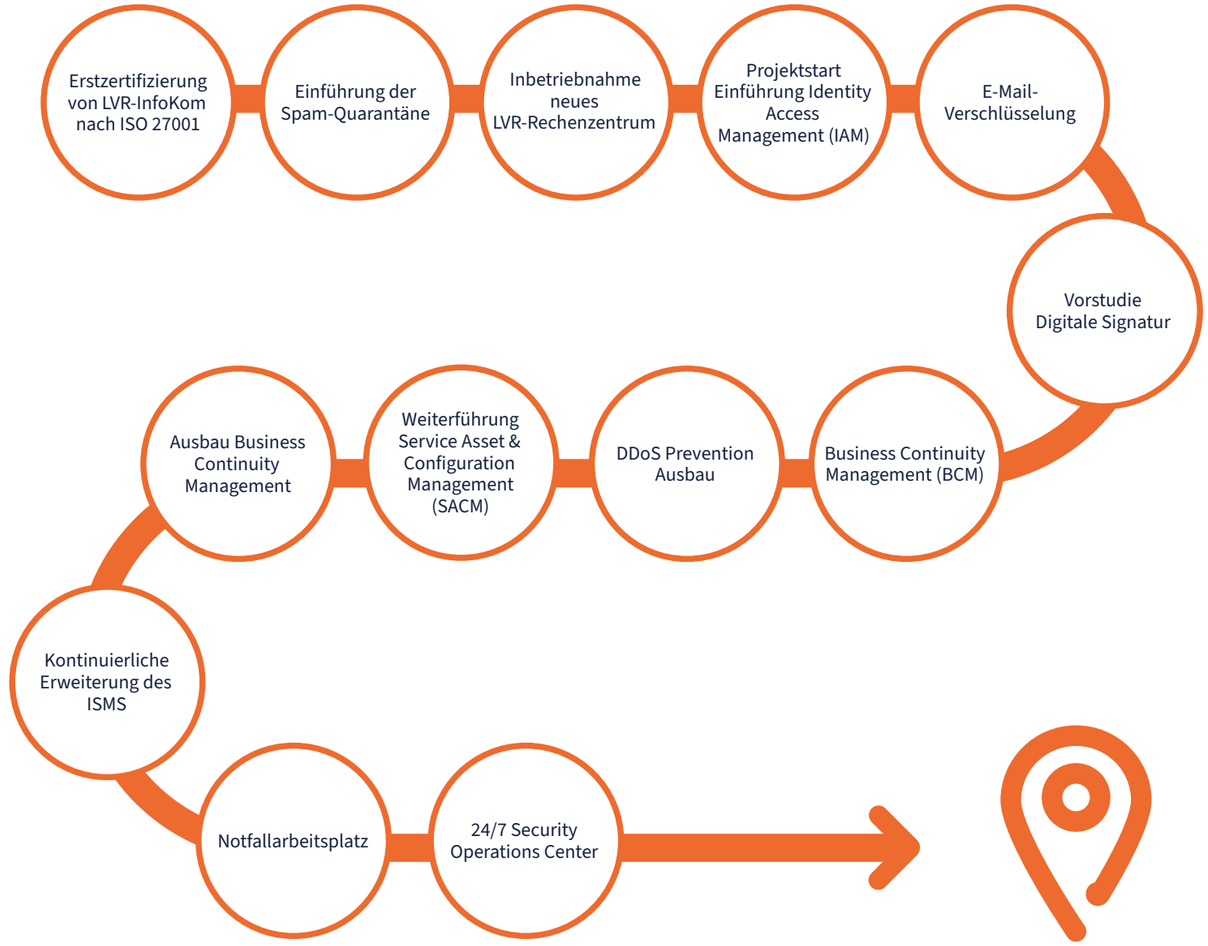
E-Mail Traffic über das **Netz des Bundes**

- 860.000 empfangene E-Mails
- 1 Million versendete E-Mails

Alle Angaben sind gerundet.

IT-Sicherheit im LVR als kontinuierlicher Prozess

Ausgewählte Meilensteine im Überblick



IT-Security Roadmap

Der LVR hat es sich zum Ziel gesetzt, den aktuellen Stand der IT-Sicherheit regelmäßig zu bewerten und Verbesserungsmaßnahmen auf Basis dieser Bewertung durchzuführen. Unter der Federführung des LVR-Dezernates „Digitalisierung, IT-Steuerung, Mobilität und technische Innovation“ werden diese Maßnahmen in Form einer fortlaufenden „IT-Security Roadmap“ geplant und umgesetzt. Schwerpunkte in diesem Jahr waren Maßnahmen aus den Bereichen IT Security Awareness, ISMS, SIEM, SACM, Netzwerk, IAM und zentrales Software Management.

III. Spezielle Sicherheitsmaßnahmen im Jahr 2025

Im Bereich IT-Sicherheit bedeutet Stillstand Rückschritt. Es gilt daher, den bestehenden Schutz durch ein Bündel spezieller technischer, organisatorischer und personeller Maßnahmen kontinuierlich weiter zu verstärken. Im Folgenden zeigen wir Ihnen einige Beispiele für den Berichtszeitraum 2025 auf. Das so wichtige Thema „Sensibilisierung der Mitarbeitenden“ wird dabei ausgeklammert und im Kapitel V separat beleuchtet.

IAM

Die Nutzung des Identity- und Access- Managements (IAM) konnte im Jahre 2025 weiter erfolgreich ausgebaut werden, so dass im ersten Halbjahr 2025 die letzten beiden LVR-Kliniken an das IAM angebunden werden konnten. Weiterhin konnte im Verlauf des Jahres auch die Anbindung der Krankenhauszentralwäscherei (KHZW) sowie der ersten Kultur-Außendienststellen an das IAM vollzogen werden. Die flächendeckende Nutzung des IAM-Tools für die internen Mitarbeitenden des gesamten LVR wird voraussichtlich im Folgejahr 2026 möglich sein. Des Weiteren wurden umfangreiche Verbesserungs- und Stabilisierungsmaßnahmen unternommen, um die Prozesse für das „Onboarding“ von neuen Mitarbeitenden, das „Offboarding“ von ausscheidenden Mitarbeitenden und beim Wechsel („Moving“) von Mitarbeitenden von einem zum anderen Organisationsbereich abzurunden und den Erfordernissen des LVR damit gerecht zu werden. Beim letztgenannten „Moving“ wurden sowohl bereichsinterne als auch -übergreifende Wechsel berücksichtigt.

Zentrales Software-Management als Sicherheitsfaktor

Im Jahr 2025 wurde ein Projekt zur Einführung eines zentralen Software-Managements initiiert. Dies ist ein wesentlicher Baustein moderner IT-Sicherheitsstrategien. Es sorgt für Transparenz über die eingesetzte Softwarelandschaft und schafft die Grundlage für ein wirksames Schwachstellen- und Patch-Management. Die damit verbundenen Aufräumarbeiten lassen sich gut mit dem Aufräumen eines Kellers vergleichen: Über Jahre sammeln sich Werkzeuge, alte Geräte und vermeintlich nützliche Gegenstände an. Irgendwann verliert man den Überblick – und im Ernstfall findet man nicht, was man braucht. Ähnlich verhält es sich in der IT: Nicht mehr benötigte, veraltete oder redundante Anwendungen erhöhen die Unübersichtlichkeit und damit auch das Sicherheitsrisiko. Insbesondere nicht mehr unterstützte Software stellt eine erhebliche Angriffsfläche dar. Solche Altlasten werden systematisch identifiziert und entfernt. Gleichzeitig wird die Softwarelandschaft stärker standardisiert. Einheitliche, definierte Softwarestände erleichtern die zeitnahe Verteilung von Sicherheitsupdates, reduzieren Fehlkonfigurationen und verbessern die Reaktionsfähigkeit bei Sicherheitsvorfällen. Wichtig ist dabei: Das „Aufräumen“ ist keine einmalige Aktion, sondern eine stetige Aufgabe. Neue Anforderungen, neue Anwendungen und neue Bedrohungen führen kontinuierlich zu Veränderungen in der IT-Landschaft. Ein wirksames zentrales Software-Management bedeutet daher, regelmäßig zu prüfen, zu konsolidieren und zu standardisieren. Aufräumarbeiten und Standardisierung sind damit nicht nur Maßnahmen zur Effizienzsteigerung, sondern leisten einen direkten und nachhaltigen Beitrag zur Erhöhung der IT-Sicherheit.

SACM

Voraussetzung für funktionierende IT-Security-Maßnahmen ist eine solide, zuverlässige Datenbasis. Zuständig hierfür ist das Service Asset & Configuration Management, bei dem alle Informationen über das vorhandene Inventar an Hard- und Software (Assets) in einer zentralen Datenbank, der CMDB, erfasst werden. Diese Datenbasis wurde im Jahr 2025 um relevante Security Controls und Assets erweitert. Security Controls sind Schutzmaßnahmen, die darauf ausgelegt sind, die Integrität, Vertraulichkeit und Verfügbarkeit der Konfigurationsdaten und IT-Assets zu gewährleisten. Eine weitere wesentliche Maßnahme

war die Neustrukturierung und Abstrahierung der bereits aufgenommenen Daten, wodurch die Übersichtlichkeit und Flexibilität beim Umgang mit den Daten verbessert werden konnte. Hiervon profitieren sowohl die Kunden als auch die Mitarbeitenden von LVR-InfoKom in der täglichen Arbeit beziehungsweise bei der Reaktion auf Sicherheitsvorfälle.

Incident Response

Im Juni 2025 gab es einen nennenswerten IT-Sicherheitsvorfall. Der Vorfall wurde durch die vorhandenen technischen und organisatorischen Sicherheitsmaßnahmen frühzeitig erkannt und gemäß den definierten Prozessen bearbeitet. Die bestehenden Sicherheits- und Meldeverfahren haben zuverlässig funktioniert. Durch die gute Zusammenarbeit mit unserem Incident Response Dienstleister konnte der Vorfall zeitnah abgeschlossen werden. Die Erkenntnisse die wir daraus gewinnen konnten, wurden zur Optimierung von Maßnahmen und Prozessen genutzt.

NIS2 als gemeinsamer Gestaltungsauftrag

Mit dem am 6. Dezember 2025 in Kraft getretenen NIS-2-Umsetzungsgesetz hat Deutschland die EU-Richtlinie NIS-2 in nationales Recht umgesetzt und damit die Resilienz von Staat und Verwaltung gegen Cyberbedrohungen gestärkt. Das Gesetz schafft verbindliche Anforderungen an das Informationssicherheitsmanagement und etabliert ein einheitliches Mindestniveau der Netz- und Informationssicherheit. Um diese Anforderungen bestmöglich zu erfüllen, setzt der LVR auf eine koordinierte Herangehensweise im Rahmen von Kooperationen mit anderen kommunalen Akteuren. In diesem Kontext ist auch das Angebot des KDN zu gemeinsamen Veranstaltungen und Austauschformaten zur NIS2-Umsetzung ein wichtiger Baustein für die kommunale Vorbereitung. Diese Formate schaffen Transparenz über regulatorische Anforderungen, ermöglichen eine abgestimmte Interpretation offener Fragestellungen und unterstützen die Entwicklung gemeinsamer Umsetzungsstrategien.

IV. Ausblick

Folgt man den Prognosen von IT-Sicherheitsexperten, wird sich die Bedrohungslage weiter verschärfen, sowohl was die Anzahl als auch die Vielschichtigkeit der Angriffe anbelangt. Um dem zu begegnen, sind für die nähere Zukunft weitere Maßnahmen geplant, die gemäß einer zwischen LVR-Dezernat 6 und LVR-InfoKom fortlaufend abgestimmten Security- beziehungsweise Informationssicherheits-Roadmap entwickelt werden.

Auf der Agenda für 2026 steht zum Beispiel die Ausweitung des Information Security Management System (ISMS) auf den gesamten LVR. Auch das Business Continuity Management (BCM) wird weiter ausgebaut.

Um in einem Notfall handlungsfähig zu sein, steht auch das Thema Notfallarbeitsplatz auf der Agenda. Ein Notfallarbeitsplatz ist ein vorgeplanter Ersatzarbeitsplatz, der den Betrieb in einer Krisen- oder Störungssituation aufrechterhalten soll.

Auch der Aufbau eines 24/7 Security Operation Centers in Verbindung mit einer Optimierung des IT-Sicherheitsmonitorings ist geplant.

Nicht zuletzt werden wir weiterhin das Sicherheitsbewusstsein der LVR-Mitarbeitenden (IT-Security Awareness) weiter intensiv fördern. Schließlich können auch noch so gute Schutzsysteme nicht sicherstellen, dass jedwede Bedrohung rechtzeitig erkannt wird. Nur wenn verantwortungsvoll und vorsichtig mit den IT-Ressourcen des LVR umgegangen wird, kann ein hohes Schutzniveau erreicht werden. Verhaltensvorschriften (Dienstanweisungen, Rundverfügungen ...), die an alle Mitarbeitenden kommuniziert sind, stellen dabei eine wichtige Grundlage dar, sind aber nur eine Komponente. Zusätzlich gilt es, über praxisnahe und ansprechende Informationen echtes Verständnis zu schaffen und die Mitarbeitenden dazu zu motivieren, als aktive Mitgestaltende von IT-Sicherheit einen wichtigen Beitrag zu leisten. Dann werden auch Maßnahmen zur Erhöhung der Sicherheit, die mit Komforteinbußen einhergehen, akzeptiert, da die Notwendigkeit erkannt und damit das Verständnis gefördert wird. Näheres hierzu finden Sie im folgenden Kapitel V.

V. Der „Faktor Mensch“ – oder die wichtige Rolle der Mitarbeitenden

Auch im aktuellen Berichtszeitraum wurde wieder größtes Augenmerk auf die Aufklärung und Sensibilisierung der Mitarbeitenden gelegt. Hier ein Überblick:

- **IT-Sicherheitstraining**
  Der LVR bietet seinen Mitarbeitenden durch den Einsatz einer Lernplattform zu Themen der IT-Sicherheit die Gelegenheit, an praktischen Beispielen ihre Kenntnisse in den Sicherheitsthemen zu vertiefen. Ein besonderer Schwerpunkt gilt hierbei dem Umgang mit externen E-Mails. Durch die Implementierung eines sogenannten Meldebuttons in der E-Mail-Software können die LVR-Mitarbeitenden verdächtige E-Mails melden. Diese werden umgehend geprüft und gegebenenfalls Maßnahmen eingeleitet. Seit Einführung des Meldebuttons ist die Anzahl der Meldungen stetig gestiegen, was auf eine zunehmende Sensibilisierung der Mitarbeitenden schließen lässt.

- **Verpflichtung der Mitarbeitenden auf Gesetze und Vorschriften**
  Wer neu eingestellt wird, erhält am ersten Arbeitstag ein umfangreiches Paket an Informationen, zu denen auch die grundlegenden Regelungen zum Datenschutz beim LVR gehören. Darüber hinaus wird jährlich eine entsprechende Dienstanweisung zur Kenntnis gegeben. Dies wird mittels Unterschrift dokumentiert.

- **Informationen im Intranet**
  Der zentrale Pool ist die LVR-Intranetseite „IT-Sicherheit“. Hier finden sich offizielle Dokumente (Richtlinien, Handbuch für Datenschutz und IT-Sicherheit ...), Tipps & Tricks, wichtige Links und vieles mehr. Auf die Präsenz der Seite wird regelmäßig über andere Medien hingewiesen.

- **Neue Medien**
  Zu den stetig wachsenden Inhalten der Intranetseite zählt auch eine Reihe von Erklärvideos, in denen auf verständliche und pointierte Weise praktische Sicherheitstipps für den Arbeitsalltag gegeben werden.

- **Aktuelle Meldungen**
  LVR-InfoKom informiert per Intranet-News über relevante IT-Ereignisse. Hierzu gehören auch Nachrichten aus dem Bereich IT-Sicherheit. Zudem versendet das InfoKom Service Center (ISC) Ad hoc-Meldungen per E-Mail an alle LVR-Mitarbeitenden, beispielsweise Warnungen, Verhaltenshinweise oder Informationen zu Verfahrensänderungen aufgrund von Sicherheitsmaßnahmen.

- **Führungsverantwortung**
  Eine besondere Verantwortung liegt beim Thema IT-Security Awareness bei den Führungskräften, die durch ihr Führungsverhalten und ihre Vorbildwirkung die IT-Sicherheit fördern sollen. Von besonderer Bedeutung ist dabei die Phase der Einarbeitung von neuen Mitarbeitenden und Auszubildenden, in der großes Augenmerk auch auf den verantwortungsvollen Umgang mit der IT gelegt werden soll.

- **Schulungen**
  Der LVR bietet seinen Mitarbeitenden interne Schulungen an. Dazu gehören neben den Datenschutzeinweisungen im Rahmen der PC-Bedienung auch Seminare zum Datenschutzrecht. Darüber hinaus schärft LVR-InfoKom das Sicherheitsbewusstsein seiner Mitarbeitenden mit weiteren Maßnahmen, weil diese durch ihre Arbeit unmittelbar mit den kritischen Systemen und Anwendungen in Kontakt sind.

VI. IT-Sicherheit am Arbeitsplatz

Checkliste für ein sicherheitsbewusstes Verhalten am digitalen Arbeitsplatz:

- **E-Mails kritisch prüfen**
  Bei E-Mails von externen Kontakten, aber ebenso so von Kolleg*innen vorsichtig sein, da Urheber von Phishing-Mails seriöse Absender immer besser nachahmen. Damit man nicht in die Falle tappt, gilt der 3-Sekunden-Sicherheits-Check: Vor dem Anklicken Absender, Betreff und Anhang prüfen.

- **Verantwortungsvoller Umgang mit Passwörtern**
  Passwörter keinesfalls auf Zetteln oder Post-its am Monitor notieren, auch nicht an vermeintlich diskreten Stellen wie unter der Tastatur. Sorge dafür tragen, dass man bei der Eingabe des Passworts nicht beobachtet wird. Für jedes Gerät und jede Anwendung jeweils verschiedene Passwörter nutzen und diese in regelmäßigen Abständen wechseln. Ein sicheres Passwort sollte aus mindestens 8 Zeichen bestehen und Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten.

- **Schutz sensibler Daten auf PC, Laptop und Co.**
  Den Zugriff auf das eigene Gerät sperren, sobald man den Arbeitsplatz verlässt – auch wenn es sich nur um eine kurze Abwesenheit handelt. Keine Wechseldatenträger unbekannter Herkunft an den Arbeitsplatzrechner anschließen. Es besteht die Gefahr einer Infektion mit Schadcode. Keine private Hardware im LVR-Netz einsetzen und keine Unternehmensdaten auf privaten Datenträgern speichern. Nur die offiziell freigegebene Software auf den Arbeitsgeräten nutzen. Auf USB-Sticks mit Arbeitsdokumenten achtgeben und diese gegebenenfalls mit einem Passwort schützen.

- **Sichere Internetnutzung**
  Das Internet ist ausschließlich dienstlich zu nutzen. Durch eine achtsame und verantwortungsbewusste Internetnutzung kann die Gefahr einer Schadsoftware-Infektion des eigenen Systems oder womöglich sogar des gesamten LVR-Netzwerks reduziert werden.

- **Die eigene Rolle ernst nehmen**
  Dass die Hauptverantwortung für die Sicherheit der Unternehmens-IT bei den dafür verantwortlichen Stellen liegt, ist klar. Dennoch können alle durch bedachtes und umsichtiges Handeln einen Beitrag zum Schutz vor Sicherheitsvorfällen leisten. Daher sollten die Informationsangebote von LVR-InfoKom zum Thema IT-Sicherheit wahrgenommen werden. Schließlich hilft dies nicht nur geschäftlich, sondern auch privat.

Im Fokus:

Kommunale Zusammenarbeit als Sicherheitsfaktor – Vernetzung, Professionalisierung und gemeinsame Verantwortung

Die im Vorwort skizzierten Ereignisse des Jahres 2025 – von koordinierten DDoS-Angriffen auf kommunale Webangebote bis hin zu Ransomware Vorfällen mit Notbetriebs Szenarien – verdeutlichen: IT Sicherheit ist längst kein isoliertes Organisationsthema mehr. Sie ist eine gemeinschaftliche Aufgabe der kommunalen Fa milie. Angesichts einer dynamischen Bedrohungslage, wachsender regulatorischer Anforderungen und eines zunehmenden Fachkräftemangels wird deutlich, dass nachhaltige Resilienz nur im Verbund entstehen kann.

Kommunale Zusammenarbeit ist dabei nicht lediglich Erfahrungsaustausch, sondern ein strategisches Instrument zur Professionalisierung. Gemeinsame Standards, abgestimmte Sicherheitsanforderungen und geteilte Bewertungsmaßstäbe schaffen Vergleichbarkeit und erhöhen die Qualität von Entscheidungen – sowohl technisch als auch organisatorisch.

AG Cybersicherheit der govdigital
Insbesondere die Strukturen der govdigital bieten hierfür eine etablierte und belastbare Plattform. Die govdigital-Arbeitsgruppen zu IT Sicherheit sowie zu integrierten Managementsystemen leisten einen wichtigen Beitrag zur gemeinsamen Weiterentwicklung kommunaler Sicherheitsstandards. Hier werden nicht nur aktuelle Bedrohungslagen diskutiert, sondern auch praxisnahe Lösungsansätze erarbeitet – etwa zu Governance Strukturen, Risikomanagement, Informationssicherheitsprozessen oder zur Verzahnung von IT Sicherheit mit Datenschutz, Notfallmanagement und Compliance. Gerade der Ansatz integrierter Managementsysteme ist für Kommunen von besonderer Bedeutung: Informationssicherheit, Datenschutz, Business Continuity Management, Qualitäts- und Risikomanagement dürfen nicht nebeneinanderstehen, sondern müssen strukturell zusammengedacht werden. Die Arbeit in den govdigital-Gremien unterstützt diesen integrierten Blick und fördert eine gemeinsame Sprache sowie ein gemeinsames Verständnis von Sicherheitsreife und Professionalisierung.

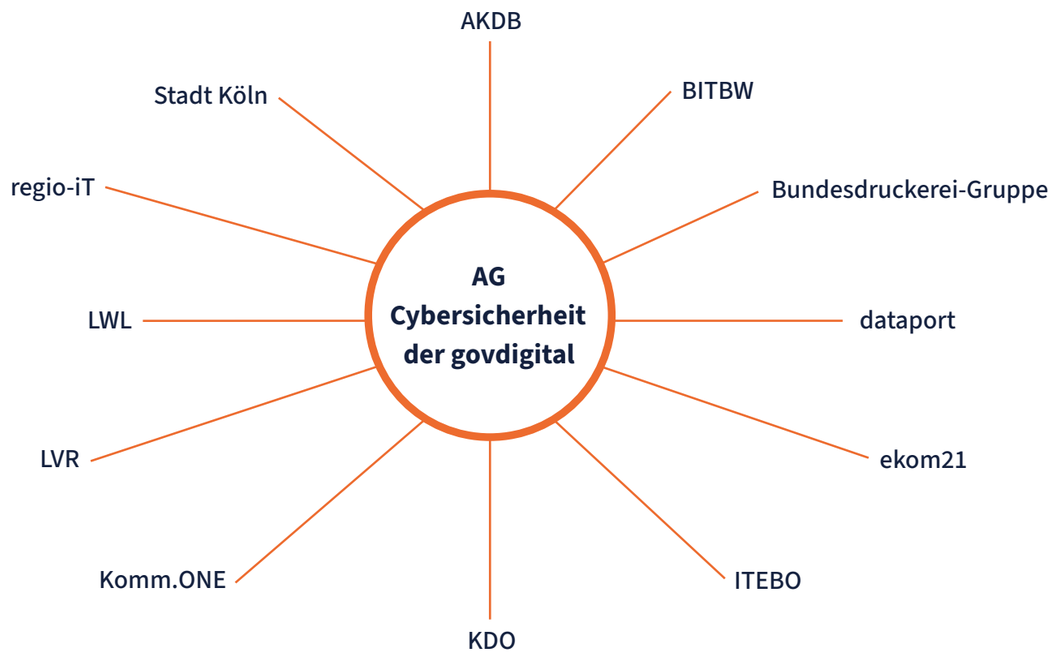
Zugleich zeigt sich, dass anerkannte Standards wie zum Beispiel ISO/IEC 27001, 22301 ihre volle Wirkung erst dann entfalten, wenn sie nicht nur formal eingeführt, sondern im Verwaltungsalltag gelebt werden. Über die kommunalen Austauschplattformen können Interpretationsspielräume geklärt, Musterprozesse geteilt, Audit-Erfahrungen reflektiert und praxistaugliche Umsetzungsansätze entwickelt werden. Der kolle giale Vergleich hilft dabei, normative Anforderungen in realistische, organisatorisch tragfähige Maßnahmen zu übersetzen und damit einen operativen Mehrwert im Alltag zu schaffen. Der Austausch ermöglicht es, von realen Vorfällen zu lernen, ohne sie selbst vollständig durchleben zu müssen.

Der Dachverband kommunaler IT-Dienstleister in NRW (KDN) stellt zu diesem Zweck für seine Mitglieder das „Forum ISB“ (IT Sicherheitsbeauftragte) zur Verfügung. Hier besteht die Möglichkeit, sich untereinander über Sicherheitsthemen und aktuelle Bedrohungen auszutauschen.

Ein weiteres Beispiel für gelingende operative Kooperation ist die Zusammenarbeit der beiden Land schaftsverbände LVR und LWL im Bereich Security Operations Center (SOC). Durch abgestimmte Prozesse, gemeinsame Lagebewertungen und den strukturierten Austausch sicherheitsrelevanter Erkenntnisse ent steht eine belastbare Sicherheitsarchitektur, die über organisatorische Grenzen hinweg wirkt. Gerade im Bereich Monitoring, Analyse sicherheitsrelevanter Ereignisse und Incident Response zeigt sich der Mehrwert arbeitsteiliger Modelle: Expertise kann gebündelt, Reaktionszeiten verkürzt und die Handlungsfähigkeit nachhaltig gestärkt werden. Diese Form der Kooperation ist zugleich eine Antwort auf den zunehmenden Fachkräftemangel. Hochspezialisierte SOC-Kompetenzen lassen sich im Verbund effizienter aufbauen und betreiben als isoliert in einzelnen Organisationen. Damit entsteht nicht nur eine quantitative Entlastung, sondern auch ein qualitativer Zugewinn an Sicherheitsniveau.

Gelungenes Beispiel für kommunale Kooperation

Über die AG Cybersicherheit der govdigital ist der LVR mit anderen Organisationen aus der kommunalen Familie vernetzt. Die Arbeitsgruppen leisten einen wichtigen Beitrag zur gemeinsamen Weiterentwicklung kommunaler Sicherheitsstandards.



Glossar

Business Continuity Management (BCM)
Business Continuity Management (deutsch: betriebliches Kontinuitätsmanagement) ist ein ganzheitlicher Managementprozess, der kritische Geschäftsprozesse bei Störungen oder Notfällen (IT-Ausfall, Katastrophen ...) schützt, aufrechterhält oder schnellstmöglich wiederherstellt. Es sichert die Existenz des Unternehmens durch präventive Strategien, Notfallpläne und regelmäßige Tests.

Botnetz
Ein Botnetz ist eine Gruppe automatisierter Schadprogramme, sogenannter Bots. Die Bots (von englisch „Robot“) laufen auf vernetzten Rechnern, deren Netzwerkanbindung sowie lokale Ressourcen und Daten ihnen, ohne Einverständnis des Eigentümers, zur Verfügung stehen.

Cybercrime
Der Begriff Cyberkriminalität (englisch: Cybercrime) umfasst alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden.

Datenschutz
Mit Datenschutz wird der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet (nicht zu verwechseln mit Datensicherheit).

Datensicherheit
Datensicherheit ist ein häufig mit dem Datenschutz verknüpfter Begriff, der von diesem zu unterscheiden ist. Datensicherheit hat das technische Ziel, Daten jeglicher Art in ausreichendem Maße gegen Verlust, Manipulationen und andere Bedrohungen zu sichern. Hinreichende Datensicherheit ist eine Voraussetzung für einen effektiven Datenschutz.

DDoS-Angriffe
Ein DDoS-Angriff ist eine spezielle Art der Cyberkriminalität. Der Distributed-Denial-of-Service (DDoS)-Angriff ist ein „verteilter“ Denial-of-Service (DoS)-Angriff, der wiederum eine Dienstblockade darstellt. Diese liegt vor, wenn ein angefragter Dienst nicht mehr oder nur noch stark eingeschränkt verfügbar ist. Auslöser ist in den meisten Fällen eine mutwillig herbeigeführte Überlastung der IT-Infrastruktur. Angreifer nutzen diese Art der Cyberkriminalität, um von ungeschützten Organisationen Lösegelder zu erpressen oder um andere kriminelle Handlungen durchzuführen, zu vertuschen oder vorzubereiten.

Deepfakes
Deepfakes (englisches Kofferwort aus den Begriffen „Deep Learning“ und „Fake“) sind realistisch wirkende Medieninhalte (Foto, Audio, Video ...), die durch Techniken der künstlichen Intelligenz abgeändert, erzeugt beziehungsweise verfälscht worden sind.

Deep Packet Inspection
Deep Packet Inspection (DPI) ist eine Art der Datenverarbeitung, bei der die über ein Computernetzwerk gesendeten Daten detailliert untersucht werden. Dabei können Aktionen wie Warnungen, Blockierungen, Umleitungen oder Protokollierungen ausgeführt werden.

Firewall
Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.

Identity und Access Management (IAM)
Unter Identity und Access Management versteht man in der IT alle Aufgaben rund um die Verwaltung von digitalen Identitäten (Identity) und den damit verknüpften Zugriffsrechten (Access).

Informationssicherheits-Management-System (ISMS)
Das ISMS ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Incident Response
Incident Response (deutsch: Reaktion auf Sicherheitsvorfälle) bezeichnet den strukturierten und organisierten Prozess, den ein Unternehmen ergreift, um auf einen Cyberangriff, eine Datenschutzverletzung oder eine schwerwiegende IT-Störung zu reagieren.

Intrusion Detection (IDS) und Intrusion Prevention Systeme (IPS)
Mit einer solchen Software lassen sich Angriffsversuche in einer frühen Phase erkennen, sodass Administrator*innen rechtzeitig alarmiert werden (zum Beispiel durch ein IDS) oder bereits eine automatisierte Reaktion auf den Angriff eingeleitet wird (zum Beispiel durch ein IPS).

ISO 27001
Diese internationale Norm spezifiziert die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufenden Verbesserung eines dokumentierten Informationssicherheits-Management-Systems unter Berücksichtigung des Kontextes einer Organisation.

IT-Sicherheit / IT-Security
IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

IT-Security Awareness:
Der Begriff „Security Awareness“ (englisch für „Sicherheitsbewusstsein“) beschreibt die Sensibilisierung von Mitarbeitenden zu IT-Sicherheit und Datenschutz.

Informationssicherheitsbeauftragter beim LVR
Der Informationssicherheitsbeauftragte ist ganzheitlich für die Belange der Informationssicherheit des LVR verantwortlich. Er arbeitet eng mit den Datenschutzbeauftragten, Personalräten und Prüfinstanzen des LVR zusammen. Er trägt die Verantwortung für die Umsetzung folgender Aufgaben:

- Ausgestaltung und Förderung des gesamten Informationssicherheitsprozesses beim LVR
- Definierung und Fortschreibung LVR-weiter Standards im Handbuch „Datenschutz und Informationssicherheit“
- Koordinierung der Erstellung von Informationssicherheitskonzepten, des Notfallvorsorgekonzepts und anderer Teilkonzepte
- Erstellung des Realisierungsplans für Informationssicherheitsmaßnahmen sowie die Initiierung und Überprüfung der Realisierung
- Sensibilisierung der Mitarbeitenden und Führungskräfte für den verantwortungsvollen Umgang mit Informationstechnik
- Feststellung evtl. auftretender sicherheitsrelevanter Zwischenfälle sowie entsprechende Sicherstellung der Dokumentation, Untersuchung und Einleitung von Gegenmaßnahmen, sowie Berichterstattung an die Behördenleitung
- Zusammenarbeit mit dem CISO von LVR-InfoKom

IT-Sicherheitsvorfall
Ein IT-Sicherheitsvorfall ist ein Ereignis, das die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten, IT-Systemen oder Netzwerken beeinträchtigt.

Leitender Informationssicherheitsbeauftragter (CISO) bei LVR-InfoKom
Der CISO ist zuständig für die Wahrnehmung aller steuernden Belange zur Informationssicherheit. Er trägt die Verantwortung für die Umsetzung folgender Aufgaben:

- Ausgestaltung, Etablierung, Überwachung der Prozesse und Verfahren zur Aufrechterhaltung und Verbesserung der Informationssicherheit bei LVR-InfoKom
- Betrieb und Weiterentwicklung des ISMS von LVR-InfoKom in seiner Gesamtheit
- Aufrechterhaltung der Zertifizierbarkeit des ISMS von LVR-InfoKom nach ISO/IEC 27001
- Koordination der Erstellung, Aktualisierung und Veröffentlichung von Richtlinien und Konzepten zur Informationssicherheit
- Initiierung von Maßnahmen zur Steigerung des Sicherheitsbewusstseins der Mitarbeitenden
- Unterrichtung der Geschäftsführung von LVR-InfoKom (Reporting)
- Leitung des IS-Management und -Lenkungskreises

NIS2-Richtlinie
Die NIS-2-Richtlinie oder zweite Richtlinie zur Sicherung von Netz- und Informationssystemen [ausführlich Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union)] ist eine EU-Richtlinie, die das Niveau der Cyberresilienz in der Union stärken soll.

Perimetersystem
Netzwerke tauschen in unserer Zeit zahllose Daten miteinander. Dabei ist zwischen lokalen beziehungsweise privaten sowie öffentlichen Netzwerken zu unterscheiden. Die Grenzlinie zwischen den Netzwerken trägt die Bezeichnung Perimeter.

Phishing
Das Wort setzt sich aus „Password“ und „Fishing“ zusammen, zu Deutsch „nach Passwörtern angeln“. Beim Phishing wird zum Beispiel mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen.

Proxy
Ein Proxy ist eine Art digitaler Stellvertreter in Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.

Ransomware
Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch: „ransom“) wieder freigeben.

Reputation
Die Reputation des Absenders einer E-Mail ist entscheidend für den Filter und damit für die Frage, ob eine E-Mail durchkommt oder blockiert wird. In die Bewertung der Reputation eines Absenders fließen verschiedene Kennzahlen ein (Reputationsmanagement).

Schadsoftware / Malware
Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computerviren, Würmer und Trojanische Pferde.

SIEM
SIEM steht für „Security Information and Event Management“ (deutsch: Sicherheitsinformations- und Ereignismanagement). Es handelt sich dabei um eine Sicherheitslösung, die Unternehmen dabei unterstützt, Bedrohungen frühzeitig zu erkennen, Sicherheitsvorfälle zu analysieren und entsprechende Maßnahmen zu ergreifen.

Security Operations Center (SOC)
Ein Security Operations Center (SOC) ist eine zentrale Funktion oder ein spezialisiertes Team innerhalb einer Organisation, das die IT-Infrastruktur rund um die Uhr (24/7) überwacht, analysiert und vor Cyberangriffen schützt. Es dient der kontinuierlichen Erkennung, Untersuchung und Abwehr von Sicherheitsbedrohungen, um Schäden zu begrenzen.

Verschlüsselungs-Gateway
Ein Verschlüsselungs-Gateway kontrolliert E-Mails, die an eine Organisation gesendet werden, auf unerwünschte Inhalte und verhindert, dass diese Nachrichten zugestellt werden.

Viren
Klassische Form von Schadsoftware, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich tragen kann. Viren treten in Kombination mit einem Wirt auf, zum Beispiel einem infizierten Dokument oder Programm.

Sie finden diese und weitere Publikationen auch in digitaler Form auf den Internetseiten von LVR-InfoKom unter: www.lvr.de/infokom

Impressum

Herausgeber
LVR-InfoKom und LVR-Dezernat 6

Inhaltlich verantwortlich
Jan Quatram,
Leitender Informationssicherheitsbeauftragter (CISO)
bei LVR-InfoKom

Thomas Eichmüller,
Informationssicherheitsbeauftragter im LVR

Redaktion
Robert Helfenbein,
Kundenmanagement und Kommunikation
bei LVR-InfoKom

Gestaltung
Melina Mertens,
Layout der LVR-Druckerei

Produktion und Druck
LVR-Druckerei,
Inklusionsabteilung
Telefon: 0221 809-2442

Informationsquelle Kapitel I
BSI-Lagebericht zur IT-Sicherheit in Deutschland 2025

Bildnachweise
Titelbild: Annette Hiller-Pahlow, LVR-ZMB
S. 2 oben: Ludolf Dahmen, LVR; unten: Heike Fischer
Sonstige Bilder: Adobe Stock

Kontakt
LVR-InfoKom
Hermann-Pünder-Str. 1
50679 Köln
Telefon: 0221 809-3770
Fax: 0221 809-2165
E-Mail: infokom@lvr.de

www.lvr.de/infokom

Stand 15.5.2026