LVR InfoKom
Das Systemhaus

Qualität für Menschen

IT-Sicherheitsbericht 2024

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 IT-Sicherheitsbeauftragter
im LVR

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

Liebe Leser*innen,

„Das einzig sichere System müsste ausgeschaltet, in einem versiegelten und von Stahlbeton ummantelten Raum und von bewaffneten Schutztruppen umstellt sein."
– Gene Spafford

Mit diesem aus dem Jahr 1989 stammenden Zitat sprach der renommierte US-amerikanische IT-Sicherheitsexperte Gene Spafford ein Thema an, dessen Relevanz inzwischen um ein Vielfaches zugenommen hat: Mit der weltweiten Digitalisierung von Daten stellt sich heute mehr denn je die Frage, ob es IT-Sicherheit überhaupt gibt und was man tun kann, um sich zu schützen.

Die Antwort auf den ersten Teil der Frage lautet: Nein, es gibt keine absolute oder garantierte Sicherheit. Auch noch so gute technische Systeme können keinen 100-prozentigen Schutz vor Cyberangriffen garantieren. Im Gegenteil – stetig spitzt sich die Bedrohungslage weiter zu und die Komplexität steigt, was sich im Detail im jährlichen BSI-Bericht zur Lage der IT-Sicherheit in Deutschland ablesen lässt. Allein angesichts der hierin ausgewiesenen Anzahl an neuen Schadprogramm-Varianten von täglich mehr als 300.000 (!) lautet die entscheidende Frage nicht ob, sondern vielmehr wann man Opfer eines Cyberangriffs wird. (siehe Kap. I)

Cyberangriffe: Die unvermeidbare Realität

Und hiervon gibt es immer mehr in allen Bereichen der Gesellschaft: Wirtschaft, Politik, Behörden und Privatpersonen. Besorgniserregend ist vor allem, dass Angreifer gezielt Schwachstellen in IT-Systemen nutzen, um kritische Infrastrukturen zu stören. Im Jahr 2024 führten Angriffe auf die Varta AG zu erheblichen Betriebsstörungen, die Angriffe auf deutsche Seehäfen, insbesondere den Hamburger Hafen haben massiv zugenommen. Neben Angriffen auf kritische Sektoren wie Rüstung, Energie, Luft- und Raumfahrt gab es auch diverse Angriffe auf politische Parteien und nicht zuletzt auf die Südwestfalen-IT (SIT) in

Nordrhein-Westfalen. Speziell dieser Vorfall führt uns vor Augen, welche katastrophalen Folgen damit verbunden sein können und wie nah die Einschläge auch an den LVR kommen. Insgesamt fielen 160 Fachverfahren aus, rund 1,6 Millionen Bürgerinnen und Bürger waren betroffen. Der Krisenmodus der SIT dauerte insgesamt elf Monate an – erst zum 30.09.2024 konnte die Organisation wieder in den Normalmodus wechseln. Bis zu diesem Stichtag fielen hierfür Zusatzaufwendungen in Höhe von ca. 2,8 Mio. Euro an. Wie wäre der LVR mit dem Ausfall von seinen Fachverfahren und entsprechendem Krisenmodus umgegangen?

Sinnvolle Vorbereitungen: Schlüssel zum Erfolg

Allerdings – und damit kommen wir zum Positiven – kann man sehr wohl eine Menge tun, um sich zu schützen. Eine zunehmend entscheidende Rolle spielt dabei – neben umfassenden technischen und organisatorischen Schutzmaßnahmen – die Vorbereitung auf den Ernstfall, um für den Ausfall der Fachverfahren gewappnet zu sein. Besonders öffentliche Verwaltungen, die auf deren reibungsloses Funktionieren angewiesen sind, sollten der kritischen Bedrohungslage mit einem durchdachten Business Continuity Management (BCM) begegnen. Ziel von BCM ist es, die betriebliche Kontinuität eines Unternehmens in Krisensituationen aufrechtzuerhalten bzw. nach einem Angriff schnellstmöglich wieder in geordnete Strukturen zu gelangen. Im Rahmen von BCM werden die potenziellen Bedrohungen ermittelt und vorbeugend Strategien, Prozesse sowie Maßnahmen entwickelt, mit denen die Ausfallzeiten im Ernstfall minimiert werden können.

Die fortlaufende Verbesserung des Business Continuity Managements (BCM) steht bei LVR-InfoKom nachhaltig im Fokus. Hierfür werden die wichtigsten Geschäftsprozesse des LVR definiert und die jeweils zugrundeliegende Infrastruktur von LVR-InfoKom analysiert und angemessen ertüchtigt. Eine weitere Facette des BCM sind Notfallpläne bzw. Wiederanlaufszenarien, die fortlaufend verifiziert, bei Bedarf modifiziert und regelmäßig erprobt werden. Mehr zum Thema BCM finden Sie im Fokus der zentralen Infografik auf der Seite 9.

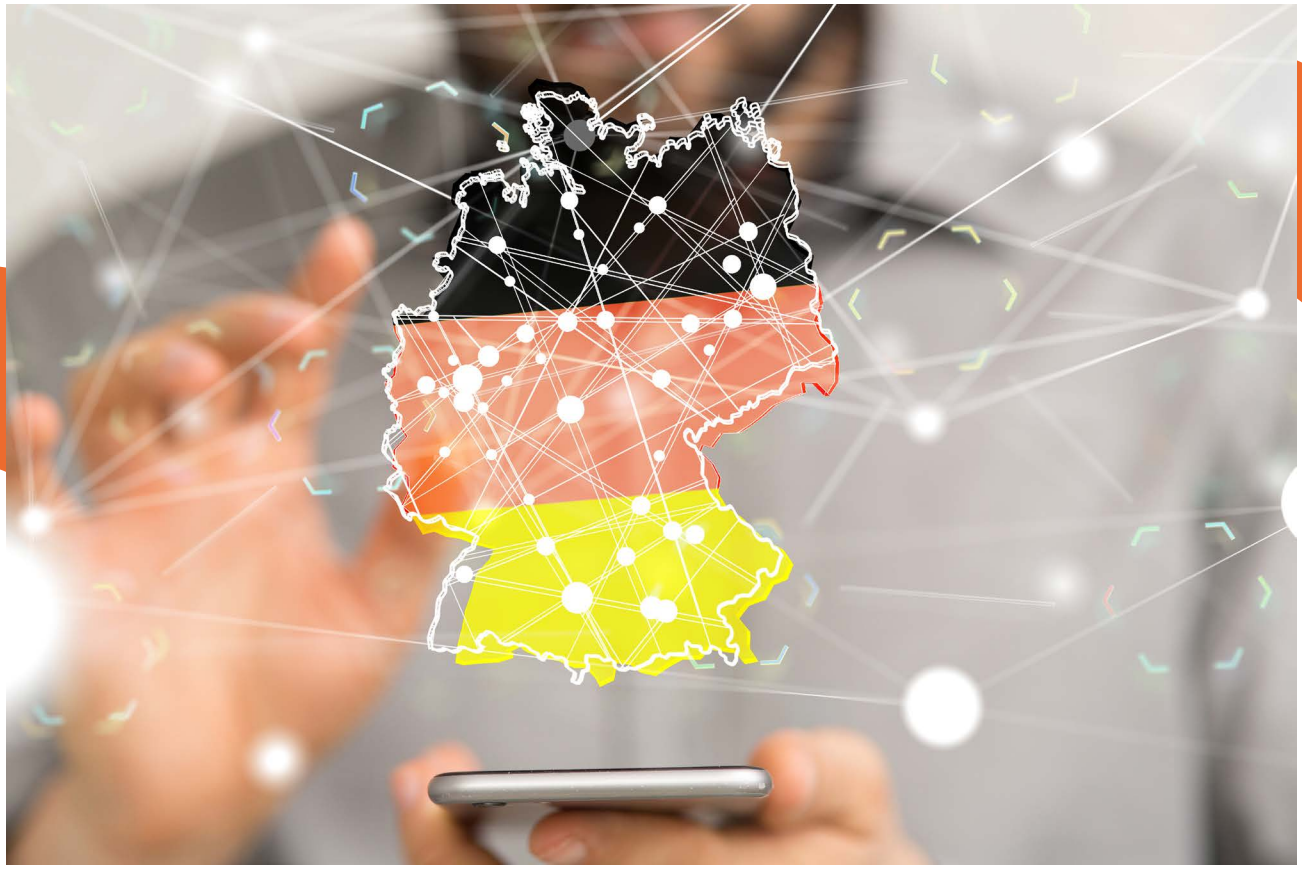
In den übrigen Kapiteln dieser Ausgabe finden Sie wie gewohnt alle wesentlichen Informationen zu den jüngst umgesetzten und zukünftig geplanten Maßnahmen (Kap. III und IV) sowie dem Faktor Mensch im Rahmen der IT-Security (Kap. V und VI).

Liebe Leser*innen, lassen auch Sie sich von diesem Bericht dazu inspirieren, die IT-Sicherheit im Alltag zu leben und mitzugestalten. Der Weg zu optimalem Schutz führt nur über Sie!

Thomas Eichmüller, LVR-Dezernat 6

Jan Quatram, 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. Im Bericht für das Jahr 2024 kommt die Cybersicherheitsbehörde des Bundes zur Einschätzung: Die Lage der IT-Sicherheit in Deutschland war und ist besorgniserregend. So wurden im Berichtszeitraum von Mitte 2023 bis Mitte 2024 täglich durchschnittlich 309.000 neue Schadprogramm-Varianten bekannt – das entspricht einem Anstieg von 26 Prozent im Vergleich zum Vorjahr.

Dabei unterliegt die Bedrohungslage weiterhin einer rasanten Entwicklung. Die digitale Angriffsfläche nimmt stetig zu, Schwachstellen bieten allzu oft gravierende Eingriffsmöglichkeiten und Angreifende finden immer schneller und geschickter Wege, diese auszunutzen.

Die Dimensionen der Cybersicherheitslage

Bedrohungen gingen im vergangenen Berichtszeitraum von diversen Gruppen aus. So zielten Cyberspionage-Angriffe von Advanced Persistant Threat (APT)-Gruppen etwa auf Behörden insbesondere der auswärtigen Angelegenheiten, der Verteidigung sowie der öffentlichen Sicherheit und Ordnung sowie auf Unternehmen und Organisationen, die in diesen Bereichen tätig sind. Auch die arbeitsteilige cyberkriminelle Schattenwirtschaft hat sich weiter professionalisiert: Während einige Gruppierungen zunehmend mit erbeuteten Zugangsdaten handelten (Access Broker), nutzten andere Cybercrime-Gruppen Zero-Day-Schwachstellen zum Datendiebstahl. Immer häufiger wurden diese Daten zu Erpressungszwecken genutzt, ohne zuvor Ransomware, sogenannte Verschlüsselungstrojaner, einzusetzen. Auch menschliches Versagen kann zur Bedrohung werden, wie der CrowdStrike-Vorfall im Juli 2024 gezeigt hat, der durch eine versehentlich fehlerhafte Software ausgelöst wurde und weltweite Folgen im Luftverkehr, Gesundheits- und Bezahlwesen hatte.

Die Angriffsflächen vergrößerten sich weiterhin im Berichtszeitraum, weil mit zunehmender Digitalisierung zugleich die Zahl komplexer und verwundbarer Systeme steigt. Neben dem Zuwachs an

täglich bekannt gewordenen Schwachstellen wurde insbesondere eine Vielzahl kritischer Schwachstellen in Firewalls, VPNs und Perimetersystemen bekannt. Gleichzeitig nahmen Angriffe auf Letztgenannte weiterhin deutlich zu. Auffällig verwundbar waren zudem Android-Systeme – insbesondere dann, wenn sie mit veralteten Software-Versionen betrieben wurden, für die zum Teil gar keine Updates mehr verfügbar sind.

Die Gefährdungen im Berichtszeitraum umfassten unterschiedlichste Angriffsarten. Die besonders im ersten Halbjahr 2024 immens gestiegene Zahl der hochvolumigen DDoS-Angriffe war alarmierend und die Schutzmaßnahmen sollten angepasst werden. Ransomware-Angriffe richteten sich massenhaft gegen leichte, weil häufig noch unzureichend geschützte Ziele wie kleine und mittlere Unternehmen und Kommunen. Allein vom Angriff auf die Südwestfalen IT Ende Oktober 2023 waren rund 100 kommunale Kunden mit über 20.000 kommunalen Arbeitsplätzen betroffen. Auch Public-Cloud-Infrastrukturen wurden angegriffen. Die mutmaßlich chinesische und staatlich gelenkte Gruppe Storm-0558 kompromittierte die Verschlüsselung von E-Mail-Accounts. Dies bedeutete eine potenzielle Gefährdung von Millionen Identitätsdaten.

Die Schadwirkungen im Berichtszeitraum waren beträchtlich: Hierzu zählen zum Beispiel die teils monatelangen Ausfallzeiten bei Kommunen durch Ransomware-Angriffe. Ebenfalls hierdurch wurden weltweit 1,1 Milliarden US-Dollar Lösegeld erbeutet, wobei die Dunkelziffer vermutlich sehr viel höher ist. Bemerkenswert ist, dass für erbeutete exfiltrierte Daten im Schnitt fast dreimal so viel gezahlt wurde wie für erbeutete verschlüsselte Daten. Auch die Zahl der mutmaßlichen Opfer von Datenleaks ist im Berichtszeitraum weiter gestiegen. Im zweiten Halbjahr 2023 wies die entsprechende Messzahl kurzzeitig sogar rund die doppelte Menge mutmaßlicher Leak-Opfer im Vergleich zum Referenzjahr 2021 aus.

II. Aktuelle Bewertung der IT-Sicherheit im LVR

Bezogen auf den Berichtszeitraum 2024 ist die Lage der IT-Sicherheit im LVR trotz der angespannten Gesamtlage insgesamt als positiv zu bewerten. Es gab keine nennenswerten IT-Sicherheitsvorfälle. Bezeichnend für das Jahr 2024 ist aber der Anstieg der Bedrohungslage. Im Gegensatz zu 2023 hat der LVR deutlich mehr E-Mails empfangen – so gab es einen Anstieg von 24 Millionen auf 36,5 Millionen. Ein Großteil davon, in Höhe von 24 Millionen, waren E-Mails, die potenzielle Bedrohungen enthielten. Auch bei den direkten Angriffen konnte ein enormer Anstieg festgestellt werden. Waren es im Jahr 2023 noch ca. 120.000 Angriffe monatlich, die durch das Intrusion Prevention System (IPS) entdeckt wurden, ist der Wert 2024 auf das 10-fache angestiegen. Im vergangenen Jahr wurden 1.150.000 Angriffe pro Monat durch das IPS verhindert.

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 Deep Fakes 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 Informations-

sicherheits-Management-Systems (ISMS), welches nach der international anerkannten Standardnorm ISO 27001 zertifiziert ist. Seit der Erstzertifizierung in 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.

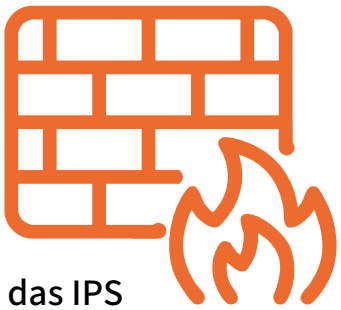
- Zentrale E-Mail-Gateways überprüfen alle eingehenden E-Mails und sorgen dafür, dass die meisten davon erst gar nicht ins LVR-Netz gelangen, weil sie eindeutig entweder unerwünschte Werbung oder Schad-Mails sind. E-Mails, die nicht eindeutig klassifiziert werden können, werden mit einer Markierung versehen, damit sie mit besonderer Vorsicht behandelt werden. In diesem Fall erhält man eine entsprechende Nachricht. Für die sichere E-Mail-Kommunikation werden Verschlüsselungs-Gateways genutzt. 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 sog. 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 inkl. 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 2024

Firewall



ca. 2,03 Petabyte Internet-Traffic
ca. 1.150.000 verhinderte Angriffe pro Monat durch das IPS

Mailing

36,5 Mio. **empfangene** E-Mails 2024 …

… davon

- 21,8 Mio. potenziell bedrohliche E-Mails
- 2,3 Mio. Massen-/Newsletter-E-Mails
- 12,4 Mio. schadfreie E-Mails und davon
- 40.000 S/MIME verschlüsselte E-Mails
- 780.000 digital signierte E-Mails

Alle Angaben sind gerundet.

4,8 Mio. **versendete** E-Mails 2024 …

… davon

- 17.000 S/MIME verschlüsselte E-Mails
- 26.000 an das LVR Sicherheitspostfach aus gesteuerte E-Mails
- 17.000 digital signierte E-Mails

Alle Angaben sind gerundet.

Im Fokus: Business Continuity Management

Im Rahmen von BCM werden die potenziellen Bedrohungen ermittelt und vorbeugend Strategien, Prozesse sowie Maßnahmen entwickelt, mit denen die Geschäftsfähigkeit eines Unternehmens oder einer Organisation im Notfall sichergestellt werden kann.

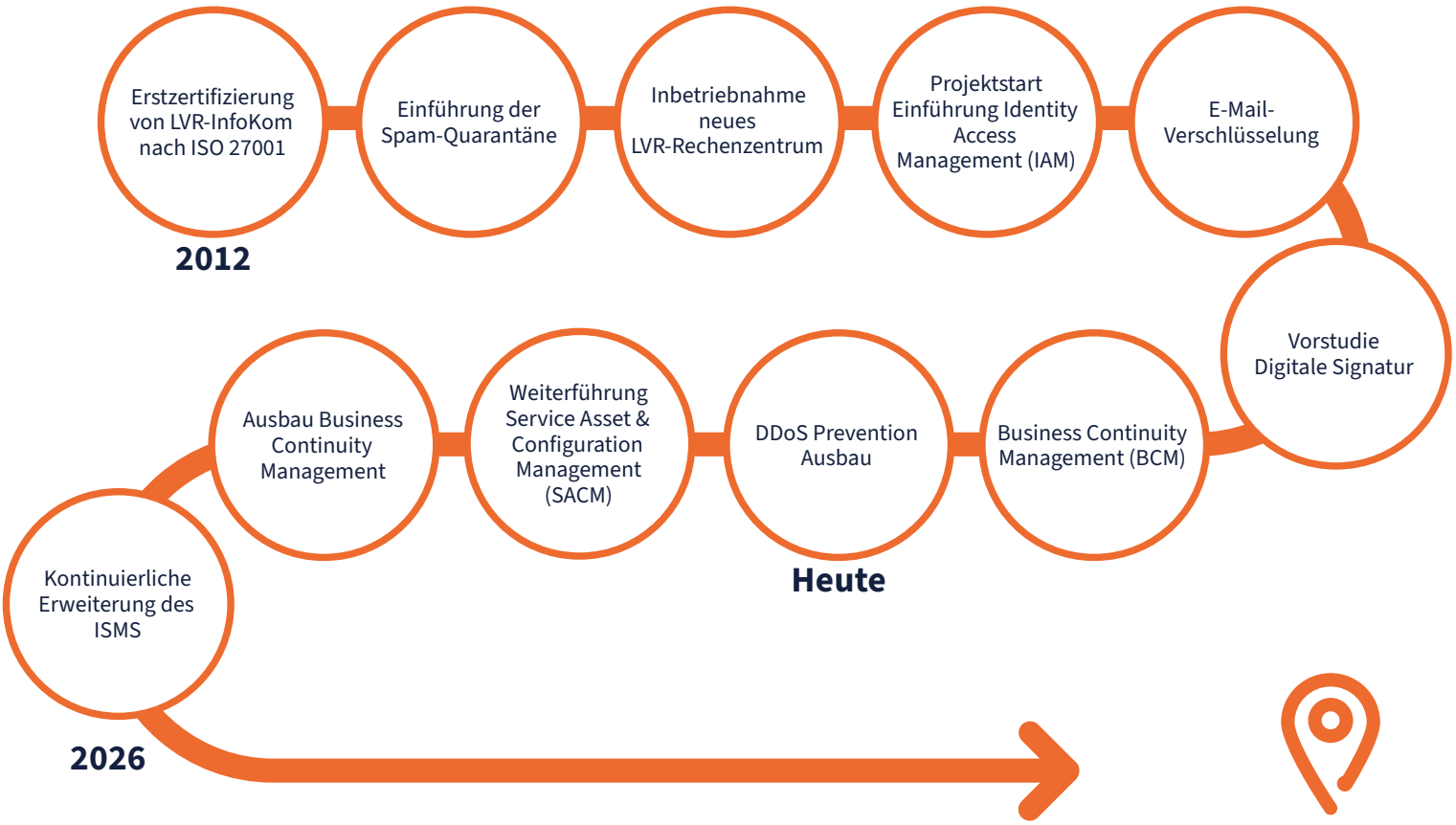
Prinzipiell bezieht sich BCM immer ganzheitlich auf alle Bereiche innerhalb eines Betriebs, die IT-Infrastruktur benötigt aber besondere Aufmerksamkeit. Denn wenn bspw. Server ausfallen, ist in vielen Fällen der komplette Betrieb beeinträchtigt.

Ein erfolgreiches BCM sorgt dafür, dass die Ausfallzeiten minimiert werden und die IT rasch wieder funktioniert.

- Verbesserung der Entscheidungsfindung in Krisenzeiten
- Verbesserte Bewältigung der wachsenden Bedrohungslandschaft
- Förderung der Präventionskultur
- Kontinuierliche Verbesserung
- Regulative Compliance
- Schutz der Reputation

IT-Sicherheit im LVR als kontinuierlicher Prozess

Ausgewählte Meilensteine im Überblick



III. Spezielle Sicherheitsmaßnahmen im Jahr 2024

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 möchten wir Ihnen einige Beispiele für den Berichtszeitraum 2024 aufzeigen. Das so wichtige Thema „Sensibilisierung der Mitarbeitenden“ wird dabei ausgeklammert und im Kapitel V separat beleuchtet.

Privileged Remote Access (PRA)

Der LVR setzt bei der Leistungserbringung im IT-Umfeld auch auf externe Unterstützung. Dies erhöht den Zugriff von außen auf die internen LVR-Systeme. Diese Zugriffe sind beispielsweise auch bei Wartungsarbeiten durch Hersteller nötig. Sie sind potenzielle Risiken und wurden in der Vergangenheit bei anderen öffentlichen Einrichtungen bereits als Einfallstor genutzt. Aktuell laufen sie über spezielle Tunnel oder die Telearbeitslösung, die eine Kontrolle nur begrenzt möglich machen. Im Jahr 2024 wurde ein Projekt aufgesetzt mit dem Ziel, den Zugang für externe Dienstleister gemäß den Maßgaben des BSI zu reglementieren und zu überwachen.

Schwachstellenmanagement

Das Schwachstellenmanagement wurde weiter optimiert. Im Fokus stand hierbei die Automatisierung der Prozesse. Somit konnte nochmals die Geschwindigkeit bei der Bearbeitung von Schwachstellenmeldungen erhöht werden. Zudem wurde das Controlling optimiert, um den Bearbeitungsstand der Schwachstellentickets abfragen zu können.

Incident Response (IR)

Incident Response ist die strategisch geplante Reaktion einer Organisation nach einem Cyberangriff. Die Reaktion erfolgt nach geplanten Verfahren, die darauf abzielen, den Schaden zu begrenzen. Ein guter Incident-Response-Prozess ist darauf ausgelegt, Bedrohungen frühzeitig zu erkennen, auf Sicherheitsvorfälle schnell und effizient zu reagieren und geeignete Maßnahmen zur Eindämmung, Beseitigung und Wiederherstellung zu ergreifen. Der LVR hat die bestehenden Prozesse optimiert und einen externen Dienstleister für die Unterstützung beauftragt, um für den Fall der Fälle schnell handlungsfähig zu sein.

Rezertifizierung ISO 27001

Anfang Juni 2024 wurde die Rezertifizierung unseres ISMS (Informationssicherheits-Management-System) durch den TÜV-Nord-Cert erfolgreich abgeschlossen. Seit der ersten Zertifizierung im Jahr 2012 konnte LVR-InfoKom damit zum fünften Mal beweisen, dass die Anstrengungen im Bereich der Informationssicherheit nachhaltig sind und den Anforderungen der ISO/IEC 27001 genügen. Im Zuge dessen wurde das aus 59 Mitarbeitenden bestehende Audit-Team in 39 Einzelterminen von zwei Auditoren auf „Herz und Nieren“ geprüft.

Erweiterung SACM

LVR-InfoKom hat mit der Einführung eines ITSM (IT-Service Management) einen Rahmen geschaffen, um die steigenden Erwartungen der Kunden an die Effizienz, Schnelligkeit und Verlässlichkeit bei der Serviceerbringung erfüllen zu können. Einen zentralen Bestandteil des ITSM bildet das Service Asset & Configuration Management, kurz SACM. Das Ziel des SACM-Prozesses ist vor allem die Erstellung einer zentralen Datenbank, in der alle Informationen über das vorhandene Inventar an Hardware und Software hinterlegt und miteinander verknüpft werden, sodass logische Zusammenhänge direkt ohne großen Aufwand ersichtlich sind und eine effizientere Fehleranalyse beim Ausfall einzelner Services ermöglicht wird. Die automatisierte Erfassung von Schwachstellen würde hier den kritischen Faktor Zeit minimieren und den personellen Aufwand optimieren. Eine erste Version dieser Configuration Management Database (CMDB) wurde bereits durch LVR-InfoKom implementiert und in Betrieb genommen. Dabei wurden zunächst insbesondere die Komponenten beschrieben, die in der Breite genutzt werden und die Basis für alle weiteren Komponenten bilden, bspw. Server, Netze und Speichersysteme. Nachdem das Fundament damit gelegt war, startete im Jahr 2024 die schrittweise Erweiterung der CMDB, um durch weitere Professionalisierung und Integration in den Schwachstellenprozess Sicherheitslücken schneller identifizieren zu können.

IAM

Im Rahmen des IAM Folgeprojektes wurde das Identity und Access Management, welches von 2022 bis 2023 konzipiert und bereits in Teilen umgesetzt wurde, weiter fortgeführt. Eine besondere Rolle spielte hierbei nach wie vor die prozessuale Automatisierung innerhalb des Onboarding- und Offboarding- sowie Umzugs-Prozesses von Mitarbeitenden sowie deren Berechtigungen, überwiegend im Rahmen der Active Directory, aber auch im Bereich der SAP-Berechtigungen. Diese Bemühungen werden auch im Jahr 2025 noch fortgeführt bzw. intensiviert, u. a. durch die Anbindung weiterer Fachverfahren an das IAM.

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 auch für die nähere Zukunft weitere Maßnahmen geplant, die gemäß einer zwischen LVR-Dezernat 6 und LVR-InfoKom fortlaufend abgestimmten Security- bzw. Informationssicherheits-Roadmap entwickelt werden.

Auf der Agenda für 2025 steht z. B. die Ausweitung des Informationssicherheits-Management-Systems (ISMS) auf den gesamten LVR. Auch das Business Continuity Management (BCM) und das Service Asset & Configuration Management (SACM) werden weiter ausgebaut. Neue Komponenten müssen beschrieben und weitere Verknüpfungen erstellt werden, damit die zentrale Datenbank vollständiger wird und weitere sicherheitskritische Bereiche erfasst werden. Diese Disziplinen sind genau wie das grundsätzliche ISMS kein einmaliges Projekt, sondern eine dauerhafte Aufgabe. Die kontinuierliche Verbesserung ist der Schlüssel, um auf sich ständig ändernde Schwachstellen und Angriffe reagieren zu können.

Nicht zuletzt werden wir auch 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 etc.), 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:

- **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 etc.), 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 der InfoKom Service Desk (ISD) Ad hoc-Meldungen per E-Mail an alle LVR-Mitarbeitenden, beispielsweise Warnungen, Verhaltenshinweise oder Informationen zu Verfahrensänderungen aufgrund von Sicherheitsmaßnahmen.

- **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. Hierzu gehören spezielle IT-Sicherheitstrainings, die jeder Mitarbeitende in einer E-Learning Plattform absolvieren kann (siehe „Im Fokus“).

- **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 bzw. Auszubildenden, in der großes Augenmerk auch auf den verantwortungsvollen Umgang mit der IT gelegt werden soll.

Im Fokus: IT-Security Awareness

2024 war das erste komplette Jahr, in dem alle Mitarbeitenden des LVR am IT Security-Awareness Training von SoSafe teilgenommen haben. Bis Ende 2024 wurden insgesamt 183.065 Phishing-Si mulations-E-Mails verschickt (im Jahr 2024) und 197.394 E-Learning Module zu den verschiedens ten Themen rund um „IT Sicherheit“ bearbeitet (seit dem Start Ende 2023 bis Ende 2024).

Durch diese Trainings konnten wertvolle Tipps zum sicheren Umgang mit IT-Geräten und sensiblen Daten erlernt sowie Taktiken der potenziellen Angreifenden besser verstanden werden. Das Ziel des Trainings ist, dass die Mitarbeitenden des LVR sich sowohl dienstlich, als auch privat besser vor Gefahren schützen können, die in der heutigen digitalen Zeit leider unumgänglich sind. Im Schnitt wurden 4,2/5 Sterne für das E-Learning und die Phishing-Simulations-E-Mails vergeben, was für eine positive Annahme des Angebots spricht. Nachfolgend sind zwei Rückmeldungen, die uns ge geben wurden:

Phishing-Simulation

„Obwohl ich dachte, dass ich keine verdächtigen E-Mails ‚einfach so‘ öffnen würde, habe ich es gemacht, wie ich es anhand dieses Beispiels anschaulich feststellen musste. Außerdem fand ich sehr gut, dass direkt erklärt wurde, worauf man achten soll bei weiteren möglichen verdäch tigen E-Mails. Vielen Dank!“

E-Learning

„Mir hat das E-Learning wirklich Spaß gemacht, weil auch komplizierte Fachbegriffe einfach erklärt wurden und die Beispiele gut verständlich waren. Ich habe sehr viel gelernt und bin motiviert, die Tipps im beruflichen sowie im privaten Alltag zu befolgen. Die Videos und auch die Übungen waren zudem anschau lich und angenehm gestaltet. Was ich zudem wirklich toll fand, war, dass ich am Ende eines Moduls immer gleich das nächste vorgeschlagen bekommen habe. So musste ich mich nicht lange durchklicken, sondern konnte direkt mit dem nächsten weitermachen. Dankeschön :)“

VI. IT-Sicherheit am Arbeitsplatz

Die folgende Checkliste fasst die wichtigsten Tipps für ein sicherheitsbewusstes Verhalten am digitalen Arbeitsplatz zusammen:

- **E-Mails kritisch prüfen**
  Bei E-Mails von externen Kontakten, aber ebenso 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 12 Zeichen bestehen und Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten.

- **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.

- **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.

- **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.


Username
****
Remember Me
Forgot Password?
LOGIN
REGISTER

Glossar

Active Directory
Active Directory ist ein Verzeichnisdienst, der das Grundgerüst für Windows-Netzwerke bildet und daher in fast allen Unternehmen, Behörden und öffentlichen Einrichtungen verwendet wird. Bei einem Verzeichnisdienst handelt es sich im Wesentlichen um eine Datenbank, welche Informationen über alle Benutzer, Computer und Geräte des Netzwerks speichert.

Advanced Persistant Threat (APT)-Gruppen
Von einem Advanced Persistent Threat (APT) spricht man, wenn ein gut ausgebildeter, typischerweise staatlich gesteuerter Täter ein Netzwerk oder System über einen längeren Zeitraum hinweg gezielt zu Spionage- oder Sabotagezwecken angreift. Der Angreifer kann in das Netzwerk oder System eindringen oder sich dort ausbreiten, um Daten zu sammeln oder zu manipulieren.

Cyberangriff
Ein Cyberangriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen.

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 bzw. 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.

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
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.

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 (z. B. durch ein IDS) oder bereits eine automatisierte Reaktion auf den Angriff eingeleitet wird (z. B. 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“ (engl. für „Sicherheitsbewusstsein“) beschreibt die Sensibilisierung von Mitarbeitenden zu IT-Sicherheit und Datenschutz.

IT-Sicherheitsbeauftragter beim LVR

Der IT-Sicherheitsbeauftragte ist ganzheitlich für die Belange der IT-Sicherheit 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 IT-Sicherheitsprozesses beim LVR
- Definierung und Fortschreibung LVR-weiter Standards
- Koordinierung der Erstellung von IT-Sicherheitskonzepten, des Notfallvorsorgekonzepts und anderer Teilkonzepte
- Erstellung des Realisierungsplans für IT-Sicherheitsmaßnahmen 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

IT-Sicherheitsvorfälle sind dadurch gekennzeichnet, dass es hierfür eine schon vordefinierte Vorgehensweise gibt, z.B. bei Virenbefall auf einem Client-PC – vom Trennen vom Netz bis zur Neuinstallation

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 bei LVR-InfoKom

Onboarding / Offboarding

Das Onboarding umfasst alle Schritte, die erforderlich sind, um einen neuen Mitarbeitenden erfolgreich einzusetzen und produktiv zu machen, während das Offboarding die Trennung eines Mitarbeitenden von einem Unternehmen umfasst.

Perimetersystem
Netzwerke tauschen in unserer Zeit zahllose Daten miteinander. Dabei ist zwischen lokalen bzw. 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 z. B. 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).

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

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

VPN
VPN steht für „Virtual Private Network“ und beschreibt die Möglichkeit, bei der Nutzung öffentlicher Netzwerke eine geschützte Netzwerkverbindung herzustellen.

Zero-Day-Schwachstellen
Als Zero-Day-Schwachstelle bezeichnet man eine Sicherheitslücke in einer Software oder einem System, die von den Entwicklern oder den für die Sicherheit Verantwortlichen noch nicht erkannt wurde. „Zero-Day“ bedeutet, dass die Verantwortlichen null Tage Zeit haben, um die Sicherheitslücke zu schließen, bevor Angreifer sie ausnutzen können.

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

Impressum

Herausgeber
LVR-InfoKom und LVR-Dezernat 6

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

Thomas Eichmüller,
IT-Sicherheitsbeauftragter 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

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

infokom.lvr.de

Stand 19.05.2025