InfoKom
Das Systemhaus des LVR

Wir finden, Software, Computer und Systeme sollten für die Menschen da sein. Also machen wir sie so: IT-Qualität für Menschen.

IT-Sicherheitsbericht 2023

LVR-InfoKom

LVR
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 Informationssicherheitsbeauftragter (ISB)

Liebe Leser*innen,

es waren teils dramatische Schlagzeilen, die im Oktober 2023 nach dem Hackerangriff auf den kommunalen IT-Dienstleister „Südwestfalen IT" (SIT) durch die Medien rollten: „Attacke auf Städte und Gemeinden in NRW" – „Cyberangriff legt Kommunen lahm" – „Zurückgeworfen in die digitale Steinzeit" – „In Südwestfalen ist nichts mehr wie es einmal war" …

So reißerisch manche Überschriften auch klangen, übertrieben war es nicht. Die Dienstleistungen von rund 70 Kommunen, welche ihre digitalen Prozesse über den Zweckverband SIT abwickeln lassen, waren praktisch lahmgelegt worden oder stark eingeschränkt – unterschiedlich in Art, Dauer und Ausmaß. Hunderte Server und mehr als 10.000 PCs in den kommunalen Verwaltungen funktionierten nicht mehr, Ämter mussten schließen und waren selbst per Telefon und E-Mail wochenlang nicht erreichbar. Die Auswirkungen spürten rund 1,7 Millionen Bürger*innen in Südwestfalen, im Ruhrgebiet und südlichen Münsterland unmittelbar. Es konnten u.a. keine Geburts-, Ehe- oder Todesbeurkundungen mehr vorgenommen, keine Pässe oder Führerscheine ausgestellt, keine Aufenthalts- oder Arbeitsgenehmigungen ausgegeben werden. Sozialleistungen oder Elterngeld konnte nur über Umwege und teilweise händisch überwiesen werden. Und umgekehrt konnten die Kommunen nicht auf ihre Finanzsoftware zugreifen, um Steuern und Gebühren einzuziehen. Die Wiederherstellung der Systeme stellte die SIT vor eine beispiellose Herausforderung. Noch im Dezember waren rund 170 Personen mit dem Neuaufbau mehrerer Hundert Server und tausender Clients in den südwestfälischen Kommunen beschäftigt, darunter etliche Unterstützende aus anderen IT-Service Unternehmen. Die Rückkehr in den Normalbetrieb begann rudimentär erst wieder im Januar 2024 und wird sich weit hinziehen.

Wie konnte das nur passieren? Die Antwort auf diese naheliegende Frage liest sich ähnlich wie bei vielen vergleichbaren Ransomware-Angriffen, über die berichtet wird: Kriminellen war es gelungen, in das Serversystem der SIT einzudringen und einen Mechanismus anzustoßen, der gespeicherte Daten verschlüsselt. Sofort wurden die Rechner heruntergefahren, doch für einen erheblichen Teil der Daten und Programme war es zu spät. Vieles war bereits unbrauchbar gemacht worden. Eine kleine Text-Datei aber war nicht verschlüsselt: Darin forderten die Hacker die SIT auf, Lösegeld zu zahlen – dann würden die Daten wieder entschlüsselt. Doch die SIT zahlte nicht – wie es auch das Bundesamt für IT-Sicherheit empfiehlt – mit beschriebenen Folgen.

Laut aktuellem Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (siehe Kap. I) ist dieses Beispiel nur eines von vielen im stetig gefährlicher werdenden Cyberraum. Die anhaltende Digitalisierung und zunehmende Vernetzung vergrößert die Angriffsflächen – und diese werden bei der geringsten Schwäche gnadenlos genutzt. Im Visier der Kriminellen sind dabei alle Bereiche: Wirtschaft, Politik, Behörden und Privatpersonen. Weitere prominente Beispiele aus 2023 waren etliche Motel-One-Kundendaten, die im Darknet veröffentlicht wurden, DDoS-Angriffe auf Flughäfen und Regierungsseiten sowie Hackerangriffe auf die Frankfurter Uniklinik und die Rheinische Post. Auch im LVR haben wir die Auswirkungen einer DDoS-Attacke gespürt, als unsere Online-Informationen ausgerechnet am Tag der Begegnung nur eingeschränkt verfügbar waren.

Es gilt also mehr denn je, dem Thema IT-Sicherheit höchste Aufmerksamkeit zu widmen. Dementsprechend handeln wir zum Schutz der LVR-IT. Mit umfassenden technischen, organisatorischen und personellen Maßnahmen sorgen wir für ein größtmögliches Sicherheitsniveau. Entscheidend ist dabei, dass das Thema IT-Sicherheit beim LVR als fundamentaler Teil der Unternehmensstrategie behandelt und konzeptionell vorangetrieben wird. Ausdruck dessen ist die in Kooperation von LVR-InfoKom und Dezernat 6 entwickelte Security Roadmap als Fahrplan für zukünftige Maßnahmen, um die Schutzaktivitäten immer auf einem aktuellen Stand zu halten. Nur wer auch nach vorne blickt, Gefahren antizipiert und zukünftige Technologien frühzeitig adaptiert, kann kontinuierlich IT-Sicherheit grundlegend gewährleisten und es den Angreifern so schwer wie möglich machen.

Einen Einblick in den aktuellen Stand unseres „Fahrplans" bietet Ihnen die vorliegende Ausgabe des IT-Sicherheitsberichts. Eine wichtige Rolle spielt dabei auch in dieser Ausgabe wieder der Faktor Mensch, u.a. mit einem Fokusbeitrag rund um die große Kampagne zur IT-Security Awareness im LVR, die im Jahr 2023 stattgefunden hat (Kap. V).

Unser Dank an dieser Stelle gilt dem gesamten IT-Sicherheitsteam. Ihre Expertise und ihr Einsatz sind unerlässlich, um die Sicherheitsstandards unseres Unternehmens kontinuierlich zu verbessern.

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 dem Lagebericht zur IT-Sicherheit beschreibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) als nationale Cyber-Sicherheitsbehörde alljährlich die Ursachen und Rahmenbedingungen der bestehenden Sicherheitslage und gibt Auskunft über die im jeweiligen Berichtszeitraum stattgefundenen Cyberangriffe. Im Fokus stehen dabei Angriffe auf Unternehmen, staatliche sowie öffentliche Institutionen und Privatpersonen, aber auch Prävention und Bekämpfung dieser Lagen.

Das BSI hat im Berichtszeitraum täglich rund 250.000 neue Varianten von Schadprogrammen und 21.000 mit Schadsoftware infizierte Systeme registriert. Die Lage ist damit weiter angespannt bis kritisch. Wie schon in den vergangenen Jahren wurde eine hohe Bedrohung durch Cyberkriminalität beobachtet. Digitale Erpressung durch Ransomware blieb hier die Hauptgefahr.

Ausbau cyberkrimineller Schattenwirtschaft

Der Berichtszeitraum war gekennzeichnet durch den weiteren Ausbau einer cyberkriminellen Schattenwirtschaft. Die bereits in den vergangenen Berichtszeiträumen begonnene Ausdifferenzierung der cyberkriminellen „Wertschöpfungskette" von Ransomware-Angriffen wurde im aktuellen Berichtszeitraum durch die Angreifer fortlaufend weiterentwickelt. Vom Zugang in ein Opfernetzwerk über die benötigte Ransomware bis hin zur Unterstützung bei Lösegeldverhandlungen können Angreifer inzwischen Werkzeuge für jeden Schritt eines komplexen Angriffs als Dienstleistung einkaufen. Die Arbeitsteilung unter den cyberkriminellen Anbietern dieser Werkzeuge führt dabei zu einer doppelten Skalierung der Bedrohung: Zum einen können cyberkriminelle Anbieter sich auf einzelne Werkzeuge spezialisieren und diese somit schneller weiterentwickeln und verbessern. Zum anderen können die verbesserten Werkzeuge auf diese Weise auch schneller einer größeren Zahl interessierter Angreifer zur Verfügung gestellt werden. Letztere, die sogenannten Affiliates, spezialisieren sich auf die tatsächliche Durchführung der Ransomware-Angriffe und zahlen von den eingetriebenen Lösegeldern Provisionen an die cyberkriminellen Anbieter der verwendeten Dienstleistungen.

Cyberresilienz

Cyberkriminelle Angreifer gingen im Berichtszeitraum zunehmend den Weg des geringsten Widerstands und wählten verstärkt solche Opfer aus, die ihnen leicht angreifbar erschienen. Nicht mehr die Maximierung des potenziellen Lösegelds stand im Vordergrund, sondern das rationale Kosten-Nutzen-Kalkül. So wurden vermehrt kleine und mittlere Unternehmen sowie Behörden der Landes- und Kommunalverwaltungen, wissenschaftliche Einrichtungen sowie Schulen und Hochschulen Opfer von Ransomware-Angriffen. Cyberresilienz ist daher das Gebot der Stunde.

DDoS-Hacktivismus

Im Kontext des russischen Angriffskriegs gegen die Ukraine kam es im Berichtszeitraum zu einer Reihe prorussischer Hacktivismus-Angriffe in Deutschland. Die Hacktivistengruppen verwendeten dafür ausschließlich Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe), die vornehmlich auf die Verfügbarkeit von Internetdiensten zielen und keinen nachhaltigen Schaden bewirken können wie etwa Ransomware-Angriffe. DDoS-Hacktivismus ist daher im Wesentlichen als Propagandawerkzeug zu werten, welches gesellschaftliche Verunsicherung stiften und das Vertrauen in die Fähigkeit des Staates zum Schutz und zur Versorgung der Bevölkerung unterminieren soll.

Schwachstellen

Im Berichtszeitraum wurden durchschnittlich täglich knapp 70 neue Schwachstellen in Softwareprodukten entdeckt – rund 15 Prozent davon waren kritisch. Cybererpresser nutzten zum Beispiel zwei Schwachstellen in Filesharing-Produkten, um Daten von zahlreichen Betroffenen in Deutschland und der Welt abzugreifen und anschließend mit deren Veröffentlichung zu drohen. Aufgrund der Verbreitung der schwachstellenbehafteten Produkte ist von einer sehr großen Zahl von Betroffenen auszugehen.

II. Aktuelle Bewertung der IT-Sicherheit im LVR

Bezogen auf den Berichtszeitraum 2023 ist die Lage der IT-Sicherheit im LVR trotz der angespannten Gesamtlage insgesamt als positiv zu bewerten. Trotz zahlreicher Angriffsversuche – hervorzuheben sind dabei die drei gezielten DDoS-Angriffe im Februar, Juni und August des Jahres – blieb die LVR-IT vor größeren IT-Sicherheitsvorfällen verschont. Während der erste DDoS-Angriff noch hohe Auswirkungen auf die Verfügbarkeit der Systeme hatte, konnten erste getroffene Maßnahmen die Verfügbarkeit während der folgenden Angriffe signifikant erhöhen. Um diese zukünftig zu steigern, sind weitere IT-Sicherheitsmaßnahmen zum Schutz vor solchen Angriffen geplant.

Weiterhin ist zu beobachten, dass die Anzahl gezielter Phishing-Mails im Berichtszeitraum stark zu genommen hat. Die Phishing-Mails haben dabei sehr an Qualität gewonnen, was eine Identifizierung durch die Mitarbeitenden des LVR zunehmend erschwert. Um auch hier sicherer zu werden, wurde ein Programm zur IT-Security Awareness gestartet (siehe Kap. V).

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 relevanten industrieüblichen Norm 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.
- 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 der LVR-interne Empfänger sie mit besonderer Vorsicht behandelt. In diesem Fall erhält der Empfänger eine entsprechende Nachricht.
- 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.
- Ein sog. Intrusion Detection und Prevention System prüft den internen und externen Netzwerkverkehr auf potenziell schädliche Aktionen und blockiert diese. Außerdem teilt es das Netzwerk in logische Abschnitte, um die Verbreitung von Schädlingen innerhalb des LVR-Netzes zu erschweren.

IT-Sicherheit in Zahlen 2023

IPS

ca. 120.000
verhinderte Angriffe pro Monat durch das IPS

Firewall
ca. 3,22 PetaByte Internet-Traffic

24 Mio.
empfangene E-Mails 2023

davon

13,5 Mio.
potenziell bedrohliche E-Mails

2,5 Mio.
Massen-/Newsletter-Mails

8 Mio.
schadfreie E-Mails und davon
- ca. 30.000 S/MIME verschlüsselte E-Mails
- ca. 590.000 digital signierte E-Mails

5,5 Mio.
versendete E-Mails 2023

und davon

- ca. 14.000 S/MIME verschlüsselte E-Mails
- ca. 18.000 an das LVR-Sicherheitspostfach ausgesteuerte E-Mails
- ca. 31.000 digital signierte E-Mails

Alle Angaben sind gerundet.

IT-Security Awareness

- Informationen im Intranet
- Führungsverantwortung
- Schulungen
- Aktuelle Meldungen
- Erklärvideos
- IT-Sicherheitstraining
  - 78.315 abgeschlossene Module im Jahr 2023
  - 800 Meldungen monatlich bzgl. vermuteter Phishing-Mails
  - 52.000 verschickte Test Phishing-Mails im Jahr 2023
- Gesetze und Vorschriften

IT-Sicherheit im LVR als kontinuierlicher Prozess
– ausgewählte Meilensteine im Überblick

2012
- Erstzertifizierung ISO 27001
- Einführung der Spam-Quarantäne
- Inbetriebnahme neues LVR-Rechenzentrum
- Umsetzung Online-Zugangs-Gesetz
- Projektstart Einführung Identity Access Management (IAM)
- E-Mail-Verschlüsselung
- Digitale Signatur

heute
- Business Continuity Management
- DDoS Prevention Ausbau
- Regelmäßige Security Assessments

2025
- Weiterführung Service Asset & Configuration Management (SACM)

III. Spezielle Sicherheitsmaßnahmen im Jahr 2023

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 2023 aufzeigen. Das so wichtige Thema „Sensibilisierung der Mitarbeitenden“ wird dabei ausgeklammert und im Kapitel V separat beleuchtet.

» Digitale Signatur

Die zunehmende Digitalisierung von Prozessen und Fachverfahren beim LVR macht den Einsatz von elektronischen Signaturen erforderlich. Im Rahmen einer Vorstudie, die bis 2024 abgeschlossen wird, soll der Frage nachgegangen werden, in welchen Leistungssegmenten durch den möglichen Verzicht auf die Schriftformerfordernis Prozesse optimiert und durch eine elektronische Signatur eingesetzt werden können. Alle Ergebnisse müssen im Anschluss hinsichtlich Relevanz, wirtschaftlicher Umsetzbarkeit und Usability bewertet werden, um die passende weitere Vorgehensweise festzulegen.

» Fortführung der KHZG-Projekte

Die im Jahr 2022 begonnenen Projekte im Rahmen der Umsetzung des Krankenhauszukunftsgesetzes (KHZG) wurden auch 2023 fortgeführt. Das Projekt IT-Security Awareness wurde erfolgreich abgeschlossen und kann nun für das IT-Sicherheitstraining der Mitarbeitenden genutzt werden. Auch das Projekt E-Mail-Verschlüsselung konnte erfolgreich abgeschlossen werden und wird bereits flächendeckend eingesetzt. Die einfache Anwendung der E-Mail-Verschlüsselung hat für eine hohe Akzeptanz bei den Mitarbeitenden des LVR gesorgt. Die zusätzliche Netzwerkabsicherung der LVR-Kliniken wurde fortgeführt und kann im Jahr 2024 abgeschlossen werden.

» Erweiterung Schwachstellenmanagement

Im Jahr 2023 wurde ein Schwachstellenmanagement-Tool implementiert, welches die IT-Systeme des LVR auf Schwachstellen scannt. Im nächsten Schritt werden die automatisiert erstellten Ergebnisse mit dem Schwachstellenmanagementprozess verknüpft, um eine dokumentierte Behebung der Schwachstellen zu gewährleisten.

» Business Continuity Management (BCM)

Für LVR-InfoKom ist die Einführung eines formalen BCM ein zentraler Schlüssel, um effektiv auf Notfälle reagieren und den Betrieb der LVR-IT aufrecht erhalten zu können. Vor diesem Hintergrund startete im September ein internes Projekt zur Gestaltung eines entsprechenden Notfallsystems gemäß Anforderungen des internationalen Standards ISO/IEC 27001. Im Mittelpunkt steht dabei die Entwicklung von Notfallplänen für alle zeitkritischen Geschäftsprozesse, die Implementierung von BCM-Prozessen für unsere technischen Services sowie die Etablierung verbindlicher Messpunkte.

» Sichere Administration

Zur Erhöhung der Sicherheit in der IT-Administration wurde der Zugriff auf Infrastruktursysteme weiter reglementiert und die Zugriffsrechte eingeschränkt.

» Cloud Security

In zunehmendem Maße nutzt der LVR Cloud-Angebote. Dies hat zur Folge, dass die „Cloud-Strategie“ mit entsprechenden Security-Maßnahmen unterstützt werden muss. Hier gilt es, bereits bei den Ausschreibungen von Cloud-Diensten die sicherheitstechnischen Anforderungen zu berücksichtigen. Entsprechende Richtlinien dienen dazu, den Rahmen festzulegen, wie Cloud-Dienste sicher genutzt und administriert werden können. Auch der Datenschutz spielt bei der Nutzung solcher Dienste eine wichtige Rolle und wird bei der Ausschreibung bereits berücksichtigt. Zudem bekommt ein sorgfältig durchdachtes Identitäts- und Zugriffsmanagement (IAM) einen höheren Stellenwert, da verlorengegangene Zugangsdaten eine der Hauptursachen für Sicherheitsvorfälle in der Cloud sind. Der Einsatz von Mehrfaktorauthentifizierung ist ein weiterer Baustein zur Absicherung der Nutzung von Clouddiensten.

» E-Mail-Verschlüsselung

Im Rahmen des Krankenhauszukunftsgesetzes (KHZG) wurde für den LVR und die Kliniken das Versenden und Empfangen verschlüsselter E-Mails vereinfacht. Konnten verschlüsselte E-Mails bisher nur über ein zentrales Postfach empfangen werden, haben nun alle Mitarbeitenden die Möglichkeit, verschlüsselte E-Mails aus dem eigenen Postfach heraus zu senden und zu empfangen. Die Mail-Systeme erkennen dabei, welche Art der sicheren Kommunikation im jeweiligen Fall anzuwenden ist, so dass die Verschlüsselung von E-Mails für die Mitarbeitenden einfach zu handhaben ist.

» Identity und Access Management (IAM)

Im Rahmen des IAM-Projektes wurde das Identity und Access Management neu konzeptioniert und umgesetzt. Hierdurch konnte das Onboarding und Offboarding von Mitarbeitenden anhand eines Rechte- und Rollenkonzeptes automatisiert werden. Einhergehend wurde eine neue Lösung für die Mehrfaktorauthentifizierung eingeführt.

IV. Ausblick

Folgt man den Prognosen von IT-Sicherheitsexpert*innen, 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 Roadmap entwickelt werden.

Die Themen der Security Roadmap umfassen z.B. den verbesserten Schutz vor DDoS-Angriffen. Weiterhin stehen Maßnahmen zum Accessmanagement auf der Agenda. Das bestehende Service Asset und Configuration Management (SACM) wird ebenso erweitert, wie unser Business Continuity Management (BCM). Im Rahmen des BCM werden regelmäßig Notfallübungen durchgeführt, um im Falle eines erfolgreichen Angriffs den Schaden zu minimieren. Flankiert werden diese Maßnahmen durch eine kontinuierliche Qualitätssicherung unseres Schwachstellen- und Logmanagements.

Allerdings können auch noch so gute Schutzsysteme nicht sicherstellen, dass jedwede Bedrohung rechtzeitig erkannt wird. Der entscheidende Erfolgsfaktor ist demnach das Sicherheitsbewusstsein (IT-Security Awareness) der Mitarbeitenden, welches wir auch in Zukunft weiter intensiv fördern werden. 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 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

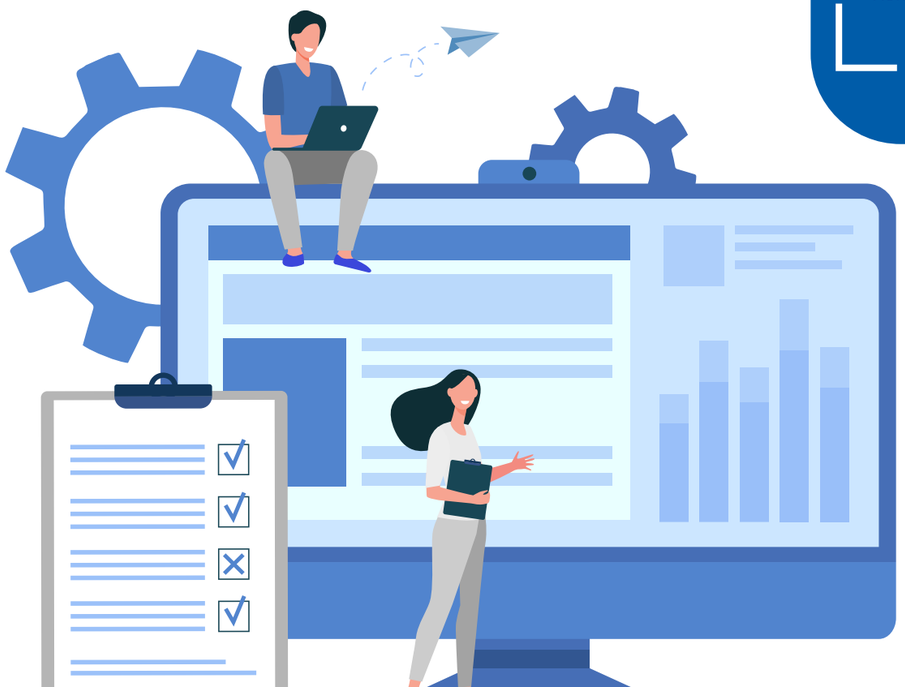
LVR-InfoKom informiert per Intranet-News über relevante IT-Ereignisse. Hierzu gehören auch Nachrichten aus dem Bereich IT-Sicherheit. Zudem versendet der InfoKom Service Desk (ISD) Ad hoc-Meldungen per E-Mail an alle LVR-Mitarbeitenden, beispielsweise Warnungen, Verhaltenshinweise oder Informationen 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. LVR-InfoKom schärft darüber hinaus das Sicherheitsbewusstsein seiner Mitarbeitenden mit weiteren Maßnahmen, weil diese durch ihre Arbeit unmittelbar mit den kritischen Systemen und Anwendungen in Kontakt sind. Hierzu gehören u.a. spezielle IT-Sicherheitstrainings.

» Führungsverantwortung

Eine besondere Verantwortung liegt beim Thema 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 Plattform

Cyberangriffe im privaten wie im beruflichen Kontext nehmen stetig zu. Zur Steigerung der Abwehrfähigkeit gegen solche Angriffe hat der LVR ein IT-Sicherheitstraining für alle Mitarbeitenden eingeführt.

Hierbei stehen drei Ziele im Fokus:
- » Erlangung von Transparenz über aktuelle Anfälligkeit für Phishing-Angriffe im LVR
- » Schulung der Mitarbeitenden durch simulierte E-Mail-Phishing-Angriffe
- » Minimierung des Risikos von Cyberangriffen für den LVR durch das IT-Sicherheitstraining

Simulierte Phishing-Angriffe

Das Sicherheitstraining beinhaltet als Kernelement eine Simulation von Phishing-Angriffen durch vorbereitete E-Mails. Pro Monat wird im Durchschnitt pro Mitarbeiter*in eine solche Mail verschickt. Sofern die E-Mail nicht als Phishing-Versuch erkannt wird, öffnet sich eine interaktive Lernseite, auf der erklärt wird, woran der Angriff zu erkennen gewesen wäre.

IT-Sicherheitstraining – die Lernplattform

Ergänzend zu der Phishing-Simulation bietet das IT-Sicherheitstraining eine Lernplattform mit einem speziellen E-Learning-Angebot. Leicht verständliche E-Learning-Module sensibilisieren für die Gefahren im Internet. In einem abschließenden Quiz können die Mitarbeitenden das neu erworbene Wissen testen.

Phishing-Angriffe melden

Die Mitarbeitenden haben jetzt die Möglichkeit über einen „E-Mail-Meldebutton“ alle verdächtigen E-Mails direkt zu melden, so dass passende Gegenmaßnahmen durch LVR-InfoKom sofort eingeleitet werden können.

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 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.

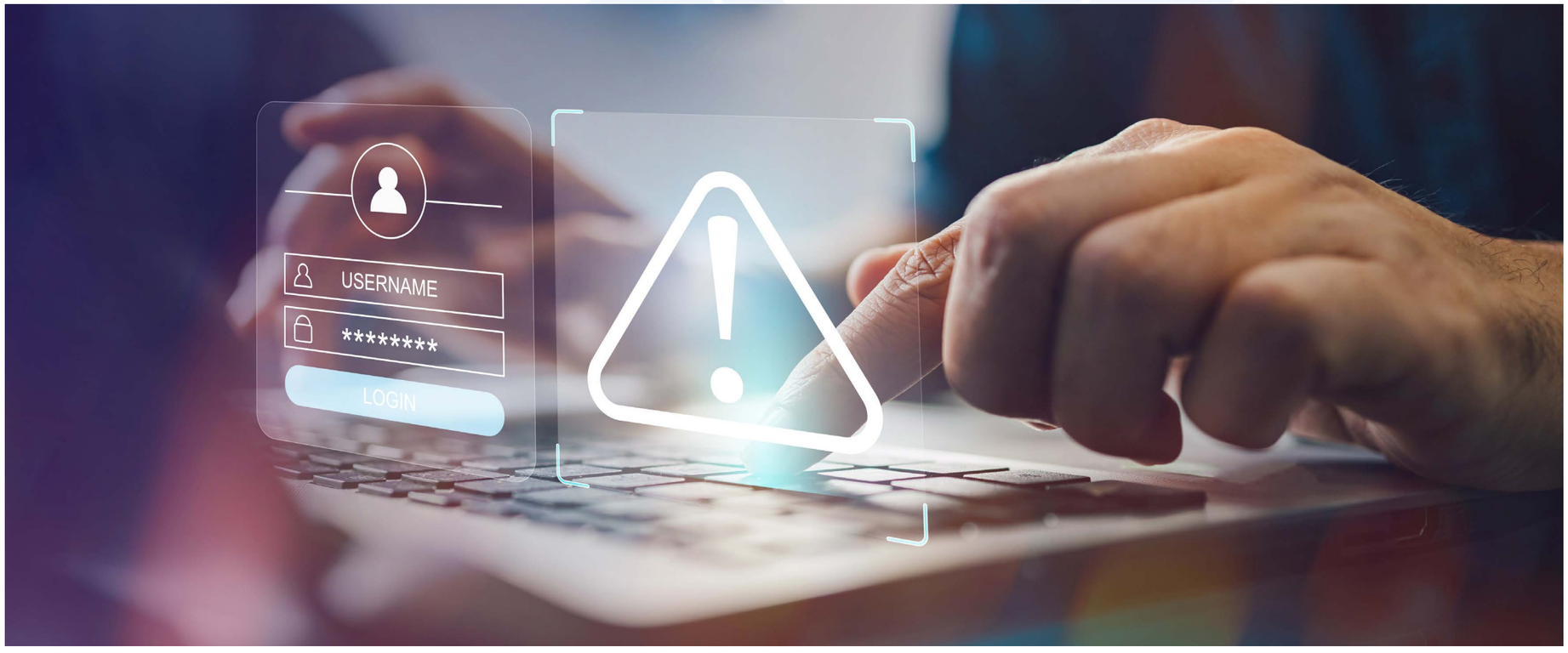
Den Zugriff auf das eigene Gerät sperren, sobald man den Arbeitsplatz verlässt – auch wenn es sich nur um eine kurze Abwesenheit handelt. Keine Wechseldatenträger unbekannter Herkunft an den Arbeitsplatzrechner anschließen. Es besteht die Gefahr einer Infektion mit Schadcode. Keine private Hardware im 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 ggf. 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.



Glossar

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.

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

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

Hacker
Ein Hacker ist eine Person, die illegal in fremde Rechnersysteme eindringt.

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.

Informationssicherheitsbeauftragter (ISB) bei LVR-InfoKom
Der ISB 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

Intrusion Detection und Intrusion Prevention Systeme (IDS/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 kümmert sich um die Belange der IT-Sicherheit des LVR. 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 im Handbuch „Datenschutz und IT-Sicherheit"
- 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 ISB

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

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 Trojaner.

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.

Impressum

Herausgeber
LVR-InfoKom und LVR-Dezernat 6

Inhaltlich verantwortlich
Jan Quatram,
Informationssicherheits-
beauftragter LVR-InfoKom

Thomas Eichmüller,
IT-Sicherheitsbeauftragter
im LVR

Redaktion
Robert Helfenbein,
Kundenmanagement und
Kommunikation LVR-InfoKom

Gestaltung
Melina Mertens,
Layout der LVR-Druckerei

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

Bildnachweise
Titelbild: Stefan Arendt, LVR-ZMB
S. 4: Ludolf Dahmen, LVR
Grafiken: pixabay, Adobe Stock

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

Stand 16.05.2024

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

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