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 2022

LVR-InfoKom

70 Jahre LVR LWL

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 war das erste Mal, dass in Deutschland wegen eines Hackerangriffs der digitale Katastrophenfall ausgerufen wurde. Der Landkreis Anhalt-Bitterfeld sah sich im Juli 2021 dazu gezwungen, weil seine IT-Systeme durch einen Erpressungstrojaner so nachhaltig lahmgelegt wurden, dass die Ämter arbeitsunfähig waren und bürgernahe Dienstleistungen (Auszahlung von Eltern-, Arbeits- und Sozialgeld, KfZ-Zulassungen u.a.) nicht mehr erbringen konnten. Erst am 2. Februar 2022 hob der Landkreis den Katastrophenfall wieder auf. Zu diesem Zeitpunkt war jedoch die Arbeitsfähigkeit immer noch nicht vollständig wiederhergestellt. Dem Landkreis sind Schätzungen zufolge durch den Angriff rund zwei Millionen Euro Kosten entstanden.

Dieser Cyber-Katastrophenfall in Deutschland war nur eine Frage der Zeit. Jahr für Jahr spitzt sich die angespannte IT-Sicherheitslage immer weiter zu und die Berichte über folgenschwere Cyber-Angriffe sind inzwischen fester Bestandteil der Nachrichtenlage. Prominente Sicherheitsvorfälle im Jahr 2022 auf Unternehmen wie Continental, Nordex oder ISTA sind dabei nur die aus den Nachrichten bekannte Spitze des Eisbergs. Tag für Tag ereignen sich unzählige mehr oder weniger fatale Attacken, befeuert durch die stetig steigende Digitalisierung und wechselnde globale Krisenherde (Pandemie, Ukraine-Krieg etc.). Dass dabei nicht nur große Unternehmen Ziel von Ransomware-Angriffen werden können, zeigen eindrücklich die Auswirkungen in mehreren betroffenen Kommunen, in denen – wie beim Fall in Sachsen-Anhalt – die Verwaltungsprozesse teils über Monate massiv gestört waren. Zeugnis davon geben die beunruhigenden Erkenntnisse aus dem aktuellen Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI), wie Sie in Kapitel I lesen können.

In diesem gefahrvollen Umfeld befindet sich auch die IT des LVR. Das Gefahrenpotenzial ist auch im LVR gegeben. Von den 27 Millionen E-Mails, die den LVR im Jahr 2022 erreichten, waren nur 7 Millionen unbedenklich. Der Rest stellte eine potenzielle Bedrohung (Spam) dar oder enthielt gefährliche Inhalte. Durchschnittlich wurden monatlich rund 240.000 Angriffe abgewehrt, wobei es über 100 verschiedene Angriffstypen gab (siehe Infografik, S. 8–9).

In Anbetracht dieser immensen und stetig wachsenden Bedrohungslage gilt es, diesen Schutz der LVR-IT weiter zu festigen und auszubauen. Denn in diesem Umfeld bedeutet Stillstand nicht nur Rückschritt, sondern echte Gefahr! Nur wer das Thema IT-Sicherheit als kontinuierlichen Prozess begreift, systematisch gestaltet und aktiv vorantreibt, wird das Risiko auf ein größtmögliches Minimum reduzieren können. Auch wenn es keine 100-prozentige Garantie für Sicherheit gibt, sollten wir es Angreifern möglichst schwermachen.

Dass der LVR in eben diesem Sinne handelt, zeigt die aktuelle Ausgabe des IT-Sicherheitsberichts, den wir Ihnen hiermit präsentieren möchten. Hierin finden Sie nicht nur alle wesentlichen Informationen zu den jüngst umgesetzten Maßnahmen (Kapitel III), sondern auch zu den bereits projektierten und zukünftig geplanten Vorhaben (Kapitel IV). Weitere Kapitel widmen sich der Rolle der Anwender*innen im LVR sowie konkreten Tipps für ein sicherheitsbewusstes Verhalten am Arbeitsplatz. Schließlich spielt der Faktor Mensch nach wie vor eine entscheidende Rolle für optimale IT-Sicherheit.

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

Wir wünschen Ihnen eine interessante Lektüre.

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 Cyber-Angriffe. Im Fokus stehen dabei Angriffe auf Unternehmen, staatliche sowie öffentliche Institutionen und Privatpersonen, aber auch Prävention und Bekämpfung dieser Lagen.

Insgesamt spitzte sich im Berichtszeitraum (Juni 2021 bis Mai 2022) die bereits zuvor angespannte Lage weiter zu. Die Bedrohung im Cyber-Raum ist damit so hoch wie nie. Im Berichtszeitraum wurde – wie schon im Vorjahr – eine hohe Bedrohung durch Cybercrime beobachtet. Ransomware blieb die Hauptbedrohung, besonders für Unternehmen. Hinzu kamen verschiedene Bedrohungen im Zusammenhang mit dem russischen Angriffskrieg auf die Ukraine, zum Beispiel durch Hacktivismus, insbesondere mittels Distributed-Denial-of-Service-Angriffen (DDoS-Angriffen), und Kollateralschäden bei Cyber-Sabotage-Angriffen. Sowohl durch Cybercrime als auch durch Cyber-Aktivitäten im Rahmen des Krieges hat es darüber hinaus im Berichtszeitraum Störungen von IT-Lieferketten gegeben. Eine Erhöhung der Resilienz gegenüber Cyber-Angriffen und technischen Störungen ist daher eine Hauptaufgabe für alle beteiligten Akteure in Staat, Wirtschaft und Gesellschaft.

Schadprogramm-Varianten

Die Anzahl neuer Schadprogramme und Malware-Varianten hat im aktuellen Berichtszeitraum um weitere rund 116,6 Millionen zugenommen. Durchschnittlich lag die Zahl der täglich neuen Schadprogramm-Varianten bei ca. 319.000. Die Zunahme fiel laut BSI-Bericht zur Lage der IT-Sicherheit 2022 insgesamt also um 19 Prozent niedriger aus, als noch im vergangenen Berichtszeitraum, der mit außergewöhnlich hohen Zahlen und Durchschnittswerten von 394.000 neuen Malware-Varianten pro Tag auffiel. Der Indikator bleibt trotz dieses leichten Rückgangs dennoch auf sehr hohem Niveau. Zudem waren erhebliche Schwankungen im Jahresverlauf zu verzeichnen. Während im Sommer 2021 täglich ca. 300.000 neue Schadprogramm-Varianten auftauchten, so wurden im Herbst desselben Jahres bereits 436.000 neue Varianten gezählt.

Russischer Angriffskrieg gegen die Ukraine

Bislang gab es in Deutschland im Zusammenhang mit dem Angriffskrieg Russlands gegen die Ukraine eine Ansammlung kleinerer Vorfälle und Hacktivismus-Kampagnen. Eine übergreifende Angriffskampagne gegen deutsche Ziele war nicht ersichtlich. Die Lage im Cyber-Raum von NATO-Partnern war dagegen teilweise angespannt und in der Ukraine teilweise existenzbedrohend kritisch.

Cyber-Erpressung als große Bedrohung

Ransomware blieb die Hauptbedrohung besonders für Unternehmen. Die im vergangenen Berichtszeitraum beobachtete Ausweitung von Erpressungsmethoden im Cyber-Raum hat sich im aktuellen Berichtszeitraum fortgesetzt. Insbesondere das sogenannte Big Game Hunting, also die Erpressung umsatzstarker Unternehmen mit verschlüsselten und exfiltrierten Daten, hat weiter zugenommen. Sowohl die von IT-Sicherheitsdienstleistern berichteten Lösegeld- und Schweigegeld-Zahlungen als auch die Anzahl der Opfer, deren Daten etwa wegen ausbleibender Zahlungen auf Leak-Seiten veröffentlicht wurden, sind weiter gestiegen.

II. Aktuelle Bewertung der IT-Sicherheit im LVR

Bezogen auf den Berichtszeitraum 2022 ist die Lage der IT-Sicherheit im LVR trotz der angespannten Gesamtlage insgesamt als positiv zu bewerten. Trotz zahlreicher Angriffsversuche blieb die LVR-IT vor größeren IT-Sicherheitsvorfällen verschont.

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 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-E-Mails sind. E-Mails, die nicht eindeutig klassifiziert werden können, werden mit einer Markierung versehen, damit LVR-interne Empfangende sie mit besonderer Vorsicht behandeln. In diesem Fall erhält man 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 2022

Firewall

ca. 1,4 PetaByte Internet-Traffic

IPS

ca. 20.000
verhinderte Angriffe pro Monat durch das IPS

27 Mio.
empfangene E-Mails in 2022

17 Mio.
potenziell bedrohliche E-Mails

davon

3 Mio.
Massen-/Newsletter-Mails

7 Mio.
schadfreie E-Mails

Alle Angaben sind gerundet.

10 Jahre TÜV 27001

Nach einjähriger Vorbereitung wurde 2012 das erste Audit des TÜV Süd zur ISO 27001 Zertifizierung des Informationssicherheits-Management-Systems (ISMS) von LVR-InfoKom durchgeführt. Das damals für 16 Bereiche (Assets) und zwei Standorte ausgestellte Zertifikat belegt die Erfüllung der Anforderungen sowohl des Gesetzgebers als auch der Kunden an ein modernes ISMS, wobei der Schwerpunkt auf ganzheitlichen Ansätzen liegt – von der Planung, Steuerung bis zur Umsetzung und dauerhaften Qualitätssicherung aller entsprechenden Sicherheitsmaßnahmen. Informationssicherheit ist eine Gemeinschaftsleistung. Nahezu alle Mitarbeitenden von LVR-InfoKom arbeiten aktiv an der stetigen Verbesserung der Informationssicherheit im Unternehmen.

41 etablierte Richtlinien

ISO 27001

10 unabhängige Zertifizierungsaudits

43 Assets

4 Standorte

233 interne Audits

2922 Verbesserungs-maßnahmen

IT-Sicherheit im LVR als kontinuierlicher Prozess –

ausgewählte Meilensteine im Überblick

2012

- Erst-zertifizierung ISO 27001
- Einführung der Spam-Quarantäne
- Inbetrieb-nahme neues LVR-Rechen-zentrum
- Umsetzung Online-Zugangs-Gesetz

heute

- Projektstart Einführung Identity Access Management (IAM)
- E-Mail-Verschlüssel-ung
- Digitale Signatur
- Business Continuity Management

2025

- Network Access Control

III. Spezielle Sicherheitsmaßnahmen im Jahr 2022

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 2022 aufzeigen. Das so wichtige Thema „Sensibilisierung der Mitarbeitenden" wird dabei ausgeklammert und im folgenden Kapitel separat beleuchtet.

» Mehrfaktorauthentisierung

Die Grid Card als zweiter Faktor für die Authentisierung wurde durch eine neue Softtoken-Lösung ersetzt. Die Grid Card war während der Pandemie eingeführt worden und von vorneherein nur als schnelle Übergangslösung geplant.

» IAM

Das Projekt IAM zur Weiterentwicklung eines einheitlichen Identitäts- und Zugriffsmanagements im LVR wurde 2022 fortgeführt. Ein fachliches und technisches Konzept wurde erstellt und abgenommen. Im ersten Schritt erfolgte die Implementierung und Produktivsetzung einer Basis-Funktionalität für einen Piloten.

» E-Mail-Verschlüsselung

Durch den Einsatz einer neuen Lösung zur E-Mail-Verschlüsselung soll der digitale Kommunikationsweg zwischen dem LVR und externen Partnern, Kunden und Patient*innen weiter ausgebaut und für sensible Daten abgesichert werden. Die Lösung soll nach aktuellem Stand der Technik den Vorgaben bzw. Empfehlungen des BSI entsprechen und EU-DSGVO-konform sein. Der Daten- und Informationsaustausch muss sowohl von externer Seite, als auch durch unsere Mitarbeitenden initialisiert werden können. Zu diesem Zweck wurde im Rahmen des Projektes zur Umsetzung des Krankenhauszukunftsgesetzes (KHZG) im Jahr 2022 eine Lösung zur Verschlüsselung von E-Mails für die Kliniken und Dezernate des LVR ausgeschrieben und 2023 implementiert.

» Anschluss an das Netz des Bundes (NdB)

Im Jahr 2022 wurde der LVR mit einem eigenen Zugang an die Netze des Bundes (NdB) angeschlossen. Bisher erfolgte die Anbindung über das Netz von IT-NRW. Durch den neuen Anschluss können nicht nur wie bisher E-Mails sicher mit anderen öffentlichen Institutionen ausgetauscht werden, sondern auch Fachapplikationen genutzt werden.

» Absicherung der Klinikstandorte

Zur Erhöhung der Sicherheit des LVR-Netzwerks wird im Rahmen des KHZG ein Konzept zur Implementierung einer Netzzugangskontrolle (NAC) sowie von Firewallsystemen (NGFW) in den Standorten der LVR-Kliniken erstellt. Vor dem Hintergrund, dass medizinische Geräte zunehmend vernetzt sind und Zugriffe auf Daten und Ressourcen im internen Netz sowie Internet benötigen, werden die Netze segmentiert. Im Jahr 2022 wurde ein Proof of Concept (Machbarkeitsnachweis) mit einer Klinik begonnen, welches nach Auswertung auf die anderen Standorte übertragen werden soll.

» Wiederaufnahme des BITS

Zu den Aufgaben des Beirats für IT-Sicherheit (BITS) gehört es u. a. IT-Sicherheitsziele und -strategien zu erarbeiten und in IT-Sicherheitsfragen zu beraten. Nach längerer Pause hat der BITS unter Teilnahme des IT-Sicherheitsbeauftragten, des Informationssicherheitsbeauftragten und der Datenschutzbeauftragten des LVR, der Rheinischen Versorgungskassen (RVK) und von LVR-Dezernat 8 seine Tätigkeit im Jahr 2022 wiederaufgenommen. Hier konnte die neue Richtlinie „Schutz vor Schadsoftware" vorgestellt und verabschiedet werden.

» Maßnahmen im Rahmen des ISMS

Neben der jährlichen Auditierung durch den TÜV-Nord CERT wurde das Informationssicherheits-Management-System (ISMS) einer zusätzlichen freiwilligen Überprüfung durch den TÜV Rheinland unterzogen. Die dabei festgestellten Verbesserungspotenziale, wie die Straffung interner Kommunikations- oder auch Produktionsprozesse, werden nun zeitnah umgesetzt. Sie sind weitere wichtige Faktoren, um den stetig steigenden Herausforderungen im Bereich der Informationssicherheit immer wieder neu begegnen zu können.

Neben dem Betrieb der Rechenzentren und den infrastrukturellen Services wurde der risikobasierende Betrieb von kundengerichteten Services intensiviert. Dabei wurden auch die IT-Services der RVK berücksichtigt. Um unsere Kunden auch bei ihren zukünftigen Aufgabenstellungen unterstützen zu können, wurden hier unter anderem die Sicherheitsanforderungen aus den Regularien VAIT (Versicherungsaufsichtliche Anforderungen an die IT) und DORA (Verordnung des Europäischen Parlaments über die Betriebsstabilität digitaler Systeme des Finanzsektors) adressiert.

» VPN für Mobile Devices

Mit zunehmender Digitalisierung des LVR erhöht sich auch der Einsatz mobiler Geräte in vielen Anwendungsbereichen. Um auch in einem solchen Einsatzszenario die Sicherheit zu gewährleisten, wurde ein Proof of Concept initiiert, um den Zugriff auf Daten im LVR-Netz durch ein VPN-Gateway für mobile Geräte abzusichern.

» Deaktivierung TLS 1.1

Die Übertragung von Daten im Netz des LVR kann durch den Einsatz des Protokolls Transport Layer Security (TLS) abgesichert werden. TLS ist ein Verschlüsselungsprotokoll, welches zur Absicherung der Übertragung von Daten im Internet eingeführt wurde. Es soll den Diebstahl und Missbrauch von Daten verhindern, die bei der Kommunikation zwischen Client und Server ausgetauscht werden. Das als nicht mehr sicher geltende TLS 1.1 wurde in allen Bereichen deaktiviert und durch TLS 1.2 ersetzt.

» Schutz vor Schadsoftware

In der Umgangssprache wird meistens nur das Wort Virus genannt, wenn man an Programme mit schädlichen Wirkungen (Schadsoftware) denkt. Die Fachwelt nennt derartige Programme/Dateien „malicious code" (Schaden verursachende / böswillige Software). Aufgrund der vielfältigen Ausprägungen von Schadsoftware setzt LVR-InfoKom auch sehr vielfältige technische und organisatorische Maßnahmen zum Schutz der betrieblichen Ressourcen des LVR ein. Im Jahr 2022 wurde ein mehrjähriges Projekt zur strategischen Bündelung all dieser Maßnahmen abgeschlossen. Neben den vielfältigen technischen Maßnahmen wurde als Essenz eine neue Richtlinie zum Schutz vor Schadsoftware LVR-weit in Kraft gesetzt.

» Erstellen von Richtlinien für den Umgang mit IoT-Geräten

Bei der Entwicklung von vernetzten Geräten aus dem Bereich IoT (Internet of Things) werden Aspekte der Informationssicherheit typischerweise nicht oder nur nachrangig beachtet. Daher geht von IoT-Geräten eine signifikante Bedrohung der (Netzwerk-) Sicherheit aus. Dazu gehören unter anderem medizinische Geräte, Smart Displays, Brand-, Gas- und andere Warnmelder, Kaffeemaschinen oder Elemente der Gebäudesteuerung wie Kameras und HVAC (Heating, Ventilation and Air Conditioning). Vor dem Hintergrund, dass IoT-Geräte ggf. ohne ausreichende Sicherheitsmaßnahmen im Netzwerk des LVR eingebunden werden könnten, wurden verbindliche Richtlinien für den Einkauf und den Betrieb solcher Geräte von LVR-InfoKom entwickelt und LVR-weit in Kraft gesetzt.

» IT Security Awareness

Neben den technischen Maßnahmen soll auch die Sensibilisierung der Mitarbeitenden weiter vorangetrieben werden. Die Aufmerksamkeit jeder/jedes Einzelnen am Arbeitsplatz ist der entscheidende Faktor für optimale IT-Sicherheit im LVR. Aufbauend auf den Überlegungen des Projektes „Secure Awareness IT" im Rahmen des Krankenhauszukunftsgesetzes (KHZG) wurde eine Plattform für Security Awareness Schulungen der Mitarbeitenden der LVR-Kliniken ausgeschrieben. Weitere Schulungen für LVR-Mitarbeitende werden folgen.

IV. Ausblick

Folgt man den Prognosen von IT-Sicherheitsfachleuten, 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 abgestimmten Security Roadmap entwickelt werden. Hier ein erster Ausblick:

» Digitale Signatur

Die zunehmende Digitalisierung von Prozessen und Fachverfahren beim LVR macht den Einsatz von elektronischen Signaturen erforderlich. Es gibt verschiedene Arten von Signaturen, von E-Mail-Signaturen bis hin zur fortgeschrittenen digitalen Signatur, bei der es sich um eine beweiskräftige Signatur im Rechtssinne handelt, die eine Überprüfung des Unterzeichnenden ermöglicht. Im Rahmen einer Vorstudie sollen bestehende Bedarfe sowie weitere potenzielle Einsatzmöglichkeiten von digitalen Signaturen identifiziert werden. Gleichzeitig soll unter Einbindung externen Sachverstandes der Frage nachgegangen werden, in welchen Leistungssegmenten durch den möglichen Verzicht auf die Schriftformerfordernis ggf. gar keine Signatur mehr erforderlich sein wird. Alle Ergebnisse müssen im Anschluss hinsichtlich Relevanz, wirtschaftliche Umsetzbarkeit und Usability bewertet werden, um die passende weitere Vorgehensweise festzulegen.

» VPN-Zugang für Mobilgeräte

Der 2022 begonnene Proof of Concept wird 2023 weitergeführt und in den IT-Betrieb überführt. Erste LVR-Anwendungen werden dann über VPN zugänglich gemacht. VPN steht für „Virtual Private Network“ und beschreibt die Möglichkeit, eine geschützte Netzwerkverbindung unter Nutzung öffentlicher Netzwerke aufzubauen. VPNs verschlüsseln den Internetverkehr und verschleiern die Online-Identität. Damit erschweren sie es Dritten, Spuren im Internet zu verfolgen und Daten zu stehlen. Die Verschlüsselung findet dabei in Echtzeit statt.

» Fortführung der KHZG-Projekte

Die im Jahr 2022 begonnenen Projekte im Rahmen der Umsetzung des Krankenhauszukunftsgesetzes (KHZG) werden auch 2023 fortgeführt. Das Projekt IT-Security Awareness geht dann online und kann für das Sicherheitstraining der Mitarbeitenden genutzt werden. Mit dem für 2023 geplanten Abschluss des Projektes E-Mail-Verschlüsselung wird zudem zukünftig der Austausch verschlüsselter E-Mails vereinfacht werden.

» Erweiterung Schwachstellenmanagement

Um die etablierten Prozesse zu unterstützen, soll die Automatisierung vorangetrieben werden. Ziel ist es, Schwachstellen noch effizienter zu entdecken und zu behandeln. Auch die Erkenntnisse, die aus der „Log4j“-Schwachstelle gezogen wurden, fließen in die Erweiterung des Schwachstellenmanagements mit ein (s. IT-Sicherheitsbericht 2020/2021). Insbesondere die Prüfung von Codes und Bibliotheken, die in den Produkten externer Hersteller genutzt werden, wird ein wichtiger Bestandteil des Schwachstellenmanagements werden.

» Business Continuity Management (BCM)

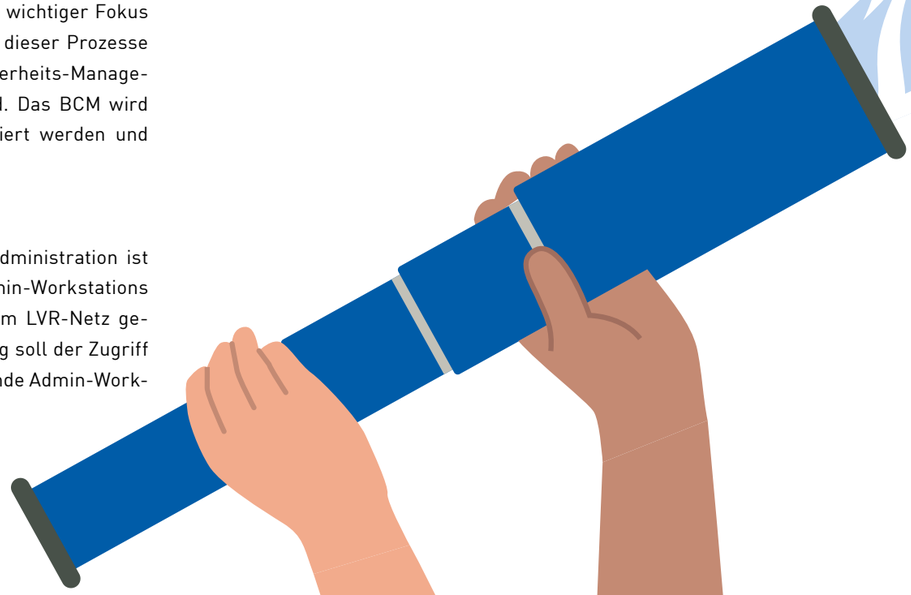
Mit dem BCM stellen Organisationen sicher, dass ihr Geschäftsbetrieb auch im Katastrophenfall fortgeführt werden kann. Es ist ein wesentlicher Prozess innerhalb der ISO-Norm 27001, der Unternehmen dabei hilft, potenzielle Risiken für ihren Betrieb zu erkennen und Strategien zu entwickeln, um die Aufrechterhaltung der Informationssicherheit im Notfall zu gewährleisten. Ein wichtiger Fokus wird im Jahr 2023 auf der Verbesserung dieser Prozesse liegen, die als Teil des Informationssicherheits-Management-Systems (ISMS) implementiert sind. Das BCM wird dann im Juli 2024 vom TÜV Nord auditiert werden und fortlaufend weiter verbessert.

» Sichere Administration

Zur Erhöhung der Sicherheit in der IT-Administration ist eine Weiterentwicklung der virtuellen Admin-Workstations (Arbeitsstationen der Systemverwalter) im LVR-Netz geplant. Durch eine Netzwerksegmentierung soll der Zugriff auf IT-Systeme nur noch über entsprechende Admin-Workstations möglich sein. Diese vAW werden für den Nutzungszweck entsprechend sicher konfiguriert. Auch für die Entwickelnden wird im Projekt „EIK“ eine Workstation speziell für den Anwendungsbereich Entwicklung konzipiert und bereitgestellt.

» 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 in den Verträgen mit den Anbietern die sicherheitstechnischen Anforderungen festzuhalten. Entsprechende Richtlinien dienen dazu, den Rahmen festzulegen, wie Cloud-Dienste sicher genutzt und administriert werden können. Zudem spielt der Datenschutz bei der Nutzung solcher Dienste eine wichtige Rolle und wird bei der Ausschreibung bereits berücksichtigt. Auch ein sorgfältig durchdachtes Identitäts- und Zugriffsmanagement (IAM) bekommt 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 Cloud-Diensten.



V. Der „Faktor Mensch“

– oder die wichtige Rolle der Mitarbeitenden

Noch so gute Schutzsysteme können nicht sicherstellen, dass jedwede Bedrohung rechtzeitig erkannt wird. Dies liegt vor allem an der rasanten Veränderungsgeschwindigkeit von Schadprogrammen. So können bislang unbekannte Viren bis in die E-Mail-Postfächer gelangen und Schaden anrichten, weil sie (noch) nicht von den Virenschutzprogrammen oder Gateways erkannt werden.

Oft beginnt ein Virenvorfall mit einem Doppelklick auf einen schadhaften Anhang. Solch potenziell gefährdendes Verhalten von Mitarbeitenden geschieht in den allermeisten Fällen aus Unachtsamkeit aufgrund mangelnden Wissens um die Gefahren aus dem Netz und die perfiden Vorgehensweisen der Cyberkriminellen. Der entscheidende Erfolgsfaktor ist demnach die Förderung des Sicherheitsbewusstseins (Awareness) der Mitarbeitenden. Nur wenn diese verantwortungsvoll und vorsichtig mit den IT-Ressourcen des LVR umgehen, 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, in Form aktiver Mitgestaltung 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.

In diesem Sinne wurde im LVR auch im aktuellen Berichtszeitraum 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 die „Dienstanweisung Nr. 192 Umgang mit zu schützenden Daten beim Landschaftsverband Rheinland bei automatisierter und nicht automatisierter Datenverarbeitung“ 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 Intranet-Seite zählt auch eine Reihe von Erklärvideos, in denen auf verständliche und pointierte Weise praktische Sicherheitstipps für den Arbeitsalltag gegeben werden.

» Aktuelle Meldungen

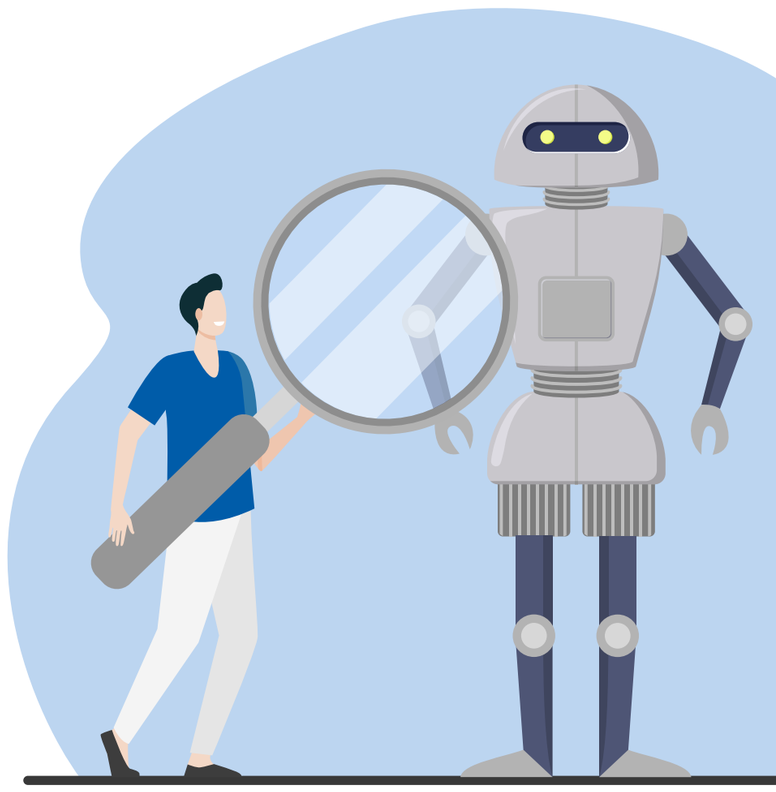
LVR-InfoKom informiert im LVR-Intranet unter „Aktuelles/LVR-News“ über relevante IT-Ereignisse. Hierzu gehören auch Nachrichten aus dem Bereich IT-Sicherheit. Zudem versendet der InfoKom Service Desk (ISD) Ad hoc-Meldungen per E-Mail an alle LVR-Mitarbeitenden, beispielsweise Warnungen, Verhaltenshinweise 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.



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 ist Vorsicht geboten, 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.

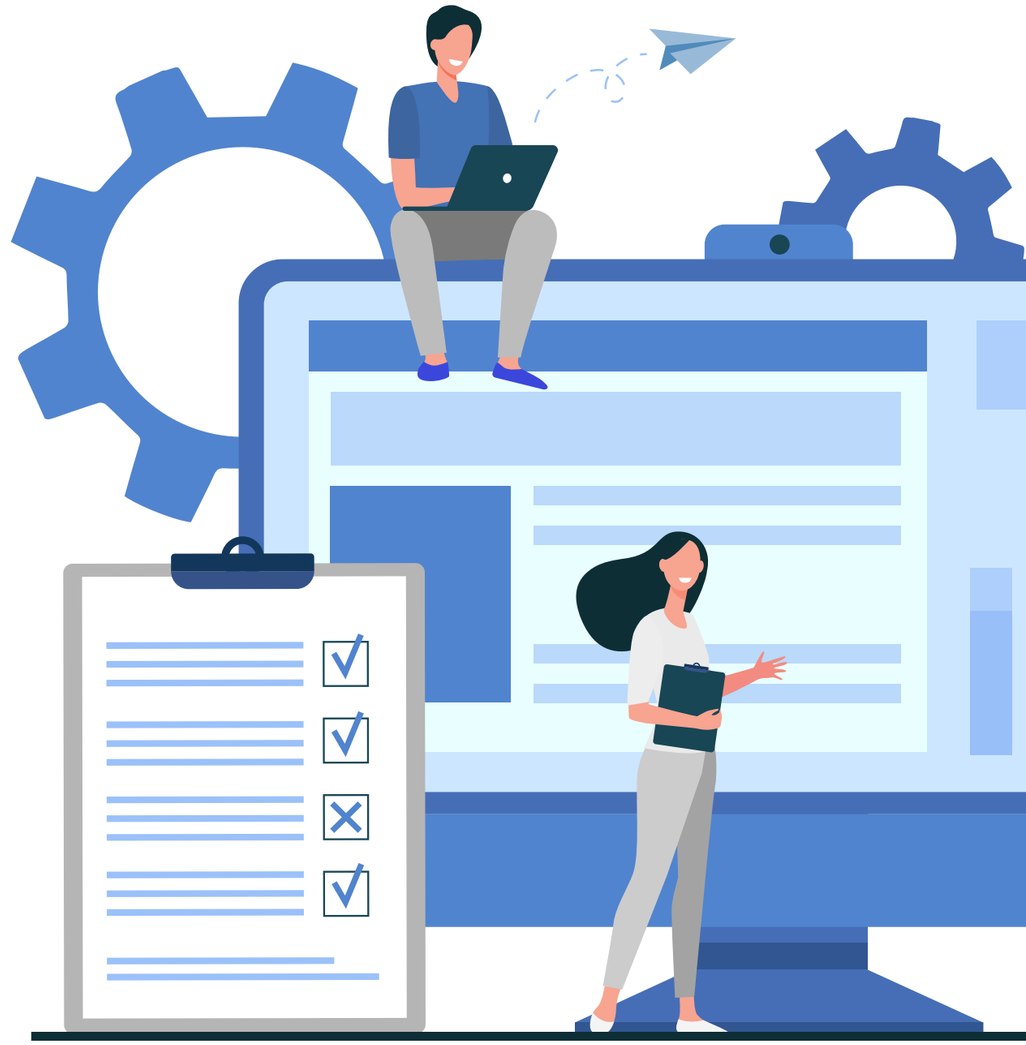
Den Zugriff auf das eigene Gerät sperren, sobald man den Arbeitsplatz verlässt – auch wenn es sich nur um eine kurze Abwesenheit handelt. Keine Wechseldatenträger unbekannter Herkunft an den eigenen Arbeitsplatzrechner anschließen. Es besteht die Gefahr einer Infektion mit Schadsoftware. Keine private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

Cyber-Angriff
Ein Cyber-Angriff 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
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 Cyber-Kriminalität, 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.

Hacktivismus
Ein Hacker ist eine Person, die illegal in fremde Rechnersysteme eindringt. Geschieht dies aus politischen oder sozialen Gründen, spricht man von Hacktivismus.

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)
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
- Betrieb und Weiterentwicklung des ISMS von LVR-InfoKom in seiner Gesamtheit
- Aufrechterhaltung der Zertifizierbarkeit des ISMS von LVR-InfoKom nach ISO 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 (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).

Internet of Things (IoT)
Geräte mit Funktionen aus dem Bereich IoT sind, im Gegensatz zu klassischen Endgeräten, vernetzte Geräte oder Gegenstände, die zusätzliche „smarte" Funktionen besitzen. Dazu gehören unter anderem medizinische Geräte, Smart Displays, Brand-, Gas- und andere Warnmelder, Kaffeemaschinen oder Elemente der Gebäudesteuerung wie Kameras und HVAC (Heating, Ventilation and Air Conditioning).

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

IT-Sicherheit
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-Sicherheitsbeauftragter
Der IT-Sicherheitsbeauftragte kümmert sich um die Belange der IT-Sicherheit des LVR. Er arbeitet eng mit den Datenschutzbeauftragten, Personalrät*innen und Prüfinstanzen des LVR zusammen. Er trägt die Verantwortung für die Umsetzung folgender Aufgaben:

- Ausgestaltung und Förderung des gesamten IT-Sicherheitsprozesses
- 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
- 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 von 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 Trojanische Pferde.

Security Awareness
Engl. für Sicherheitsbewusstsein - das Wissen und die Einstellung, die Mitarbeiter einer Organisation zum Schutz der IT einer Organisation mit allen ihren Werten besitzen.

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
Jasmin Rübel,
Layout der LVR-Druckerei

Barrierefreie Version
Solveig Kemsies,
LVR-Druckerei

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

Bildnachweise
Titelbild u. S. 4 unten:
Stefan Arendt, LVR-ZMB,
S. 4 oben: Thomas Eichmüller
Grafiken: pixabay

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

Stand 31.12.2022

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 **www.infokom.lvr.de**.