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 2020/2021

LVR-InfoKom

LVR
Qualität für Menschen

Im:Fokus

Um Ihnen die Informationen zur IT-Sicherheit im LVR möglichst anschaulich nahezubringen, wollen wir Sie gern mit einem konkreten Praxisbeispiel durch die einzelnen Kapitel begleiten. Für den Berichtszeitraum 2020/2021 nehmen wir dabei die alles beherrschende Pandemie-Situation in den Fokus, welche für alle Lebensbereiche einschneidende Auswirkungen mit sich gebracht hat. Nie zuvor war die Wirtschaft und Gesellschaft in so einem Maße gefordert, möglichst schnell auf die vorherrschenden neuen Rahmenbedingungen zu reagieren.

Dies bedeutete auch eine Verlagerung diverser Lebensbereiche in den digitalen Raum – ein Umstand, welcher zahlreiche neue Gefahren im Hinblick auf IT-Sicherheit mit sich gebracht hat. Auf den nächsten Seiten erfahren Sie, wie im LVR auf diese außergewöhnliche Situation reagiert wurde.

Inhalt

Vorwort

Thomas Eichmüller, LVR-Dezernat 6
Leiter des Fachbereichs 62 (IT-Gesamtsteuerung im LVR) und Sicherheitsbeauftragter der IT im LVR

Jan Quatram, LVR-InfoKom
Leiter der Abteilung Strategie und Projektmanagement und Beauftragter für das Informations-Sicherheits-Management (ISMS)

Liebe Leser*innen,

es begann um drei Uhr nachts am 10. September 2020 – plötzlich fielen 30 Server des Universitätsklinikums Düsseldorf (UKD) aus, die gesamte IT ging in rasantem Tempo in die Knie. Wenige Tage später stellte sich heraus: Das Klinikum war Opfer einer Cyberattacke mit Erpressersoftware geworden, unzählige Daten des Hauses wurden absichtlich verschlüsselt und waren damit nicht mehr verfügbar. Infolgedessen musste sich das Krankenhaus für 13 Tage aufgrund des Ausfalls zentraler Systeme von der Notfallversorgung abmelden. Planbare und ambulante Behandlungen wurden abgesagt bzw. verschoben und die Aufnahme neuer Patient*innen eingestellt. Besonders tragisch: Eine Notfallpatientin starb, weil ein Rettungswagen das Klinikum nicht anfahren konnte und ins 25 Kilometer entfernte Wuppertal ausweichen musste. Erst am 12. Oktober 2020 – und damit mehr als vier Wochen später – kehrte das Klinikum nach eigenen Angaben wieder in den Normalbetrieb zurück.

Dies ist nur eines der drastischen Beispiele, anhand derer uns das BSI in seinem aktuellen Lagebericht zur IT-Sicherheit in Deutschland die nach wie vor äußerst angespannte Bedrohungslage vor Augen führt (s. Kapitel. I). Demnach steigen sowohl die Quantität als auch die Qualität von Cyberangriffen. Zunehmend nehmen Hacker elementare Bereiche unserer Gesellschaft ins Visier und verursachen schwerwiegende IT-Ausfälle in Kommunen, Krankenhäusern und Unternehmen. Sowohl im Bereich der Cyber-Kriminalität als auch in den Bereichen Cyber-Spionage und -Sabotage entwickeln Angreifer ständig neue Methoden und machen sich dabei auch aktuelle Umstände, wie zum Beispiel die Corona-Pandemie oder den Krieg in der Ukraine, zunutze.

Mit anderen Worten: Sicherheit, insbesondere in der Informationstechnologie, ist keineswegs ein Zustand, der konstant andauert, nur weil man bisher nicht im Fokus von entsprechenden Angriffen gewesen ist. Aufgrund des permanenten Wechsels und der Weiterentwicklung ändern sich die Rahmenbedingungen stetig. Sicherheit ist daher ein ständiger und komplexer Prozess, der aktiv gestaltet werden muss. Auch wenn niemand eine 100-prozentige Sicherheit garantieren kann, gilt es, die Daten und Anwendungen effektiv vor Angriffen zu schützen und diesen Schutz kontinuierlich anzupassen.

Genau in diesem Sinne handelt der LVR. Bereits seit zehn Jahren sind der RZ-Betrieb und das Informationssicherheits-Management-System (ISMS) von LVR-InfoKom nach dem internationalen Standard ISO 27001 zertifiziert. Nach der Erstzertifizierung ist das ISMS als Prozess etabliert und wird jährlich durch externe Auditoren geprüft und alle drei Jahre rezertifiziert (s. Kapitel II). Ergänzt wird dieser Grundschutz stetig durch spezielle Maßnahmen, die sich aus jeweils aktuellen Entwicklungen und Erfordernissen ergeben. Hierzu zählen beispielsweise Maßnahmen im Rahmen der Umsetzung des Krankenhauszukunftsgesetzes im LVR-Klinikverbund (s. Kapitel III). Wie eingangs veranschaulicht, stellt insbesondere auch die IT-Sicherheit in Kliniken zurzeit einen wichtigen Aspekt dar.

Eine optimale IT-Sicherheit wird nur erreicht, wenn sie als fundamentaler Teil der Unternehmensstrategie behandelt und konzeptionell weiterentwickelt wird. Mit der Verankerung der Rolle des IT-Sicherheitsbeauftragten im Rahmen der IT-Gesamtsteuerung des LVR-Dezernates 6 fand auch in organisatorischer Hinsicht ein wichtiger Schritt statt. Als zentrale Sicherheitsinstanz sorgt er für die Ausgestaltung und Realisierung von IT-Sicherheitskonzepten und die Förderung des gesamten IT-Sicherheitsprozesses im LVR und arbeitet hierfür u.a. eng mit dem Informationssicherheitsbeauftragen (ISB) von LVR-InfoKom zusammen. Dessen Aufgabe ist es, die Strategie des IT-Sicherheitsbeauftragten durch geeignete Konzepte und Prozesse zur Aufrechterhaltung und Verbesserung der Informationssicherheit zu operationalisieren (eine genauere Rollenbeschreibung finden Sie im Glossar). Gemeinsam wird ein Realisierungsplan für IT-Sicherheitsmaßnahmen sowie zur Erstellung von Richtlinien und Verfahren abgestimmt und umgesetzt.

Symbolisch für diese übergreifende Zusammenarbeit präsentieren wir Ihnen hiermit gemeinsam die neue Ausgabe des IT-Sicherheitsberichts. Hierin finden Sie in kompakter Form wichtige Informationen zur allgemeinen Sicherheitslage, zur Situation beim LVR sowie zu allen wesentlichen Maßnahmen aus dem Berichtszeitraum 2020/2021. Weitere Kapitel widmen sich der Rolle der Anwender*innen im LVR sowie konkreten Tipps für ein sicherheitsbewusstes Verhalten am Arbeitsplatz. Zudem nehmen wir auch in diesem Bericht wieder ein anschauliches Praxisbeispiel in den „Fokus". In diesem Fall geht es naheliegend um die Auswirkungen der Corona-Pandemie auf die IT-Sicherheit im LVR.

In dieser Ausgabe finden sich einige Themen, die bereits eingeführt worden sind bzw. sich aktuell noch in der Implementierung (z. B. ein zentrales Rollen- und Berechtigungs-Werkzeug – Identity Access Management) befinden. In Kooperation zwischen Dezernat 6 und LVR-InfoKom soll perspektivisch eine Security Roadmap entstehen, die zukünftige Technologien für den LVR ankündigt und sukzessive einführt. So sind wir bereits im regen Austausch und evaluieren Optionen zu E-Mail-Verschlüsselung oder der Einführung einer Mehrfaktorauthentifizierung über Software Token im LVR. Weitere Ausführungen finden Sie im Kapitel IV.

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 (Digitalisierung, IT-Steuerung, Mobilität und technische Innovation)

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.

Der aktuelle Lagebericht (1. Juni 2020 bis 31. Mai 2021) macht deutlich: Die erfolgreiche Digitalisierung ist aufgrund der zunehmenden Vernetzung, einer Vielzahl gravierender Schwachstellen in IT-Produkten sowie der Weiterentwicklung und Professionalisierung von Angriffsmethoden zunehmend gefährdet. Wie angespannt und kritisch die IT-Sicherheitslage ist, zeigt die deutliche Beschleunigung der Produktion neuer Schadsoftware-Varianten. Wurden im Berichtszeitraum des Vorjahres noch durchschnittlich 322.000 neue Varianten pro Tag bekannt, so lag der Tagesindikator im aktuellen Berichtszeitraum bei durchschnittlich 394.000 Varianten pro Tag. Das entspricht einem Zuwachs von gut 22 Prozent. Insgesamt haben Angreifer im aktuellen Berichtszeitraum damit rund 144 Millionen neue Varianten produziert.

Das BSI beobachtet zudem die Weiterentwicklung von kriminellen Methoden. So wird bei Ransomware-Angriffen neben der Forderung nach einem Lösegeld immer öfter damit gedroht, zuvor gestohlene Daten zu veröffentlichen. Mit dieser Schweigegelderpressung erhöhen Cyber-Kriminelle den Druck auf Betroffene. Auch Distributed-Denial-of-Service (DDoS)-Angriffe haben im Berichtszeitraum deutlich zugenommen. Sie werden dazu eingesetzt, digital Schutzgeld zu erpressen.

Ebenso die Qualität und die Verbreitung vieler gravierender Schwachstellen in IT-Produkten gibt Anlass zur Sorge. Eine solche wurde beispielsweise in Microsoft-Exchange auf 98 Prozent aller geprüften Systeme festgestellt. Das BSI hatte darauf mit einer Warnung der Stufe Rot reagiert und öffentlich und gezielt die Betroffenen zum Handeln aufgerufen.

Erhöhte Gefahrenlage durch die Covid 19-Pandemie

Aufgrund der massiven Verlagerung diverser Lebensbereiche in den digitalen Raum infolge der Corona-Krise konnte das BSI auch in diesem Zusammenhang zahlreiche neue Gefahren, wie beispielsweise Cyber-Angriffe auf Videokonferenzen, ausmachen. Dies wurde unter anderem durch als Sitzungseinladung gekennzeichnete Phishing-Mails erreicht, welche dann auf gefälschte Websites weiterleiteten.

Ziel der Angreifer ist dabei die Beschaffung von Informationen aus privaten Konferenzen – teilweise mit gravierenden Folgen für die betroffenen Unternehmen, da Inhalte von Videokonferenzen dem Angreifer tiefgreifende Einblicke in interne Prozesse, verwendete Software und vertrauliche Informationen oder Geschäftsgeheimnisse geben können. Nicht selten kann mittels der so gewonnenen Informationen ein weiterer gezielter Cyber-Angriff auf das Unternehmen stattfinden.

Im:Fokus

Die vergangenen zwei Jahre waren maßgeblich durch die Corona-Pandemie gekennzeichnet. Um die Kontakte zu reduzieren, haben die LVR-Mitarbeitenden zunehmend von zu Hause aus gearbeitet und Besprechungen mit mehreren Teilnehmenden sind weitgehend durch Videokonferenzen ersetzt worden. Dass Cyber-Kriminelle schnell auf gesellschaftlich relevante Themen und Trends reagieren, zeigen unterschiedliche Angriffe unter Ausnutzung dieser neuen Situation. So auch beim LVR: Allein zu Beginn der Pandemie sind im Zeitraum 13. bis 17. März 2020 4,6 Millionen E-Mails vom Reputationsfilter des LVR gestoppt worden. Dies entsprach ca. 21 Prozent des Jahresaufkommens 2020.

Glücklicherweise war der LVR zu diesem Zeitpunkt bereits sehr gut aufgestellt. Schon vor der Pandemie gab es ca. 3.600 Zugänge für Heim- und Telearbeit. Viele der hierfür notwendigen Technologien befanden sich längst im Einsatz und mussten lediglich mengenmäßig angepasst werden. Trotzdem wurde in Anbetracht dieser erhöhten Bedrohungslage der Schutz der LVR-Systeme und Mitarbeitenden an vielen Stellen erhöht.

Zusätzliche Risiken birgt auch die infolge der Pandemie stark gestiegene Zahl von Homeoffice-Nutzer*innen: Die hier häufig anzutreffende Nutzung von privaten IT-Geräten wie Computern oder Smartphones stellt für Arbeitgeber und Arbeitnehmer*innen zwar eine komfortable Lösung dar, birgt aufgrund der Verknüpfung dieser meist schwächer gesicherten Geräte mit dem Unternehmensnetzwerk aber auch zahlreiche Gefahren und Einfallstore für Schadsoftware.

Wie die LVR-IT speziell für diese außergewöhnliche Gefahrenlage gewappnet wurde, erfahren Sie Im:Fokus.

II. Aktuelle Bewertung der IT-Sicherheit im LVR

Bezogen auf den Berichtszeitraum 2020/2021 ist die Lage der IT-Sicherheit im LVR trotz der angespannten Gesamtlage insgesamt als positiv zu bewerten. Obwohl es zahlreiche Angriffsversuche gab, blieb die LVR-IT vor größeren IT-Sicherheitsvorfällen verschont.

Im Januar 2020 gab es eine Mitteilung des BSI, dass eine im Dezember gefundene Sicherheitslücke im Citrix Application Delivery Controller – trotz der vom Hersteller empfohlenen und von LVR-InfoKom sofort durchgeführten Abmilderung der Schwachstelle – weiterhin für bestimmte Versionen besteht. Der LVR war hiervon nicht betroffen, da auf den Systemen regelmäßig Updates vorgenommen werden. Um eine Betroffenheit der Systeme auszuschließen, wurden im Nachgang sowohl interne als auch externe Tests durchgeführt. Direkt betroffen war der LVR von einer DDoS-Attacke im Februar 2020. Hier kam es zu einer kurzzeitigen Überlastung der Firewall-Systeme. Dank des schnellen und umsichtigen Handelns der Kolleg*innen konnte größerer Schaden vom LVR abgewendet werden. Indirekt betroffen war der LVR von einem Angriff auf das Universitätsklinikum Düsseldorf, da es eine Verbindung beider Netze gibt. Die Verbindung wurde sofort nach Bekanntwerden des Vorfalls unterbrochen. Es gab somit keinen technischen Schadensfall beim LVR.

Im Jahresverlauf 2021 gab es keine nennenswerten sicherheitsrelevanten Vorfälle, erst mit Bekanntwerden der kritischen Sicherheitslücke „Log4j“ im November 2021 änderte sich dies. Zwar waren hiervon mehrere Systeme und Applikationen betroffen, dank der neuen Prozesse im Schwachstellenmanagement und auch einigem manuellen Aufwand konnte eine Kompromittierung des LVR allerdings erfolgreich verhindert werden.

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 PC‘s, 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 Empfänger*innen 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 2020/2021

Firewall

ca. 12 TB reiner Datenverkehr

Angaben im Durchschnitt pro Monat

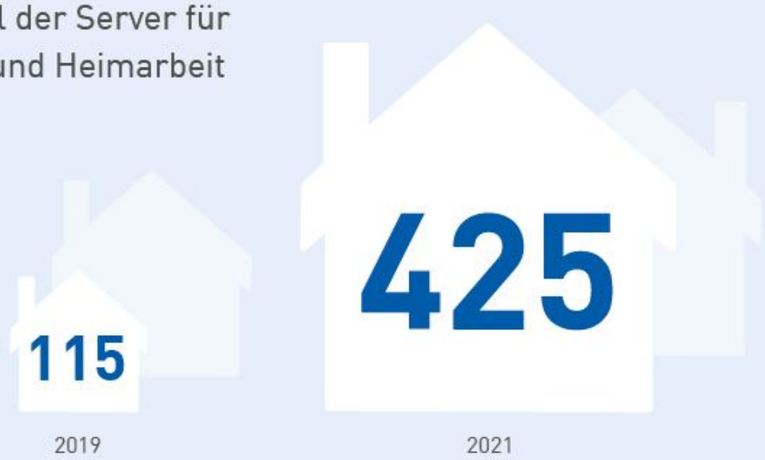
davon **4.360.900** unterbundene Verbindungen

davon **1.306.400** erlaubte Verbindungen

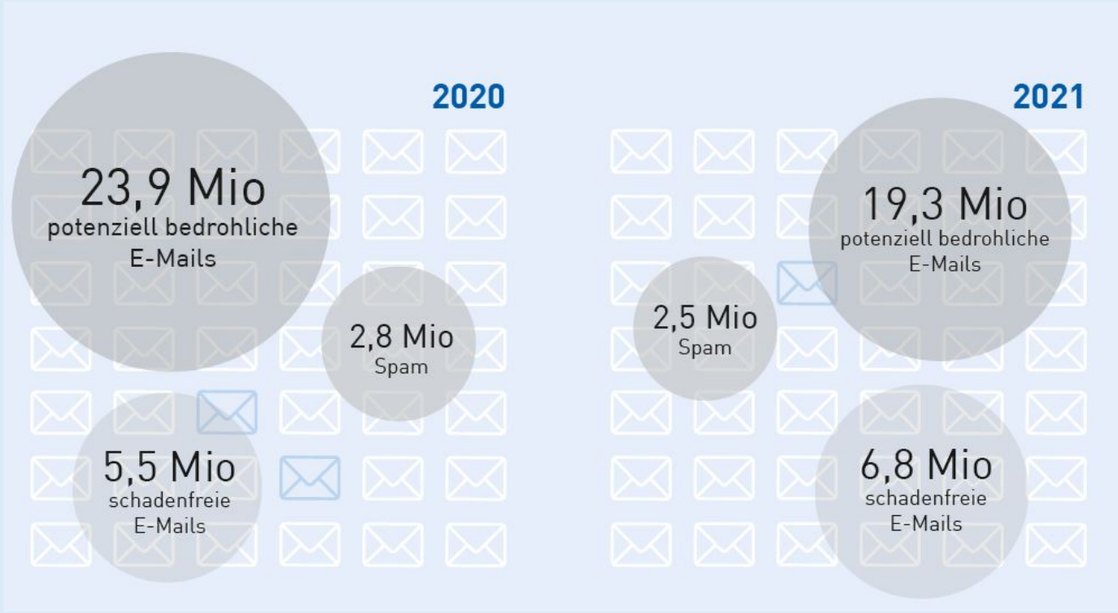
436.000 Verbindungen vorgemerkt
(unter Beobachtung, da potenziell schädlich)

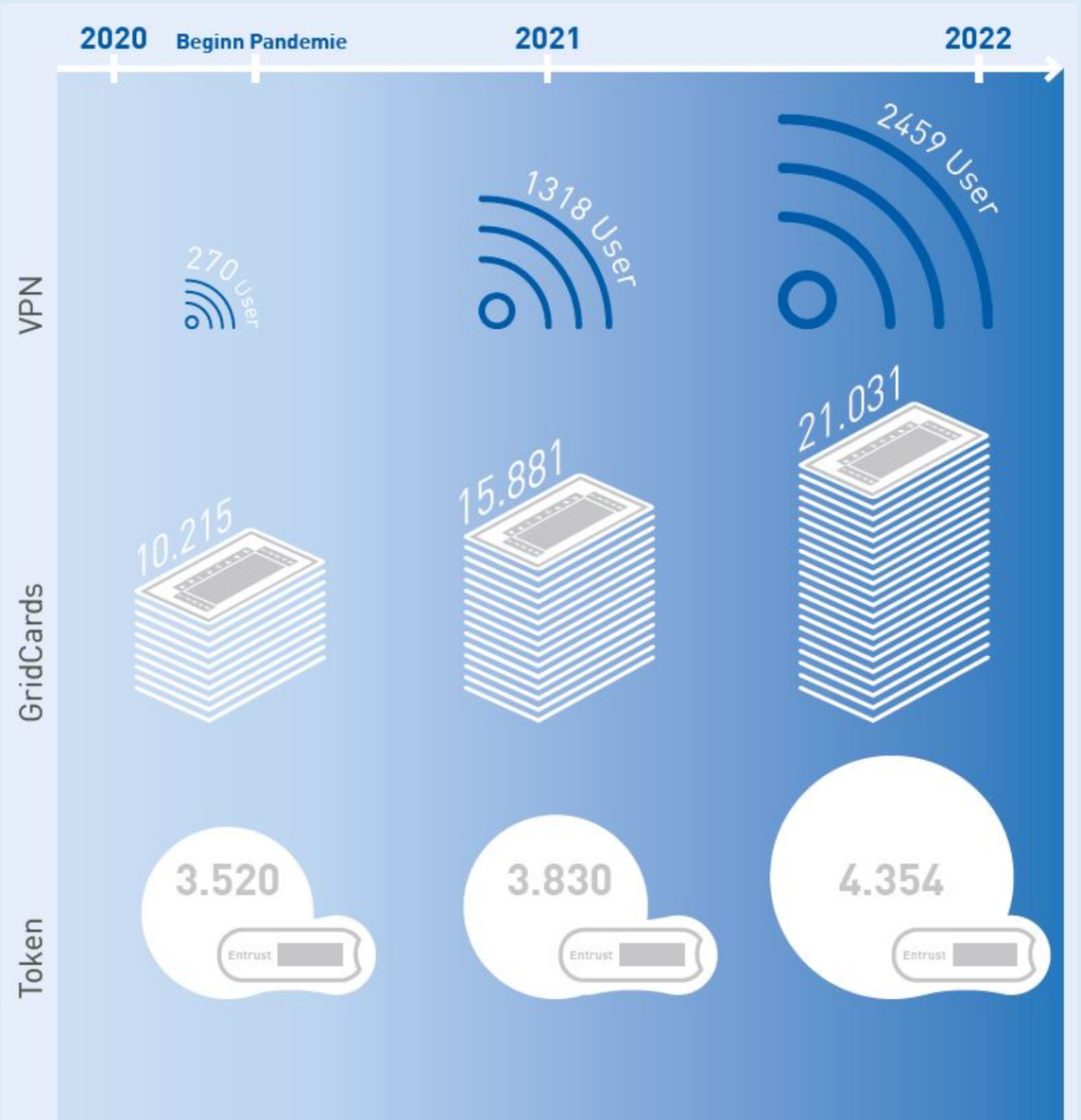
156 unterschiedliche Arten von Angriffen
Durchschnittlich wurden ca. 40.600 Angriffe pro Monat abgewehrt

Anzahl der Server für Tele- und Heimarbeit



Alle Angaben sind teilweise gerundet.





III. Spezielle Sicherheitsmaßnahmen

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 werden einige Beispiele für den Berichtszeitraum 2020/2021 aufgezeigt. Das so wichtige Thema „Sensibilisierung der Mitarbeitenden" wird dabei ausgeklammert und im folgenden Kapitel separat beleuchtet.

2020

» Malware Protection

Nach der 2019 erfolgten Optimierung des Virenschutzes auf den Clients und im Storage-Bereich, standen 2020 die Serversysteme auf der Prüfliste. Auch hier wurden die derzeitigen Schutzmaßnahmen neu bewertet und ggfs. entsprechende Maßnahmen eingeleitet.

» Durchführung von Penetrationstests

Unter einem Penetrationstest versteht man die Prüfung der Sicherheit möglichst aller Systembestandteile und Anwendungen eines Netzwerks oder Softwaresystems mit Mitteln und Methoden, die ein Angreifer anwenden würde, um unautorisiert in das System einzudringen (Penetration). Im Zuge der Anpassung des Regelwerks hat sich auch die Anzahl solcher Tests erhöht.

» Einführung eines ganzheitlichen Identity Access Management (IAM) Systems

Mit einer Vorstudie startete im Sommer 2020 ein groß angelegtes Projekt zur Weiterentwicklung eines einheitlichen Identitäts- und Zugriffsmanagements im LVR. Ziel ist es, die Betriebs- und Datensicherheit bei der Bereitstellung von digitalen Informationen zu erhöhen sowie die Ergonomie durch automatisierte und zentralisierte Berechtigungsprozesse zu steigern. Dies bedeutet neben der Einführung eines IAM-Tools auch die Schaffung eines zentralen Rollenmodells sowie die LVR-weite Weiterentwicklung von Standards, Konzepten, Regelungen und Prozessen. Die Umsetzung erfolgt seit 2021 im Rahmen eines mehrstufigen Realisierungsprojektes.

» Online-Ticketing in den LVR-Museen

Eine wichtige Rolle spielte der Aspekt der Datensicherheit auch im Rahmen der Einführung eines modernen Besuchermanagements in den LVR-Museen. Für die sichere und effiziente Abwicklung der Transaktionen beim Kauf von Online-Tickets wurde ein externer Zahlungsdienstleister eingebunden. Als Schnittstelle zwischen Kunde und den neuen Webshops sorgt dieser für die verschlüsselte Übermittlung der Zahlungsdaten gemäß den gesetzlichen Vorgaben im Online-Handel. Bei den ebenfalls neu beschafften Kassen in den Museumsshops vor Ort hat LVR-InfoKom zudem für eine sichere Anbindung an das LVR-Netz gesorgt.

» SAP Single Sign-On

Im Rahmen des SAP-HANA-Projektes erfolgte Ende 2020 die Umstellung auf „Single-Sign-On". Dies bewirkt, dass sich unsere SAP-Systeme automatisch mit der morgendlichen Windows-Anmeldung authentifizieren und somit keine Passworteingabe in den SAP-Systemen des LVR notwendig ist.

» Einführung Virtueller Admin PC

Die Verwendung virtueller Admin Workstations (kurz: vAWS) zum Administrieren der Systeme in der LVR-Domäne erhöht die IT-Sicherheit des LVR, da hoch privilegierte Accounts nicht mehr in der Standardumgebung verwendet werden. Dadurch erfolgt eine Trennung von Office-Umgebung und administrativer Umgebung. Die vAWS stellen somit eine sichere Plattform zum Administrieren von Systemen dar.

» Telematik-Infrastruktur

Für die LVR-Kliniken begann der Anschluss an die Telematik-Infrastruktur. Hiermit wird ein sicherer Austausch sensibler Daten unter allen Akteuren im Gesundheitswesen wie Praxen, Krankenkassen und Apotheken über gesicherte Verbindungen gewährleistet.

2021

» Funktion des Servicekonto.NRW und Einbindung in den LVR

Das Servicekonto.NRW (SK.NRW) erlaubt es Bürger*innen, Identitätsdaten einmalig zu hinterlegen und dann in allen angeschlossenen Portalen und Online-Angeboten zu nutzen. Anträge können dabei mit den in SK.NRW hinterlegten Identitätsdaten automatisiert vorausgefüllt werden. Weiterhin ermöglicht das SK.NRW, mittels eID-Funktion des Personalausweises/elektr. Aufenthaltstitels der eID-Karte für EU-Ausländer*innen, die Schriftform bei der Nutzung elektr. Formulare zu ersetzen und erlaubt somit, eine Vielzahl von Angeboten online durchzuführen. Dies wird über Vertrauensniveaus (niedrig/normal, substanziell, hoch) gesteuert. Im LVR wird das SK.NRW derzeit im LVR-Beratungskompass eingesetzt. So ist hier die Datenübernahme zwecks Terminanfrage implementiert. In Umsetzung ist die Einbindung der Identifizierung mittels SK.NRW in die elektr. OZG-Antragsprozesse, die mit LIP 3.7 (Lucom) realisiert werden.

» Umsetzung des Online-Zugangsgesetzes

Seit Ende August werden die LVR-OZG-Leistungen über den „Beratungskompass", ein Online-Portal für Rat- und Hilfesuchende sukzessive digital zugänglich gemacht. Dabei werden auch sicherheitsrelevante Aspekte berücksichtigt, unter anderem durch den Einsatz von HTTPS und HTTP 2.0. Im September 2021 wurde das Online-Portal seitens einer externen Prüfstelle einer Sicherheitsüberprüfung in Form eines technischen Penetrationstests auf Anwendungsebene unterzogen. Ziel der Prüfung war die Identifikation von technischen Schwachstellen in der Anwendung. Ergebnis des Tests: Im Rahmen der Untersuchung wurden keine kritischen Schwachstellen gefunden.

» Zugang zum sicheren Behördennetzwerk

Der Bund betreibt ein eigenes abgeschottetes Netzwerk mit dem Namen „Netze des Bundes" (NdB), ehemals D.O.I.-Netz, an welches alle Behörden der Bundesrepublik sich anbinden können. Hierdurch kann jeglicher Datenverkehr, der an andere Behörden geht oder von anderen Behörden kommt, den Weg durch das unsichere Internet umgehen. LVR-InfoKom hat 2021 die entsprechende Beantragung für die Aufnahme in dieses Netz auf den Weg gebracht und strebt die Anbindung 2022 an.

» beBPo – das besondere elektronische Behördenpostfach

Das besondere elektronische Behördenpostfach (beBPo) ist ein Werkzeug, das der sicheren Kommunikation von Behörden oder Körperschaften öffentlichen Rechts dient. Jede Körperschaft öffentlichen Rechts, welche auch Ordnungswidrigkeiten verfolgt, ist gesetzlich verpflichtet, über alle sicheren Übertragungswege erreichbar zu sein und somit auch verpflichtet, ein beBPo zu betreiben. Für alle Dezernate des LVR konnte die Anbindung fristgerecht umgesetzt werden.

» Realisierung eines IAM-Systems

Die 2020 durchgeführte Vorstudie ging 2021 in die nächste Phase. Für die Umsetzung der Konzepte aus der Vorstudie wurde 2021 ein Projekt mit mehreren Phasen zur Realisierung gestartet. Es erfolgte zunächst eine Ausschreibung mit anschließender Umsetzungsphase, die derzeit noch andauert.

Im:Fokus

Die verstärkte Nutzung von Home Office bedeutete für die IT-Sicherheit im LVR vor allem, dass sich der „geschützte Raum" immer mehr in die heimischen vier Wände der Mitarbeitenden verlagert hat. Dadurch ergab sich unter anderem sowohl eine erhöhte Ausgabe von Telearbeitszugängen und Notebooks mit aktuellen Sicherheitsstandards als auch ein verstärkter Rollout der Mehrfaktor-Authentifizierungslösung Grid Card sowie der Ausbau der VPN Gateways. Aufgrund der zeitkritischen Situation mussten Wege gefunden werden, die Bereitstellung der benötigten Arbeitsmittel so weit wie möglich zu beschleunigen. Dabei galt es, eine Ausgewogenheit zwischen Praktikabilität und der Aufrechterhaltung bestehender Sicherheitsstandards zu schaffen.

» Maßnahmen im Rahmen der Umsetzung des Krankenhauszukunftsgesetzes (KHZG) im LVR

» Absicherung der Klinikstandorte

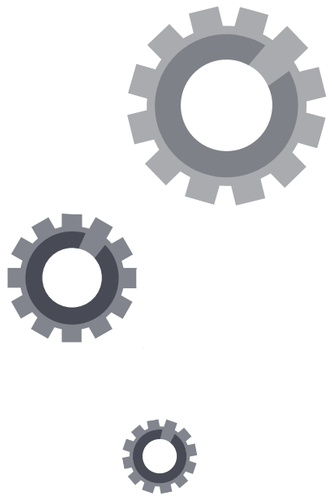
In den LVR-Kliniken werden viele hochsensible Daten von Patientinnen und Patienten verwaltet. Dementsprechend hoch sind die Anforderungen an die IT-Sicherheit. Nachdem zuletzt die Infrastruktur in den LVR-Rechenzentren ertüchtigt wurde, gilt es nun, auch die Außendienststandorte sicherheitstechnisch auf das nächste Level zu heben. Hierzu wurde im Rahmen des KHZG ein Projekt aufgesetzt, in welchem die Netzwerke neu konzeptioniert und abgesichert werden. Zusätzlich wird ein Network Access Controll System geplant.

» Secure Awareness IT

Der sichere Umgang mit IT-Systemen ist ein wichtiger Baustein für die Implementierung von Sicherheitsmaßnahmen. Zur Sensibilisierung der Mitarbeitenden wurde ein Projekt gestartet, welches die bisherigen Maßnahmen in diesem Bereich unterstützt.

» Monitoring kritischer Applikationen

Im Rahmen des Projektes soll das Monitoring der Systeme in den Rechenzentren auf die kritischen Applikationen der Kliniken ausgeweitet werden.



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 abgestimmten Security Roadmap entwickelt werden. Hier ein erster Ausblick:

» Mehrfaktorauthentifizierung

Die Grid Card-Lösung, die in der Pandemie als schnelle Übergangslösung im HomeOffice etabliert wurde, soll perspektivisch nicht als Standardlösung dienen, da es bessere Varianten gibt. Da die Hardware-Token zwar deutlich sicherer, aber auch deutlich teurer sind, soll auch der Einsatz einer Software-Token-Lösung geprüft werden, so dass die Anwendenden bestmöglich auch für das mobile Arbeiten gerüstet sind. Ebenfalls erprobt werden soll ein Unternehmenskonto zur sicheren Authentifizierung für institutionelle Partner.

» IAM

Das in Kapitel III erwähnte Projekt IAM soll auch 2022 fortgeführt werden. Im ersten Schritt wird eine Basis-Funktionalität etabliert, die dann sukzessive ausgebaut wird. Dabei wird auch eine dauerhafte User-ID geprüft, die man auch bei einem Wechsel innerhalb des LVR behalten kann und somit den administrativen Aufwand reduziert.

» Awareness

Neben den technischen Maßnahmen soll auch die Sensibilisierung der Mitarbeiter*innen 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“ wird u.a. ein Schulungskonzept für alle LVR-Mitarbeitenden geplant.

» 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 aktuellen 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.

» Wiederaufnahme des BITS

Zu den Aufgaben des Beirats für IT-Sicherheit (BITS) gehören u. a. IT-Sicherheitsziele und -strategien zu erarbeiten und in IT-Sicherheitsfragen zu beraten. Nach längerer Pause soll der BITS unter Teilnahme des IT-Sicherheitsbeauftragten, des Informationssicherheitsbeauftragten und der Datenschutzbeauftragten des LVR, der RVK und Dezernat 8 wieder aufgenommen werden.

Im:Fokus

Die Mitarbeitenden gelangten durch diese neue Arbeitssituation ebenfalls verstärkt in eine noch verantwortungsvollere Rolle, da der Schutz von personenbezogenen Daten laut DSGVO auch zu Hause gewährleistet werden muss. Mit dem Ausbau der VPN-Umgebung ist nun der Zugriff auf die digitalen Daten unabhängig von Zeit und Ort sicher möglich. Darüber hinaus finden wie auch im Büro die bewährten Verhaltensregeln Anwendung – zum Beispiel das Sperren des Bildschirms, sobald das (Arbeits-)zimmer verlassen wird.

Eine wichtige Aufgabe der nächsten Zeit wird es sein, die Themen in diesem Zusammenhang (noch) genauer zu beleuchten. Ob es sich nun um ausgedruckte Dokumente, den Umgang mit E-Mails, das erhöhte Telefonaufkommen oder weitere Schnittstellen „nach draußen“ handelt. **Denn eines ist sicher: Aspekte wie Flexibilität und Mobilität werden auch weiterhin feste Bestandteile unserer Arbeitswelt darstellen.**

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, durch aktive 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

Jede*r neu eingestellte Mitarbeiter*in 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 – beispielsweise im Hinblick auf den Umgang mit unerwünschten Werbemails oder auch schädlichen Mails.

» Aktuelle Meldungen

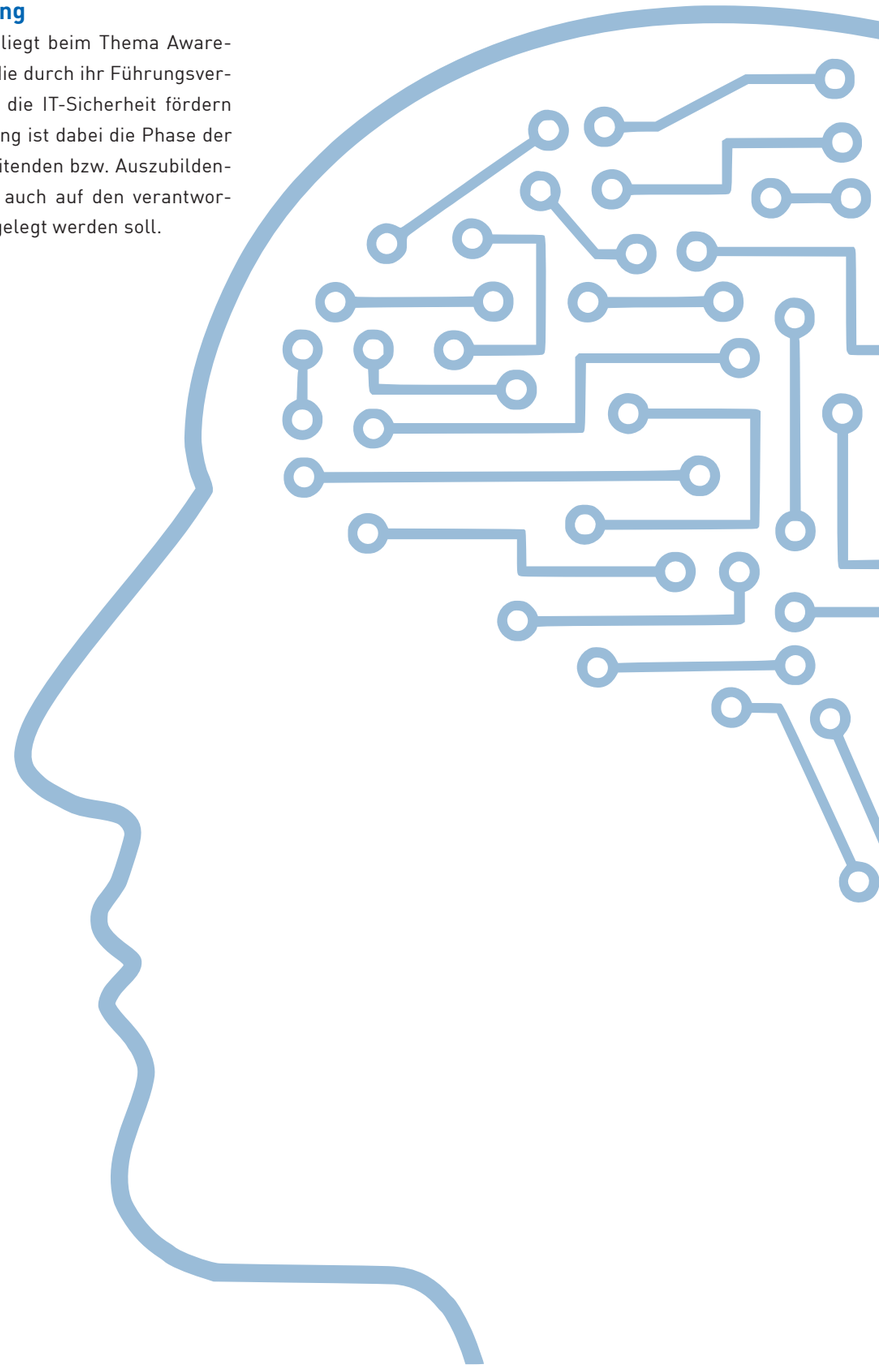
LVR-InfoKom informiert im LVR-Intranet unter „Aktuelles/LVR-News“ über relevante IT-Ereignisse. Hierzu gehören auch Nachrichten aus dem Bereich IT-Sicherheit. Zudem versendet das InfoKom Service Center (ISC) Ad hoc-Meldungen per E-Mail an alle LVR-Mitarbeitenden, beispielsweise Warnungen, Verhaltenshinweise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

» Schulungen

Der LVR bietet den 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, aber auch alternative Methoden wie beispielsweise ein interner Wettbewerb zum Thema IT-Sicherheit.

» 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

Der „Faktor Mensch“ spielt beim Schutz des LVR-Netzes sowie der geschäftlichen Daten eine wichtige Rolle, um Sicherheitsvorfälle zu vermeiden. 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 Sie nicht in die Falle tappen, sollten Sie sich Zeit für den 3-Sekunden-Sicherheits-Check nehmen: Prüfen Sie Absender, Betreff und Anhang vor dem Anklicken.

» Verantwortungsvoller Umgang mit Passwörtern

Notieren Sie Ihre Passwörter keinesfalls auf Zetteln oder Post-its am Monitor, auch nicht an vermeintlich diskreten Stellen wie unter der Tastatur. Tragen Sie Sorge dafür, dass Sie bei der Eingabe Ihres Passworts nicht beobachtet werden. Nutzen Sie für jedes Gerät und jede Anwendung jeweils verschiedene Passwörter und wechseln Sie diese in regelmäßigen Abständen. 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.

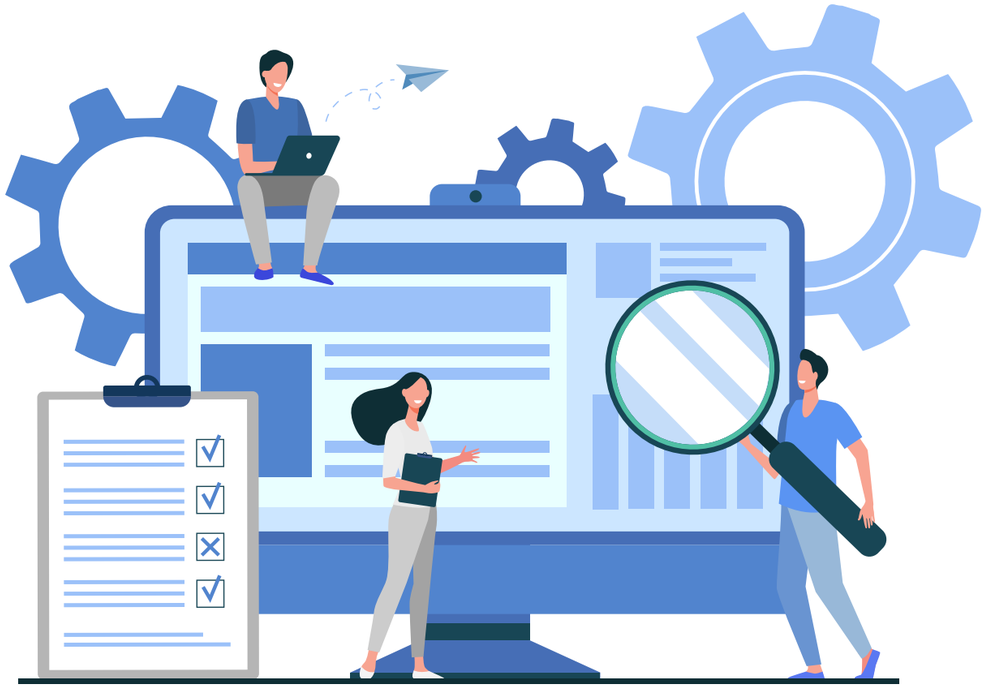
Sperren Sie den Zugriff auf Ihr Gerät, sobald Sie Ihren Arbeitsplatz verlassen – auch wenn es sich nur um eine kurze Abwesenheit handelt. Schließen Sie keine Wechseldatenträger unbekannter Herkunft an Ihren Arbeitsplatzrechner an. Es besteht die Gefahr einer Infektion mit Schadcode. Setzen Sie keine private Hardware im LVR-Netz ein und speichern Sie keine Unternehmensdaten auf privaten Datenträgern. Nutzen Sie nur die offiziell freigegebene Software auf Ihren Arbeitsgeräten. Geben Sie auf USB-Sticks mit Arbeitsdokumenten acht und schützen Sie diese ggf. ebenfalls mit einem Passwort.

» Sichere Internetnutzung

Das Internet ist ausschließlich dienstlich zu nutzen. Durch eine achtsame und verantwortungsbewusste Internetnutzung können Sie die Gefahr einer Schadsoftware-Infektion Ihres Systems oder womöglich sogar des gesamten LVR-Netzwerks reduzieren.

» 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 Mitarbeitenden durch bedachtes und umsichtiges Handeln ihren Beitrag zum Schutz vor Sicherheitsvorfällen leisten. Nehmen Sie daher die Informationsangebote von LVR-InfoKom zum Thema IT-Sicherheit wahr. Schließlich hilft Ihnen das nicht nur geschäftlich, sondern auch privat.



Glossar

Awareness
Engl. „Bewusstsein“ oder „Gewahrsein“, auch übersetzt als „Bewusstheit“, zur Betonung der aktiven Haltung bzgl.-IT-Sicherheit, auch „Aufmerksamkeit“.

Cyber-Angriff
Ein Cyber-Angriff ist eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyber-Raum, 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).

DDos-Angriffe
Ein DDoS-Angriff ist eine spezielle Art der Cyber-Kriminalität. 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.

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/IEC 27001
- Koordination der Erstellung, Aktualisierung und Veröffentlichung von Richtlinien und Konzepten zur Informationssicherheit
- Initiierung von Maßnahmen zur Steigerung des Sicherheitsbewusstseins der Mitarbeiter*innen
- Unterrichtung der Geschäftsführung (Reporting)
- Leitung des IS-Management und -Lenkungskreises
- Führung und Überwachung des IS-Managers

Intrusion Detection (IDS) und Intrusion Prevention Systeme (IPS)
Damit lassen sich Angriffsversuche in einer frühen Phase erkennen, sodass der Administrator rechtzeitig alarmiert (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 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, Personalräten 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 Mitarbeiter*innen und Führungskräfte für den verantwortungsvollen Umgang mit Informationstechnik
- Unterrichtung des Beirats für IT-Sicherheit in der Leitungsebene
- Feststellung evtl. auftretender sicherheitsrelevanter Zwischenfälle sowie entsprechende Sicherstellung der Dokumentation, Untersuchung und Einleitung von Gegenmaßnahmen
- Initiierung bzw. Durchführung von Kontrollen für die Wirksamkeit und Effektivität von Sicherheitsmaßnahmen
- Übernahme der Geschäftsführung des Beirates für IT-Sicherheit (BITS)

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 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.

Impressum

Herausgeber
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

Inhaltlich verantwortlich
Frank Beermann,
Leiter Kundenservice
LVR-InfoKom

Redaktion
Robert Helfenbein,
Kundenmanagement und
Kommunikation LVR-InfoKom

Gestaltung, Produktion und Druck
Jasmin Rübel,
LVR-Druckerei,
Inklusionsabteilung,
Tel.: 0221 809-2418

Bildnachweise
Titelbild: Stefan Arendt, LVR-ZMB
Fotos: S. 4: LVR-Dezernat 6 (oben),
LVR-InfoKom (unten)
Grafiken: pixabay

Stand 31.12.2021

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**.

Wir danken unseren Kolleg*innen für die Unterstützung bei der Erstellung dieser Broschüre.