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 2019

LVR-InfoKom

LVR
Qualität für Menschen

Im:Fokus
Emotet

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. In diesem Fall geht es um den Trojaner Emotet, der im Berichtsjahr 2019 erhebliche Schäden in der deutschen Wirtschaft, aber auch bei Behörden und Organisationen verursacht hat. Auf den nächsten Seiten erfahren Sie, was diese Schadsoftware so gefährlich macht und warum der LVR – auch dank Ihrer Aufmerksamkeit – davor verschont geblieben ist.

Inhalt

Vorwort

Liebe Leserinnen und Leser,

die Digitalisierung in der Gesellschaft schreitet ungebremst voran und durchdringt zunehmend weitere Lebensbereiche der Menschen. Diese Entwicklung macht auch vor der öffentlichen Verwaltung und deren Dienstleistungen für die Bürger*innen nicht Halt. Ein gutes Beispiel hierfür ist das Onlinezugangsgesetz (OZG), welches den digitalen Zugang zu Verwaltungsleistungen von Bund, Ländern und Kommunen verbessern und weiterentwickeln soll.

Dies ist nur eine Facette, die deutlich machen soll, dass zunehmend auf sensible Daten von Kunden und Anwendenden auch von außerhalb der geschützten, internen Kommunikationswege zugegriffen werden muss. Eine weitere stellen die von uns allen genutzten „Cloud-Services" dar, sprich die Nutzung von externen Netzwerken und Dienstleistungen über das Internet. Cloud-Dienste werden in Zukunft auch für die öffentliche Verwaltung mehr und mehr an Bedeutung gewinnen, um den Bürger*innen effizientere und wirtschaftlichere Bearbeitungsprozesse für ihre Bedürfnisse anbieten zu können.

Diese Entwicklungen stellen auch die IT-Abteilungen im öffentlichen Sektor vor die große Herausforderung, einerseits die Benutzerfreundlichkeit der IT-Services und andererseits die Anforderungen an einen sicheren IT-Betrieb und den damit zwingend verbundenen Datenschutz in einer gesunden Balance zu halten.

Wie dieser schwierige Spagat beim LVR vor dem Hintergrund einer sich stetig verschärfenden Bedrohungslage bewältigt wird, erfahren Sie in der vorliegenden dritten Ausgabe des IT-Sicherheitsberichts. Hierin finden Sie in kompakter Form wichtige Informationen zur allgemeinen Sicherheitslage, zur Situation beim LVR sowie zu allen wesentlichen technischen und organisatorischen Maßnahmen aus dem Berichtszeitraum. Weitere Kapitel widmen sich einem Ausblick auf künftig geplante Vorkehrungen sowie dem so wichtigen „Faktor Mensch", sprich der Rolle der Anwender*innen im LVR.

Zudem nehmen wir auch in diesem Bericht wieder ein anschauliches Praxisbeispiel in den „Fokus". In diesem Fall geht es um den Trojaner Emotet, der zurzeit eine der größten Bedrohungen darstellt. Im Bemühen um eine möglichst verständliche Darstellung haben wir die wesentlichen Zahlen und Fakten auch diesmal wieder in Form einer zentralen Infografik aufbereitet. Gleichwohl lassen sich Fachtermini nicht gänzlich vermeiden, weshalb wir auch dieser Ausgabe wieder ein Glossar hinzugefügt haben, in dem die farblich markierten Begriffe erläutert werden.

Liebe Leserinnen und Leser, 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!

Ich wünsche Ihnen eine interessante Lektüre.

Reiner Limbach
Erster Landesrat
LVR-Dezernent Personal und Organisation

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. Er macht aber auch deutlich, dass diese erfolgreich abgewehrt werden können, wenn IT-Sicherheitsmaßnahmen konsequent umgesetzt werden.

Laut BSI waren 2019 Infektionen durch Schadprogramme eine der größten IT-Bedrohungen. So wurde häufig mittels Ransomware versucht, den Zugriff auf Daten und Systeme einzuschränken oder zu verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (engl. „ransom") wieder freizugeben. Ein Trend dabei sei der gezielte Angriff auf zentrale Dienstleister, über die dann deren Kunden oder angeschlossene Netzwerke mit Ransomware infiziert werden können. Das Schadenspotenzial ist enorm: Immer wieder kommt es zu Komplettausfällen von Rechnern und Netzwerken. Die Kosten u.a. für Datenverlust, Bereinigung und Wiederherstellung der Systeme gehen zum Teil in die Millionen, Dienstleistungen von Einrichtungen des Gemeinwesens sind nicht oder nur eingeschränkt verfügbar. Auch die Malware „Emotet", die vom BSI als gefährlichste Schadsoftware der Welt bezeichnet wurde, sorgte 2019 für erhebliche Schäden. Mithilfe von schädlichen Office-Dokumenten wurde das Schadprogramm verteilt – mit immer ausgefeilteren Mechanismen.

Obwohl die Zahl derartiger E-Mails stark abnimmt, steigt im Gegenzug die Qualität und somit die Effektivität von Spam. Das liegt unter anderem an Innovativität, technischem Sachverstand und starkem personellen Aufwand der Angreifer. Das BSI beobachtet eine hohe Dynamik der Angreifer bei der (Weiter-) Entwicklung von Schadprogrammen und Angriffswegen. So wurden rund 114 Millionen neue Schadprogramm-Varianten registriert.

Auch im Bereich der Distributed-Denial-of-Service (DDoS)-Angriffe, die sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen richten, wird das Spektrum der Angriffstechnologie permanent erweitert. Durch die Nutzung von Bot-Software haben Cyber-Kriminelle Zugriff auf eine große Zahl von fremden Systemen (Computer, Smartphones, Router etc.) und können diese für eigene Zwecke missbrauchen. Täglich bis zu 110.000 Bot-Infektionen deutscher Systeme wurden registriert. Der Fokus rückt hier auf mobile Endgeräte oder Geräte des Internets der Dinge (IoT). Denn diese bieten durch die täglich zunehmende Verbreitung bei gleichzeitig oft nur mangelhafter Absicherung eine willkommene Möglichkeit der unbefugten Übernahme und missbräuchlichen Nutzung durch Kriminelle. Weitere Angriffsmethoden zielen auf die kryptografischen Sicherheitsmechanismen von IT-Produkten sowie auf die Ausnutzung moderner Prozessorarchitektur.

Im:Fokus

Im Berichtsjahr 2019 war der Trojaner „Emotet" das vorherrschende Thema vieler Sicherheitsmeldungen. Emotet gilt zurzeit als gefährlichste Schadsoftware weltweit. Durch das sogenannte „Outlook-Harvesting" ist Emotet in der Lage, authentisch aussehende Spam-Mails, oft auch als Antwort auf reale Mails, zu verschicken. Dazu liest die Schadsoftware Kontaktbeziehungen und E-Mail-Inhalte auf infizierten Systemen aus. Diese Informationen nutzen die Täter zur weiteren Verbreitung des Schadprogramms. Hat der Schädling das System infiziert, sammelt er Daten, die für weitere Angriffe genutzt werden können. Zudem lädt er weitere Schadsoftware auf das System nach. Hierbei kann es durch Verbreitung im Netzwerk zum kompletten Ausfall der Systemlandschaft kommen.

Umso erfreulicher erscheint in diesem Kontext die Bilanz des LVR. Obwohl die Angriffe insbesondere durch Emotet in den letzten Monaten des Jahres nochmals stark zugenommen haben, blieb die LVR-IT erfreulicherweise vor dieser gefährlichen Schadsoftware verschont.

Laut BSI ist eine regelmäßige und gezielte Neubewertung der bestehenden Risiken aufgrund der dynamischen Entwicklung der Cyber-Sicherheitslage unabdingbar, um geeignete präventive und reaktive Maßnahmen auszuwählen.

II. Aktuelle Bewertung der IT-Sicherheit im LVR

Bezogen auf den Berichtszeitraum 2019 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.

Nach wie vor steht die Bedrohung durch schadhafte E-Mails an erster Stelle (u.a. durch die Schadsoftware „Emotet", siehe „Im:Fokus"). Die hierzu durchgeführten Awareness-Maßnahmen der letzten Jahre bewirken bei den Mitarbeitenden des LVR ein stetig wachsendes Sicherheitsbewusstsein und einen sensiblen Umgang mit dem Medium E-Mail.

Diese positive Bilanz ist zudem auf das bestehende Sicherheitskonzept in Form des Handbuches für IT-Sicherheit und Datenschutz und seine konsequente Umsetzung zurückzuführen, über das der LVR seit vielen Jahren verfügt. 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 Virenschutz-programmen 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-Mails sind. Spam 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. Dieser verfügt über einen Antivirusschutz und kategorisiert Webseiten nach deren Inhalten und Reputation.

» Ein sog. Intrusion Detection und Prevention System (IDPS) prüft den internen und externen Netzwerkverkehr auf potenziell schädliche Aktionen und blockiert diese.

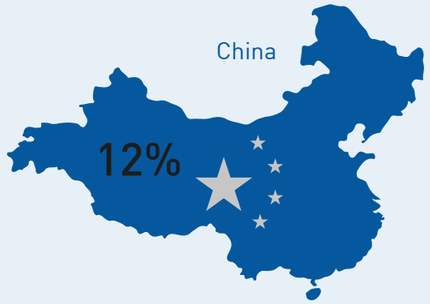
» Das Netzwerk ist in logische Abschnitte unterteilt, die durch eine Next Generation Firewall voneinander getrennt sind, um die Verbreitung von Schädlingen innerhalb des LVR-Netzes zu erschweren.

IT-Sicherheit in Zahlen - 2019

Top 5 Länder - Angriffe aus dem Internet auf unsere Systeme

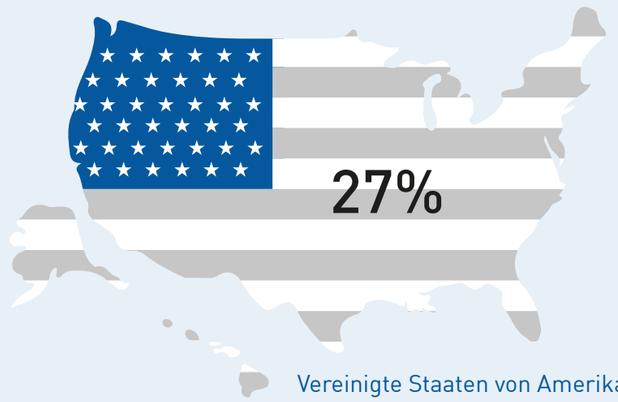
Ukraine

Vereinigtes Königreich



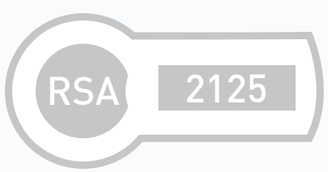
China

Deutschland



Vereinigte Staaten von Amerika

Mehrfaktor-Authentifizierung im LVR



RSA-Token

Entrust-Token

GridCards

Alle Angaben sind gerundet.

37,4 Mio.
empfangene E-Mails in 2019

Davon

32,6 Mio.
potenziell bedrohliche E-Mails

80 Tsd.
Gefährliche Inhalte

1 Tsd.
Viren

1 Mio.
SPAM-Mails

0,3 Mio.	3,8 Mio.	28,5 Mio.
Falscher Empfänger	In E-Mail-Quarantäne	Abgefangen durch den **Reputationsfilter**

4,8 Mio.
Schadfreie E-Mails

116
unterschiedliche Arten von Angriffen

78000
Angriffe wurden 2019 abgewehrt

In weniger als **24 Stunden** finden erste Angriffsversuche auf eine neu entdeckte Schwachstelle in einem System statt.

III. Spezielle Sicherheitsmaßnahmen 2019

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 2018 aufzeigen. Das so wichtige Thema „Sensibilisierung der Mitarbeitenden" wird dabei ausgeklammert und im folgenden Kapitel separat beleuchtet.

» Etablierung eines übergreifenden Pseudonymisierungsverfahrens für SAP- und non-SAP-Komponenten

Die Rheinischen Versorgungskassen (RVK) betreiben diverse Fachverfahren für ihre Fachbereiche, die gemeinsam ein zentrales SAP-System nutzen. Die Systemlandschaft ist komplex und eng gekoppelt, der Fachbereich Zusatzversorgung hat zudem einen sehr großen und alten Datenbestand.

Um realitätsnahe Tests vornehmen zu können, besteht sowohl für interne Test-Umgebungen als auch extern beim Hersteller der Wunsch nach pseudonymisierten Produktivdaten. Pseudonymisierung bedeutet hierbei die Trennung der personenbezogenen Daten von den Identifikationsmerkmalen einer konkreten Person.

Auf diese Weise lassen sich die Informationen im Datenbestand nicht mehr oder nur erschwert einer bestimmten Person zuordnen. Die Dateninhalte bleiben aber in sich konsistent und bilden das gesamte Spektrum an Fallkonstellationen der Produktion ab.

Um konsistente Integrationsumgebungen bereitstellen zu können, muss die Pseudonymisierung gleichermaßen für SAP- und non-SAP-Komponenten erfolgen. Nach einer Prüfung durch den Fachbereich ist der pseudonymisierte Datenbestand für die Testumgebung zur Verfügung gestellt worden.

» Netzwerksegmentierung

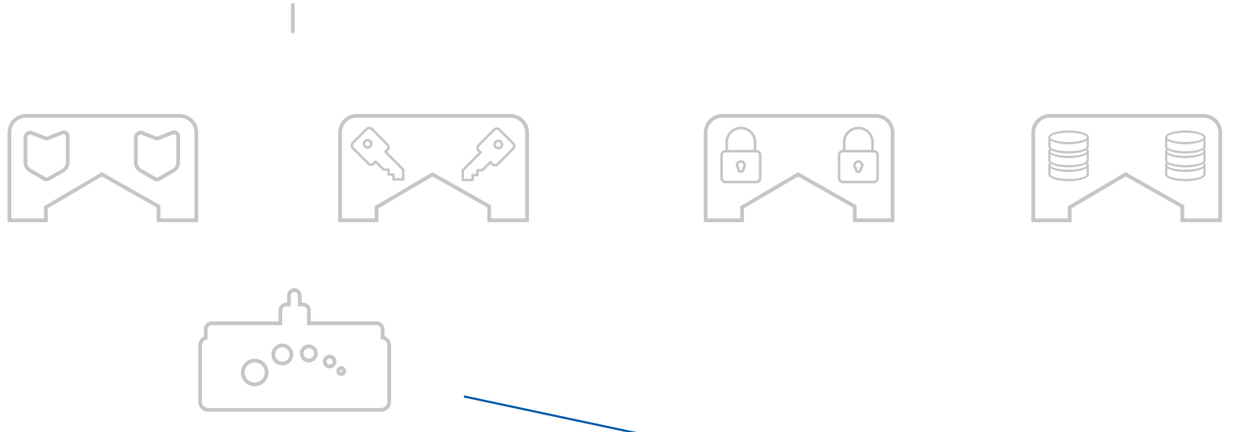
Im Rahmen der Inbetriebnahme des neuen Rechenzentrums wurde auch eine Datacenter Firewall in Funktion genommen, welche das neue Netzwerkdesign unterstützt. Dies soll die Ausbreitung von Schädlingen erschweren.

» Zwei-Faktor-Anmeldung

Nach der erfolgreichen Einführung der Zwei-Faktor-Authentifizierung wurden in 2019 weitere Web-Applikationen über dieses Verfahren abgesichert (bspw. SherpA, TeamNet, Auftragsmanagement, Wiki-Kollaborationsplattform).

» Next Generation Firewall – IDS/IPS

Um den Schutz des LVR-Netzwerks weiter zu optimieren, wurden weitere Funktionen der neuen NGFW Gateways implementiert. Die erweiterte Intrusion Detection & Prevention Funktionalität erlaubt eine bessere Analyse und ggf. Veränderung des Netzwerkverkehrs, welcher über die Firewall geführt wird.



Wir schützen Sie gegen die Invasion auf den Arbeitsplatzrechner.

» Mobiles Arbeiten

Da mobiles Arbeiten einen immer größeren Anteil im Arbeitsumfeld einnimmt, wurde die bestehende VPN-Lösung durch ein verbessertes System mit mehr Konfigurationsmöglichkeiten abgelöst. Die Sicherheit der genutzten Notebooks wurde hierbei durch den Einsatz einer geeigneten Verschlüsselungssoftware auf den Geräten zusätzlich erhöht.

» Malware Protection

Zur Verbesserung des Client- und Serverschutzes wurde die Malware Protection einer Qualitätssicherung unterzogen. In einem sehr kurzen Zeitrahmen von nur drei Monaten wurde auf allen 6.500 Endgeräten der Antivirenschutz von Symantec Endpoint Protection gegen den McAfee Endpoint Client ausgetauscht. Ebenfalls wurde das gesamte Sicherheitskonzept (Malware-Schutz und Firewall) überarbeitet, erneuert und den aktuellen Gegebenheiten angepasst.

Im:Fokus

Wie verheerend ein Angriff von Emotet verlaufen kann, zeigt das Beispiel von Neustadt am Rübenberge, wo der Trojaner im September 2019 mit voller Wucht zuschlug und das gesamte IT-System der Stadtverwaltung lahmlegte. Die Computer im Rathaus blieben aus, die KFZ-Zulassungsstelle geschlossen. Die Mitarbeitenden des Bürgerbüros konnten Anfragen nur noch mündlich beantworten. Daraufhin wurde entschieden, alle Geräte auszuschalten und die Systeme mithilfe von IT-Spezialisten zu bereinigen. Bereits zehn Tage später sollte alles wieder laufen, aber aufgrund von Problemen bei der Beseitigung der Schadsoftware blieb der Betrieb der Stadtverwaltung noch mehr als drei lange Monate eingeschränkt.

Um das Risiko eines ähnlichen Szenarios beim LVR zu minimieren, wurde der Virenschutz auf den Clientsystemen verbessert. Zudem wurde im Fall einer Infizierung eines Clients durch Intrusion Detection & Prevention, Netzwerksegmentierung und Schutz des Datenspeichers vor Ransomware dafür gesorgt, dass sich die Schadsoftware nicht ausbreiten kann. Auf diese Weise konnte die LVR-IT effektiv vor einem kritischen Ausfall der Systemlandschaft bewahrt werden.

» Schutz vor Ransomware

Eine neue Software schützt alle über das Netzwerk angeschlossenen Speichersysteme vor dem Befall mit Ransomware. Damit werden Dateizugriffe sicherheitstechnisch überprüft und somit ein noch höheres Niveau an Datenintegrität im Gesamten gewährleistet. Die Software wird für alle zentral auf den NAS-Systemen gespeicherten Dateien der Anwender*innen eingesetzt. Dies ist bei dem Konzept des neuen NAS-Speichersystem, wonach jeder Kunde eine eigene Umgebung für seine Daten erhält, kundenspezifisch einstellbar.

» BIOS-Updates gegen aktuelle Sicherheitsbedrohungen wie Spectre und Meltdown

Im Zuge des LVR-weiten Roll-outs von Windows 10 wurden alle Geräte im LVR mit den nötigen Sicherheits-Updates (BIOS, Firmware) der jeweiligen Hersteller versehen. Dies wurde notwendig, da in diversen Intel-Prozessoren mehrere Sicherheitslücken (Spectre und Meltdown) vorhanden waren, welche dringend durch Updates geschlossen werden mussten.

IV. Der „Faktor Mensch“

– 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 erkannt werden.

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, als aktive Mitgestalter 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 hat LVR-InfoKom auch in 2019 wieder großes Augenmerk auf die Aufklärung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter des LVR gelegt. Hier ein aktueller Überblick:

» Schulungen

Im Rahmen der Awareness-Kampagne bietet LVR-InfoKom seit 2019 auch spezielle Info-Veranstaltungen zur IT-Sicherheit an. Themen wie Passwort-Sicherheit, Umgang mit E-Mails, Sicheres Surfen im Internet, Mobiles Arbeiten usw. werden hier lebens- und praxisnah besprochen und diskutiert. Dabei sind Erfahrungen und Fragen aus dem Publikum sehr willkommen. Ziel der etwa zweistündigen Treffen ist es, das Bewusstsein für die Gefahren im Netz mit eindrücklichen Beispielen zu schärfen – Erkenntnisse, die im Büro und auch zu Hause wertvoll sein können.

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.

» 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. Bislang wurden drei Teile produziert zu den Themen „Umgang mit gefährlichen E-Mails“, „Sicheres Surfen im Netz“ und „Sichere Passwörter“.

2019 wurde im LVR-Intranet erstmalig ein Quiz zu den Themen der Erklärvideos durchgeführt, welches von den LVR-Mitarbeitenden sehr gut angenommen wurde.

» 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.

» IT-Sicherheitsbericht

Seit 2017 veröffentlicht LVR-InfoKom alljährlich den IT-Sicherheitsbericht. Hierin finden sich Informationen zur allgemeinen Sicherheitslage, zur Situation beim LVR, zur Rolle des „Faktors Mensch“ sowie zu den wesentlichen IT-Sicherheitsvorkehrungen aus dem Berichtszeitraum.

V. Ausblick

» Sicherheitstechnische Vorgaben auf Netzwerkebene

Die sicherheitstechnischen Vorgaben auf Netzwerkebene wurden angepasst. Die aus dem Redesign des Netzwerkes resultierenden Maßnahmen werden auch in 2020 fortgesetzt. Darüber hinaus wird die Absicherung der LVR-Außendienststandorte konzeptionell überarbeitet und umgesetzt.

» Malware Protection

Nach der in 2019 erfolgten Optimierung des Virenschutzes auf den Clients und im Storagebereich, stehen in 2020 die Serversysteme auf der Prüfliste. Auch hier werden die derzeitigen Schutzmaßnahmen neu bewertet und ggfs. entsprechende Maßnahmen eingeleitet.

» Einführung eines zentralen Log-Managements

An vielen Stellen im LVR werden Informationen in Log-Dateien gesammelt und im Bedarfsfall aus den unterschiedlichsten Anforderungen heraus ausgewertet. Oft sind einzelne Auswertungen aber nicht aussagekräftig genug. Erst mit der Korrelation der unterschiedlichen Logdateien können Bedrohungen besser erkannt und somit abgewehrt bzw. bekämpft werden.

» Umsetzung Onlinezugangsgesetz

Alle Verwaltungen müssen bis 2022 ihre dazu fähigen Verwaltungsleistungen online anbieten. Darüber hinaus sind Bund, Länder und Kommunen verpflichtet, ihre Angebote auch in einem übergreifenden Portalverbund nutzbar zu machen. Die zur Gewährleistung der IT-Sicherheit erforderlichen Standards werden durch Rechtsverordnungen des Bundesministeriums des Inneren festgelegt. Im Rahmen der Umsetzung des Onlinezugangsgesetzes (OZG) im LVR müssen im Zuge dessen auch sicherheitsrelevante Aspekte berücksichtigt werden.

» 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 wird sich auch die Anzahl solcher Tests erhöhen.

» Erweiterung des Pseudonymisierungsverfahrens

Für 2020 ist die Realisierung eines Verfahrens zur Pseudonymisierung von Dateien geplant, welche aus externen Quellen über Schnittstellen importiert werden.

Im:Fokus

Dass der LVR vor Emotet verschont blieb, liegt zum einen an den etablierten technischen Abwehrmaßnahmen, zum anderen aber auch daran, dass die Awareness-Kampagne von LVR-InfoKom offensichtlich Früchte trägt. So hat die systematische Aufklärung und Sensibilisierung der LVR-Mitarbeitenden ein stetig wachsendes Sicherheitsbewusstsein und damit auch einen sensiblen Umgang mit dem Medium E-Mail bewirkt. Schließlich gilt dieses nach wie vor als das Haupt-Einfallstor für Schadsoftware wie Emotet. Vor diesem Hintergrund wird LVR-InfoKom auch in Zukunft auf eine kombinierte Vorgehensweise von technischen Sicherheitsmaßnahmen und systematischer Awareness-Maßnahmen setzen.

Glossar

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

Bot-Software
Unter einem Bot (von englisch robot ‚Roboter‘) versteht man ein Computerprogramm, das weitgehend automatisch sich wiederholende Aufgaben abarbeitet, ohne dabei auf eine Interaktion mit einem menschlichen Benutzer angewiesen zu sein.

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).

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.

Internet der Dinge (Internet of Things/IoT)
Vernetzung von Gegenständen mit dem Internet, damit diese Gegenstände selbstständig über das Internet kommunizieren und so verschiedene Aufgaben für den Besitzer erledigen können.

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-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.

NAS-System
Ein NAS ist ein konfigurierbarer Datenspeicher, um in einem Netzwerk Speicherplatz zur Verfügung zu stellen.

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.

Spam
Unter Spam versteht man unerwünschte Nachrichten, die massenhaft und ungezielt u.a. per E-Mail versendet werden. In der harmlosen Variante enthalten Spam-Nachrichten meist unerwünschte Werbung, häufig jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten etc.

Trojaner
Ein Trojaner ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Ein Trojaner verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.

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

VPN
Mit einem Virtual Private Network, kurz VPN, lassen sich Daten im öffentlichen Internet geschützt übertragen. Über das Transportmedium Internet wird ein virtuelles, in sich geschlossenes Netzwerk zwischen mehreren Kommunikationspartnern aufgebaut.

Impressum

Herausgeber
LVR-InfoKom
Ottoplatz 2
50679 Köln

Tel.: 0221 809-3770
Fax: 0221 809-2165
E-Mail: infokom@lvr.de
www.lvr-infokom.de

Inhaltlich verantwortlich
Frank Beermann
Leiter Kundenservice
LVR-InfoKom

Redaktion
Robert Helfenbein,
Kundenmanagement und
Kommunikation LVR-InfoKom

Gestaltung
Ronja Semerak,
Kundenmanagement und
Kommunikation LVR-InfoKom

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

Bildnachweise
Titelbild
Alexandra Kaschirina,
LVR-ZMB Düsseldorf

Seite 4
Uwe Weiser,
LVR

Stand 31.12.2019

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.lvr-infokom.de**.

Wir danken unseren Kolleginnen und Kollegen für die Unterstützung bei der Erstellung dieser Broschüre.