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 2018

LVR-InfoKom

LVR
Qualität für Menschen

Im:Fokus
Spear Phishing

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 einen größeren Cyber-Angriff aus dem Januar 2018, als im Rahmen einer Spear Phishing-Kampagne ca. 100 Nutzerkonten erbeutet wurden. Lesen Sie auf den nächsten Seiten wie es dazu kam, wie der Angriff erfolgreich abgewehrt werden konnte und wie sich dies in Zukunft – mit Ihrer Unterstützung – verhindern lässt.

Inhalt

Vorwort

Die digitale Transformation des öffentlichen Sektors schreitet laufend voran. Schon heute wird die überwiegende Mehrzahl aller Verwaltungsprozesse elektronisch unterstützt, die Vision der vielzitierten „Verwaltung 4.0“ nimmt zunehmend Gestalt an. Hieraus ergeben sich enorme Potenziale – sowohl für die Mitarbeitenden als auch für die Bürgerinnen und Bürger, die heutzutage effiziente und moderne Dienstleistungen erwarten. Dies gilt selbstverständlich auch für den LVR als großen öffentlichen Leistungsträger.

Technische und organisatorische Neuerungen wie Verwaltungs-Services im Internet, das Angebot von Informations-Apps, die Einbindung von Telearbeitsplätzen in das Verwaltungsnetz oder die elektronische Versorgung der politischen Vertretung mit Sitzungsunterlagen verlangen einen umfassenden Schutz. Schließlich nehmen die potenziellen Angriffsmöglichkeiten sowie die Risiken von Störungen mit der stetig wachsenden Komplexität der Systeme und der fortschreitenden Vernetzung erheblich zu. In Anbetracht einer unverändert kritischen Bedrohungslage (siehe Kapitel I) gilt es deshalb, die IT-Sicherheit weiter mit Hochdruck voranzutreiben. Einen positiven Effekt wird dabei die am 25. Mai 2018 in Kraft getretene neue europäische Datenschutz-Grundverordnung (DSVGO) haben, deren konsequente Umsetzung für ein gesteigertes Daten- und Informationssicherheitsniveau sorgen wird. Doch bei allen organisatorischen Voraussetzungen und technischen Vorkehrungen kommt es letztlich auf das Sicherheitsbewusstsein der Mitarbeitenden am Arbeitsplatz an. Sie sind der entscheidende Faktor, wenn es um optimale IT-Sicherheit geht.

Vor diesem Hintergrund präsentieren wir Ihnen hiermit die zweite 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. Im Bemühen um eine möglichst verständliche Darstellung haben wir die wesentlichen Zahlen und Fakten in Form einer zentralen Infografik aufbereitet. Zudem wird Sie diesmal ein anschauliches Praxisbeispiel zum Thema „Spear Phishing“ durch die einzelnen Kapitel begleiten.

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.

Dieser Bericht erscheint in elektronischer Form auch im LVR-Intranet unter „Wissen und Service/Anleitungen/Informationstechnologie/IT-Sicherheit“. Hier finden Sie darüber hinaus viele weitere interessante Informationen in Form von Dokumenten, Tipps, Filmen, Links u.v.m.

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. Laut dem aktuellen Bericht für 2018 hat sich die Gefährdungslage im Vergleich zur vorangegangenen Erhebung weiter verschärft und ist zudem vielschichtiger geworden. So stieg die Anzahl weltweit bekannter Schadprogramme von rund 600 auf mehr als 800 Millionen. Bemerkenswert sei dabei insbesondere die hohe Dynamik der Angreifer bei der Weiterentwicklung von Schadprogrammen – pro Tag kommen rund 390.000 neue Varianten hinzu. Zudem werden bekannte Schadsoftware-Familien fortlaufend verändert und mit zusätzlichen Schadfunktionen ausgestattet. Auch die Wege zur massenhaften Verteilung von Schadsoftware wurden weiterentwickelt.

Im Unterschied zu den Vorjahren sind größere Angriffswellen mit Verschlüsselungs-Software (Ransomware) ausgeblieben. Dennoch bleibe diese Form von Schadsoftware eine massive Gefährdung. Auch Anfang 2018 erhielt das BSI noch Meldungen von einem Rechnerbefall mit der Schadsoftware „WannaCry“, die vor allem im Mai 2017 für schwerwiegende Cyberangriffe genutzt wurde. Diese späten Infektionen stehen aber laut dem Bericht, insbesondere hinsichtlich ihrer Auswirkungen, deutlich hinter der ersten WannaCry-Welle zurück. Außerdem stellt das BSI eine deutliche Zunahme von Software fest, mit der Kryptowährungen „geschürft“ werden. Aufgrund der hohen finanziellen Attraktivität und der Unauffälligkeit der Infektionen sei illegales „Krypto-Mining“ als signifikant zunehmendes Cyber-Risiko zu bewerten. Auch im Bereich Spam und Phishing besteht nach wie vor eine kritische Sicherheitslage.

Insgesamt macht der Bericht deutlich, dass Cyber-Sicherheit in der immer weiter fortschreitenden Digitalisierung kontinuierlich betrachtet und beachtet werden muss. Die Sicherheitsarchitektur von computergestützten Arbeitsplätzen und Unternehmensabläufen muss ebenso von Anfang an mitgedacht werden wie die IT-Sicherheit von Produkten und Dienstleistungen.

Im:Fokus

Phishing: das klingt nach fischen gehen und genau das ist es auch. Zusammengesetzt aus den Wörtern „Password“ und „fishing“ bedeutet es „nach Passwörtern angeln“. Immer häufiger fälschen Phishing-Betrüger E-Mails und Internetseiten, um an vertrauliche Daten wie Passwörter, Zugangsdaten und Kreditkartennummern zu gelangen. Die Nutzer*innen geben ihre Daten oftmals freiwillig preis, weil die gefälschte E-Mail von einer vertrauenswürdigen Quelle zu stammen scheint. Noch gefährlicher ist das sogenannte Spear Phishing (von engl. „Speer“). Dabei beschaffen sich Kriminelle auf illegalen Wegen persönliche Daten und E-Mail-Adressen von einer bestimmten Nutzergruppe und schreiben diese mit auf sie zugeschnittenen Nachrichten an.

Im Januar 2018 wurde auch der LVR Opfer eines solchen Angriffs. Mit einer gefälschten und scheinbar vertrauenswürdigen E-Mail wurden LVR-Mitarbeitende dazu aufgefordert, zwecks Durchführung eines Support-Updates auf einen Link in der E-Mail zu klicken und ihre persönlichen Zugangsdaten einzugeben. Auf diese Weise konnten 100 Konten erbeutet und zum massenhaften Versand von ca. 1,3 Mio. Spam-Mails missbraucht werden. Hierdurch wurde der LVR auf Sperrlisten gesetzt, bspw. war ein E-Mail-Versand an Microsoft-Adressen zeitweilig nicht mehr möglich.

II. Aktuelle Bewertung der IT-Sicherheit im LVR

Bezogen auf den Berichtszeitraum 2018 ist die Lage der IT-Sicherheit im LVR trotz der angespannten Gesamtlage insgesamt als positiv zu bewerten. Die LVR-IT blieb von größeren IT-Sicherheitsvorfällen verschont. Es gab nur einen größeren erwähnenswerten Sicherheitsvorfall, als im Januar 2018 im Rahmen einer Phishing-Kampagne ca. 100 AD (Active Directory)-Konten erbeutet wurden (siehe „Im Fokus“). Durch umgehend getroffene Maßnahmen ist hierdurch kein Schaden entstanden. Die rund 325 verzeichneten Standardvorfälle wurden routinemäßig nach den bei LVR-InfoKom definierten Prozessen abgearbeitet und stellten somit keine Bedrohung dar.

Diese positive Bilanz ist im Wesentlichen 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 Schutzprogrammen ausgestatte Infrastruktur, die sowohl die PC`s, die Server, die Dateien sowie die Verbindungen zum Internet vor Viren, Trojanern etc. 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. Zudem wird das Netzwerk in logische Abschnitte unterteilt, um die Verbreitung von Schädlingen innerhalb des LVR-Netzes zu erschweren.

IT-Sicherheit in Zahlen - 2018

E-Mails

37,1 Mio.
eingehende E-Mails

davon

30,9 Mio.
geblockt

davon

2,7 Mio.
in Quarantäne

3,5 Mio.
schadfrei

Virenschutz

180
Virenfunde
gemeldet und behandelt

960
Spyware

Internet

164,4 Tsd.
verhinderte Aufrufe

und

592,6 Mio.
zugelassene Aufrufe

davon

592,7 Mio.
Aufrufe

RSA Tokens

RSA 3800

GridCards

GRIDCARD 3300

6600
geschützte
Endgeräte

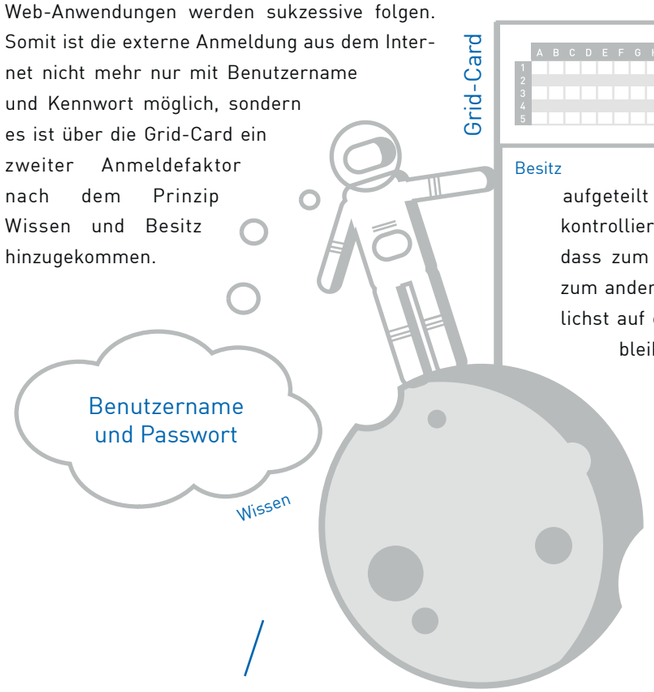
Alle Angaben sind gerundet.

III. Spezielle Sicherheitsmaßnahmen 2018

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.

» Zwei-Faktor-Anmeldung

In der zweiten Jahreshälfte wurde ein neues Authentifizierungsverfahren für einen noch höheren Sicherheitsstandard eingeführt – die sogenannte Grid-Card-Technologie (Rasterkarten mit Koordinaten). Der Start erfolgte mit der Absicherung von OWA (Outlook Web Access) – weitere Web-Anwendungen werden sukzessive folgen. Somit ist die externe Anmeldung aus dem Internet nicht mehr nur mit Benutzername und Kennwort möglich, sondern es ist über die Grid-Card ein zweiter Anmeldefaktor nach dem Prinzip Wissen und Besitz hinzugekommen.



*Ein kleiner Schritt für Sie als Anwender*in, aber ein großer Schritt für den Schutz der LVR-IT.*

Die Zwei-Faktor-Authentifizierung ist ein Authentifizierungsverfahren mit zwei Komponenten, das eine erhöhte Sicherheit zum Schutz vor Identitätsdiebstahl bietet. Der große Vorteil der Zwei-Faktor-Authentifizierung besteht darin, dass der Diebstahl oder das unbefugte Kopieren von Zugangskennungen zum Beispiel per Phishing Angriff, Hackerangriff oder Virus noch keine Anmeldung am System ermöglicht. Damit dies dem Angreifer gelingt, muss er gleichzeitig in den Besitz des zweiten Faktors gelangen. Die im Internet häufigsten Bedrohungsszenarien für den Identitätsdiebstahl können dadurch ausgeschlossen werden. So wird durch einen einzigen weiteren Schritt das Niveau der IT-Sicherheit um ein Vielfaches erhöht – auch wenn dies das Anmeldeverfahren ein wenig unbequemer macht.

» Neues Netzdesign

Im Rahmen der Vorbereitungen für die Inbetriebnahme des neuen LVR-Rechenzentrums in Kalk erfolgte die Einführung eines sicherheitstechnisch optimierten Netzwerkdesigns, welches den heutigen Anforderungen an Sicherheit gerecht wird. Dabei wird das Netzwerk je nach Anforderung und Sicherheitsklasse der darin befindlichen Geräte bzw. Funktionen in Segmente aufgeteilt und der Zugriff zwischen den Segmenten kontrolliert und reglementiert. Hierdurch wird erreicht, dass zum einen nur gewünschte Zugriffe erfolgen und zum anderen bei Sicherheitsvorfällen der Schaden möglichst auf einen kleinen Teil des LVR-Netzes beschränkt bleibt und sich nicht ungehindert verbreiten kann.

Da die Rechenzentren des LVR eine logische Einheit darstellen, werden die neuen Netzwerkstrukturen hierbei nicht nur in Kalk bereitgestellt, sondern stehen auch im Rechenzentrum Chorweiler zur Verfügung.

» Informationssicherheits-Management-System (ISMS)

Um die neuen Anforderungen im Zuge des anstehenden Rezertifizierungsaudits durch den TÜV zu erfüllen, wurde 2018 der bestehende Wirkungsbereich des ISMS erweitert. Damit fließen neben dem eigentlichen RZ-Betrieb auch unterstützende Bereiche innerhalb der Wertschöpfungskette bei LVR-InfoKom wie z.B. Einkauf oder Personal in die Sicherheitsbetrachtung mit ein. In den kommenden Jahren werden auch die restlichen Bereiche sukzessive in das System integriert.

» Datenschutzrecht

Die neue europäische Datenschutzverordnung (EU-DSGVO) wurde am 25. Mai 2018 geltendes Recht in allen Mitgliedsstaaten der Europäischen Union. Zur Einhaltung der DSGVO musste eine Reihe von Regelungen und Prozessen angepasst werden. Insbesondere wurde die Allgemeine Rundverfügung Nr. 192 zum Umgang mit zu schützenden Daten beim LVR komplett überarbeitet. Das Verzeichnis der Verarbeitungstätigkeiten (VVT) hat das bisherige Verfahrensverzeichnis (VVZ) abgelöst. Hierbei hat es auch Änderungen bezüglich der Handhabung und der zu erfassenden Daten gegeben. Es konnten bereits eine Vielzahl von VVTs wie z.B. die „Elektronische Zeiterfassung und Zutrittskontrolle" final abgestimmt werden. Um dem Art. 13 der DSGVO (Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person) nachzukommen, wurde u.a. im Klinikumfeld ein Dokument zur Patienteninformation erstellt. Darüber hinaus tagt turnusmäßig eine Arbeitsgruppe zur Umsetzung der EU-DSGVO, an der neben den Vertretungen aus den Dezernaten auch LVR-InfoKom teilnimmt. Außerdem wurde eine Reihe von Fortbildungen und Workshops mit dem spezifischen Fokus auf die EU-DSGVO durchgeführt.

» Schutz für VoIP-Telefonie

Durch die Einführung eines neuen technischen Verfahrens ist das Risiko des Abhörens von interner VoIP-Telefonie angemessen reduziert worden. Dadurch ist es möglich, die zwischen Sender und Empfänger übermittelten Daten zu analysieren, zu verändern und anhand bestimmter Kriterien zu filtern. Auf diese Weise wird die Netzwerkadressenvergabe effektiv geschützt. Der Betrieb dieser Sicherheitsfunktion führt nicht zur Beeinträchtigung von benötigten Telefoniefunktionen.

» Next Generation Firewall (NGFW)

Innerhalb von einem Jahr wurde die zentrale Firewall-Infrastruktur im LVR aktualisiert und durch Next-Generation-Firewall-Systeme getauscht. Diese bieten zusätzlich zu den Funktionen klassischer Firewalls weitere Sicherheitsfunktionen, u.a. IPS und Anwendungskontrolle. Dabei wurde nicht nur die reine Hardware getauscht, sondern auch das interne Design (wie z.B. das Regelwerk) neu entwickelt und im laufenden Betrieb umgestellt. Durch die Implementierung neuer Funktionalitäten ist der Schutz des LVR-Netzwerks vor Gefahren aus dem Internet weiter erhöht worden.

Im:Fokus

Durch unmittelbar eingeleitete Sicherheitsmaßnahmen ist für die LVR-IT kein Schaden entstanden. Die Passwörter wurden ad hoc zurückgesetzt und die Phishing-E-Mails aus den betroffenen Postfächern entfernt – ein Zugriff von außen war somit nicht mehr möglich. Dies zeigte sich eine Woche später, als vergeblich versucht wurde, nochmals Spam-E-Mails über die gekaperten Accounts zu versenden. Als weitere Maßnahme wurde der Zugriff auf die LVR-Webseiten aus Nigeria heraus komplett unterbunden, da alle Zugriffe aus diesem Land heraus erfolgten.

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 2018 wieder großes Augenmerk auf die Aufklärung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter des LVR gelegt. Hier ein aktueller Überblick:

» 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 neue 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“.

» 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 seinen Mitarbeitenden interne Schulungen an. Dazu gehören neben den Datenschutzeinweisungen im Rahmen der PC-Bedienung auch Seminare zum Datenschutzrecht. Darüber hinaus schärft LVR-InfoKom das Sicherheitsbewusstsein seiner Mitarbeitenden u.a. mit speziellen Sicherheitstrainings, weil diese durch ihre Arbeit unmittelbar mit den kritischen Systemen und Anwendungen in Kontakt sind.

V. Ausblick

Laut Prognosen von IT-Sicherheitsexperten wird sich die Bedrohungslage auch 2019 nicht entschärfen, sondern im Gegenteil noch komplexer und vielschichtiger darstellen. Um dem zu begegnen, sind u.a. folgende Maßnahmen geplant:

» Next Generation Firewall – IDS/IPS

In Zukunft werden sukzessive weitere Funktionen der neuen NGFW Gateways implementiert, um den Schutz des LVR-Netzwerks stetig zu optimieren. Die erweiterte Intrusion Detection & Prevention Funktionalität erlaubt eine bessere Analyse und ggf. Veränderung des Netzwerkverkehrs, welcher über die Firewall geführt wird. Im Rahmen der Inbetriebnahme des neuen Rechenzentrums wird auch eine Datacenter Firewall in Funktion genommen, welche das neue Netzwerkdesign unterstützt.

» Awareness-Maßnahmen

Um die bislang durchgeführten Awareness-Maßnahmen zu den Schwerpunkt Themen sicheres Mailing, sicheres Surfen und sicherer Umgang mit Passwörtern zu vertiefen, sind interaktive Online-Maßnahmen geplant.

» Zwei-Faktor-Anmeldung

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

» Schutz vor Ransomware

Mit einer neuen Software sollen zukünftig alle über das Netzwerk angeschlossenen Speichersysteme vor dem Befall mit Ransomware geschützt werden. Dann werden Dateizugriffe sicherheitstechnisch überprüft und somit ein noch höheres Niveau an Datenintegrität im Gesamten gewährleistet. Geplant ist, die Software für alle zentral auf den NAS-Systemen gespeicherten Dateien der Anwender*innen einzusetzen. Dies ist bei dem Konzept des neuen NAS-Speichersystem, wonach jeder Kunde eine eigene Umgebung für seine Daten erhält, kundenspezifisch einstellbar.

» Mobiles Arbeiten

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

Im:Fokus

Das Beispiel zeigt sehr deutlich, welch bedeutende Rolle der „Awareness“, sprich der Aufmerksamkeit der Nutzer*innen zukommt. Technische Sicherheitsmaßnahmen können nicht jeden Angriff abwehren, besonders wenn diese derart gezielt erfolgen. Letztlich ist es der einzelne Mitarbeitende als Mensch, auf den es ankommt. Um beispielsweise Spear Phishing-Versuche abzuwehren, müssen Mitarbeitende in der Lage sein, die Bedrohungen (wie gefälschte E-Mails) zu erkennen.

In technischer Hinsicht wird die Nutzung der in 2018 eingeführten Zwei-Faktor-Authentifizierung (siehe Kapitel III) die Gefahr von Passwortdiebstahl erheblich senken. Darüber hinaus können bei Bedarf weitere Regionen oder Länder ggf. grundsätzlich für den Zugriff auf LVR-Internetdienste blockiert werden, wenn der Datenverkehr aus diesen Quellen feindselig oder aggressiv ist (sogenanntes Geo Blocking).

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).

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.

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.

Kryptowährung
Eine Kryptowährung ist ein digitales Zahlungsmittel, das mit Prinzipien der Kryptographie erstellt und transferiert wird, um ein dezentrales und sicheres Zahlungssystem zu realisieren (Bsp. Bitcoin). Die Qualifizierung von Kryptowährung als Währung ist mitunter strittig.

OWA (Outlook Web Access)
Eine von Microsoft entwickelte Technik zum Zugriff auf E-Mail-Postfächer über einen Webbrowser.

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.

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.

Spyware
Bei Spyware handelt es sich um eine Software, die ohne Wissen des Anwenders Aktivitäten auf dem Rechner oder im Internet ausspioniert und aufzeichnet.

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.

VoIP-Telefonie
VoIP steht für Voice-over-IP. Es bezeichnet die Übermittlung von Sprache über internetbasierte Netzwerke anstelle klassischer Telefonnetze.

VPN
Ein Virtual Private Network (VPN) ermöglicht eine verschlüsselte, zielgerichtete Übertragung von Daten über öffentliche Netze wie das Internet. Es etabliert geschützte und in sich geschlossene Netzwerke mit verschiedenen Endgeräten. Häufige Anwendung ist die Anbindung von Home Offices oder mobilen Mitarbeitern.

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 Kundenmanagement,
Marketing LVR-InfoKom

Redaktion
Robert Helfenbein,
Marketing LVR-InfoKom

Gestaltung
Ronja Semerak,
Marketing LVR-InfoKom

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

Bildnachweise
Titelbild
Alexandra Kaschirina,
LVR-ZMB Düsseldorf

Seite 4
Julia Reschucha,
LVR

Stand 31.12.2018

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

www.lvr-infokom.de/publikationen

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