ifib consult

Ergebnisbericht (Kurzgutachten)

Version 1.01 vom 31.08.2023

Untersuchung im Zeitraum Q4/2022 - Q2/2023: Identifizierung und Kostenabschätzung von Maßnahmen der Informationssicherheit in Schulen und Verwaltung der Stadt Rheine

August 2023

Herausgeber
ifib consult GmbH
Am Fallturm 1
28359 Bremen
Geschäftsführer: Björn Eric Stolpmann, Prof. Dr. Andreas Breiter
Gerichtsstand: Amtsgericht Bremen, HRB 26806 HB

Telefon: 0421 218-56590
Telefax: 0421 218-56599
E-Mail: info@ifib-consult.de
www.ifib-consult.de

Im Auftrag der Stadt Rheine

Autor:innen / Verantwortliches Projektteam
Dr. Jörg Hofmann
Nadine Knoke

Ansprechperson
Dr. Jörg Hofmann

Inhaltsverzeichnis

1 Auftrag

1.1 Ausgangslage

Die Stadt Rheine konnte in den vergangenen Jahren die IT-Ausstattung der in Trägerschaft befindlichen Schulen systematisch erweitern und die Digitalisierung der Schulen durch Optimierung des Betriebs und der technischen Unterstützung gezielt vorantreiben. Der weitere Ausbau des IT-Betriebs und der schulübergreifenden IT-Supportstrukturen ist geplant und basiert u. a. auf einem kommunalen Medienentwicklungsplan sowie einem Gutachten zur Supportbemessung, das die ifib consult GmbH gemeinsam mit der Stadt Rheine im Jahr 2020 entwickeln konnte.

Im Zuge der immer weiter fortschreitenden Digitalisierung von immer mehr Aspekten des täglichen Lebens gewinnt die Informationssicherheit zunehmend an Bedeutung. Insbesondere im kommunalen Bereich ist es von großer Bedeutung, die IT-Infrastrukturen und Daten vor unbefugtem Zugriff zu schützen, um das Vertrauen der Bürgerinnen und Bürger zu wahren und die öffentlichen Dienstleistungen reibungslos bereitstellen zu können. Ein wichtiger Aspekt der Informationssicherheit betrifft auch die Schulen einer jeder Kommune, da hier sensible Daten von Schülerinnen und Schülern sowie Lehrkräften verarbeitet werden und somit ein besonderer Schutz erforderlich ist.

Angesichts wachsender Bedrohungen der Informationssicherheit sieht die Stadt Rheine sowohl für die städtische IT-Dienststelle, für die Feuerwehr als auch in den Schulen Handlungsbedarf zur technischen und organisatorischen Absicherung der IT-Systeme. Beide Seiten strebten daher eine Kooperation bei der Prüfung und Initiierung von Maßnahmen der Informationssicherheit an. In diesem Kurzgutachten werden die Ergebnisse einer Untersuchung durch die ifib consult GmbH und die sich aus der Untersuchung ableitenden Erkenntnisse und Empfehlungen dargestellt, mit dem Ziel, die Informationssicherheit in der Stadt Rheine unter Einbezug der Schulen nachhaltig zu verbessern.

1.2 Auftrag gemäß Angebot

Gegenstand des vorliegenden kompakten Gutachtens bildet gemäß Auftrag die Identifizierung erforderlicher Maßnahmen zur Optimierung der Informationssicherheit und die Abschätzung der dafür notwendigen Kosten für die Stadt Rheine unter Berücksichtigung der Schulen. Inhalte des Gutachtens basieren auf der Erhebung des Ist-Stands und auf der Ermittlung eines Soll-Zustands mit beiden IT-Teams für die die städtische und die schulische Informationstechnologie[1]. Diese sind im Rahmen von insgesamt drei Expertengesprächen mit Workshop-Charakter durchgeführt worden. Die Expertengespräche ergänzten eine Prüfung einschlägiger Dokumente. Die Ergebnisse werden durch das Kurzgutachten dokumentiert, das notwendige Maßnahmen aufzeigt und eine Aufwandsabschätzung beinhaltet.

[1] Im weiteren Verlauf wird von der Verwaltungs-IT und der Schul-IT gesprochen.

2 Bedrohungslage

2.1 Gefährdungen gemäß BSI IT-Grundschutz

Das Bundesamt für Sicherheit in der Informationstechnik listet in seinem IT-Grundschutz-Kompendium 47 Gefährdungen, beginnend bei Feuer, ungünstigen klimatischen Bedingungen, Wasser, über Naturkatastrophen, Versorgungsausfälle, den Diebstahl und Verlust von Geräten, Datenträgern und Dokumenten, den Missbrauch von Berechtigungen, dem Identitätsdiebstahl, Sabotage, Social Engineering und andere mehr.

G 0.1 – G 0.16	G 0.17 – G. 0.32	G 0.33 – G. 0.47
Feuer	Verlust von Geräten, Datenträgern oder Dokumenten	Personalausfall
Ungünstige klimatische Bedingungen	Fehlplanung oder fehlende Anpassung	Anschlag
Wasser	Offenlegung schützenswerter Informationen	Nötigung, Erpressung oder Korruption
Verschmutzung, Staub, Korrosion	Informationen oder Produkte aus unzuverlässiger Quelle	Identitätsdiebstahl
Naturkatastrophen	Manipulation von Hard- oder Software	Abstreiten von Handlungen
Katastrophen im Umfeld	Manipulation von Informationen	Missbrauch personenbezogener Daten
Großereignisse im Umfeld	Unbefugtes Eindringen in IT-Systeme	Schadprogramme
Ausfall oder Störung der Stromversorgung	Zerstörung von Geräten oder Datenträgern	Verhinderung von Diensten (Denial of Service)
Ausfall oder Störung von Kommunikationsnetzen	Ausfall von Geräten oder Systemen	Sabotage
Ausfall oder Störung von Versorgungsnetzen	Fehlfunktion von Geräten oder Systemen	Social Engineering
Ausfall oder Störung von Dienstleistern	Ressourcenmangel	Einspielen von Nachrichten
Elektromagnetische Störstrahlung	Software-Schwachstellen oder -Fehler	Unbefugtes Eindringen in Räumlichkeiten
Abfangen kompromittierender Strahlung	Verstoß gegen Gesetze oder Regelungen	Datenverlust
Ausspähen von Informationen (Spionage)	Unberechtigte Nutzung oder Administration von Geräten und Systemen	Integritätsverlust schützenswerter Informationen
Abhören	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	Schädliche Seiteneffekte IT-gestützter Angriffe
Diebstahl von Geräten, Datenträgern oder Dokumenten	Missbrauch von Berechtigungen	

Abbildung 1: 47 Gefährdungen gem. BSI IT-Grundschutz, eigene Darstellung

Laut dem Bundesamt für Sicherheit in der Informationstechnik entstehen solche Gefährdungen durch

- höhere Gewalt,
- organisatorische Mängel,
- menschliche Fehlhandlungen und / oder
- vorsätzliche Handlungen.

Insbesondere im Bereich der organisatorischen Mängel und bei den menschlichen Fehlhandlungen liegen die größten Potentiale zur Verbesserung der Informationssicherheit. Viele Gefahren lassen sich teilweise erheblich verringern, sofern dem Thema Informationssicherheit in der jeweiligen Organisationseinheit als auch übergreifend der erforderliche Stellenwert beigemessen wird und das Thema vor allem auch als Managementthema verstanden wird. Im Idealfall wird ein sogenanntes Informationssicherheitsmanagementsystem aufgebaut, um die Informationssicherheit nachhaltig zu etablieren, messbar zu machen und kontinuierlich zu verbessern. Im Rahmen eines strukturierten Prozesses lassen sich bestehende organisatorische Schwachstellen und Gefahren durch menschliche Unkenntnis oder fehlendes Problembewusstsein sukzessive verringern. Unter anderem kommt der Komponente Schulung und Sensibilisierung sowohl im Bereich der Kernverwaltung als auch im Bereich der Schulen eine wichtige Rolle zu.

2.2 Schnelle Entwicklung und neue Themen

Die Bedrohungslage in Bezug auf Informationssicherheit hat sich in den vergangenen Jahren deutlich verschärft, sodass sowohl in Unternehmen als auch im Bereich der Öffentlichen Verwaltung bei den IT-Einheiten stellenweise der Eindruck entstanden ist, dass man nur noch auf Ereignisse reagiere, aber kaum noch Ressourcen für Planungen oder Vorsorge habe. Die fortschreitende Digitalisierung und die zunehmende Vernetzung von Systemen haben neue Möglichkeiten geschaffen, um durch Cyberangriffe auf sensible Daten zuzugreifen, bewusst Schaden anzurichten oder beispielsweise einmalig oder wiederholt hohe Geldsummen zu erpressen.

Die folgende Abbildung des Bundesamtes für Sicherheit in der Informationstechnik zur Lage der IT-Sicherheit in Deutschland im Jahr 2022 liefert einen Eindruck, welche Bedrohungen und Mengengerüste im vergangenen Jahr zutreffend waren.

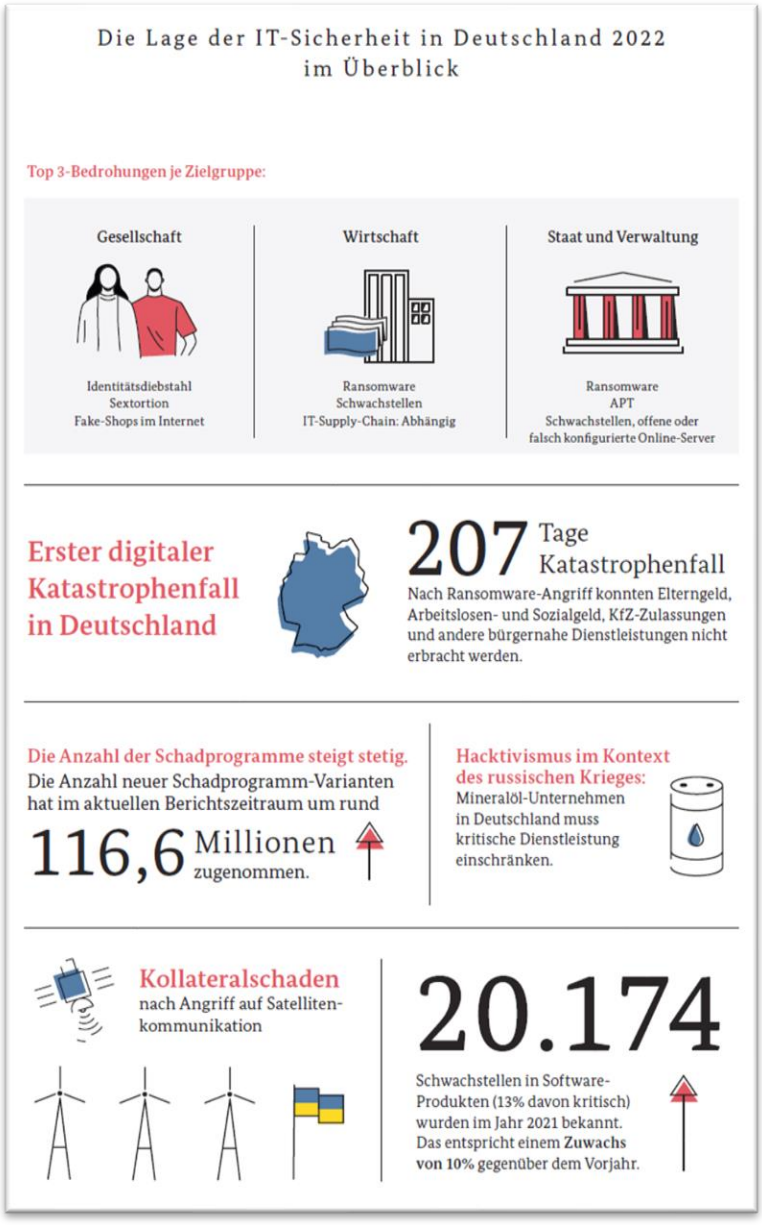


Abbildung 2: Bundesamt für Sicherheit in der Informationstechnik (2022): Die Lage der IT-Sicherheit 2022 im Überblick – Teil 1 von 2

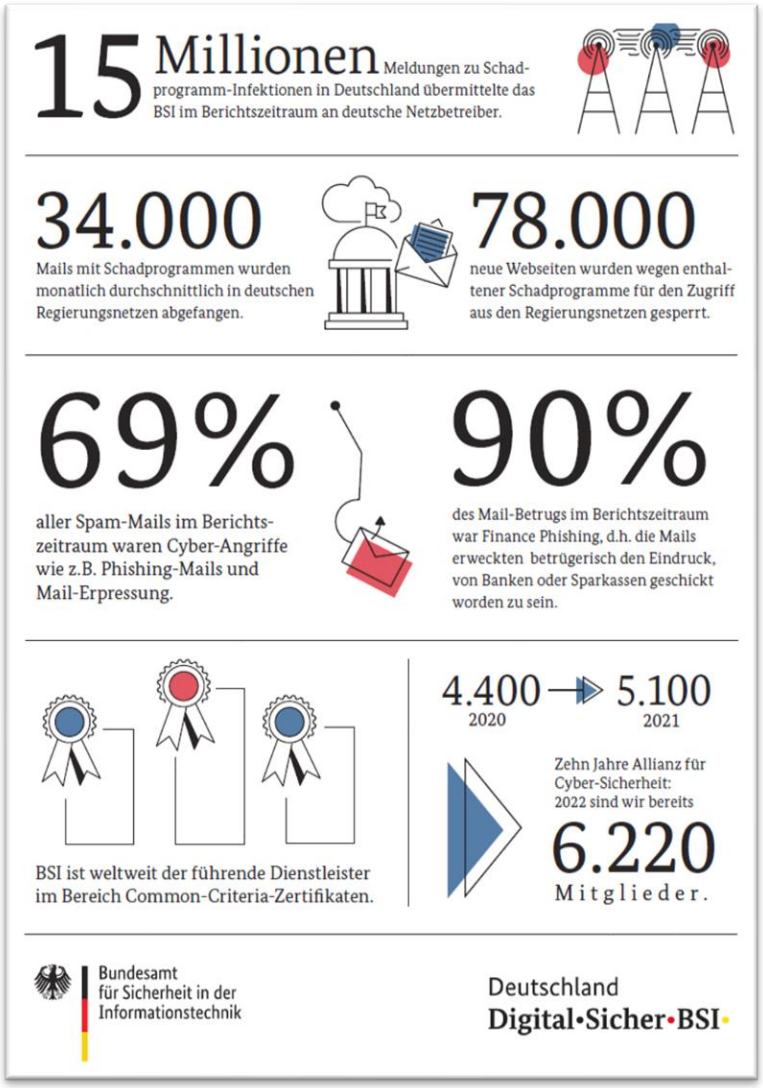


Abbildung 3: Bundesamt für Sicherheit in der Informationstechnik (2022): Die Lage der IT-Sicherheit 2022 im Überblick – Teil 2 von 2

Weitere Ausführungen zu den dargestellten Aspekten sind auf der entsprechenden Website[2] des Bundesamtes zu finden.

Die verschärfte Bedrohungslage ist darauf zurückzuführen, dass Angreifende immer raffiniertere und anspruchsvollere Methoden einsetzen, um bestehende Schwachstellen auszunutzen. Dazu gehören beispielsweise gezielte Phishing-Angriffe, Ransomware-Angriffe, so genannte Zero-Day-Exploits und Social Engineering-Techniken. Die Angreifenden werden zunehmend geschickter darin, unbemerkt vorzugehen. Dies kann beispielsweise sogar dazu führen, dass Schadsoftware in eine Infrastruktur eingeschleust wird, aber nicht unmittelbar, sondern bewusst verzögert nach einigen Wochen oder Monaten mittels dieser Schadsoftware ein Verändern, das komplette Verschlüsseln oder das Abfließen von Daten erfolgt. Sowohl Anzahl als auch Komplexität von Cyberangriffen haben in den vergangenen Jahren erheblich zugenommen. Kriminelle Organisationen haben sich professionalisiert und sind zunehmend finanziell motiviert, da gestohlene Daten verkauft oder direkte

[2] https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Lösegeldforderungen gestellt werden können, um Unternehmen oder öffentliche Organisationen nach Erhalt der Zahlung wieder Zugriff auf ihre Daten zu geben.

Grundsätzlich kann davon ausgegangen werden, dass jede Software oder jedes System potenzielle Schwachstellen aufweist, die von Angreifenden ausgenutzt werden können. Wenn diese Schwachstellen nicht rechtzeitig erkannt und behoben werden, können sie zu Sicherheitslücken führen. Auch unsichere Konfigurationen in IT-Systemen können dazu führen, dass Angreifende Zugang zu Netzwerken und Systemen erhalten. Die steigende Komplexität von Software und die Verwendung von Drittanbieterkomponenten erhöhen das Risiko von Schwachstellen und erfordern eine proaktive Sicherheitsstrategie.

Es ist wichtig, dass öffentliche Verwaltungsorganisationen wie die Stadt Rheine aber auch Einzelpersonen, bspw. Mitarbeitende oder Lehrkräfte der Stadt Rheine in ihrem privaten Umfeld, sich dieser verschärften Bedrohungslage bewusst sind und angemessene Sicherheitsmaßnahmen ergreifen, um ihre Systeme und Daten zu schützen. Regelmäßige Aktualisierungen von Software, Schulungen der Mitarbeiterinnen und Mitarbeiter in Bezug auf Sicherheitsbewusstsein, die Implementierung von Sicherheitsrichtlinien und technische Sicherheitsmaßnahmen sind nur einige der Maßnahmen, die ergriffen werden können, um der steigenden Bedrohung entgegenzuwirken.

Ein anschauliches Beispiel dafür, wie schnell neue Themen aufkommen können, mit denen man sich als Öffentliche Verwaltung hinsichtlich Informationssicherheit beschäftigen muss, ist ChatGPT[3]. Zu Beginn dieses Projekts im Oktober 2022 zeigte sich noch keine wesentliche Relevanz für den öffentlichen Bereich. Dies hat sich seit Ende des Jahres 2022 erheblich geändert, da dieses Thema nun allgegenwärtig zu sein scheint und neben erheblichen Potenzialen auch eine Reihe von Risiken mit sich bringt. Mit dieser neuen Situation müssen sich Bund, Länder und Kommunen in unterschiedlichem Detailgrad befassen. Das Bundesamt für Sicherheit in der Informationstechnik hat im Mai 2023 eine Veröffentlichung herausgegeben, die Chancen und Risiken dieser so genannten großen KI-Sprachmodelle für Industrie und Behörden beschreibt[4].

2.3 Aktuelle Beispiele

Öffentliche Verwaltungen, Schulen und Bildungseinrichtungen können weltweit Ziel von Cyberangriffen werden können. In den letzten Jahren wurden verschiedene Arten von Angriffen auf Verwaltungen gemeldet, bspw. auch seit wenigen Jahren verstärkt im Bereich von Hochschulen. Da Schulen in der technologischen Entwicklung erfahrungsgemäß den Hochschulen gegenüber einige Jahre zurückliegen[5], bilden sich vermehrte Angriffsszenarien möglicherweise erst in der nahen Zukunft. Grundsätzlich kann keine Kommune und

[3] ChatGPT ist ein Sprachmodell, das auf der GPT-3.5-Architektur von OpenAI basiert. Es wurde entwickelt, um menschenähnliche Gespräche zu simulieren und Fragen zu beantworten. ChatGPT kann eine Vielzahl von Themen behandeln, indem es auf das Wissen zugreift, das während seines Trainings erworben wurde. Es kann Text verstehen, generieren und darauf reagieren, um mit Benutzer:innen in natürlicher Sprache zu interagieren. Das Modell wird kontinuierlich verbessert, basierend auf fortlaufendem Training und Updates von OpenAI. (https://chat.openai.com)

[4] Bundesamt für Sicherheit in der Informationstechnik (2023): Große KI-Sprachmodelle - Chancen und Risiken für Industrie und Behörden

[5] Vgl. z.B. die nahezu flächendeckende Verbreitung von Campus-Management-Systemen und Identity- und Access-Management-Systemen seit Mitte der 2000er Jahre an Hochschulen im Gegensatz zur Verbreitung von Schulmanagementsystemen und entsprechender Infrastrukturen.

keine Einrichtung ausschließen, Opfer solcher Angriffe zu werden. Diese können sich jedoch entsprechend darauf vorbereiten, das Sicherheitsniveau und damit die Auswirkungen möglicher Attacken massiv abzumildern. Die Stadt Rheine und ihre Schulen könnten und sollten in die Lage versetzt werden, bei entsprechenden Angriffen strukturiert und vorausgeplant im Sinne eines Notfallmanagements zu agieren.

Sehr stark treten in der aktuellen Zeit so genannte Phishing-Angriffe auf, die darauf abzielen, sensible Informationen wie Zugangsdaten zu stehlen, indem sie sich als vertrauenswürdige Quellen ausgeben. Angreifende können gefälschte E-Mails oder Websites verwenden, um beispielsweise Schüler:innen, Lehrkräfte oder Angestellte der Schulverwaltung dazu zu verleiten, persönliche Informationen preiszugeben. Auch so genannte Ransomware-Angriffe sind weit verbreitet. Bei solchen Angriffen werden beispielsweise die Systeme der Schulen mit schädlicher Software infiziert, um unmittelbar oder verzögert den Zugriff auf Daten und Systeme zu blockieren. Die Angreifenden verlangen dann in der Regel ein Lösegeld, um den Zugriff auf die blockierten Daten und Systeme wiederherzustellen. Ein drittes Beispiel sind so genannte Distributed Denial of Service (DDoS)-Angriffe. Bei diesen wird versucht, eine Website oder ein Netzwerk durch eine Überlastung mit Datenverkehr lahmzulegen, sodass die regulären Benutzer:innen keinen Zugriff mehr haben.

Es ist wichtig zu beachten, dass die Bedrohungslandschaft ständig im Wandel ist und kontinuierlich neue Angriffstechniken entwickelt werden. Daher ist es nicht nur ratsam, sondern dringend erforderlich, dass Kommunen wie die Stadt Rheine hinsichtlich der Informationssicherheit nicht mehr nur „auf Sicht fahren“ beziehungsweise schlimmstenfalls nur auf Ereignisse reagieren, sondern in Form einer explizit und ausschließlich für die Informationssicherheit zuständigen Personen einen deutlichen Vorsprung aufbauen und sich neben der Bearbeitung der Themen auch informieren und auf dem Laufenden halten können, um Bedrohungslagen einschätzen und adäquat reagieren zu können.

Laut Berichten der Rheinischen Post im Dezember 2022 nehmen Cyberangriffe in den kommunalen Verwaltungen und Universitäten Nordrhein-Westfalens stetig zu. Der Sprecher der Zentral- und Ansprechstelle Cybercrime (ZAC) berichtete in diesem Zuge, dass er die Anzahl an Angriffen, wie sie zur aktuellen Zeit stattfinden würden, während seiner bisherigen Amtszeit noch nicht erlebt habe. **Die Mehrheit dieser Vorfälle würde der Öffentlichkeit gar nicht bekannt gegeben**. Eine interne Umfrage der Rheinischen Post ergab, dass insbesondere die IT-Infrastruktur von Stadtverwaltungen und Hochschulen in Nordrhein-Westfalen nahezu täglich mit Cyberangriffen konfrontiert werden würden. Aus Sicht der Behörden basiere die Herangehensweise auf hoher Professionalität. Laut dem ZAC werden Universitäten normalerweise nicht gezielt angegriffen, sondern werden vielmehr zu Kollateralschäden großer Cyberattacken, die auf Sicherheitslücken im Internet abzielen.[6] Demgegenüber wurde die Universität Duisburg-Essen (UDE) im November 2022 gezielt Opfer eines Ransomware-Angriffes der Hackergruppe Vice Society, die sich auf Ransomware-Angriffe im Gesundheits- und Bildungssektor spezialisiert hat. Nach dem Cyberangriff mussten alle E-Mail-, Kommunikations- und IT-Systeme außer Betrieb genommen werden, sodass der Lehrbetrieb der Universität, die 43.000 Studierende, 4.000 akademische Mitarbeiter und 1.500 Verwaltungsmitarbeiter umfasst, über mehrere Tage eingestellt

[6] RHEINISCHE POST. Cyberangriffe nehmen zu. NRW-Städte fast täglich Ziel von Hackern. 10.12.2022. https://rp-online.de/nrw/panorama/hacker-cyberangriffe-auf-staedte-und-universitaeten-in-nrw_aid-81175575. Abgerufen am: 25.05.2023

wurde. Die UDE teilte mit, dass der Schaden 1.200 Server und die Kompromittierung des zentralen Autorisierungssystems betreffe, was dazu führte, dass die gesamte IT-Infrastruktur wieder neu aufgebaut werden musste. Sowohl die IT-Infrastruktur als auch die Datenlage konnte bis heute nicht vollständig wiederhergestellt werden. Nachdem sich die Universität gegen das Zahlen der Lösegeldforderungen entschieden hatte, veröffentlichte die Vice Society gestohlene Datensätze der Universität im Darknet.[7]

Die Hochschule Ruhr West in Mühlheim und Bottrop, die Anfang 2023 Opfer eines Hackerangriffes wurde, konnte dem Datenverlust aufgrund der schnellen Reaktionsfähigkeit der IT-Mitarbeitenden entgegenwirken. In Folge des Angriffes wurden alle Hochschulsysteme vom Netzbetrieb getrennt, die Endgeräte der Lehrenden und der etwa 6.500 Studierenden heruntergefahren. Für die Gesamtheit der Nutzergruppen wurden neue Zugänge mit entsprechenden Zugangsdaten generiert. Der zu der Zeit stattfindende Prüfungsbetrieb konnte bis auf die Abnahme der Online-Prüfungen weitestgehend durchgeführt werden.[8]

Mit einem ähnlichen Ausmaß sah sich die Fachhochschule Münster, die im Juni 2022 Opfer eines Hackerangriffes wurde, konfrontiert. Nachdem der Angriff durch die IT-Mitarbeitenden erkannt wurde, konnten alle universitären Systeme umgehend vom Netzbetrieb getrennt werden. Als provisorische Lösung für den Lehrbetrieb wurde eine Website eingerichtet, die den 15.400 Studierenden und Lehrenden zur Verfügung gestellt wurde. Zu einer Datenverschlüsselung kam es in diesem Fall nicht.[9]

Wesentlich weitreichender sind die Auswirkungen des aktuell veröffentlichen Cyberangriffes durch die BianLian auf das Basler Schulnetz, genauer genommen auf den Bildungsserver eduBS. Bereits im Januar 2023 haben sich Angreifer vermutlich über ein kompromittiertes Passwort eines Mitarbeitenden Zugriff auf den Bildungsserver verschafft und die dort hinterlegten sensiblen Daten, wie schulpsychologische Berichte, Zeugnisse und diverse weitere Datensätze heruntergeladen. Das zuständige Erziehungsdepartment, vergleichbar mit dem deutschen Bildungsministerium, schätzte das Schadensausmaß zunächst als geringfügig ein, kam der gestellten Lösegeldforderung nicht nach und erstellte Strafanzeige. Daraufhin wurden etwa 1,2 Terabyte der gestohlenen, unter anderem hochsensible Datensätze im Darknet veröffentlicht. Der Regierungsrat teilte mit Bedauern mit, dass sie die Maßnahmen hinsichtlich der Datensicherheit bereits lange vor dem Angriff unter intensiven Bemühungen optimiert hätten. Da selbst diese Maßnahmen mittlerweile wieder überholt seien, schlussfolgerte er, dass man bereits viel eher in die Sicherheitsinfrastruktur hätte investieren müssen.[10]

---

[7] Bleeping Computer. Vice Society ransomware leaks University of Duisburg-Essen's data. 16.01.2023. https://www.bleepingcomputer.com/news/security/vice-society-ransomware-leaks-university-of-duisburg-essen-s-data/. Abgerufen am: 25.05.2023

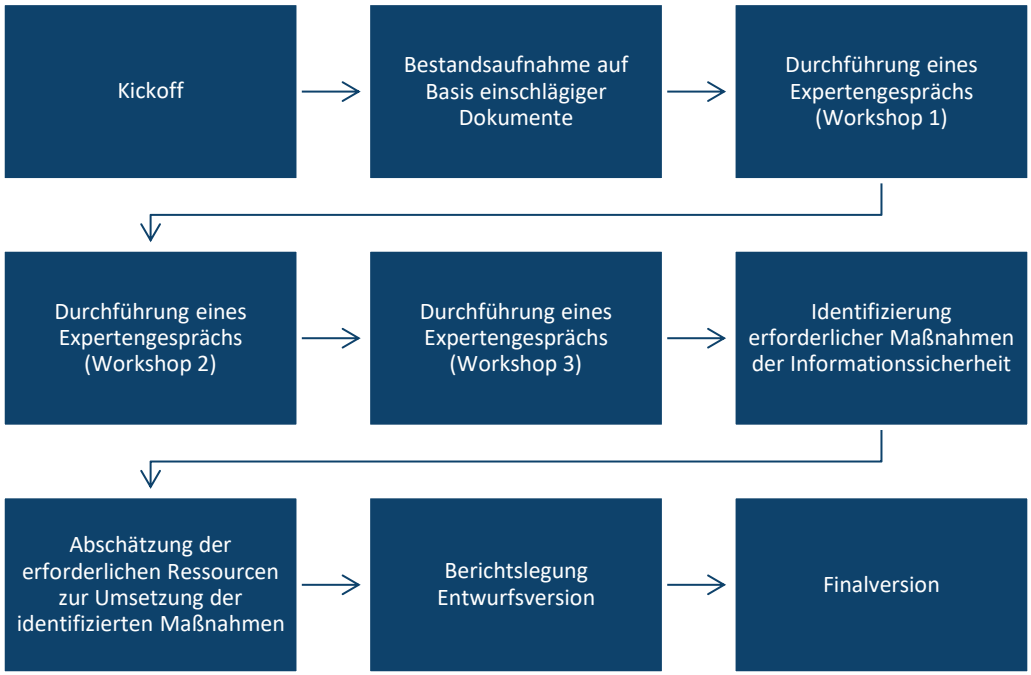
[8] WDR. Kein Datenklau bei Hackerangriff auf Hochschule Ruhr West. 06.02.2023. https://www1.wdr.de/nachrichten/ruhrgebiet/hochschule-ruhr-west-wohl-opfer-von-hackeran-griff-100.html. Abgerufen am: 25.05.2023

[9] WDR. Hackerangriff auf Fachhochschule Münster. 23.06.2022. https://www1.wdr.de/nachrichten/westfalen-lippe/hackerangriff-fachhochschule-muenster-fh-100.html. Abgerufen am: 25.03.2023

[10] heise online. Basler Schulnetz gehackt, Schülerdaten im Darknet. 16.05.2023. https://www.heise.de/news/Gescheiterte-Erpresser-posten-Daten-Basler-Schueler-9056730.html. Abgerufen am: 25.05.2023

3 Vorgehen

Das Vorgehen im Rahmen der Untersuchung bestand aus den folgenden Schritten:



3.1 Dokumentenanalyse

Zu Beginn des Projekts sind dem Auftragnehmer Dokumente bereitgestellt worden, von denen eine Einschlägigkeit für die Analyse der Situation zur Informationssicherheit in der Stadt Rheine angenommen werden konnte. Darunter befanden sich unter anderem eine Leitlinie für Informationssicherheit der Stadt Rheine, eine IT-Sicherheitsrichtlinie der Stadt Rheine sowie ein Netzplan.

Im Bereich der Schul-IT sind im Rahmen eines Vorläuferprojektes bereits Daten erhoben worden, die im aktuellen Projekt in aktualisierter Form weiterverwendet werden sollten. Daher sind die Kollegen der Schul-IT gebeten worden, diese Daten zu aktualisieren. Die Kollegen der Verwaltungs-IT sind gebeten worden, diese Daten ebenfalls zu erheben und zu liefern.

Ergänzend zu den erhaltenen Daten und Dokumenten sind eigene Recherchen durchgeführt worden, um einschlägige Dokumente zu berücksichtigen. Dies waren Dokumente zu fachlich relevanten Themen, beispielsweise des Bundesamtes für Informationssicherheit in der Informationstechnik zu IT-Grundschutz[11], zu den betreffenden Standards zu Managementsystemen für Informationssicherheit (200-1)[12], zur Grundschutz-Methodik (200-2)[13],

[11] Bundesamt für Sicherheit in der Informationstechnik (2023): IT-Grundschutz-Kompendium

[12] Bundesamt für Sicherheit in der Informationstechnik (2017): BSI-Standard 200-1 - Managementsysteme für Informationssicherheit (ISMS)

[13] Bundesamt für Sicherheit in der Informationstechnik (2017): BSI-Standard 200-2 - IT-Grundschutz-Methodik

zur Risikoanalyse (200-3)[14] und dem Business Continuity Management (200-4)[15] sowie der frühere BSI-Standard zu Notfallmanagement (100-4)[16], aber beispielsweise auch eine Informationssicherheitsleitlinie des für Schulen zuständigen Landesministeriums.[17]

3.2 Expertengespräche / Workshops

Um über die Dokumenteninhalte hinausgehende Informationen zu konkreten Themen der Informationssicherheit sowie zu individuellen Sichtweisen zu erfassen, wurden Expertengespräche mit einschlägigen Vertretern der Stadt Rheine geführt. Dabei waren Kollegen sowohl von der Verwaltungs-IT als auch von der Schul-IT vertreten und jeweils aktiv beteiligt.

Für die Zusammenarbeit wurde das Tool Conceptboard gewählt, welches eine kollaborative Zusammenarbeit an Themen und deren Dokumentation ermöglicht.

Auf Basis der 47 im IT-Grundschutz-Kompendium formulierten Gefährdungslagen[18] erfolgte eine inhaltliche Befassung, indem das BSI IT-Grundschutz Schichtenmodell[19] herangezogen worden ist und so für die Stadt Rheine relevante Themenbereiche vertieft werden konnten.

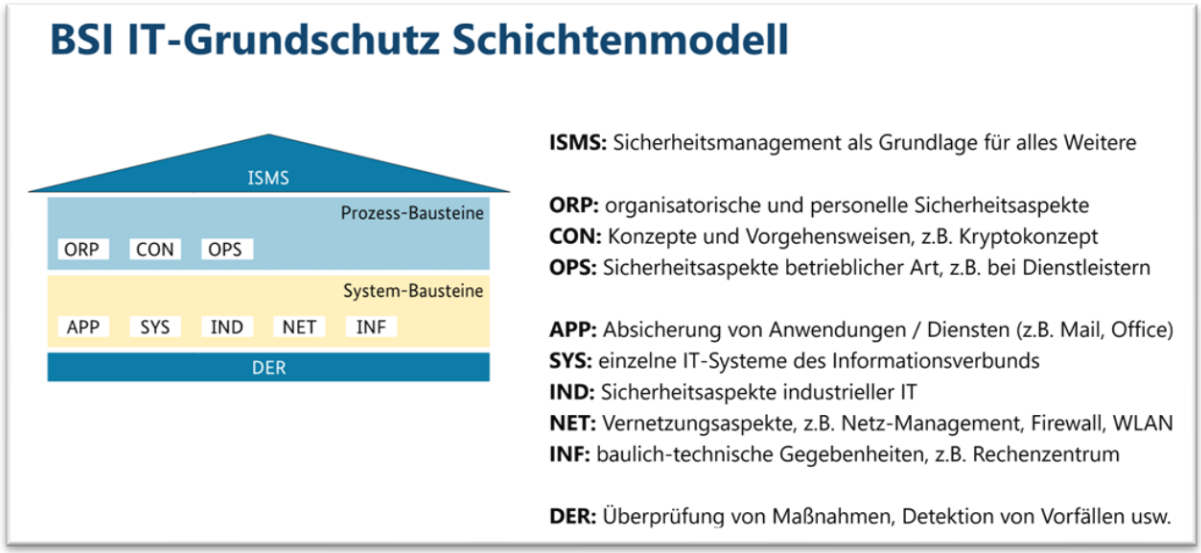


Abbildung 4: IT-Grundschutz Schichtenmodell aus dem Grundschutz Kompendium mit eigenen Anmerkungen zu den Bausteinen

[14] Bundesamt für Sicherheit in der Informationstechnik (2017): BSI-Standard 200-3 - Risikoanalyse auf der Basis von IT-Grundschutz

[15] Bundesamt für Sicherheit in der Informationstechnik (2022): BSI-Standard 200-4 - Business Continuity Management (Hinweis: Lag zum Untersuchungszeitpunkt als sog. Community Draft 2.0 vor und ersetzt und erweitert den früheren Standard 100-4)

[16] Bundesamt für Sicherheit in der Informationstechnik (2008): BSI-Standard 100-4 - Business Continuity Management (Notfallmanagement)

[17] Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen (2022): Informationssicherheitsleitlinie MSB

[18] Bundesamt für Sicherheit in der Informationstechnik (2023): IT-Grundschutz-Kompendium, S. 11ff.

[19] Bundesamt für Sicherheit in der Informationstechnik (2023): IT-Grundschutz-Kompendium, S. 9f.

Ausgewählte Bausteine wurden bearbeitet, wobei das Erkenntnisinteresse zum einen im „Reifegrad“ des jeweiligen Bereichs lag sowie in der Identifizierung individuellen Handlungsfeldern, um mittelfristig durch die Stadt Rheine eine Umsetzung der Basis- und Standardanforderungen des IT-Grundschutzes zu gewährleisten. Dabei wurde auch besonderes Augenmerk auf mögliche Synergiepotenziale gelegt.

Die Behandlung der Themen aus den Bausteinen ISMS und DER, aus den Prozess-Bausteinen ORP und OPS sowie aus den System-Bausteinen APP, SYS, NET, INF lieferte wertvolle Hintergrundinformationen zum jeweiligen Ist-Stand und ermöglichte eine Reihe von themenbezogenen Diskussionen.

Zur Ergebnissicherung erfolgte die Dokumentation seitens der Teilnehmenden im Conceptboard, sodass hier je Themenbereich der aktuelle Stand, individuelle Bedarfe sowie Synergiepotenziale festgehalten werden konnten.

Die Bereiche und Bausteine, die Gegenstand der Workshops waren, sind in Anhang A.1 aufgelistet.

3.3 Konsolidierung und Berichtslegung

Im April und Mai 2023 wurden die Ergebnisse ausgewertet und ein Bericht (Kurzgutachten) gefertigt. Eine Vorversion des Berichts wurde vereinbarungsgemäß in der 22. KW 2023 zur Prüfung an die Verwaltungs-IT und an die Schul-IT übermittelt.

Nach erfolgter Rückmeldung wurde eine finale Berichtsversion (Version 1.0) gefertigt und am 07.07.2023 vorgelegt. Aufgrund zusätzlicher Rückmeldung wurde eine erweiterte finale Berichtsversion (Version 1.01) am 31.08.2023 vorgelegt.

4 Erkenntnisse

In diesem Kapitel werden die wesentlichen Erkenntnisse dargestellt, die sich einerseits aus der Dokumentenanalyse und andererseits aus den Expertengesprächen (Workshops) ergeben haben. Insbesondere die Workshops lieferten viele nützliche Details, die erheblich zu den im Folgenden skizzierten Erkenntnissen beigetragen haben.

4.1 Nutzbare Erkenntnisse aus GPA-Gutachten

Die überörtliche Prüfung der Stadt Rheine im Jahr 2021 durch die Gemeindeprüfungsanstalt Nordrhein-Westfalen (GPA) kommt zu der Einschätzung, dass aufgrund des aktuellen Standes der Digitalisierung bei einem Ausfall der IT die Arbeit in nahezu allen Verwaltungsbereichen vollständig zum Erliegen kommen würde und dass die Verwaltung mehr denn je davon abhängig sei, dass die IT möglichst störungsfrei funktioniert und die zu verarbeitenden Daten angemessen geschützt sind. Der entsprechende Prüfbericht hält weiterhin fest, dass die technische Infrastruktur und der konzeptionelle Rahmen dem Schutzbedarf der zu verarbeitenden Daten und den strategischen Vorgaben gerecht werden müssen und empfiehlt das Auseinandersetzen mit Notfallszenarien sowie die Erarbeitung verbindlicher Vorgaben für die operative IT hinsichtlich potenzieller Systemausfälle und Datenverluste. [20]

Der Prüfbericht gibt weiterhin an, dass Defizite im konzeptionellen Bereich der Schulen bestehen. Vor dem Hintergrund der steigenden Abhängigkeit der Schul-IT von einer funktionierenden und verfügbaren IT-Infrastruktur sieht es die GPA als erforderlich an, ein umfassendes Notfall- und Sicherheitsmanagement zu etablieren. Die GPA beschreibt dies als die konzeptionelle Basis für eine nachhaltig wirksame Informationssicherheit.[21]

Zugleich wurde der Stadt Rheine damit im Jahr 2021 ein hohes Sicherheitsniveau bescheinigt. Handlungsbedarf wird beim Notfallkonzept gesehen. Es wird angegeben, dass die Stadt Rheine im Verhältnis zu den geprüften großen kreisangehörigen Städten einen Spitzenplatz belegt und dass der festgestellte Gesamterfüllungsgrad bei 81,9 Prozent und damit über dem Mittelwert von 75,0 Prozent liegt. Begründet wird das erreichte Sicherheitsniveau durch eine gute technische und räumliche Infrastruktur sowie durch bereits umgesetzte Maßnahmen. Im Bereich Notfallvorsorge wird Handlungsbedarf attestiert.[22]

Zur Interpretation sollten die Rahmenbedingungen der GPA-Prüfung berücksichtigt werden. Es wird angegeben, dass die Betrachtung der IT-Sicherheit rein systemisch, d.h. in Form ausgewählter Sicherheitsaspekte erfolgt, um Rückschlüsse auf die gesamte IT-Sicherheitsstruktur der Verwaltung zu ziehen. Dabei ist das Ziel herauszulesen, grundsätzliche Problemstellungen in den Verwaltungen zu identifizieren. Im Detail sind dabei 77 ausgewählte Einzelaspekte des BSI-Grundschutzkataloges geprüft worden. Die Ergebnisse liegen im Prüfbericht aufgrund möglicher Sensibilität bewusst zusammengefasst vor.[23]

Das gute Abschneiden im Vergleich zu anderen Kommunen ist für die Stadt Rheine grundsätzlich erst einmal zu begrüßen. Dies sollte aber nicht zum Anlass genommen werden, der

[20] Für die Untersuchung lag die Version des GPA-Berichts für die Stadt Rheine mit der Angabe 050.010.030_02370 vor. Im Rahmen der Untersuchung wurden die Seiten 28 bis 35 ausgewertet. Die Kernaussagen für den relevanten Untersuchungsgegenstand werden hier wiedergegeben.

[21] ebd.

[22] ebd.

[23] ebd.

Informationssicherheit fortan keine besondere Bedeutung mehr beizumessen. Wie eingangs geschildert, erlaubt die Bedrohungslage kein Pausieren. Das Gegenteil ist der Fall: Die Kommunen müssen sich genauso wie private Unternehmen stärker als je zuvor bewusst um das Thema kümmern.

Die folgenden Abschnitte erläutern exemplarisch, dass Bedarf dafür besteht, Informationssicherheit in der Stadt Rheine inklusive der Schulen strukturiert umzusetzen. Zur im Vergleich überdurchschnittlichen Bewertung ist anzumerken, dass die theoretische Möglichkeit besteht, dass die Gemeindeprüfanstalt beispielsweise die Existenz einer Person in der Rolle des bzw. der Informationssicherheitsbeauftragten bewertet hat. Dies wäre für die Stadt Rheine in der Theorie der Fall und damit erfüllt. Im Rahmen der Expertenworkshops ist jedoch bekannt geworden, dass diese Rolle nicht im Sinne der Aufgabenbeschreibung eines beziehungsweise einer Informationssicherheitsbeauftragten ausgefüllt wird. Falls diese Rahmenbedingung in die Bewertung mit einfloss, bestünde hier im Papier ein Vorteil im Vergleich zur Realität.

4.2 Veralteter Stand der Leitlinie für Informationssicherheit und der IT-Sicherheitsrichtlinie der Stadt Rheine

Für die Stadt Rheine existiert eine fünfseitige Leitlinie zur Informationssicherheit, unterzeichnet im März 2015 durch die damalige Bürgermeisterin. Die Leitlinie besteht aus sechs Kapiteln und regelt auf insgesamt drei inhaltlichen Seiten Notwendigkeit und Geltungsbereich, Sicherheitsziele und Sicherheitsstrategie, Organisation und Verantwortlichkeiten, Sanktionen, Umsetzung sowie Inkrafttreten.

Darüber hinaus existiert eine elfseitige IT-Sicherheitsrichtlinie der Stadt Rheine, ebenfalls unterzeichnet im März 2015 durch die damalige Bürgermeisterin. Die Richtlinie beschreibt auf acht inhaltlichen Seiten in insgesamt elf Kapiteln erneut Sicherheitsziele und Sicherheitsstrategie und unter anderem Ausführungen zur Verwaltung und Nutzung der IT-Infrastruktur und von IT-Diensten sowie einzelne Sicherheitsmaßnahmen und Regelungen für spezifische Dienste.

Zwar ist in der Leitlinie angegeben, dass die IT-Sicherheitsrichtline in regelmäßigen Abständen unter Berücksichtigung aktueller Gegebenheiten überprüft und gegebenenfalls aktualisiert werden soll, dennoch wirkt das Dokument veraltet. Schulen werden nicht thematisiert, auf aktuelle Gegebenheiten und eine veränderte Bedrohungslage wird aus dem naheliegenden Grund des Entstehungszeitraums nicht eingegangen.

Auch wenn der Dokumentenstand nicht aktuell und in Hinblick auf ein professionelles Informationssicherheitsmanagement nicht vollständig erscheint, wurde in den Workshops deutlich, dass die Verwaltungs-IT der IT-Sicherheit seit jeher einen hohen Stellenwert einräumt. So wurden viele Aspekte eher restriktiv gehandhabt, um Sicherheitsrisiken zu minimieren. In Hinblick auf Schulen funktioniert diese Restriktivität nicht oder nur bedingt. Beispielsweise sind USB-Sticks ein beliebtes Hilfsmittel, um Dateien auszutauschen oder auf Schulhardware zu verwenden. Eine Sperrung von USB-Ports würde hier sicherlich nicht zielführend sein, sodass hier geeignetere Maßnahmen, z.B. Schulung und Sensibilisierung, eine wichtige Rolle spielen.

4.3 Informationssicherheitsstrategie des Ministeriums für Schule und Bildung

Hinweise auf die Beantwortung der Frage nach Zuständigkeiten in Hinblick auf die Informationssicherheit liefert die elfseitige Leitlinie zur Informationssicherheit im Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen (Informationssicherheitsleitlinie MSB) in der aktualisierten Fassung vom 07.11.2022.[24]

Die Leitlinie trifft u.a. Aussagen zum Stellenwert der Informationssicherheit, zum angestrebten Schutzniveau, zu Sicherheitszielen sowie zum organisatorischen Rahmen der Umsetzung. Kapitel 3 regelt den Geltungsbereich der Leitlinie. Dieser umfasst neben dem Ministerium die Qualitäts- und Unterstützungsagentur - Landesinstitut für Schule, das Landesprüfungsamt für Lehrämter an Schulen, die Zentren für schulpraktische Lehrerausbildung, das Haus für Lehrerfortbildung Kronenburg und die staatlichen Schulen.

In Abschnitt 3.2 werden Aussagen über Kommunen des Landes getroffen. **Die Leitlinie hat für diese nur empfehlenden Charakter, sodass die öffentlichen Schulen in kommunaler Trägerschaft, die Ersatzschulen und weitere Stellen nicht in den Geltungsbereich fallen. Dennoch wird die Anwendung dieser Leitlinie seitens des Ministeriums empfohlen.**

Die Leitlinie des Ministeriums regelt in Kapitel 6 Einzelheiten zur Informationssicherheitsstrategie. Der zu etablierende Sicherheitsprozess basiert auf der Einführung eines Informationssicherheitsmanagementsystems (ISMS) auf der Basis von IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik. Die Sicherheitsstrategie enthält gemäß Leitlinie die Komponenten Sensibilisierung, Risikoanalyse, Vorfallmanagement und Notfallmanagement.

Darüber hinaus wird die Zusammenarbeit mit den Kommunen wie folgt beschrieben:

„Das MSB kooperiert insbesondere mit den kommunalen Spitzenverbänden, den kommunalen IT-Dienstleistern, den Schulleitungen und den benannten IT-Sicherheitsbeauftragten der Kommunen.

Für die sächliche Ausstattung der öffentlichen Schulen sowie für die der staatlichen Schulämter und der Ämter für Ausbildungsförderung sind die Kommunen zuständig. Die Schulleitungen und die Landesbeschäftigten in Leitungsfunktionen haben auf die Sachausstattung, die installierte Software, die Netzwerke und die Sicherheitsmechanismen in der Regel keinen Einfluss. Beschaffung, Wartung, Pflege und Administration von informationsverarbeitenden Systemen sind in kommunaler Hand.“[25]

Daraus leitet sich ab, dass die Informationssicherheitsleitlinie des Ministeriums für die vorliegenden Fragestellungen lediglich empfehlenden Charakter hat. Die Frage der Zuständigkeit von Aspekten der Informationssicherheit (Schul-IT, Schulleitungen) lässt sich im Rahmen dieses Gutachtens nicht abschließend klären. Problematisch könnte dies dann werden,

[24] Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen (2022): Informationssicherheitsleitlinie MSB, https://schulministerium.nrw/system/files/media/document/file/informationssicherheitsleitlinie_msb_221219.pdf, Abruf: 24.05.2023

[25] Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen (2022), S. 7 f.: Informationssicherheitsleitlinie MSB, https://schulministerium.nrw/system/files/media/document/file/informationssicherheitsleitlinie_msb_221219.pdf, Abruf: 24.05.2023

wenn die Schul-IT übergreifende Vorgaben (z.B. zu Passwortrichtlinien) machen möchte, (einzelne) Schulleitungen jedoch eine Kooperation ablehnen.

Grundsätzlich sollte versucht werden, die Akzeptanz für umzusetzende Maßnahmen bei den Schulleitungen zu erlangen, sodass Schul-IT und Schulleitungen beim Thema Informationssicherheit an einem Strang ziehen, nennenswerte Fortschritte erzielen und keine Seite dieses wichtige Thema ausbremst.

Jeder Fortschritt bei der Informationssicherheit bedeutet ein reduziertes Risiko für Angriffe und Gefährdungen, deren Folgen einerseits nicht absehbar sind, aber erfahrungsgemäß großen Aufwand zur Wiederherstellung von Daten und zum Wiederanlauf von Intrastrukturen und Systemen nach sich ziehen würden.

Sollte es im Verlauf der Umsetzung zu Konflikten hinsichtlich der Zuständigkeiten kommen, kann ggf. ein Erfahrungsaustausch mit ähnlich aufgestellten Kommunen zu Best Practices betrieben werden. Darüber hinaus könnte das zuständige Ministerium um Einschätzung zum Sachverhalt gebeten werden.

4.4 Fehlende reale Zuständigkeiten für Informationssicherheit

In den Workshops wurde berichtet, dass die Verwaltungsleitung grundsätzlich ihre Gesamtverantwortung für Informationssicherheit kenne. Eine Person mit der Rolle Informationssicherheitsbeauftragte:r ist zwar formal vorhanden, verfügt aber nur über geringe Ressourcen. Eine für die Schulen zuständige Person in der Rolle Informationssicherheitsbeauftragte:r existiert nicht.

Im Rahmen der Workshops wurde deutlich, dass bereits heute von den Kollegen der Verwaltungs-IT im Tagesbetrieb der IT, bei der Durchführung von IT-Projekten oder bei der Mitarbeit von verwaltungsweiten Projekten von allen IT-Mitarbeitenden operative Tätigkeiten im Bereich der Sicherheit wahrgenommen werden. Es wurde jedoch erkennbar, dass dies oftmals eher intuitiv und unstrukturiert sowie ohne aktuellem IT-Sicherheitskonzept und ebenfalls ohne Abstimmung mit einem bzw. einer Informationssicherheitsbeauftragten geschieht, weil eine solche Person defacto nicht vorhanden ist.

Die Kollegen stellen bereits heute Defizite in den Bereichen Notfallmanagement und -vorsorge, Benutzersensibilisierung, Updatemanagement und allgemeines proaktives Handeln für IT-Security fest.

4.5 Hohe IT-Eigenständigkeit

Da die Stadt Rheine über ein sehr hohes Maß an IT-Eigenständigkeit verfügt, haben die wahrgenommenen Tätigkeiten im Bereich der Informationssicherheit auch aus Sicht der entsprechenden Kollegen eine enorme Wichtigkeit und Wertigkeit.

Als wichtige Rahmenbedingung ist zu bewerten, dass die Stadt Rheine keinem kommunalen Rechenzentrum angehört. Notwendige operative Maßnahmen zur Informationssicherheit können daher nicht ausgelagert werden.

Folgende Infrastrukturkomponenten bzw. Dienste werden durch die Verwaltungs-IT der Stadt Rheine eigenständig betrieben:

- Daten- und das TK-Netz inkl. der kompletten Netzinfrastruktur (auch zu/in den städtischen Nebengebäuden),

- sämtliche Firewall- und Netzwerksicherheitssysteme,
- geschützte Zugriffe der Benutzer:innen auf das Web,
- die Absicherung eigener Webserver,
- E-Mail-Infrastruktur inkl. Mail-Server, Spam- und Content-Filter, mehrstufiger Virenschutz,
- redundantes File-Hosting und Datenbankinstallationen inkl. Rechtevergabe,
- Endpointsecurity am Arbeitsplatz.

Die Kollegen haben berichtet, dass der Prüfbericht der Gemeindeprüfungsanstalt NRW aus 2021 bescheinigt hat, dass die Stadt Rheine die sich aus ihrem IT-Betriebsmodell ergebenden Kostenvorteile nutze und dass das Betriebsmodell der weitestgehend eigenverantwortlichen IT-Bereitstellung strategische Möglichkeiten biete, die IT unmittelbar und zielgerichtet zu gestalten.

Aufgrund der hohen IT-Eigenständigkeit der Stadt Rheine berühren fast alle operativen Tätigkeiten der IT-Mitarbeiter den Bereich der Informationssicherheit und erfordern dort personellen Aufwand.

4.6 Eigene:r ISB vs. externer ISB

Der beschriebene erforderliche personelle Aufwand wird sich notwendigerweise absehbar erhöhen, wenn es zukünftig eine Interaktion zwischen einem bzw. einer Informationssicherheitsbeauftragten und den IT-Einheiten geben wird. Der zukünftige operative Aufwand der IT-Einheiten wird dann maßgeblich von den definierten Anforderungen des oder der Informationssicherheitsbeauftragten abhängig sein und deutlich ansteigen[26].

Dies spricht für die Notwendigkeit einer Person vor Ort, die die Rolle des oder der Informationssicherheitsbeauftragten ausfüllt. Eine nur gelegentliche Inanspruchnahme eines bzw. einer externen Informationssicherheitsbeauftragten erscheint überhaupt nicht zielführend. Eine solche Person sollte neben der IT-Abteilung permanent und grundsätzlich in alle Prozesse der Stadt eingebunden werden, die Auswirkungen auf die Informationssicherheit haben. Dies gilt in gleichem Maße für alle relevanten Belange der Schulen. Neben der Kernverwaltung und den Schulen haben auch andere Stellen wie Feuerwehr und Eigenbetriebe Bedarf an einer guten Arbeit des bzw. der Informationssicherheitsbeauftragten und an individueller Berücksichtigung.

[26] Vgl. Tabelle 1 auf Seite 17 zur groben Gegenüberstellung strategischer und operativer Tätigkeiten bzw. Themen der Informationssicherheit

Strategische Tätigkeiten	Operative Tätigkeiten
Compliance-Management Überwachung und Einhaltung von Sicherheitsstandards, Vorschriften und gesetzlicher Bestimmungen. Regelmäßige Bewertung der Sicherheitsmaßnahmen. Sicherstellung der Konformität mit Datenschutzbestimmungen und branchenspezifischen Anforderungen.	**Sicherheitsüberwachung** Kontinuierliche Überwachung von Systemen, Netzwerken und Anwendungen. Erkennung verdächtiger Aktivitäten, Anomalien oder Sicherheitsverletzungen. Auswertung von Sicherheitsprotokollen und Durchführung von Analysen.
Konzeption einer Sicherheitsarchitektur Entwicklung und Aufbau einer umfassenden Sicherheitsarchitektur. Gestaltung von Netzwerkarchitekturen, Firewalls, Angriffserkennungssystemen und weiteren Sicherheitsinfrastrukturen. Berücksichtigung von Sicherheitsaspekten bei der System- und Softwareentwicklung.	**Reduzierung von Schwachstellen** Identifizierung von Schwachstellen in Systemen und Anwendungen. Durchführung von Schwachstellenscans und Penetrationstests. Behebung oder Minderung von Schwachstellen zur Reduzierung von Angriffsmöglichkeiten.
Entwicklung von Sicherheitsrichtlinien Erstellung und Anpassung von Richtlinien, die den Umgang mit IT-Systemen regeln, bspw. Richtlinien zur Passwortverwaltung und Zugriffskontrolle. Etablierung von Standards und Best Practices für die Informationssicherheit der gesamten Stadt Rheine bzw. bestimmter Bereiche (z.B. für alle Schulen).	**Benutzerverwaltung und Zugriffssteuerung** Verwaltung von Benutzerkonten, Zugriffsrechten und Berechtigungen. Einrichtung, Aktualisierung und Deaktivierung von Benutzerkonten gemäß den Sicherheitsrichtlinien. Überwachung und Kontrolle des Zugriffs auf vertrauliche Daten und Systemressourcen.
Risikoanalyse und Risikobewertung Durchführung von Risikoanalysen -bewertungen in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit, um Schwachstellen und potenzielle Bedrohungen zu identifizieren.	**Einspielen von Sicherheitspatches und Updates** Verwaltung und Einspielen von Sicherheitsupdates, Patches und Upgrades. Schließen bekannter Sicherheitslücken und Aufrechterhaltung der Systemsicherheit. Aktualisierung von Betriebssystemen, Anwendungen und Netzwerkkomponenten.
Konzeption und Umsetzung Notfallmanagement Erstellung von Plänen und Verfahren zum Umgang mit Ereignissen, die Notfall- oder Krisenpotenzial haben. Einrichtung eines Notfallteams bzw. Krisenstabs und Durchführung von Schulungen und Notfallübungen.	**Reaktion auf Ereignisse** Reaktion auf Sicherheitsvorfälle in Echtzeit. Untersuchung von Sicherheitsverletzungen und Wiederherstellung von Systemen und Daten. Kommunikation mit relevanten Stakeholdern und Behörden.
Konzeption von Schulungs- und Sensibilisierungsprogrammen Entwicklung von Programmen für Schulungen und Sensibilisierungsmaßnahmen zur Steigerung des Sicherheitsbewusstseins der Mitarbeiter unter Berücksichtigung von Themen wie Phishing, Social Engineering und sichere Nutzung von Passwörtern. Reaktion auf aktuelle Themen.	**Durchführung von Schulungen und Sensibilisierungsmaßnahmen** Durchführung von Schulungen zu Sicherheitsrichtlinien, Best Practices und sicherheitsrelevanten Themen. Sensibilisierung der Mitarbeiter für potenzielle Sicherheitsbedrohungen und Risiken. Förderung einer Sicherheitskultur in der Organisation.
Planung regelmäßiger Überprüfungen Planung und Auswertung regelmäßiger Überprüfungen (ggf. Audits) zur Sicherstellung der Wirksamkeit und effektiven Implementierung der Sicherheitsmaßnahmen. Überwachung sicherheitsrelevanter Aktivitäten. Grundsätzliche Identifizierung von Schwachstellen und Verbesserungspotenzial.	**Durchführung von Überprüfungen** Regelmäßige Überprüfung der Einhaltung von Sicherheitsrichtlinien und Konfigurationsstandards. Prüfung von Systemeinstellungen, Zugriffsberechtigungen, Anwendungsschwachstellen und anderen Sicherheitsaspekten. Identifizierung von Sicherheitslücken und Empfehlung von Gegenmaßnahmen.

Tabelle 1: Strategische und operative Tätigkeiten / Themen der Informationssicherheit (Auswahl)

Exkurs:
Im Rahmen der Workshops wurde berichtet, dass die Stadt Rheine über den Zweckverband Kommunale ADV-Anwendergemeinschaft West (KAAW) die Leistungen des Informationssicherheitsbeauftragten (ISB) in Anspruch nehmen könnte. Der Zweckverband bietet diese Leistung allen Mitgliedskommunen an und erhebt hierfür eine einwohnerbezogene Umlage. Der Vorteil bestünde darin, dass nicht jede Kommune gleichartige konzeptionelle Überlegungen anstellen müsste. Der aktuelle Stellenumfang für die Leistungen des interkommunalen ISB beträgt 1,2 Stellen.
Auch wenn dies auf politischer Ebene erst einmal verlockend klingen kann, so sollte sorgfältig geprüft werden, welche Vor- und Nachteile für diese Lösung sprechen und wie eine gute Lösung für die Stadt Rheine aussehen kann.
Als große kreisangehörige Kommune sind die Aufgabenstellungen im Bereich der Informationssicherheit umfassender und komplexer als in vielen der kleineren kreisangehörigen Kommunen. Der mit der Umlage (rd. 20.000 Euro) verbundene rechnerische Stellenanteil für den ISB wird den individuellen zeitlichen Anforderungen der Stadt Rheine im Umfang nicht gerecht werden können.

Aufgrund der derzeitigen „Marktlage“ kann es derzeit jedoch schwierig sein, zeitnah eine eigene Person zu finden. Dennoch sollten entsprechende Anstrengungen (ggf. wiederholt) unternommen werden. Bei einer entsprechenden Ausschreibung ist zu berücksichtigen, dass eine solche Stelle auf Leitungsstellenebene eingruppiert werden sollte. Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt: „Die Rolle des oder der ISB sollte von einer Person mit eigener Fachkompetenz zur Informationssicherheit in einer Stabsstelle eines Unternehmens oder einer Behörde wahrgenommen werden.“[27] Hinweise zu erforderlichen Qualifikationen und Kenntnissen eines bzw. einer Informationssicherheitsbeauftragten finden sich in Abschnitt 5.1.3. Bei der Erstellung einer Stellenausschreibung sollten lokale Gegebenheiten (z.B. hinsichtlich Eingruppierung) berücksichtigt werden. Ein Austausch mit anderen Kommunen kann an dieser Stelle hilfreich sein. Sofern die Stelle auch nach wiederholtem Versuch nicht intern besetzt werden kann, sollte eine externe Besetzung geprüft werden.

Die **Vorteile einer eigenen Person in der Rolle des oder der Informationssicherheitsbeauftragten** liegen darin, dass sie Teil der Stadt Rheine wäre und somit die Abläufe, Prozesse und Verwaltungsangehörigen im Laufe der Zeit gut kennen und einschätzen könnte. Durch die ständige Präsenz des oder der Rolleninhaberin könnten beispielsweise Schulungen und Sensibilisierungsmaßnahmen zielgerichtet vorbereitet und durchgeführt werden. Eine solche interne Person könnte zudem stets schnell auf Ereignisse reagieren und ohne Verzögerung gezielte Maßnahmen ergreifen.

Ein **möglicher Nachteil** kann sein, dass eine interne Person dazu neigen könnte, Konflikte zu vermeiden oder gegenüber der Leitung nicht offen über bestehende Mängel in der Informationssicherheit zu berichten, um sich selbst zu schützen. Es kann zudem zu Interessenskonflikten kommen, wenn die interne Person auch andere Aufgaben in der Stadt Rheine wahrnehmen würde. Dies sollte unbedingt vermieden werden. Bei dieser Rolle handelt es sich um eine Schlüsselrolle für Informationssicherheit. Daher sollte diese Person weder technische noch weitere als die originären Aufgaben eines beziehungsweise einer Informationssicherheitsbeauftragten übernehmen. Eine fehlende Vertretung bei Abwesenheit, Urlaub oder Krankheit wäre ein weiterer möglicher Nachteil.

[27] Bundesamt für Sicherheit in der Informationstechnik (2023): Glossar zum IT-Grundschutz-Kompendium, S. 3

Die **Vorteile einer externen Person** könnten sein, dass diese über spezielles Fachwissen und Erfahrungen auch aus anderen Kommunen, Verwaltungen oder Unternehmen verfügt, da er oder sie ggf. für verschiedene Organisationen tätig ist. Eine externe Person könnte möglicherweise eine objektivere Sichtweise auf bestimmte Situationen und Sachverhalte in der Stadt Rheine und deren Schulen haben. Aufgrund des Austausches mit anderen Organisationen kann eine externe Person Entwicklungen und mögliche Best Practices besser in die Arbeit für die Stadt Rheine einbringen.

Wesentliche Nachteile können allerdings darin bestehen, dass diese Person in Abhängigkeit der konkreten Beauftragung ggf. nicht vor Ort wäre und ggf. nicht zeitnah auf Ereignisse reagieren könnte. So müsste man lange Reaktionszeiten in Kauf nehmen. Sofern die Person nicht regelhaft vor Ort ist, kann die Zusammenarbeit zwischen einem oder einer externen Informationssicherheitsbeauftragten und anderem Personal der Stadt Rheine oder der Schulen erheblich schwieriger sein. Sofern eine externe Besetzung in gleichem Umfang wie bei einer internen Stelle erfolgen soll, würde dies ggf. höhere Kosten verursachen. Darüber hinaus wird bei Einsatz einer externen Person kein „eigenes“ Wissen in der Stadt Rheine aufgebaut. Zudem besteht die Gefahr, dass eine externe Besetzung auftragnehmerseitig ausgetauscht wird. Eine Nachfolgeperson müsste sich ebenfalls einarbeiten, was erneut zu internem Aufwand in der Stadt Rheine führen würde.

Interne Besetzung der Rolle ISB	Externe Besetzung der Rolle ISB
Mögliche Vorteile • wäre Teil der Stadt Rheine • kennt Abläufe, Prozesse und Verwaltungsangehörige und kann diese einschätzen • ständige Präsenz • zielgerichtete Vorbereitung und Durchführung von Schulungen und Sensibilisierungsmaßnahmen durch gute Kenntnis des Umfelds • schnelle Reaktion auf Ereignisse • Ergreifung gezielter Maßnahmen ohne Verzögerung	**Mögliche Vorteile** • könnte über spezielles Fachwissen und Erfahrungen auch aus anderen Kommunen, Verwaltungen oder Unternehmen verfügen, da er oder sie ggf. für versch. Organisationen tätig ist • könnte mglw. eine objektivere Sichtweise auf bestimmte Situationen und Sachverhalte in der Stadt Rheine und deren Schulen haben • kann aufgrund des Austausches mit anderen Organisationen ggf. Entwicklungen und mögliche Best Practices besser einbringen
Mögliche Nachteile • könnte dazu neigen, Konflikte zu vermeiden • könnte gegenüber der Leitung nicht offen über bestehende Mängel in der Informationssicherheit berichten, um sich selbst zu schützen • es kann zu Interessenskonflikten kommen, wenn die interne Person auch andere Aufgaben in der Stadt Rheine wahrnehmen würde • keine Vertretung bei Abwesenheit, Urlaub, Krankheit	**Mögliche Nachteile** • wäre in Abhängigkeit der Verfügbarkeit ggf. nicht vor Ort und könnte ggf. nicht zeitnah auf Ereignisse reagieren • ggf. ist in Abhängigkeit der konkreten Beauftragung mit langen Reaktionszeiten zu rechnen • ggf. kann die Zusammenarbeit zwischen einem oder einer externen Informationssicherheitsbeauftragten und anderem Personal der Stadt Rheine oder der Schulen erheblich schwieriger sein, da sich die Personen kaum kennen • eine externe Besetzung in gleichem Umfang wie bei einer internen Stelle wäre ggf. mit deutlichen höheren Kosten verbunden • es wird kein „eigenes“ Wissen in der Stadt Rheine aufgebaut • ggf. höhere Gefahr, dass eine externe Person auftragnehmerseitig ausgetauscht wird und sich Nachfolgepersonen erneut einarbeiten müssten

Tabelle 2: Mögliche Vor- und Nachteile bei interner bzw. externer Besetzung der Rolle ISB

4.7 Weitere Ergebnisse aus den Workshops

Im Rahmen der Workshops erfolgte eine Beschäftigung entlang der Bausteine des BSI IT-Grundschutz mit vielfältigen Themen (Serverräume in Schulen, Zutrittsschutz, Serverbetrieb, Netzbetrieb, Notfallmaßnahmen, Netzersatzanlage, Backupverfahren, Office-Lösungen, Insellösungen, Benutzerkonten, Softwarebeschaffung, mobile Geräte in Schulen und vieles andere mehr).

Es zeigt sich, dass alle Kollegen grundsätzlich sehr bemüht sind, die vielfältigen Themen ernst zu nehmen, dass aber in vielen Bereichen hinsichtlich des wichtigen Themas Informationssicherheit grundlegende Strukturen fehlen und aufgebaut werden müssen. So kann beispielsweise übergreifend[28] festgehalten werden, dass Sicherheitsleitlinien in der Stadt Rheine zwar existieren, diese aber veraltet sind. Im Bereich der Schul-IT fehlt eine konsolidierte Verschriftlichung, zusammenzufügende Fragmente sind vorhanden.

[28] BSI IT-Grundschutz Baustein ISMS

So zieht sich die Betrachtung durch die vielfältigen Themen. Hinsichtlich organisatorischer und personeller Sicherheitsaspekte[29] haben die Kollegen der Schul-IT berichtet, dass der Zutrittsschutz nicht an allen Schulen gewährleistet ist, sodass Lehrkräfte Zutrittsmöglichkeiten zu Serverräumen und weiteren IT-Räumen der schulischen Verwaltung haben. Die baulichen Gegebenheiten in den Schulen entsprechen nicht dem BSI-Standard. Darüber hinaus existiert beispielsweise kein klarer Prozessablauf beim Weggang von Lehrkräften und weiterem Personal (Sekretariatsmitarbeitende, Personal der IT- Administration und des Hausdienstes). Damit ist letztendlich nicht sichergestellt, dass Zugänge zu IT-Systemen deprovisioniert werden, d.h. dass alle vergebenen Zugriffsrechte entzogen werden.

Die drei Workshops haben gezeigt, dass die Stadt Rheine dedizierte Personen benötigt, um die vielfältigen Themen[30] in einer strukturierten Art und Weise zur Planung und zur Umsetzung zu bringen. Dazu zählen auch individuelle Bedarfe und Themen, die mögliches Synergiepotenzial zwischen den Bereichen der Stadt Rheine aufweisen. So sehen die Kollegen der Verwaltungs-IT unter anderem individuellen Bedarf im Rahmen der Erstellung eines detaillierten Notfallmanagements. Das Notfallmanagement wird in diesem Bereich als eine ständige Aufgabe begriffen, für die jedoch zurzeit keine Ressourcen bereitstehen, da Tagesgeschäft und Projekte stets Vorrang haben. Im Bereich der Schul-IT besteht beispielsweise individueller Bedarf hinsichtlich der IT-Ablaufbeschreibungen und der Umsetzung von Dokumentationsstrategien. Übergreifende Bedarfe bestehen in der Betrachtung von Kernprozessen und in der Bereitstellung von Ressourcen zur Umsetzung informationssicherheitsrelevanter Aspekte. Konkrete Fragen stellen sich beispielsweise auch zur Reichweite der Gültigkeit von Leitlinien der Verwaltungs-IT (z.B. Relevanz für Sekretariatsmitarbeitende oder Mitarbeitende des Hausdienstes).

Die weiteren Ergebnisse der Workshops sind auf einem Conceptboard festgehalten worden. Alle Workshopteilnehmer haben einen Auszug erhalten, um auch später noch auf die Ergebnisse zur aktuellen Situation, zu individuellen Bedarfen und möglichen Synergien hinsichtlich der behandelten Bausteine des IT-Grundschutz-Kompendiums zurückzugreifen. Auch ein oder eine zukünftige Informationssicherheitsbeauftragte kann sich damit einen ersten Überblick über die derzeitige Lage verschaffen.

[29] BSI IT-Grundschutz Prozess-Baustein ORP

[30] BSI IT-Grundschutz System-Bausteine APP, SYS, NET und INF

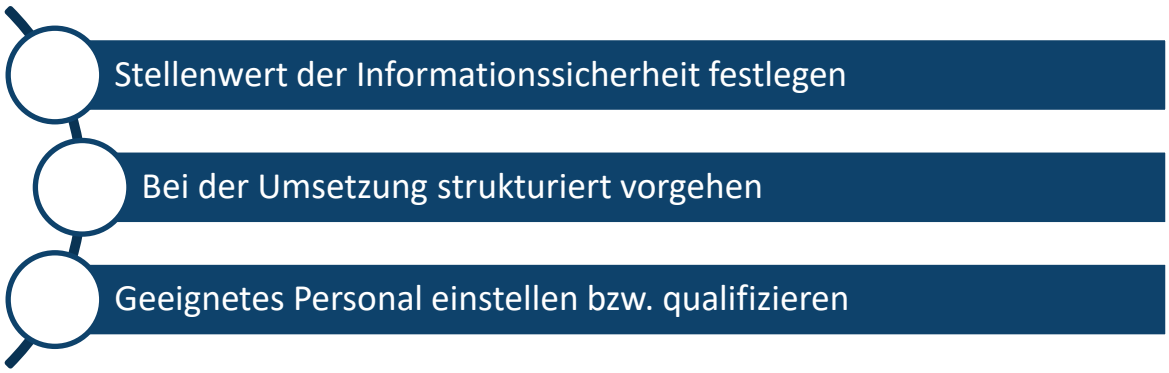
5 Maßnahmen

Besonders lobenswert ist die Tatsache, dass sich die Stadt Rheine unter Berücksichtigung der Schulen im Bereich Informationssicherheit besser aufstellen möchte. Die Stadt Rheine greift damit teilweise Empfehlungen des vorausgegangenen GPA-Prüfberichts auf, z.B. in Hinblick auf den notwendigen Ausbau des Notfallmanagements. Die erkannte Notwendigkeit für den Aufbau eines Notfallmanagements ist sehr zu begrüßen und wird im Rahmen dieses Gutachtens stark empfohlen, um der aktuellen und zukünftigen Bedrohungslage gerecht zu werden. Dies allein reicht jedoch nicht aus, denn Notfallmanagement bedeutet „lediglich“ ein vorbereitetes und strukturiertes Reagieren im Fall eines Ereignisses mit Schadenspotenzial. Damit werden grundsätzlich keine Angriffe oder Gefährdungen verhindert.

Die Gespräche haben gezeigt, dass die Teilnehmenden selbst sehr stark den Bedarf für ein strukturiertes Informationssicherheitsmanagement erkannt haben. Ein wesentliches Defizit liegt in der Tatsache, dass die Rolle des bzw. der Informationssicherheitsbeauftragten (ISB) nur auf dem Papier existiert und nicht gelebt wird. Dies ist allerdings eine absolute Grundvoraussetzung für das erfolgreiche Umsetzen von Informationssicherheit. Die Dokumentationslage erscheint in verschiedener Hinsicht ausbau- und aktualisierungsfähig und bildet die wesentliche Grundlage für eine Reihe weiterer Schritte der Informationssicherheit. Hier besteht die Notwendigkeit in der Aktualisierung, der inhaltlichen Ergänzung und der Neuerstellung geforderter Dokumente. Im CISIS12®-Rahmenwerk[31] wird beispielsweise eine zweistellige Anzahl an elementaren Dokumenten für Informationssicherheit aufgelistet, die im Rahmen der Einführung eines Informationssicherheitsmanagementsystems zu erstellen sind. Darüber hinaus wurde insbesondere für den Bereich der Schulen die Notwendigkeit für Schulungen und Sensibilisierungen erkannt.

Auch unter Berücksichtigung der Rahmenbedingung, dass die Stadt Rheine sehr viel IT selbst betreibt und dass die Schulen mit in der Zuständigkeit liegen, werden folgende Maßnahmen abgeleitet.

5.1 Aufbau organisatorischer Strukturen



[31] Bei CISIS12® handelt es sich um ein vom IT-Sicherheitscluster e.V. entwickeltes und herausgegebenes ISMS. Weitere Informationen: https://cisis12.de

5.1.1 Stellenwert der Informationssicherheit festlegen

In einer Zeit, in der digitale Technologien und vernetzte Systeme immer stärker in den Verwaltungsalltag integriert werden, ist der Schutz sensibler Daten und die Sicherstellung der IT-Infrastruktur von entscheidender Bedeutung. Die Stadt Rheine ist wie jede andere deutsche Kommune auch für eine Vielzahl von Aufgaben und Dienstleistungen zuständig, die einen vertraulichen Umgang mit sensiblen Informationen erfordern. Dazu gehören beispielsweise personenbezogene Daten der Bürgerinnen und Bürger, Finanzdaten, interne Kommunikation und andere vertrauliche Informationen. Sicherheitsvorfälle, wie z.B. Cyberangriffe oder Datenlecks, können nicht nur das Vertrauen der Bürgerinnen und Bürger in die Verwaltung beeinträchtigen, sondern auch erhebliche finanzielle und rechtliche Konsequenzen nach sich ziehen. Darüber hinaus spielt Informationssicherheit auch eine wichtige Rolle bei der Gewährleistung der Verfügbarkeit und Integrität der IT-Systeme der Stadt Rheine. Störungen oder Ausfälle von IT-Systemen können den reibungslosen Ablauf der Verwaltungsprozesse beeinträchtigen und somit die Effizienz und Effektivität der Arbeit der Verwaltungsmitarbeiterinnen und -mitarbeiter verringern. Dies gilt für die Kernverwaltung gleichermaßen, wie auch für die Schulen, die mit der gleichen Wichtigkeit wie Ämter der Stadt mit ihren jeweiligen Besonderheiten behandelt werden sollten.

Auch vor dem Hintergrund, dass die Stadt Rheine eine nennenswerte Anzahl an IT-Systemen und Infrastrukturen selbst betreibt und dass die Schulen mit im Verantwortungsbereich für IT liegen, ist grundsätzlich ein hoher Stellenwert der Informationssicherheit erkennbar.

Das Thema Informationssicherheit sollte in der Stadt Rheine sowohl für die Verwaltungs-IT als auch für die Schul-IT einen hohen Stellenwert einnehmen. Im Idealfall sollte sukzessive ein Informationssicherheitsmanagementsystem (ISMS) aufgebaut werden.

Um einen angemessenen Schutz zu gewährleisten, sollte Informationssicherheit grundsätzlich sowohl für die Verwaltungs-IT als auch für die Schul-IT als Querschnittsthema betrachtet. In allen relevanten Bereichen sollten erforderliche Maßnahmen implementiert werden. Dazu gehören die Etablierung einer geeigneten IT-Sicherheitsorganisation, die regelmäßige Schulung aller Angehörigen im Umgang mit sensiblen Daten und die kontinuierliche Ausweitung und Verbesserung technischer Sicherheitsmaßnahmen wie z.B. Firewalls, Antivirus-Software und Verschlüsselungstechnologien, die auf dem Stand der Zeit sind. Ergänzend sollte die Stadt Rheine im Rahmen der Möglichkeiten, idealerweise wahrgenommen durch die informationssicherheitsbeauftragte Person, mit anderen Kommunen und ggf. weiteren auf kommunaler Ebene agierenden Organisationen Austausch über aktuelle Bedrohungen, erfolgte Angriffe und bewährte Sicherheitspraktiken (Best Practices) betreiben. Indem Informationssicherheit bei der Stadt Rheine einen hohen Stellenwert einnimmt, demonstriert sie ihr Engagement für den Schutz sensibler Daten und die Gewährleistung eines sicheren und effizienten Verwaltungsbetriebs.

5.1.2 Bei der Umsetzung strukturiert vorgehen

Grundsätzlich sollte die Umsetzung der Informationssicherheit für die Stadt Rheine inklusive der Schulen im Rahmen eines strukturierten und in der Regel mehrjährigen Vorgehens erfolgen. Nur ein strukturiertes Vorgehen ermöglicht eine systematische Identifizierung und Bewertung von Risiken und bestehenden Schwachstellen im Zusammenhang mit

Informationssicherheit. Durch eine gründliche Analyse können potenzielle Bedrohungen und Schwachstellen erkannt werden, sodass angemessene Maßnahmen ergriffen werden können, um diese Risiken zu mindern oder zu vermeiden.

Dabei ist zu berücksichtigen, dass Informationssicherheit viele verschiedene organisatorische Aspekte wie beispielsweise Regelungen, Dokumentationen und Abläufe, aber auch eine Reihe von technischen Maßnahmen betrifft. Alle relevanten Bereiche der Stadt und der Schulen sollten identifiziert und abgedeckt werden, um sicherzustellen, dass keine Restrisiken unentdeckt bleiben. Eine sorgfältige Planung der Umsetzung des Sicherheitsprozesses unter Berücksichtigung der notwendigen Ressourcen lässt eine effiziente und gleichförmige Implementierung der notwendigen Maßnahmen zu, sodass letztendlich keine Bereiche unberücksichtigt bleiben und dadurch benachteiligt werden. Dies bedeutet nicht, dass die Maßnahmen in allen Bereichen, beispielsweise in allen Schulen, identisch umzusetzen sind, sondern vielmehr, dass in allen Bereichen alle notwendigen Themen strukturiert und im Idealfall unter Nutzung vieler Synergien bearbeitet werden.

Erschwerend kommt hinzu, dass die Informationssicherheit, wie eingangs beschrieben, einer schnellen Entwicklung unterliegt, da sich Bedrohungen und Technologien sowohl auf Seite der Angreifenden als auch auf Seiten der Angegriffenen ständig weiterentwickeln. Ein strukturiertes Vorgehen ermöglicht eine kontinuierliche Überwachung und Bewertung der Sicherheitslage, dies beinhaltet sowohl veränderte Bedrohungslagen als auch beispielsweise neue oder angepasste Schutzmöglichkeiten, um die Informationssicherheit kontinuierlich zu verbessern.

Es bietet sich an, auf etablierte Methoden und Vorgehensmodelle zurückzugreifen. Somit bietet das Bundesamt für Informationssicherheit mit dem IT-Grundschutz-Kompendium und den ergänzenden Standards 200-1, 200-2, 200-3 und 200-4 bewährte Grundlagen, um alle relevanten Themen zu bearbeiten. Es sei an dieser Stelle jedoch angemerkt, dass es sich um komplexe und umfangreiche Darstellungen handelt, die üblicherweise durchdrungen und schließlich umgesetzt werden müssen. Hierbei ist es zwingend erforderlich, dass dies durch kompetentes Personal (in erster Linie durch eine Person, die die Rolle des bzw. der Informationssicherheitsbeauftragten übernommen hat) geschieht. Dieser Person kommt bei der Umsetzung die wesentliche Rolle zu. Die fünf genannten BSI-Dokumente haben in Summe einen Umfang von 1.374 Seiten. Eine denkbare Vorgehensalternative besteht bspw. in der Anwendung von CISIS12®, einem Rahmenwerk zur Umsetzung der Informationssicherheit im Rahmen von 12 Schritten. Die drei einschlägigen Dokumente, die hier heranzuziehen wären, nehmen in Summe einen Umfang von 1.072 Seiten ein. Für die öffentliche Verwaltung wäre die Nutzung des CISIS12®-Rahmenwerks nach letztem Kenntnisstand grundsätzlich kostenfrei. Sofern entsprechende Beratung erforderlich werden würde, entstünden dafür Kosten. Die BSI-Dokumente sind grundsätzlich kostenfrei erhältlich. Auch hier gilt, dass jegliche externe Beratung selbstverständlich Kosten verursachen würde. Es kann jedoch ein Weg sein, entsprechende Kompetenz intern vorzuhalten und die Anwendung weitgehend aus einer Kraft zu bewältigen und ggf. punktuell für Teilaspekte Beratung einzukaufen.

5.1.3 Geeignetes Personal einstellen bzw. qualifizieren

Die mit Abstand wichtigste Empfehlung des vorliegenden Kurzgutachtens lautet, die Rolle der bzw. der Informationssicherheitsbeauftragten zu besetzen und entsprechendes

ergänzendes Personal für die operativen Belange sowohl im Bereich der Verwaltungs-IT als auch im Bereich der Schul-IT vorzusehen.

Die wesentliche Rolle kommt dem bzw. der Informationssicherheitsbeauftragten zu. Es handelt sich nicht um eine Projektaufgabe, sondern um eine dauerhafte Beschäftigung.

Die Person muss einerseits fachlich geeignet sein und das Thema Informationssicherheit für die gesamte Stadt Rheine inklusive der Schulen eigeninitiativ vorantreiben, um spürbare und zu einem späteren Zeitpunkt auch messbare Ergebnisse zu erzielen. Sowohl die geeignete Besetzung als auch die aktive Ausübung der Rolle sind wesentliche Erfolgsfaktoren, um die Informationssicherheit nennenswert zu verbessern. Einen weiteren wichtigen Erfolgsfaktor stellen Gegenparts in den IT-Bereichen der Verwaltungs-IT und der Schul-IT dar, um die vielfältigen Maßnahmen zur Informationssicherheit operativ umzusetzen.

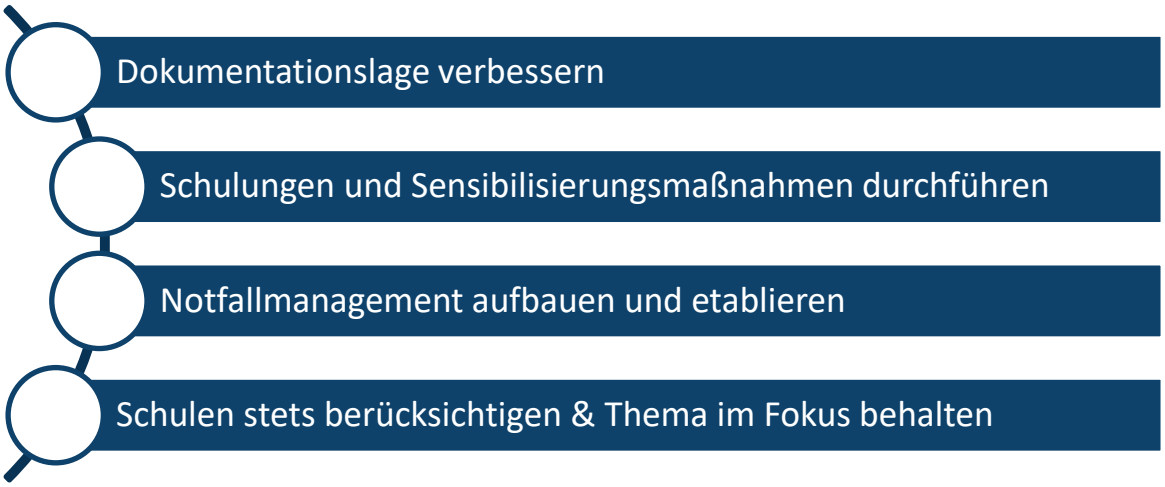
Nimmt eine Kommune das Thema Informationssicherheit ernst, so kann sie auch mit einem VZÄ in der Rolle Informationsicherheitsbeauftragte:r und den Gegenparts bei der technischen Umsetzung (empfohlen werden je 0,5 VZÄ in der Verwaltungs-IT und in der Schul-IT) mittelfristig an die personellen Ressourcengrenzen kommen, sodass in einigen Jahren die Auskömmlichkeit zu prüfen wäre. Darüber hinaus ist stets ein Budget für Informationssicherheit festzulegen und in den Haushalt einzuplanen (siehe Kapitel 6).

Ein beziehungsweise eine Informationssicherheitsbeauftragte:r sollte über ein breites Spektrum an Qualifikationen und Kenntnissen verfügen, um effektiv in dieser Rolle agieren zu können: Die Person sollte einerseits über umfangreiche Kenntnisse in den Bereichen Informationssicherheit, Datenschutz und rechtliche Rahmenbedingungen verfügen. Dazu gehören Kenntnisse über gängige Standards wie ISO 27001, BSI IT-Grundschutz oder bspw. CISIS12®. Andererseits ist ein Verständnis für Risikomanagementprinzipien und die Fähigkeit, Risiken zu identifizieren, zu bewerten und zu behandeln, entscheidend. Die Person sollte in der Lage sein, Risikoanalysen durchzuführen, Schwachstellen zu identifizieren und angemessene Sicherheitsmaßnahmen zu empfehlen. Ein grundlegendes technisches Verständnis ist erforderlich, um die technischen Aspekte von Informationssicherheit zu verstehen und mit den IT-Einheiten der Verwaltungs-IT und der Schul-IT effektiv zusammenzuarbeiten. Dies beinhaltet unter anderem Kenntnisse über Netzwerkarchitekturen, Sicherheitsinfrastrukturen und Verschlüsselungstechnologien. Die Person sollte außerdem über gute Kommunikationsfähigkeiten verfügen, um komplexe Sicherheitskonzepte und Sicherheitsanforderungen klar und verständlich zu vermitteln. Die Fähigkeit, Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiterinnen und Mitarbeiter in den Verwaltungen und in den Schulen durchzuführen, ist ebenfalls von großer Bedeutung. Weiterhin sollte ein oder eine Informationssicherheitsbeauftragte:r über analytische Fähigkeiten verfügen, um Sicherheitsvorfälle zu untersuchen, Schwachstellen zu analysieren und geeignete Gegenmaßnahmen zu entwickeln und fundierte Entscheidungen zu treffen. Da das Thema Informationssicherheit auch rechtliche und regulatorische Aspekte umfasst, ist es von Vorteil, wenn die Person Kenntnisse im Datenschutzrecht und anderen relevanten Rechtsvorschriften besitzt. Dies ermöglicht, die Einhaltung gesetzlicher Anforderungen sicherzustellen. Ein solider Mix aus Fachkenntnissen, technischem Verständnis, analytischen Fähigkeiten und Kommunikationskompetenz erscheint erforderlich, um die Herausforderungen der Informationssicherheit erfolgreich zu bewältigen.

Im Idealfall erfolgt im Bereich der Informationssicherheit eine vertrauensvolle Zusammenarbeit zwischen dem oder der Informationssicherheitsbeauftragten und dem Personal für die technische und operative Umsetzung der Informationssicherheit (insgesamt zwei IT-Personen mit je 0,5-anteiligem Stellenumfang für die Verwaltungs-IT und für die Schul-IT). Dies geschieht durch die Unterstützung bei der Umsetzung von erstellten Sicherheitsrichtlinien und Sicherheitsvorgaben für die jeweilige Dienststelle oder die jeweilige Schule, durch die Überwachung der Einhaltung dieser Richtlinien und Vorgaben sowie durch korrekte Konfiguration der IT-Systeme, aller Netzwerkkomponenten, der Software und der Benutzerkonten entsprechend den Sicherheitsvorgaben.

Dies umfasst in den Schulen beispielsweise konkret die grundlegende Konfiguration, Überwachung und Aktualisierung von diversen Servern, fest installierten und mobilen Arbeitsgeräten, Netzwerken und deren Komponenten, Firewalls und ggf. weiteren Infrastrukturkomponenten. Dabei ist sicherzustellen, dass die genannten Infrastrukturen und Systeme angemessen geschützt und somit gegen Angriffe abgesichert sind. Das Personal für die technische und operative Umsetzung der Informationssicherheit ist verantwortlich für die Durchführung von Updates und das Einspielen von Patches bei allen sichtbaren und unsichtbaren Komponenten, um bestehende Schwachstellen zu beheben. Es unterstützt bei der Verwaltung von Benutzerkonten, Berechtigungen und Zugriffsrechten, um sicherzustellen, dass ausschließlich berechtige Personen gemäß der Sicherheitsrichtlinien Zugriff auf Systeme und damit letztlich auf ggf. sensible Daten haben. Durch eine enge Zusammenarbeit des Personals für die technische und operative Umsetzung der Informationssicherheit mit dem oder der Informationssicherheitsbeauftragten wird sichergestellt, dass die vielfältigen Facetten der Informationssicherheit sowohl durch die Verwaltungs-IT als auch durch die Schul-IT nachhaltig in der Stadt Rheine inklusive ihrer Schulen bearbeitet und nachhaltig umgesetzt werden.

5.2 Umsetzung von Maßnahmen



5.2.1Dokumentationslage ausbauen und verbessern

Auch die Verbesserung der Dokumentationslage im Bereich Informationssicherheit erfordert eine systematische und strukturierte Herangehensweise. Die Rahmenwerke für Informationssicherheit helfen dabei, entsprechende Dokumentationsstrukturen festzulegen. Bei CISIS12® entspricht dies beispielsweise einem der zwölf Schritte[32].

Grundsätzlich sollte der Überblick über die zu erstellenden Dokumentationen und der jeweiligen Umsetzungsstände in Händen des oder der Informationssicherheitsbeauftragten liegen. Dabei sind die erforderlichen Dokumente wie Sicherheitsrichtlinien, Risikoanalysen, Sicherheitskonzepte, Notfallpläne usw. vorzusehen. Dabei ist auch festzulegen, wie sie erstellt, aktualisiert, gespeichert und zugänglich gemacht werden sollen. Für die Dokumentenerstellung bietet sich die Verwendung standardisierter Vorlagen an, um eine konsistente Struktur und Formatierung zu gewährleisten. Diese Vorlagen können beispielsweise Checklisten, Berichtsvorlagen, Vorlagen für Richtlinien und Verfahren oder Formulare für Risikobewertungen umfassen. Der oder die Informationssicherheitsbeauftragte sollte klare Prozesse und Verantwortlichkeiten für die Erstellung, Überprüfung, Genehmigung und Aktualisierung von Dokumenten festlegen und sicherstellen, sodass alle relevanten Stakeholder in den Prozess einbezogen werden. Erstellte Dokumentationen hinsichtlich Informationssicherheit sollten regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie den aktuellen Anforderungen und Best Practices entsprechen. Daher sind regelmäßige Überprüfungen und Aktualisierungen fest einzuplanen. Darüber hinaus ist zu klären, wie die Dokumentationen effizient verwaltet, gespeichert, versioniert und den relevanten Akteuren zur Verfügung gestellt werden können. Mitarbeiterinnen und Mitarbeiter der Verwaltungen und der Schulen sollten auch zu den Anforderungen der Dokumentation im Bereich Informationssicherheit geschult werden. Dabei sollte sichergestellt werden, dass sie die Bedeutung der Dokumentation verstehen und in der Lage sind, entsprechend den festgelegten Richtlinien und Verfahren zu handeln.

Die Verbesserung der Dokumentationslage erfordert Zeit, Ressourcen und Engagement. Es ist jedoch ein wichtiger Schritt, um die Informationssicherheit effektiv zu managen, Compliance-Anforderungen zu erfüllen und im Falle von Vorfällen oder Audits nachvollziehbare Nachweise zu haben.

5.2.2 Schulungen und Sensibilisierungsmaßnahmen durchführen

Zur Verbesserung der Dokumentationslage zählt auch die Erarbeitung eines Konzepts zur Durchführung von Schulungen und Sensibilisierungsmaßnahmen in allen Bereichen der Stadt Rheine. Im Konzept sollte geregelt sein, welche Maßnahmen mit welchen Inhalten für welche Zielgruppen angeboten werden sollen und wie und in welchen zeitlichen Dimensionen die Umsetzung erfolgen soll.

Schulungen und Sensibilisierungen für Mitarbeiterinnen und Mitarbeiter der Verwaltungen und der Schulen sollen auf die Bedeutung der Informationssicherheit aufmerksam machen und den Teilnehmenden ermöglichen, ihr Wissen und ihre Fähigkeiten in allen relevanten Bereichen zu verbessern. Der oder die Informationssicherheitsbeauftragte spielt eine wesentliche Rolle bei der Planung und Durchführung von Schulungen und Sensibilisierungsmaßnahmen. Auch wenn sich die fachlichen Inhalte zwischen verschiedenen Einheiten der

[32] Weitere Informationen: https://cisis12.de/was-ist-cisis12

Stadt Rheine untereinander und insbesondere zu den Schulen unterscheiden, so sind die wesentliche Themenblöcke dennoch vergleichbar (grundsätzliche Gefährdungen, Auslöser, Passwörter, Phishing usw.).

Wichtiger Bestandteil sollten Grundlagenschulungen sein, sodass die Mitarbeiterinnen und Mitarbeiter der Stadt Rheine inklusive der Schulen über grundlegende Aspekte der Informationssicherheit Bescheid wissen. Dazu gehört beispielsweise das Kennenlernen möglicher Bedrohungen, das Zeigen und Erläutern von medienwirksamen Beispielen, den geeigneten Umfang mit Passwörtern, das Erkennen von Phishing-Mails, den Umgang mit öffentlichen WLANs, den Umgang mit externen Datenträgern wie USB-Sticks und anderes mehr. Hier geht es vorrangig darum, dass die Teilnehmenden für Informationssicherheit sensibilisiert werden und überhaupt ein Gefahrenpotenzial erkennen. Nur so kann die Vermittlung von konkreten Maßnahmen helfen, die Gefährdungslage, die von stadt- und schuleigenem Personal ausgeht, zu reduzieren. Solche Schulungen sollten inhaltlich nicht überladen sein, sodass die Zielgruppe tatsächlich wesentliche Informationen mitnimmt. Sinnvoll ist auch, im Rahmen solcher Schulungen Fragen zu ermöglichen, die die Mitarbeiterinnen und Mitarbeiter beschäftigen und treffend zu beantworten. Grundsätzlich ist die für Informationssicherheit beauftragte Person für das Durchführen von Schulungen und Sensibilisierungsmaßnahmen zuständig.

Nach solchen Grundlagenschulungen sollten weitere themenspezifische Schulungen und Sensibilisierungen durchgeführt werden. Hier bietet es sich an, konkrete Themen zu fokussieren (beispielsweise Home Office oder Dienstreisen) beziehungsweise aus der Grundlagenschulung zu vertiefen (z.B. Phishing und Social Engineering). Auch in der Stadt oder in der Schule geltende Leit- und Richtlinien oder Dienstanweisungen sollten den Mitarbeiterinnen und Mitarbeiter bekannt gemacht werden. Die Schulungen sollten dabei helfen, die Inhalte solcher regelnden Dokumente zu verstehen, da nicht zu erwarten ist, dass diese von allen Personen eigeninitiativ durchgearbeitet werden. Je passender die Schulungen und Sensibilisierungen auf den konkreten Arbeitsalltag bzw. Anwendungskontext und ggf. auch auf konkrete Systeme und Infrastrukturen zugeschnitten sind, desto größer ist die Chance, dass Gefahren reduziert werden.

Sukzessive sollte das Sicherheitsbewusstsein im Verwaltungs- und Schulalltag geschärft werden. Dies kann anhand kontinuierlicher (Auffrischungs-) Schulungen geschehen, um auch möglicher Personalfluktuation zu begegnen. Zwei einfache Beispiele sind das Sperren von Bildschirmen bei Verlassen des Büros oder der kritische Umfang mit Fremdpersonen, die beispielsweise angeblich im Auftrag der IT-Abteilung Hardware abholen sollen. Sobald ein Notfallmanagement aufgebaut worden ist, sollten die betreffenden Mitarbeiterinnen und Mitarbeiter dazu geschult werden, wie einerseits potenzielle Notfälle identifiziert werden können und vor allem, mittels welcher Verfahren diese konkret zu melden sind.

Im Bereich Schule können spezifische Schulungen und Sensibilisierungen angeboten werden, um Lehrkräfte, Schülerinnen und Schüler sowie Verwaltungspersonal für die besonderen Aspekte der Informationssicherheit in einer schulischen Umgebung zu sensibilisieren.

Grundsätzlich gelten hier die gleichen Grundlagen, punktuell erweitert um weitere Aspekte sowohl für Lehrkräfte als auch Schülerinnen und Schüler: Die Bedeutung und das Erstellen starker Passwörter, das sichere Surfen im Internet, das Erkennen von Phishing-Angriffen und Social Engineering-Techniken, den Schutz vor Cybermobbing und Belästigungen sowie

die Gefahren von Online-Interaktionen. Wenn Lehrerinnen und Lehrer über aktuelle Risiken und Bedrohungslagen (z.B. Phishing) gut Bescheid wissen, können sie ggf. auch Vorkehrungen treffen, um ihre Schülerinnen und Schüler gut zu schützen oder im einfachsten Fall Ereignisse mit Schadenspotenzial überhaupt erkennen.

Die Schülerinnen und Schüler sollten bereits frühzeitig und wiederholt über mögliche Risiken bei der Nutzung des Internets aufgeklärt werden. Dies betrifft vielfach den richtigen Umgang mit bestimmten Themen, beispielsweise hinsichtlich persönlicher Informationen, Schutz der Privatsphäre, Bedrohungen, Belästigungen u.a.m. Zudem sollten sie anwendbare Hinweise erhalten, wie Technologien verantwortungsvoll zu nutzen sind.

Jegliche Schulungen und Sensibilisierungsmaßnahmen müssen zielgruppengerecht und in Schulen vor allem altersgerecht gestaltet sein. Jede Schulung und Sensibilisierung sollte Bewusstsein schaffen und die Zielgruppe positiv und nachhaltig in ihrem Handeln in Bezug auf Informationssicherheit beeinflussen.

Zur praktischen Umsetzung kann es nützlich sein, dass die informationssicherheitsbeauftragte Person mit einem sorgfältig erstellen Schulungs- und Sensibilisierungs-Foliensatz sukzessive alle Verwaltungen, Ämter und Schulen besucht, um initial zu zeigen, dass das Thema nun proaktiv in der Stadt Rheine bearbeitet wird, dass es eine konkrete Ansprechperson gibt und nun erste Inhalte vermittelt werden. Dabei kann die Person direkt ein individuelles Bild zum jeweiligen Reifegrad (z.B. aller Schulen) gewinnen und zukünftig auf ggf. unterschiedlichen Ausgangslagen aufbauen. Auch eine Schulleitungsdienstbesprechung kann eine geeignete Runde darstellen, um das Thema „ins Rollen zu bringen“.

5.2.3 Notfallmanagement aufbauen und etablieren

Das Notfallmanagement für Informationssicherheit der Stadt Rheine inklusive der Schulen sollte verschiedene Aspekte berücksichtigen, um effektiv auf Sicherheitsvorfälle oder Bedrohungen reagieren zu können. Es bietet sich an, den Standard 200-4 des Bundesamtes für Informationssicherheit dafür heranzuziehen. Dieser Standard umfasst mittlerweile das gesamte Business Continuity Management und löst den nur halb so umfangreichen und bereits sehr betagten Standard 100-4- für das Notfallmanagement ab (vgl. Abschnitte 3.1 und 3.2). Um das Notfallmanagement auf die kritischen Prozesse der Stadt Rheine und der Schulen abzubilden, bietet sich auch das Heranziehen des Standards 200-3 (Risikomanagement) an, um Risiken und Eintrittswahrscheinlichkeiten zu ermitteln und eine entsprechende Priorisierung sowie darauffolgend den Umgang mit den identifizierten und priorisierten Risiken zu erarbeiten.

Für das Notfallmanagement bietet es sich an, szenarienbasiert vorzugehen. Das Bundesamt für Sicherheit in der Informationstechnik bietet dafür hinsichtlich des Standards 200-4 verschiedene Vorlagen an, u.a. eine Vorlage, um das Vorgehen beim Notfallmanagement auszuarbeiten. Letztlich sollte die Dokumentation klare Vorgaben enthalten, wie Sicherheitsvorfälle erkannt und gemeldet werden können. Dies kann die Implementierung von Sicherheitsüberwachungssystemen, die Schulung von Mitarbeitenden zur Erkennung von Anzeichen von Vorfällen und die Einrichtung von Meldemechanismen umfassen. Die Dokumentation sollte auch detaillierte Verfahren enthalten, wie auf Sicherheitsvorfälle reagiert werden sollte. Dies umfasst die Identifizierung des Umfangs des Vorfalls, ggf. die Zusammenstellung eines Krisenstabs, das rasche Eindämmen der Bedrohung, die Sammlung von

Beweisen und die Kommunikation mit den Betroffenen. Es ist erforderlich, klare Kommunikationskanäle und -verfahren festzulegen, um eine effektive Zusammenarbeit zwischen den beteiligten Parteien sicherzustellen. Dazu gehören interne Abteilungen, externe Sicherheitsdienstleister, Strafverfolgungsbehörden und andere relevante Akteure.

Zudem sollte die Dokumentation Maßnahmen zur Wiederherstellung der betroffenen Systeme und Daten enthalten. Dies kann die Durchführung von Backups, die Bereitstellung von Redundanzen, die Implementierung von Wiederherstellungsplänen und die Sicherstellung einer reibungslosen Fortsetzung der Geschäftstätigkeit umfassen.

Regelmäßige Schulungen und Notfallübungen sind entscheidend, um sicherzustellen, dass Mitarbeitende mit den Verfahren und Protokollen vertraut sind und im Falle eines Sicherheitsvorfalls effektiv reagieren können. Diese Übungen können das Bewusstsein schärfen und die Reaktionsfähigkeit verbessern.

Das Notfallmanagement sollte genau wie die anderen Bestandteile der Informationssicherheit ein kontinuierlicher Prozess sein, der regelmäßig überprüft und verbessert wird. Dies beinhaltet die Analyse von Vorfällen, das Identifizieren von Schwachstellen, das Aktualisieren von Richtlinien und Verfahren sowie die Anpassung an sich ändernde Bedrohungsszenarien und technologische Entwicklungen. Eine umfassende und gut koordinierte Herangehensweise an das Notfallmanagement ermöglicht es der Stadt Rheine inklusive der Schulen auf Sicherheitsvorfälle angemessen zu reagieren und ihre Systeme und Daten effektiv zu schützen.

5.2.4 Schulen stets berücksichtigen & Thema im Fokus behalten

Schulen sollten beim Thema Informationssicherheit genau wie andere Ämter berücksichtigt und nicht nachgelagert behandelt werden, da sie eine große Menge an personenbezogenen Daten von Schülerinnen und Schülern verarbeiten und speichern, einschließlich Namen, Adressen, Noten, Gesundheitsinformationen und vielem mehr. Der Schutz dieser Daten ist von entscheidender Bedeutung, um die Privatsphäre und den Schutz der Schülerinnen und Schüler zu gewährleisten. Schulen sind genauso wie andere Organisationen anfällig für verschiedene Cyberbedrohungen wie Phishing-Angriffe, Malware-Infektionen, Hacking-Versuche und Datenlecks, in der Regel aber unsicherer aufgestellt als Kernverwaltungen. Ein solider Informationssicherheitsansatz hilft, entsprechende Schwachstellen zu erkennen, abzuwehren und zu minimieren, um den reibungslosen Betrieb der Schulen der Stadt Rheine sicherzustellen.

Mit der wachsenden Nutzung digitaler Technologien und Lernplattformen in Schulen wird der Schutz von Systemen und den darin enthaltenen Daten immer wichtiger. Eine robuste Informationssicherheit stellt sicher, dass den Schülerinnen und Schülern eine vertrauenswürdige und geschützte Lernumgebung geboten wird. Schulen verfügen über eine Vielzahl an Unterrichtsmaterialien, Administrationsdaten und vieles andere mehr. Ein guter Ansatz bei der Informationssicherheit hilft dabei, Datenverluste zu verhindern, Backups durchzuführen und bei Erforderlichkeit, eine Wiederherstellung zu gewährleisten.

Die Berücksichtigung der Informationssicherheit in Schulen ist daher von großer Bedeutung, um den Schutz von sensiblen Daten, die Sicherheit von IT-Infrastrukturen und IT-Systemen und den verantwortungsvollen Umgang mit Daten und Informationen zu gewährleisten. Auch die Schulen der Stadt Rheine haben die Verantwortung, Schülerinnen und

Schüler über den sicheren Umgang mit Informationen und digitalen Medien zu unterrichten. Indem Schulen das Thema Informationssicherheit priorisieren, können sie dazu beitragen, das Bewusstsein und das Wissen der Schülerinnen und Schüler auch in Bezug auf Datenschutz, sichere Online-Praktiken und den Schutz persönlicher Informationen zu stärken.

Grundsätzlich, auch unabhängig von der Einbindung der Schulen der Stadt Rheine gilt, stets am Thema Informationssicherheit „dranzubleiben“ und dieses über den oder die Informationssicherheitsbeauftragte:n nachhaltig in der Verwaltungs-IT und der Schul-IT zu verankern. Es muss klar sein, dass dies niemals mit einem kurzen Projekt erreicht werden kann, sondern dass entsprechende dauerhafte Strukturen zu schaffen und zu finanzieren sind.

6 Ressourcenabschätzung

Vor dem Hintergrund der Erkenntnisse der Untersuchung wird empfohlen, das Thema Informationssicherheit als Daueraufgabe mit folgendem eigenem Personal zu bearbeiten und ggf. entsprechende Ausschreibungen zügig auf den Weg zu bringen:

- 1,0 Stelle Informationssicherheitsbeauftragte:r für die Stadt Rheine inkl. der Schulen (Personal ohne technische Aufgaben)
- 0,5 Stelle technische und operative Umsetzung der Informationssicherheit für die Verwaltungs-IT (technisches Personal)
- 0,5 Stelle technische und operative Umsetzung der Informationssicherheit für die Schul-IT (technisches Personal)

Es bietet sich an, die beiden 0,5 Stellen technische und operative Umsetzung der Informationssicherheit in Personalunion vorzusehen.

Grundsätzlich sollte zusätzliches Budget für die Umsetzung der Informationssicherheit im Haushalt fest eingeplant werden. Es lassen sich keine allgemein gültigen Formeln oder feste Prozentzahlen finden, die für alle Kommunen gelten, da die Höhe des grundsätzlichen Budgets für Informationssicherheit im Verhältnis zum gesamten IT-Budget je nach Organisation und deren individuellen Bedürfnissen variieren kann. Die Stadt Rheine zeichnet sich dadurch aus, dass seitens der IT-Einheiten viele Infrastrukturkomponenten, IT-Systeme und Fachverfahren eigens betrieben werden, die dementsprechend auch aus eigenen Anstrengungen abgesichert werden müssen. Dementsprechend ist der Bedarf für Mittelbedarf hinsichtlich der Informationssicherheit höher, als wenn dies nicht der Fall wäre.

Die Festlegung des Budgets für Informationssicherheit basiert im Idealfall auf einer fundierten Risikoanalyse. Es ist wichtig, die spezifischen Anforderungen, Risiken und Prioritäten der gesamten Organisation inkl. der Schulen zu berücksichtigen. Ein bewährter Ansatz ist es, das Budget für Informationssicherheit als Prozentsatz des Gesamtbudgets für IT festzulegen. Ein häufig genannter Richtwert liegt bei 5%, 10% oder 15% des IT-Budgets. Das Bundesamt für Sicherheit in der Informationstechnik hat sogar bereits in ihrem Lagebericht zur Informationssicherheit im Jahr 2021 empfohlen, „[…] 20 Prozent der IT-Ausgaben für Cyber- und Informationssicherheit zu verwenden.“[33]. Diese Spanne kann als Ausgangspunkt dienen. Es ist allerdings wichtig, die spezifischen Bedürfnisse der Stadt Rheine zu berücksichtigen. Gegebenenfalls können externe Faktoren wie regulatorische Anforderungen, Compliance-Vorgaben oder spezielle Risikosituationen zumindest zeitweise zu einer höheren Priorisierung und Zuweisung von Ressourcen führen.

Es ist auch wichtig zu beachten, dass Informationssicherheit nicht nur ein einmaliger Kostenpunkt ist, sondern ein kontinuierlicher Prozess. Neben dem Budget für Investitionen in Sicherheitsmaßnahmen sollten auch Kosten für Schulungen, Schaffung von Mitarbeiterbewusstsein, Notfallausstattung, regelmäßige Überprüfungen und Aktualisierungen von Sicherheitsmaßnahmen, Durchführung von Penetrationstests, später ggf. Durchführung von Sicherheits-Audits und anderes mehr berücksichtigt werden. Eine gute Praxis hinsichtlich eines angemessenen Budgets für Informationssicherheit besteht darin, regelmäßig das Budget zu überprüfen und anhand aktueller Bedrohungen und Risiken anzupassen, um

[33] Bundesamt für Sicherheit in der Informationstechnik (2021): Die Lage der IT-Sicherheit in Deutschland 2021, S. 66

sicherzustellen, dass ausreichend Ressourcen für einen angemessenen Schutz bereitgestellt werden.

Initial kann es ein guter Weg sein, das IT-Budget moderat zu erhöhen, sodass der erhöhte Anteil einem Gesamtanteil von mindestens zehn Prozent entspricht, der ausschließlich für Informationssicherheit zur Verfügung steht.

Anhang

A.1 Expertengespräche: Behandelte Bereiche / Bausteine des IT-Grundschutz

Folgende Bereiche, Bausteine und Themen waren Gegenstand der Workshops:

ISMS: Sicherheitsmanagement als Grundlage für alles Weitere

- Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitung | Festlegung der Sicherheitsziele und -strategie | Erstellung einer Leitlinie zur Informationssicherheit | Benennung eines Informationssicherheitsbeauftragten | Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten | Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit | Festlegung von Sicherheitsmaßnahmen | Integration der Mitarbeiter:innen in den Sicherheitsprozess |Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse

ORP: organisatorische und personelle Sicherheitsaspekte

- Organisation: Festlegung von Verantwortlichkeiten und Regelungen |Zuweisung der Zuständigkeiten | Beaufsichtigung oder Begleitung von Fremdpersonen |Funktionstrennung zwischen unvereinbaren Aufgaben
- Personal: Geregelte Einarbeitung neuer Mitarbeiter:innen | Geregelte Verfahrensweise beim Weggang von Mitarbeiter:innen| Festlegung von Vertretungsregelungen | Festlegung von Regelungen für den Einsatz von Fremdpersonal | Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal
- Sensibilisierung und Schulung zur Informationssicherheit: Sensibilisierung der Institutionsleitung für Informationssicherheit | Einweisung des Personals in den sicheren Umgang mit IT | Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit
- Identitäts- und Berechtigungsmanagement: Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen | Einrichtung, Änderung und Entzug von Berechtigungen | Dokumentation der Benutzerkennungen und Rechteprofile | Aufgabenverteilung und Funktionstrennung | Vergabe von Zutrittsberechtigungen | Vergabe von Zugangsberechtigungen | Vergabe von Zugriffsrechten | Regelung des Passwortgebrauchs | Identifikation und Authentisierung

APP: Absicherung von Anwendungen / Diensten (z.B. Mail, Office)

- Office-Produkte: Einschränken von aktiven Inhalten | Sicheres Öffnen von Dokumenten aus externen Quellen | Verzicht auf Cloud-Speicherung | Verwendung von Viewer-Funktionen
- Anwendungen/ Internet/ Web-Browser: Verwendung von grundlegenden Sicherheitsmechanismen | Unterstützung sicherer Verschlüsselung der Kommunikation | Verwendung von vertrauenswürdigen Zertifikaten
- Benutzer-Authentifizierung: Erstellung einer Sicherheitsrichtlinie für Verzeichnisdienste | Planung des Einsatzes von Verzeichnisdiensten | Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste | Sichere Installation von Verzeichnisdiensten | Sichere Konfiguration und Konfigurationsänderungen von Verzeichnisdiensten | Sicherer Betrieb von Verzeichnisdiensten | Erstellung eines Sicherheitskonzepts für den Einsatz von Verzeichnisdiensten |Planung einer Partitionierung und Replikation im Verzeichnisdienst | Geeignete Auswahl von Komponenten für Verzeichnisdienste | Einrichtung des Zugriffs auf Verzeichnisdienste | Überwachung von Verzeichnisdiensten | Absicherung der Kommunikation mit Verzeichnisdiensten | Geregelte Außerbetriebnahme eines Verzeichnisdienstes | Migration von Verzeichnisdiensten
- Dateiablage: Einsatz von RAID-Systemen | Einsatz von Viren-Schutzprogrammen | Strukturierte Datenhaltung

SYS: einzelne IT-Systeme des Informationsverbunds

- Drucker- und Kopierraum / Netzwerk-Drucker und Multifunktionsgerät: Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten | Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte | Erstellung einer Sicherheitsrichtlinie für den Einsatz von Druckern, Kopieren und Multifunktionsgeräten | Beschränkung der administrativen Fernzugriffe auf Drucker, Kopierer und Multifunktionsgeräte
- Serversystem: Geeignete Aufstellung | Benutzerauthentisierung an Servern | Schutz von Schnittstellen | Deaktivierung nicht benötigter Dienste | Einsatz von Virenschutz-Programmen auf Servern | Protokollierung | Unterbrechungsfreie und stabile Stromversorgung | Betriebsdokumentation für Server | Geregelte Außerbetriebnahme eines Servers
- Virtualisierungshost: Sicherer Einsatz virtueller IT-Systeme | Sichere Konfiguration virtueller IT-Systeme | Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen | Schutz der Administrationsschnittstellen | Protokollierung in der virtuellen Infrastruktur | Zeitsynchronisation in virtuellen IT-Systemen | Rechte- und Rollenkonzept für die Administration einer virtuellen Infrastruktur
- Arbeitsplatz-PC: Sichere Benutzerauthentisierung | Aktivieren von Autoupdate-Mechanismen | Einsatz von Schutzprogrammen gegen Schadsoftware | Absicherung des Bootvorgangs | Geregelte Außerbetriebnahme eines Clients
- Mobiler Arbeitsplatz: Sichere Benutzerauthentisierung | Aktivieren von Autoupdate-Mechanismen | Einsatz von Schutzprogrammen gegen Schadsoftware | Absicherung des Bootvorgangs | Geregelte Außerbetriebnahme eines Clients
- Laptop: Regelungen zur mobilen Nutzung von Laptops | Sicherheitsrichtlinien für Laptops | Sicherer Anschluss von Laptops an Datennetze | Abgleich der Datenbestände von Laptops | Verlustmeldung für Laptops | Verschlüsselung von Laptops
- Smartphones und Tablets (inkl. „BYOD“ von Ratsmitgliedern): Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets | Festlegung einer Strategie für die Cloud-Nutzung | Sichere Grundkonfiguration für mobile Geräte | Verwendung eines Zugriffsschutzes | Updates von Betriebssystem und Apps | Datenschutzeinstellungen und Berechtigungen | Verhaltensregeln bei Sicherheitsvorfällen | Installation von Apps | Richtlinie für Mitarbeiter:innen zur Benutzung von mobilen Geräten | Verschlüsselung des Speichers | Deaktivierung nicht benutzter Kommunikationsschnittstellen

NET: Vernetzungsaspekte, z.B. Netz-Managem., Firewall, WLAN

- Netzarchitektur und -design: Sicherheitsrichtlinie für das Netz | Dokumentation des Netzes | Anforderungsspezifikation für das Netz | Netztrennung in Zonen | Client-Server-Segmentierung | Endgeräte-Segmentierung im internen Netz | Absicherung von schützenswerten Informationen | Grundlegende Absicherung des Internetzugangs
- WLAN-Nutzung: Festlegung einer Strategie für den Einsatz von WLANs | Auswahl eines geeigneten WLAN-Standards | Auswahl geeigneter Kryptoverfahren für WLAN
- Server- und Administrationsnetz: Planung des Netzmanagements | Anforderungsspezifikation für das Netzmanagement | Regelmäßige Datensicherung | Grundlegende Protokollierung von Ereignissen |Zeit-Synchronisation | Absicherung der Netzmanagement-Kommunikation und des Zugriffs auf Netz-Management-Werkzeuge | Beschränkung der SNMP (Simple Network Management Protocol)-Kommunikation | Schulungen für Management-Lösungen
- Demilitarisierte Zone: Planung des Netzmanagements | Anforderungsspezifikation für das Netzmanagement | Regelmäßige Datensicherung | Grundlegende Protokollierung von Ereignissen | Zeit-Synchronisation | Absicherung der Netzmanagement-Kommunikation und des Zugriffs auf Netz-Management-Werkzeuge | Beschränkung der SNMP Kommunikation | Schulungen für Management-Lösungen
- Netzwerk für reguläre Arbeitsplätze: Planung des Netzmanagements | Anforderungsspezifikation für das Netzmanagement | Regelmäßige Datensicherung | Grundlegende Protokollierung von Ereignissen | Zeit-Synchronisation | Absicherung der Netzmanagement-Kommunikation und des Zugriffs auf Netz-Management-Werkzeuge | Beschränkung der SNMP Kommunikation | Schulungen für Management-Lösungen
- WLAN (intern / ggf. öffentlich): Planung des Netzmanagements |Anforderungsspezifikation für das Netzmanagement | Regelmäßige Datensicherung | Grundlegende Protokollierung von Ereignissen | Zeit-Synchronisation | Erstellung eines Netzmanagement-Konzepts
- Gebäudeübergreifende Vernetzung: Planung des VPN-Einsatzes | Auswahl eines VPN-Dienstleisters | Sichere Installation von VPN-Endgeräten | Sichere Konfiguration eines VPN | Sperrung nicht mehr benötigter VPN-Zugänge | Planung der technischen VPN-Realisierung | Sichere Anbindung eines externen Netzes
- Firewall: Erstellung einer Sicherheitsrichtlinie | Festlegen der Firewall-Regeln | Einrichten geeigneter Filterregeln am Paketfilter | Sichere Konfiguration der Firewall | Schutz der Administrationsschnittstellen | Notfallzugriff auf die Firewall | Unterbindung von dynamischem Routing | Protokollierung | Abwehr von Fragmentierungsangriffen am Paketfilter | Deaktivierung von IPv4 oder IPv6 | Administration über ein gesondertes Managementnetz | Schutz vor TCP SYN Flooding, UDP Paket Storm und Sequence Number Guessing am Paketfilter | Absicherung von grundlegenden Internetprotokollen
- Router / Switche: Sichere Grundkonfiguration eines Routers oder Switches | Schutz der Administrationsschnittstellen | Schutz vor Fragmentierungsangriffen | Notfallzugriff auf Router und Switches | Protokollierung bei Routern und Switches | Regelmäßige Datensicherung | Betriebsdokumentationen
- TK-Anlage (inkl. Fax): Anforderungsanalyse und Planung für TK-Anlagen | Auswahl von TK-Diensteanbietern | Protokollierung bei TK-Anlagen | Geeignete Aufstellung eines Faxgerätes | Informationen für Mitarbeiter:innen über die Faxnutzung | Sicherer Betrieb eines Faxservers | Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen
- VoIP (Voice-over-IP): Planung des VoIP-Einsatzes | Sichere Administration und Konfiguration von VoIP-Endgeräten | Einschränkung der Erreichbarkeit über VoIP | Sichere Konfiguration der VoIP-Middleware | Sicherer Umgang mit VoIP-Endgeräten | Anforderungen an eine Firewall für den Einsatz von VoIP | Trennung des Daten- und VoIP-Netzes

INF: baulich-technische Gegebenheiten, z.B. Rechenzentrum

- Verwaltungsgebäude: Planung der Gebäudeabsicherung | Angepasste Aufteilung der Stromkreise | Einhaltung von Brandschutzvorschriften | Branderkennung in Gebäuden | Handfeuerlöscher | Geschlossene Fenster und Türen | Zutrittsregelung und -kontrolle | Rauchverbot | Sicherheitskonzept für die Gebäudenutzung
- Außenstelle: Planung der Gebäudeabsicherung| Angepasste Aufteilung der Stromkreise | Einhaltung von Brandschutzvorschriften | Branderkennung in Gebäuden | Handfeuerlöscher | Geschlossene Fenster und Türen | Zutrittsregelung und -kontrolle | Rauchverbot | Sicherheitskonzept für die Gebäudenutzung
- Büroraum: Geeignete Auswahl und Nutzung eines Büroraumes | Geschlossene Fenster und abgeschlossene Türen | Ergonomischer Arbeitsplatz | Aufgeräumter Arbeitsplatz | Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger
- Bürgerbüro (Arbeitsplatz mit Publikumsverkehr): Geeignete Auswahl und Nutzung eines Büroraumes | Geschlossene Fenster und abgeschlossene Türen | Aufgeräumter Arbeitsplatz | Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger | Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen | Geschlossene Fenster und Türen | Einrichtung sicherer Netzzugänge
- Besprechungsraum: Sichere Nutzung von Besprechungs-, Veranstaltungs- und Schulungsräumen | Geschlossene Fenster und abgeschlossene Türen |Einrichtung sicherer Netzzugänge
- Häuslicher Arbeitsplatz: Sichern von dienstlichen Unterlagen am häuslichen Arbeitsplatz | Transport von Arbeitsmaterial zum häuslichen Arbeitsplatz | Schutz vor unbefugtem Zutritt am häuslichen Arbeitsplatz | Entsorgung von vertraulichen Informationen am häuslichen Arbeitsplatz
- Mobiler Arbeitsplatz: Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes | Regelungen für mobile Arbeitsplätze | Zutritts- und Zugriffsschutz | Arbeiten mit fremden IT-Systemen | Zeitnahe Verlustmeldung | Entsorgung von vertraulichen Informationen
- Serverraum: Festlegung von Anforderungen | Bildung von Brandabschnitten | Einsatz einer unterbrechungsfreien Stromversorgung | Notabschaltung der Stromversorgung | Einhaltung der Lufttemperatur und -feuchtigkeit | Zutrittskontrolle | Verschließen und Sichern | Einsatz einer Brandmeldeanlage | Einsatz einer Lösch- oder Brandvermeidungsanlage | Inspektion und Wartung der Infrastruktur | Automatische Überwachung der Infrastruktur | Überspannungsschutzeinrichtung
- Archivraum: Handfeuerlöscher | Zutrittsregelung und -kontrolle | Schutz vor Staub und anderer Verschmutzung | Geschlossene Fenster und abgeschlossene Türen

ifib consult

Am Fallturm 1
28359 Bremen
Tel. 0421 218-56590
Fax: 0421 218-56599
E-Mail: info@ifib-consult.de
www.ifib-consult.de