Informationssicherheit für die Stadt Rheine

Vorstellung des Kurzgutachtens

30. Oktober 2023

Dr. Jörg Hofmann

Kurze Vorstellung

Das ifib

ifib research — Forschung & Entwicklung — Beratung & Transfer — ifib consult

Ende 2002 gegründet als GmbH an der Universität Bremen (anerkannte Gemeinnützigkeit)

Schwerpunkte:
- Datafizierung
- Medienbildung, Medien- und IT-Kompetenz
- Partizipation und Teilhabe
- Data Science, Maschinelles Lernen und Künstliche Intelligenz

Gründung Ende 2010 als 100%-ige Tochter des ifib

Schwerpunkte:
- Digitale Schule und Bildung
- Digitale Verwaltung und E-Government
- Digitale Hochschule und Wissenschaft

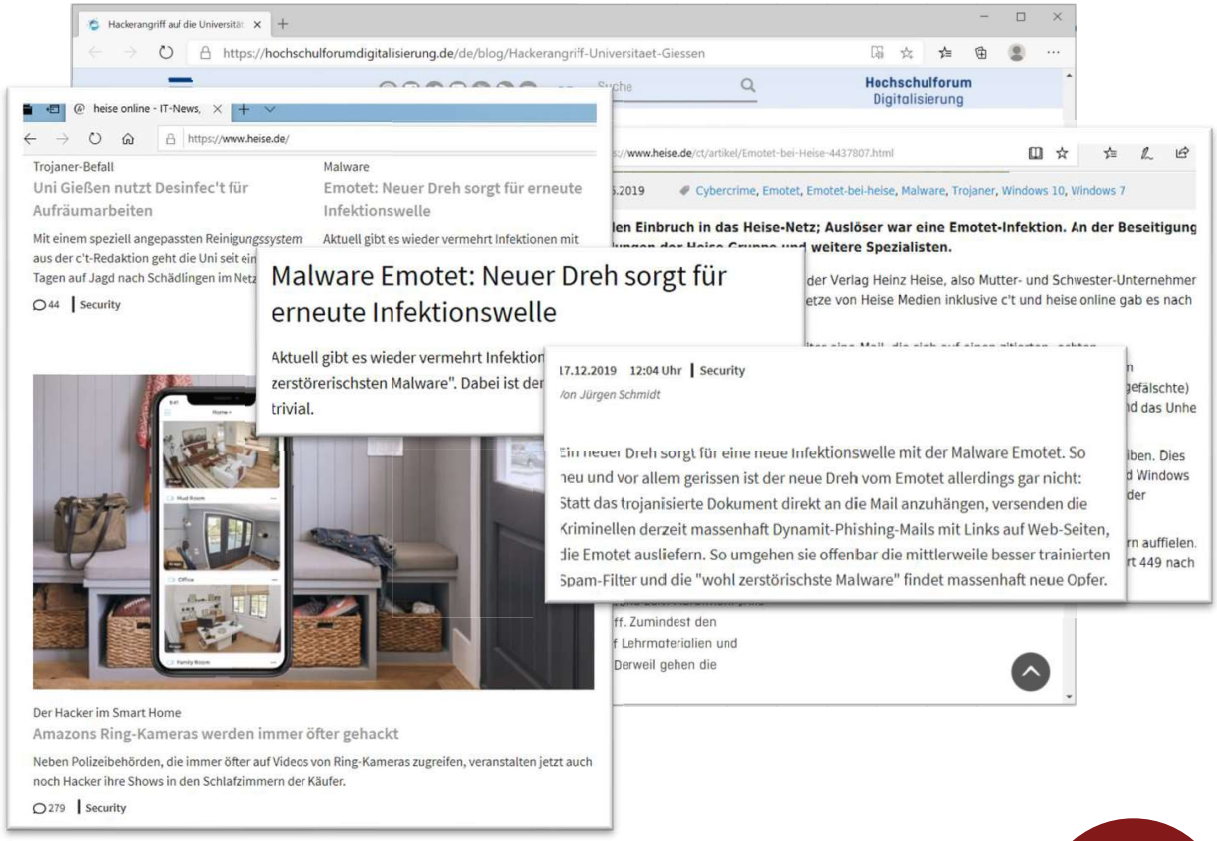
ca. 35 Mitarbeiter*innen aus zahlreichen Disziplinen

Mittelgeber: EU, Bund, Länder und Kommunen sowie Förderinstitutionen

Warum Informationssicherheit?

Gründe für Informationssicherheit (I)

- Starke Abhängigkeit von einer verfügbaren und gegen Angriffe geschützten IT-Infrastruktur
- Daten und Informationen einer Organisation sind Werte mit einem Schutzbedarf



Gründe für Informationssicherheit (II)

Bericht zur IT-Sicherheit in Deutschland

Weiterhin angespannte Lage

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht – als Cybersicherheitsbehörde – jährlich seinen Bericht zur Lage der IT-Sicherheit in Deutschland. Im aktuellen Betrachtungszeitraum hat sich die angespannte Lage weiter zugespitzt, auch im Kontext des russischen Angriffskrieges gegen die Ukraine.

Bundesinnenministerin Faeser kündigte am Dienstag einen erheblichen Ausbau der IT-Sicherheitsstruktur in Deutschland an.
Foto: mauritius images / NicoElNino / Alamy / Alamy Stock Photos

BSI-Bericht Oktober 2022: https://www.bundesregierung.de/breg-de/aktuelles/bsi-bericht-it-sicherheit-2022-2137774

Die Lage der IT-Sicherheit in Deutschland 2022 im Überblick

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft	Wirtschaft	Staat und Verwaltung
Identitätsdiebstahl Sextortion Fake-Shops im Internet	Ransomware Schwachstellen IT-Supply-Chain: Abhängig	Ransomware APT Schwachstellen, offene oder falsch konfigurierte Online-Server

Erster digitaler Katastrophenfall in Deutschland

207 Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

Die Anzahl der Schadprogramme steigt stetig.

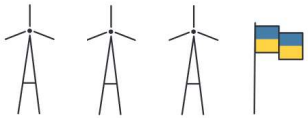
Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund

116,6 Millionen zugenommen.

Hacktivismus im Kontext des russischen Krieges:

Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

Kollateralschaden
nach Angriff auf Satellitenkommunikation



20.174

Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10%** gegenüber dem Vorjahr.

15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.

34.000

Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

78.000

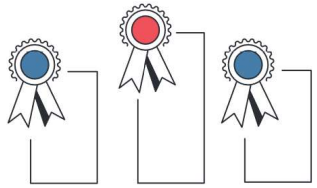
neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

69%

aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.

90%

des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.



BSI ist weltweit der führende Dienstleister im Bereich Common-Criteria-Zertifikaten.

4.400 (2020) → **5.100** (2021)

Zehn Jahre Allianz für Cyber-Sicherheit:
2022 sind wir bereits

6.220 Mitglieder.

Bundesamt für Sicherheit in der Informationstechnik

Deutschland **Digital•Sicher•BSI•**

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

Gute Lektüre: IT-Grundschutz-Kompendium

- IT-Grundschutz-Kompendium 2023
- 858 Seiten
- Inhalte:
  - Elementare Gefährdungen
  - Prozess-Bausteine (ISMS, Konzepte und Vorgehensweisen, Betrieb, Detektion und Reaktion)
  - System-Bausteine (Anwendungen, IT-Systeme, Industrielle IT, Netze und Kommunikation, Infrastruktur)

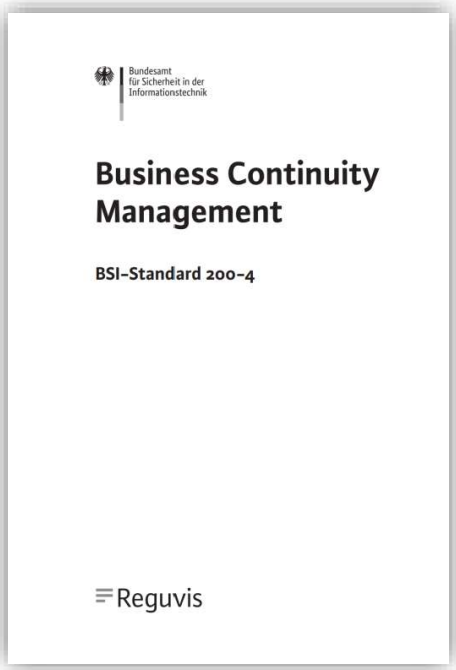
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

47 Elementare Gefährdungen*

* = G 0.1 bis G 0.47 nach IT-Grundschutz-Kompendium

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	

Ergänzende Lektüre: BSI Standards 200-1 bis 200-4



Aus dem Vorwort des Kompendium 2022:

- „Angriffe mit Ransomware sind die derzeit größte Bedrohung für Unternehmen und Behörden. Immer wieder gelingt es Kriminellen erfolgreich, Betroffene zu kompromittieren und zu erpressen, darunter sind auch kritische Infrastrukturen wie Krankenhäuser oder ganze Lieferketten von produzierenden Unternehmen.

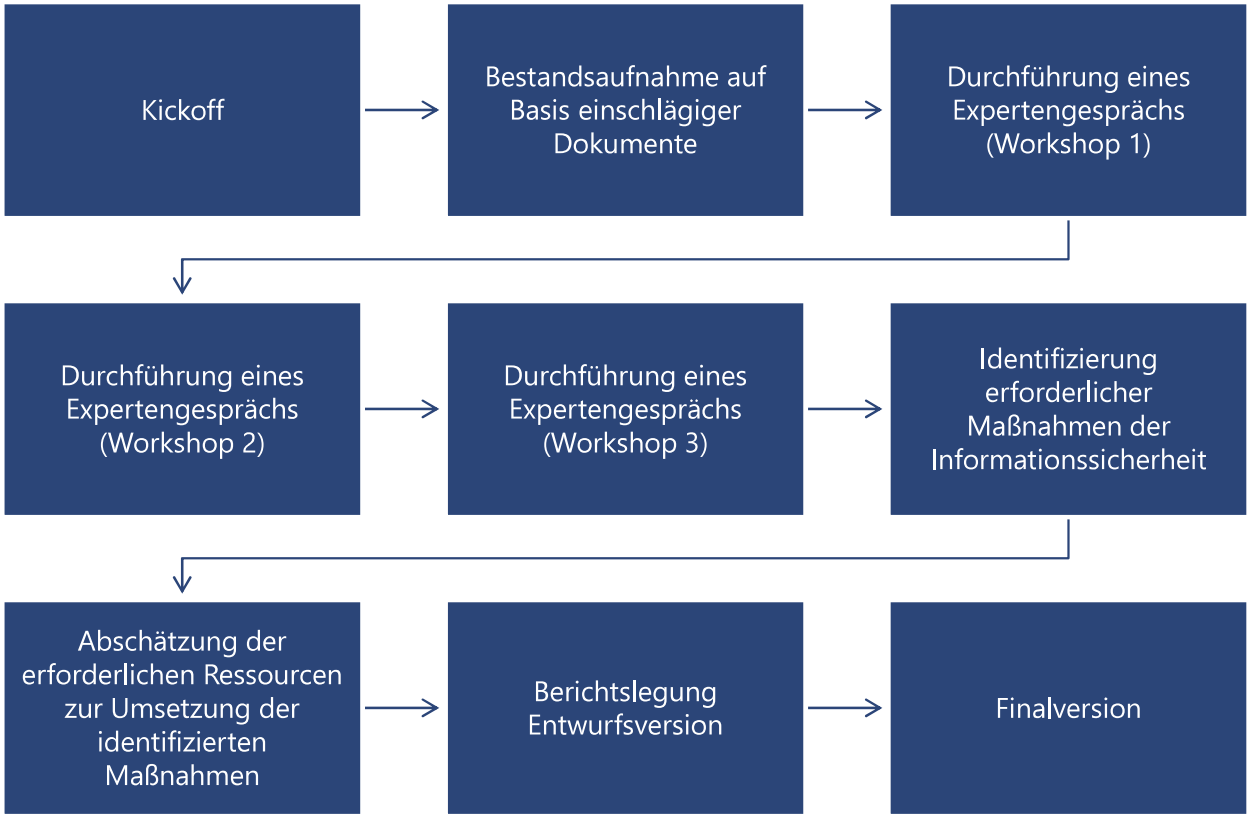
- Einfallstor für Angriffe dieser Art sind neben den immer wieder auftretenden Software-Schwachstellen leider auch Mitarbeiterinnen und Mitarbeiter, die durch immer ausgefeiltere Methoden – das so genannte Social Engineering – auf das digitale Glatteis geführt werden. “

Projekt und Vorgehen

Ziel des Projekts

- Identifizierung und Aufwandsbemessung für die Umsetzung erforderlicher Maßnahmen zur Gewährleistung grundlegender Ziele der Informationssicherheit gemäß BSI-Grundschutz für den IT-Betrieb der Schulen der Stadt Rheine, unter Einbezug von Synergieeffekten in der Zusammenarbeit mit der Rheiner Stadt-IT

Vorgehen im Projekt



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

Inhaltsverzeichnis

Version 1.01 vom 31.08.2023

Ergebnisse

Erkenntnisse

- Nutzbare Erkenntnisse aus GPA-Gutachten
- Veralteter Stand der Richtlinie für Informationssicherheit und der IT-Sicherheitsrichtlinie der Stadt Rheine
- Informationssicherheitsstrategie des Ministeriums für Schule und Bildung
- Fehlende reale Zuständigkeit für Informationssicherheit
- Hohe IT-Eigenständigkeit
- Eigene:r vs. externer ISB

Ausführliche Darstellung siehe Kurzgutachten Kapitel 4

Interne oder externe Besetzung der ISB-Rolle

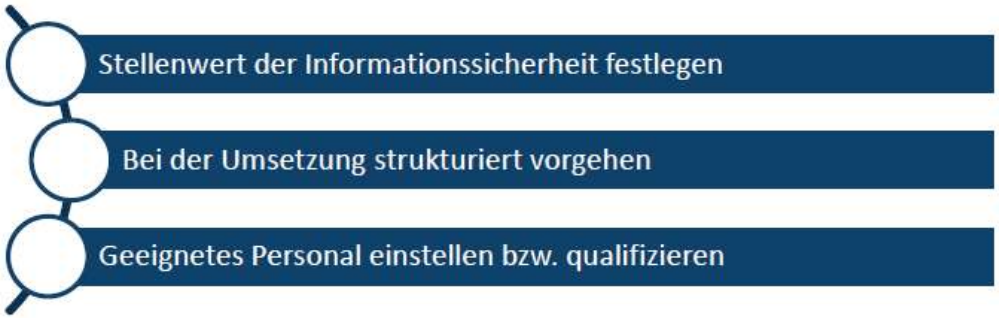
Interne Besetzung der Rolle ISB	Externe Besetzung der Rolle ISB
Mögliche Vorteile • wäre Teil der Stadt Rheine • kennt Abläufe, Prozesse und Verwaltungsangehörige und kann diese einschätzen • ständige Präsenz • zielgerichtete Vorbereitung und Durchführung von Schulungen und Sensibilisierungsmaßnahmen 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

strategisch / operativ

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.

Maßnahmen (I)

Aufbau organisatorischer Strukturen



Maßnahmen (II)

Umsetzung von Maßnahmen

Ressourcenabschätzung

- 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)
- Moderate Erhöhung des IT-Budgets, sodass der erhöhte Anteil einem Gesamtanteil von mind. 10% entspricht, der ausschließlich für Informationssicherheit zur Verfügung steht.
- Regelmäßige Überprüfung und Anpassung anhand aktueller Bedrohungen und Risiken

Vielen Dank für Ihre Aufmerksamkeit!

Am Fallturm 1
28359 Bremen

Tel.: 0421 218-56590
Fax: 0421 218-56599
E-Mail: info@ifib.de
www.ifib-consult.de

 ifib.de/blog  twitter.com/ifibGmbH  facebook.com/ifib-consult