Informationssicherheits- und Datenschutz-Management
STADTVERWALTUNG KOBLENZ

Tätigkeitsbericht

(01.01.2023 bis 31.08.2023)

Für die Sitzung des Werkausschusses KGRZ am 28.09.2023

KOBLENZ
VERBINDET.

Wichtige Informationen zu diesem Dokument

Dokumentenklasse:	öffentlich
Dokumententitel:	Bericht zur Informationssicherheit
Verantwortliche/r Autor/in:	Merlin Wolf
Dateiname:	Wa_2023_09_28_Bericht
Fassung vom:	14.09.2023
Letzte Veröffentlichung:	28.09.2023
Seitenzahl:	11
freigegeben durch:	Informationssicherheits- und Datenschutz-Management

Impressum

Informationssicherheits- und Datenschutz-Management
STADTVERWALTUNG KOBLENZ
Der Oberbürgermeister

Informationssicherheitsbeauftragter
Schängel-Center, 3. OG, Zimmer 303
Rathauspassage 2
56068 Koblenz

Tel: 0261 / 129 -1263
Fax: 0261 / 129 -1250

Datenschutzbeauftragter
Rathausgebäude II, 1. OG, Zimmer 110
Willi-Hörter-Platz 2
56068 Koblenz

Tel: 0261 / 129 -1214
Fax: 0261 / 129 -1200

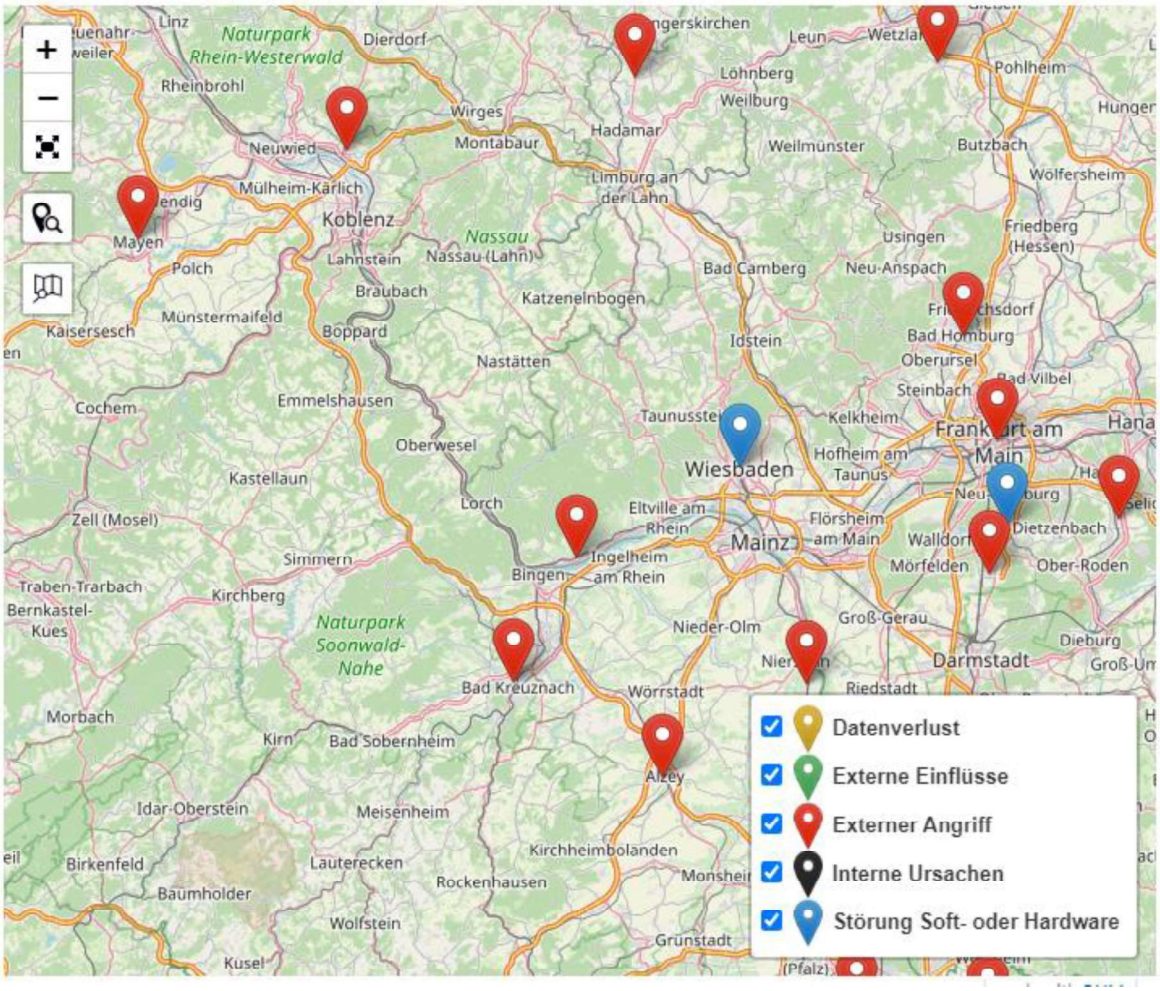
E-Mail: security.managment@stadt.koblenz.de

Inhaltsverzeichnis

1. Vorwort

Der Bericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Lage der IT-Sicherheit in Deutschland 2022 bringt es auf den Punkt: Die Gefährdungslage ist so hoch wie nie! Cyber-Kriminelle nutzen modernste Technologien für ihre Angriffe auf Privatpersonen, Unternehmen und staatliche Institutionen. Diesem Handeln muss entschieden entgegengetreten werden. Die Bürgerinnen und Bürger von Koblenz erwarten von Ihrer Verwaltung zu Recht, dass sie vorrausschauend handelt und die über sie erhobene, verarbeitete Daten und Informationen vor Gefahren im digitalen Raum schützt.

So kann man inzwischen sagen, es ist nicht mehr eine Frage, **OB** die Stadtverwaltung Opfer eines Cyberangriffes wird, sondern **WANN**. Die Internetseite www.kommunaler-notbetrieb.de liefert hier eine sehr gute Übersicht und man kann feststellen, dass sich im Umkreis von 150km schon viele Angriffe ereignet haben.



Umso wichtiger ist es, ein funktionierendes InformationsSicherheitsManagement zu betreiben und die Vorgaben des BSI umzusetzen. Denn nur so ist es möglich, einen nachweislichen Schutz gegen Bedrohungen durch Dritte zu erhalten und nicht fahrlässig mit den Daten und Informationen, die uns unserer Bürgerinnen und Bürger anvertrauen, umzugehen.

2. Tätigkeiten

Das Security Management hat im Berichtszeitraum (01.01.2023 bis 31.08.2023) 1248 Anfragen bearbeitet. Hierunter fallen unter anderem:

- 47 Anträge für mobiles Arbeiten mit Telearbeit und
  658 Anträge für mobiles Arbeiten nach der neuen Dienstanweisung zur Flexibilisierung des Arbeitsortes (DVFlexAO).
- 74 allgemeine Anfragen zu Themen der Informationssicherheit und des Datenschutzes
- 45 Anträge des IT Managements zur Einführung neuer Software

Neben den oben genannten Anfragen wurden weiterhin folgende Tätigkeiten wahrgenommen:

- Bearbeitung von Sicherheitsvorfällen
- Begleitung der K2 Zertifizierung im Bereich des KGRZ
- Erstellen von Richtlinien
- Benennen der Anforderungen an einen Penntest im Rahmen der Beratung der Verwaltung zu Fragen rund um das Thema Informationssicherheit und Datenschutz
- Erstellen eines Schulungskonzeptes einschließlich Schulung zum Thema Informationssicherheit und Datenschutz
- Erfassen der in der Verwaltung zum Einsatz kommenden Software durch Werksstudenten im Wiki der Verwaltung und in der zentralen Informationssicherheits- und Datenschutzmanagementsoftware
- Planung weiterer Maßnahmen zur Weiterentwicklung der Informations-sicherheit und des Datenschutzes innerhalb der SV Koblenz

3. Sicherheitsvorfälle

Im Rahmen des Sicherheitsvorfallmanagement des KGRZ wurden bis jetzt für das Jahr 2023 zwei Vorfälle gemeldet. Die geringe Anzahl beruht darauf, dass das KGRZ nur Vorfälle erfasst, die die Schutzziele „Vertraulichkeit“ oder „Integrität“ gefährden bzw. verletzten. Alle Vorfälle, die das Schutzziel „Verfügbarkeit“ betreffen, werden aktuell durch das KGRZ nicht erfasst, da es noch keine detaillierte Regelung gibt, ab welchem Zeitpunkt eine Erfassung erfolgen muss. Hierzu befindet sich das Security Management aktuell in Abstimmung mit dem IT Management. Das Ergebnis der Abstimmung wird anschließend mit dem KGRZ besprochen und die weitere Vorgehensweise festgelegt.

Gemeldete Vorfälle:

1.1. Rogue Device (AP)

Am 20.01.23 wurde durch das Team „Zentralen Dienste“ des KGRZ ein sogenanntes Rogue Device (Begriff aus dem Bereich der drahtlosen Netzwerke, der zur Beschreibung nicht autorisierter Geräte verwendet wird, die mit dem Netzwerk verbunden sind und ein erhebliches Risiko für die Organisation darstellen) gemeldet.
Im Verlauf der weiteren Untersuchungen konnte ermittelt werden, dass es sich um einen im Rahmen des Wlan Ausbaus in der Verwaltung installierten Accesspoint gehandelt hat, der im Auftrag des IT Managements montiert wurde. Das IT Management wird das KGRZ zukünftig über die Installation der weiteren Accesspoints informieren, damit es zu keinen weiteren „Fehlalarmen“ kommt.

1.2. Link in einer E-Mail

Am 11.04.23 wurde das Team „E-Collaboration“ des KGRZ durch die Stadtkasse informiert, dass in einer E-Mail ein Link aufgerufen wurde, die Mail sich aber im weiteren Verlauf als unglaubwürdig herausgestellt habe. Eine daraufhin durchgeführte Überprüfung durch die Kollegen des KGRZ bestätigte den Verdacht; der Vorgang wurde daraufhin als kritisch eingestuft.

Bereits 4 Minuten nach Eingang der Meldung durch die Stadtkasse wurde die betroffene Virtuelle Maschine durch die Kollegen des KGRZ deaktiviert und nach weiteren 11 Minuten neuinstalliert. Ein anschließend durchgeführter Scan der Laufwerke, auf die über die Virtuelle Maschine Zugriff bestand, verlief ohne positiven Befund.
Durch die Kollegen des Teams „E-Collaboration“ konnte später noch ermittelt werden, dass die verdächtige E-Mail insgesamt viermal bei der Stadtverwaltung eingegangen war, bei den anderen Empfängern der entsprechende Link innerhalb der E-Mail nicht aktiviert wurde.

4. BSI Zertifizierung der K2 Umgebung

Im Rahmen der Rechenzentrumskopplung der KDZ Mainz und des KGRZ Koblenz und der gemeinsam betriebenen „K2 Umgebung“ fand zu Beginn dieses Jahres eine Re-Zertifizierung des bei der KDZ Mainz betriebenen Teils des K2 Umgebung durch das BSI statt. Hierbei wurde jener Teil, der durch das KGRZ betrieben wird, im Rahmen des Bausteins OPS.3.1 Outsourcing für Dienstleister (Edition 2022) bzw. OPS.2.1 Outsourcing für Kunden betrachtet.
Das Audit wurde erfolgreich bestanden und die neuerliche Re-Zertifizierung steht nun für April 2025 an. Im Rahmen des erteilten Zertifikates für die KDZ Mainz wurde von Auditor jedoch mitgeteilt, dass das gewählte Konstrukt (Outsourcing) für die anstehende Re-Zertifizierung nicht mehr verwendet werden darf.
Aus diesem Grund wurde zwischen den Werkleitungen des KGRZ und der KDZ Mainz vereinbart, dass sich das KGRZ ebenfalls nach ISO 27001 auf Basis von IT-Grundschutz für den durch das KGRZ betriebenen Teil der K2 Umgebung bis April 2025 zertifizieren lassen wird.

5. Penntest

Das Security Management hat im Rahmen der Prüfung der sich im Einsatz befindlichen HCM Software für das „Personalmanagement-Modul“ nach Rücksprache mit dem IT Management einen Penntest empfohlen.
Durch den Penntest soll vor dem produktiven Einsatz des Moduls ermittelt und geprüft werden, in wieweit eventuell ein Zugriff auf die im System vorhandenen Mitarbeiterdaten durch unbefugte Dritte unter Ausnutzung möglicher

Schwachstellen erfolgen kann. Der Penntest wurde zwischenzeitlich beauftragt und wird in KW 38/2023 (18. – 22.09.2023) durchgeführt.
Sobald das Ergebnis vorliegt wird entschieden, ob ein Produktiveinsatz des Personalmanagement-Moduls erfolgen kann, Nachbesserungen notwendig sind oder ein produktiver Einsatz nicht möglich ist.

6. Schulungskonzept

Vom Security-Management wurde ein Schulungskonzept zu den Themen „Informationssicherheit und Datenschutz“ entwickelt. Die Schulungsunterlagen sind inzwischen fertiggestellt bzw. aufbereitet und durch die Werksstudenten des Security Managements haben damit begonnen, diese in die bei der Stadtverwaltung Koblenz eingeführte Learning Experience Plattform (LXP) „Datango“ zu überführen. Seitens des Security Managements ist geplant, die Schulungen ab Q4/2023 für die Mitarbeiter der Verwaltung bereitzustellen.

7. Softwareerfassung

Im Rahmen des Projektes „Softwareerfassung“ des Security Managements haben zwei Werksstudenten damit begonnen, alle bei der Stadtverwaltung Koblenz eingesetzten Softwareprodukte zu erfassen. Vorrangig geht es hierbei um die sogenannten Fachverfahren, wie MACH, GeDok etc. Bisher wurden bereits 180 Verfahren ermittelt und dokumentiert. Aktuell fehlen noch ca. 74 Verfahren. Anschließend werden noch weitere, kleinere Verfahren bzw. Tools erfasst. Die im Rahmen der Erfassung ermittelten Daten wurden sowohl im Wiki der Stadt Koblenz (Confluence) als auch im zentralen Informationssicherheits- und Datenschutzmanagementsystem (Otris) erfasst. Die in Otris erfassten Daten dienen im weiteren Prozess dazu, eine Basis für das Verzeichnis der Verarbeitungstätigkeiten zu bilden, da die meisten Verarbeitungstätigkeiten der Verwaltung in den genutzten Fachverfahren stattfinden.

8. Geplante / geforderte Maßnahmen

Ein der vielfältigen Aufgaben des Security Managements ist die „Initiierung und Kontrolle der Umsetzung von Informationssicherheits- und Datenschutz-maßnahmen“.
Aktuell sieht das Security Management bei den nachfolgend genannten Themenfeldern einen dringenden Handlungsbedarf:

8.1. Passwortmanager

Sichere Passwörter für alle Onlinekonten bzw. Fachanwendungen sind essenziell. "123456", "hallo" und "Passwort" zählen immer noch zu den am häufigsten vorkommenden Passwort-Kombinationen.
Aus diesem Grund soll allen Mitarbeitenden der Verwaltung ein zentraler Password Manager zur Verfügung gestellt werden, in dem die Mitarbeitenden alle von Ihnen genutzten Kennwörter zentral abspeichern können und nicht – wie es bisher oft Praxis ist – in Word oder Excel Dateien auf dem Rechner. Der Passwort-Manager hilft dabei, unterschiedliche und komplexe Passwörter zu verwalten. Diese mind. 13-stelligen Passwörter entsprächen damit auch den Festlegungen der neuen Passwortrichtlinie (siehe Punkt 9).

8.2. Endpoint Security durch zwei Faktor Authentifizierung

Im Rahmen des neuen NRX Konzeptes für Notebooks der Stadtverwaltung Koblenz wurde für die Anmeldung am städtischen Netzwerk ein sogenannter zweiter Faktor mittels eines „Yubikey“ eingeführt. Im Rahmen des IT Grundschutzkompendium des BSI wird nach dem Baustein ORP.4: Identitäts- und Berechtigungsmanagement ebenfalls ein solcher, zweiter Faktor gefordert. Da hierdurch die Sicherheit der Endgeräte deutlich gegenüber einer Anmeldung mit nur einem Faktor (Windowskennwort) erhöht wird, fordert das Security Management den Rollout des zweiten Faktors für alle Rechner der Verwaltung bis Ende Q4/2023.

8.3. Penntests

Aus Sicht des Security Managements bedarf es sowohl eines Penntests gegenüber dem Verwaltungsnetz als auch dem GLT-Netz. Hierdurch ließen sich große Schwachstellen – so denn welche vorhanden wären – schnell

und effektiv feststellen und entsprechende Maßnahmen könnten ergriffen werden, um diese zu schließen.

8.4. Veröffentlichung von Richtlinien

Das Security Management der Stadtverwaltung Koblenz hat die nachfolgend genannten Richtlinien erstellt. Diese befinden sich aktuell in der Abstimmungsphase mit den Ämtern 10/Personal und Organisation, 30/Rechtsamt und dem Personalrat und sollen im Laufe des 4. Quartals 2023 veröffentlicht werden:

- Richtlinie zur Sensibilisierung und Schulung im Bereich Informations-sicherheit und Datenschutz
- Richtlinie zur Verpflichtung auf das Datengeheimnis
- Richtlinie zur Löschung und Vernichtung von Datenträgern
- Richtlinie zur Löschung und Aussonderung von Mobile Devices

9. Schlusswort

Erlauben Sie mir, zum Abschluss dieses Berichtes – anders als in meinen vorangegangenen Berichten – einige wenige, persönliche Worte an Sie zu richten.

In den vergangenen Jahren konnten wir gemeinsam bereits einige grundlegende Maßnahmen zur Verbesserung der Informationssicherheit umsetzen. So wurde beispielsweise mit dem Neubau des sicheren Rechenzentrums (SRZ) ein solides Fundament geschaffen, welches erstmalig ermöglichte, die Anforderungen des BSI umzusetzen. Auch für die Zukunft sehe ich hier die Stadtverwaltung Koblenz und den Eigenbetrieb Kommunales Gebietsrechenzentrum Koblenz auf einem guten Weg.

Für sich alleine betrachtet, repräsentiert das SRZ allerdings nur einen Bruchteil jener umfangreichen Maßnahmen, die das BSI für die Einhaltung der Informationssicherheit in seinem Grundschutzkompendium einfordert. Die Verwaltung ist daher gut beraten, in ihren Anstrengungen für die Umsetzung dieser Anforderungen nicht nachzulassen.

Einen entscheidenden aber sehr wichtigen Faktor für ein erfolgreiches InformationsSicherheitsManagementSystem darf die Verwaltung dabei keinesfalls aus den Augen verlieren…. ihre Mitarbeitenden!

Sie sind es, die sich immer wieder aufs Neue hinterfragen müssen, ob sie auch wirklich alles in ihren Möglichkeiten Stehende zur Wahrung der Informationssicherheit berücksichtigen und die Daten ihrer Bürger sicher erhoben, be- bzw. verarbeitet und gespeichert haben.

Rückblickend ist mir dieses Bewusstsein und die erforderliche Sensibilität – insbesondere auf der Mitarbeitenden-Ebene – schon oft begegnet. Was die Sensibilisierung der einen oder anderen Führungsebene allerdings betrifft scheint mir, ist noch Einiges an Luft nach oben offen und wird wohl noch einige Zeit in Anspruch nehmen, bis auch dort die Notwendigkeit für die vielen noch umzusetzenden Maßnahmen zur Herstellung von Informationssicherheit wahr- und angenommen wird.

Dieses Selbstverständnis zu schaffen und aufrecht zu halten wird in den kommenden Jahren eine der wichtigsten Aufgaben im Rahmen der Umsetzung von weiteren Maßnahmen nach den Vorgaben des IT Grundschutzkompendiums sein!

Die Stadtverwaltung Koblenz wird künftig bei der – zugegebener Maßen – schwierigen Aufgabenerfüllung nicht mehr auf meine Unterstützung zurückgreifen können, da ich die Verwaltung zum 31.03.2024 verlassen werde.
Der Ihnen heute vorliegende Bericht ist daher mein letzter Bericht als InformationsSicherheitsBeauftragter der Stadtverwaltung Koblenz.

Ich bedanke mich ganz herzlich für Ihr Interesse an meiner Arbeit, der Arbeit des Security Managements der Stadtverwaltung Koblenz und den Themen „Informationssicherheit und Datenschutz“.