Informationssicherheits- und Datenschutz-Management

STADTVERWALTUNG KOBLENZ

Bericht zur Informationssicherheit

Für die Sitzung des Werkausschusses KGRZ am 17.02.2022

KOBLENZ
VERBINDET.

Wichtige Informationen zu diesem Dokument

Dokumentenklasse:	öffentlich
Dokumententitel:	Bericht zur Informationssicherheit
Verantwortliche/r Autor/in:	Merlin Wolf
Dateiname:	2022-02-07_Bericht
Fassung vom:	07.02.2022
Letzte Veröffentlichung:	07.02.2022
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. Log4j

Das Jahr endete mit einer fulminanten IT-Krise: Die Log4j Sicherheitslücke machte Unternehmen sowie Behörden angreifbar, das BSI gab eine Cyber-Sicherheitswarnung der Warnstufe Rot heraus.

Was ist die Log4j Sicherheitslücke?
Bei Log4j handelt es sich um eine weitverbreitete Protokollierungsbibliothek für Java-Anwendungen. Die Protokolldaten von Anwendungen lassen sich mittels Log4j performant aggregieren – Ereignisse im Serverbetrieb lassen sich also mithilfe von Log4j protokollieren. Am 10. Dezember 2021 wurde die Log4j Sicherheitslücke (CVE-2021-44228) bekannt, nachdem sie auf den Servern des Online-Games „Minecraft“ auffiel.

Was kann durch die Log4j Sicherheitslücke passieren?
Betroffen von der Log4j Sicherheitslücke sind die sehr weit verbreiteten Versionen 2.0 bis 2.14.1. Angreifende können die zum Logging verwendete Log4J-Java-Bibliothek nutzen, um remote Code zu injizieren. Angreifende, denen es gelingt, Zeichenketten, die aus Text oder Befehlen bestehen können, auf von ihnen kontrollierten Servern in der durch Log4j verwalteten Protokolldatei anzugeben, können dann Server erfolgreich übers Logging kapern („Log4Shell“).

Ein Beispiel zur Verdeutlichung: Eine Webshop-Betreiberin nutzt Log4j auf ihrem Apache-Server. Der Befehl, Kontakt zu einem Server – nämlich dem Server des Angreifers – aufzunehmen, wird durch Log4j protokolliert. In Zuge dessen wird der Shop-Server einen mit Malware versehenen Java-Code annehmen und ausführen. Mittels der Malware kann ein potentieller Angreifer die Kontrolle über den Rechner erlangen.

Es sind nicht nur Online-Systeme, sondern auch Anwendungen gefährdet. Durch die Lücke wäre es möglich, dass Angreifende Ransomware verteilen oder Hintertüren einbauen, die sie erst zu einem späteren Zeitpunkt nutzen. Die Schwachstelle ist leider sehr leicht angreifbar; es kursierte sogar ein Proof-of-Concept. Durch Beispiel-Skripte lassen sich Systeme auf Verwundbarkeit untersuchen. Diese Skripte geben Administratoren jedoch keinerlei Sicherheit – Angreifende können dennoch nach verwundbaren Systemen scannen.

Auch bei der Stadtverwaltung Koblenz waren zahlreiche Systeme von der Schwachstelle betroffen. Jedoch konnten alle entdeckten Systeme durch das KGRZ gepatcht und somit potenzielle Lücken für Angreifen geschlossen werden. Insgesamt 15 Personentage wurden durch die Kollegen des KGRZ für die Bearbeitung der Log4j Schwachstelle aufgewendet.

2. BSI Zertifizierung der K2 Umgebung

Aktuell befindet sich die durch die KDZ Mainz und das KGRZ Koblenz betriebener K2 Umgebung in einer durch die KDZ verantworteten BSI Zertifizierung. Im Rahmen des Audits fand auch eine Begehung des Sicheren Rechenzentrums (KGRZ.SRZ) durch den Auditor statt, bei dem der Baustein INF.2: Rechenzentrum sowie Serverraum des Grundschutzkompendiums des BSI geprüft wurde.

Durch den Auditor wurden keine Beanstandungen bei der Umsetzung der einzelnen Maßnahmen des Bausteins durch das KGRZ festgestellt.

3. Penetrationstest in der Stadtbibliothek

Zu Beginn des Jahres 2022 wurde durch die Firma PWC ein Penetrationstest der in der Bibliothek eingesetzten Software „Concerto“ der Firma BiblioMondo durchgeführt. Dem Security Management lag zum Zeitpunkt der Berichterstattung der finale Bericht des Pen-Tests noch nicht vor. In dem freundlicherweise vorab zur Verfügung gestellten Draft des Berichts wurden bereits mehrere Schwachstellen in der Software benannt, die eine potentielle Gefahr für die Nutzer der Software darstellen. Unter anderem besteht die Gefahr von Cross Side Scripting (Ausnutzen einer Computersicherheitslücke in Webanwendungen, indem nicht vertrauenswürdige Informationen in einen anderen Kontext eingefügt werden).

Hierdurch besteht eine akute Gefahr für alle Bürger, die in vollem Vertrauen in Stadtbibliothek auf deren angebotenen online Dienste zugreifen, da in einem Fall von Cross Side Scripting deren Heimrechner kompromittiert werden.

Das KGRZ teilte dem Security Management nach Vorlage des Drafts mit, dass es einen sicheren Betrieb der Anwendung nicht gewährleisten kann. Als nächster Schritt wird das Security Management mit dem Hersteller der Software klären, ob die Sicherheitslücken innerhalb einer angemessenen Frist geschlossen werden können. Sollte dies nicht der Fall sein, wird der Informationssicherheitsbeauftragte den Sachverhalt bewerten und dem Herrn Oberbürgermeister eine Empfehlung aussprechen, wie mit den Sicherheitslücken weiter zu verfahren ist.

4. Penetrationstest des Bewerberportals

Ende letzten Jahres wurde durch die Firma PWC ein Penetrationstest des Bewerberportals der Stadtverwaltung Koblenz durchgeführt. Die hierbei festgestellten Mängel / Schwachstellen konnten direkt durch den Hersteller und das KGRZ behoben werden.

5. Cyberversicherung

Das Security Management der Stadtverwaltung Koblenz ist aktuell dabei, den aktuellen Stand der Informationssicherheit in der Verwaltung aufzubereiten. Hierbei gilt es unter anderem alle Ämter und Eigenbetriebe mit deren eingesetzten Fachverfahren auf potenzielle Gefährdungen im Bereich Informationssicherheit zu prüfen.

Das hierbei gewonnene Ergebnis soll dazu dienen, eine bessere Einschätzung darüber zu gewinnen, ob die Verwaltung eine Cyberversicherung abschließen muss. Darüber hinaus soll das Ergebnis der Einschätzung dazu dienen, den Versicherungen eine Basis für ein später zu unterbreitendes Angebot an die Hand zu geben.