Handreichung zur Log4Shell-Erstanalyse

Version 1.0, Stand:14.12.2021

Herausgeber:
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18
91522 Ansbach

Tel.: 0981 180093-0
E-Mail: poststelle@lda.bayern.de
Web: www.lda.bayern.de

Ausgangslage

Log4Shell bezeichnet eine Schwachstelle in der weit verbreiteten Log4j-Java-Protokollierungsbibliothek. Die Schwachstelle wird unter CVE-2021-44228 geführt.

Ziel dieses Dokuments

Das Dokument soll Verantwortlichen und deren betriebliche Datenschutzbeauftragten wesentliche datenschutzrechtlich gebotene Abhilfemaßnahmen und weiterführende Links zur Erstanalyse bei eigener Log4Shell-Betroffenheit aufzeigen. Die darin enthaltenen Punkte sind weder als abschließend zu verstehen noch ungeprüft umzusetzen, sondern jeweils vom Verantwortlichen auf die individuell vorherrschenden Rahmenbedingungen anzupassen.

Maßnahmen

Hinweis: Voraussetzung zur angemessenen Reaktion und Durchführung einzelner Sicherheitsmaßnahmen ist technisch versiertes Personal.

Betroffene Systeme müssen schnellstmöglich von Verantwortlichen „entschärft" werden. Dies gelingt entweder durch das Einspielen der aktuellsten Version von Log4j, dem vorübergehenden Abschalten nicht-zwingend benötigter, aber betroffener Systeme und eine erhöhte Wachsamkeit insbesondere bei Servern, die bei der Verarbeitung personenbezogener Daten über das Internet eingesetzt werden, in Einzelfällen aber auch bei Systemen, die (manipulierte) Daten abseits einer direkten Internetanbindung verarbeiten. Gerade bei Systemen und Diensten, die von Dienstleistern oder Software-Anbietern zur Verfügung gestellt werden, besteht eine direkte Abhängigkeit bei der Zurverfügungstellung von Updates. Sofern die Hersteller schon die entsprechenden Sicherheitsupdates anbieten, sind diese zu installieren. Einen Überblick der technischen und organisatorischen Maßnahmen, insbesondere für die Administratoren der Verantwortlichen, findet man bspw. Auch in einem Dokument des BSI zu Log4Shell: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.html

Das BayLDA fasst im Folgenden einige wesentliche datenschutzrechtliche Handlungsempfehlungen für Verantwortliche kompakt zusammen:

☐ Ausreichend Ressourcen zur Analyse und Behandlung der Schwachstelle unter Einbindung des betrieblichen Datenschutzbeauftragten zur Verfügung stellen

☐ Verwundbare Systeme schnellstmöglich identifizieren bzw. lokalisieren und behandeln oder im Idealfall eine Verwundbarkeit ausschließen. Dazu wird empfohlen, das Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO als Prüfgrundlage zu verwenden, um einen vollständigen Überblick über die verwendeten Softwareprodukte und Dienste zu erlangen - diese können dann auch mit einschlägigen Quellen[1] zu betroffenen Softwareprodukten abgeglichen werden.

☐ **Update auf neueste Log4j-Version** (2.15.0) bei eigenen Systemen **durchführen**, sofern möglich.

☐ Sofern (noch) kein Update möglich ist, prüfen:
- Unterbindung von Namensauflösungen durch spezifische Konfiguration der Log4J-Protokollierung (z.B. Option log4j2.formatMsgNoLookups auf „true" setzen)
- Alternativ die Umgebungsvariable LOG4J_FORMAT_MSG_NO_LOOKUPS auf „true" setzen
- Entfernen der Klasse JndiLookup in Java-JAR-Dateien, sofern möglich
- Sofern JNDI-Anfragen für den Betrieb einer Anwendung erforderlich sind, muss eine Blockierung derartiger Netzwerkaufrufe an nicht vertrauenswürdige (externe) Server mittels Firewallkonfiguration unterbunden werden.

☐ Im Rahmen von Auftragsverarbeitung genutzte Dienste hinsichtlich der Verwundbarkeit untersuchen bzw. Rücksprache mit Auftragsverarbeiter führen. Die Analyse und Behebung der Log4Shell-Schwachstelle gehört zu technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO, die auch für Auftragsverarbeiter gelten. Zur verbesserten Einschätzung, ob und welche Dienstleister betroffen sein könnte, kann auch hier das Verzeichnis der Verarbeitungstätigkeiten (VVT) zu Rate gezogen werden.

☐ Ausgehende Netzwerkaktivitäten von Servern weiterhin gründlich mittels geeignetem Firewall- und Proxy Einsatzes auf das erforderliche Mindestmaß reduzieren und nach zur Log4Shell-Schwachstelle passenden Angriffsmustern (z.B. z.B. http-Header mit Zeichenkette `${jndi:ldap://` oder auch „merkwürdigen" Zeichenketten wie `${${::-j}n${::-d )` suchen. Sofern nicht erforderlich, sollten LDAP-Aufrufe (an externe) Systeme durch die Firewall unterbunden werden. Es sollte auch geprüft werden, ob überhaupt eine wirksame Netzwerkprotokollierung stattfindet.

☐ Nutzung der Funktionalitäten von Intrusion Prevention Systemen und Web Application Firewalls soweit wie möglich – es ist aber zu beachten, dass zeichenkettenbasierte Schutzfunktionen durch modifizierte Angriffsstrings ggf. umgangen werden können

☐ Nachverfolgung und Berücksichtigung der veröffentlichen Informationen zu Log4Shell sowohl seitens der Anbieter, der Fachpresse als auch der Sicherheitsbehörden

☐ Prüfen, ob die Meldevoraussetzungen aus Art. 33 DS-GVO erfüllt sind und bei Bedarf fristgerecht eine Meldung einer Datenschutzverletzung unter www.lda.bayern.de/datenpanne durchführen.

[1] z.B. unter https://github.com/NCSC-NL/log4shell

E. Datenschutzrechtliches Ergebnis

Eine Sicherheitslücke alleine löst bekanntlich noch keine datenschutzrechtliche Meldeverpflichtung aus. Jedoch bedeutet ein Vorliegen der Schwachstelle Log4Shell in Log4j eine Verletzung der Vorgaben zur Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO bei den jeweiligen Verantwortlichen. Finden sich dann Anzeichen, dass die Schwachstelle ausgenutzt wurde und personenbezogene Daten betroffen sind, ist im Regelfall davon auszugehen, dass eine meldepflichtige Datenschutzverletzung nach Art. 33 DS-GVO vorliegt, da derart kompromittierte IT-Systeme seltenst „nicht zu einem Risiko" für die Rechte und Freiheiten der davon betroffenen Personen führen dürfte. Die maßgeblichen Feststellungen, insbesondere ob eine Risiko für die betroffenen Personen besteht oder nicht, sind nach Art. 5 Abs. 2 DS-GVO (Rechenschaftspflicht) umfassend zu dokumentieren. Eine Meldung nach Art. 33 DS-GVO zur Datenschutzverletzung kann von bayerischen Verantwortlichen aus dem nicht-öffentlichen Bereich über den Online-Service des BayLDA durchgeführt werden.

Weiterführende Links

- BSI Cyber-Sicherheitswarnung zu Log4Shell: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.html
- BSI Pressemitteilung zu Log4Shell: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/211211_log4Shell_WarnstufeRot.html
- BayLDA Meldung einer Datenschutzverletzung nach Art. 33 DS-GVO für bayerische Verantwortliche aus dem nicht-öffentlichen Bereich: https://www.lda.bayern.de/datenschutzverletzung
- BayLDA Cybersicherheit Checkliste mit Prüfkriterien nach Art. 32 DS-GVO: https://www.lda.bayern.de/media/checkliste/baylda_checkliste_medizin.pdf (ohne Kapitel 9)
- BayLDA Patch Management Checkliste nach Art. 32 DS-GVO: https://www.lda.bayern.de/media/checkliste/baylda_checkliste_patch_mgmt.pdf
- Cyberabwehr Bayern - Ansprechpartner zur Cybersicherheit in Bayern: https://www.lda.bayern.de/media/Behoerdenuebersicht_Cybersicherheitsvorfall.pdf
- Zentrale Ansprechstelle Cybercrime (ZAC) des Bayerischen Landeskriminalamtes (LKA): https://www.polizei.bayern.de/kriminalitaet/internetkriminalitaet/002464/index.html