Kritische IT Sicherheitslücke wird aktiv für Cyberangriffe genutzt

KRITISCHE CYBERSICHERHEITSWARNUNG

Die Sicherheitslücke („Log4shell“) in der weit verbreiteten Programmbibliothek (Log4j) der Programmiersprache Java stellt aktuell eine **extrem große Gefährdung österreichischer Unternehmen und Organisationen** dar. Die Menge an potentiell betroffenen Systemen ist enorm, da die Programmiersprache Java weltweit auf mehreren Milliarden von Produkten, Anwendungen und Geräten implementiert ist.

Log4shell ist sehr einfach ausnutzbar und wird bereits jetzt von **Angreifern aller Art** massiv **ausgenutzt**. Das Spektrum reicht von **Cyberkriminellen**, beispielsweise durch das Einspielen von **Erpressungstrojanern** in Unternehmensnetzwerke (Ransomware), bis hin zu staatlich gesteuerten Akteuren, umfasst aber auch unbedarfte Trittbrettfahrer.

Es ist davon auszugehen, dass Angreifer nach einem ersten Eindringen in ein Unternehmensnetzwerk auch **alle weiteren Systeme des Unternehmens ins Visier** nehmen und **diese in ihre Gewalt bringen** bzw. übernehmen können.

Es besteht daher **dringender Handlungsbedarf**:

1) **Aktualisierung** aller betroffenen Systeme, für die der Hersteller Softwareupdates bereits zur Verfügung stellt.
2) **Deaktivieren** der Sicherheitslücke und **Überprüfung** ob bereits ein Angreifer diese ausnutzen konnte. Da sich diese Aufgabe als durchaus komplex herausstellen kann, sollte hierzu bei Bedarf professionelles IT Know-How herangezogen werden.

Für weiterführende technische Informationen, welche regelmäßig aktualisiert werden, verweisen wir auf die Warnungen und Beiträge

- des nationalen Computernotfallteams Österreichs unter https://cert.at/de/warnungen/2021/12/kritische-0-day-sicherheitslucke-in-apache-log4j-bibliothek,
- der europäischen Agentur für Cybersicherheit unter https://www.enisa.europa.eu/news/statement-on-log4shell,
- des deutschen BSI unter https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf sowie
- der US Behörde CISA unter https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance.

Permanent aktualisierte Verzeichnisse **betroffener Produkte, Anwendungen und Geräte** sind unter folgenden Links abrufbar:

- https://github.com/cisagov/log4j-affected-db
- https://github.com/NCSC-NL/log4shell/tree/main/software