Java-Sicherheitslücke "Log4Shell": Ernste Cybergefahren für bayerische Betriebe!

Mittwoch, 15 Dezember 2021

https://www.datenschutz.de/java-sicherheitsluecke-log4shell-ernste-cybergefahren-fuer-bayerische-betriebe/

LDA-Checkliste zu datenschutzrechtlichem Handlungsbedarf

Pressemitteilung des Bayerischen Landesamts für Datenschutzaufsicht vom 14.12.2021

Die Java-Protokollierungsbibliothek „Log4j“ ist weit verbreitet. Sie ist Bestandteil vieler kommerzieller Produkte genauso wie von Open-Source-Software, aber auch selbst entwickelter Java-Anwendungen. Durch die kürzlich aufgedeckte Schwachstelle „Log4Shell“ (CVE-2021-44228) können Angreifer über das Internet eigene Programmcodes ausführen und damit einen Brückenkopf für weitere Cyberattacken installieren. Dadurch droht auch längerfristig die Kompromittierung vieler Dienste und vielfach sogar Einschränkungen des Regelbetriebs wichtiger Systeme.

Michael Will, Präsident des BayLDA, bewertet die Lage aus Datenschutzsicht als alarmierend: „Das Bedrohungspotential der Schwachstelle Log4Shell kann kaum ernst genug genommen werden. Verantwortliche müssen nun umgehend aktiv werden, um die eigenen Systeme zu prüfen und die Schwachstelle zu beseitigen. Bereits in der jüngeren Vergangenheit haben Cyberangriffe über andere Sicherheitslücken zu enormen Schäden geführt. Log4Shell hat das Potential, diese Risiken zu übertreffen und branchenübergreifend zahlreiche Betriebe in ihrem Arbeitsalltag massiv zu stören. Wir beobachten die Entwicklung daher intensiv und mit größter Sorge. Unser erstes Augenmerk gilt wirksamen Abhilfemaßnahmen, für die wir eine Checkliste bereitstellen. Unsere Erfahrungen mit der Nachlässigkeit zahlreicher Verantwortlicher trotz schwerwiegender Cybergefahren – zuletzt etwa der Schwachstelle bei Exchange-Servern im Frühjahr diesen Jahres – zeigen aber auch, dass Nachkontrollen zur Gewährleistung des Datenschutzes unerlässlich sind. Daher prüfen wir bereits, wie bayerische Verantwortliche einer automatisierten Datenschutzkontrolle unterzogen werden können, die Versäumnisse bei der Java-Sicherheitslücke aufdecken wird. Verstöße gegen die Sicherheitsanforderungen der Datenschutz-Grundverordnung können von uns mit empfindlichen Geldbußen geahndet werden.“

Welches Ausmaß die Java-Sicherheitslücke Log4Shell für bayerische Unternehmen, Vereine und Verbände, Ärzte, Rechtsanwälte etc. haben wird, ist trotz allseitiger Aufklärungsbemühungen längst noch nicht absehbar. Jedoch ist bereits zum jetzigen Zeitpunkt bekannt, dass flächendeckende Scans nach verwundbaren Systemen stattfinden und auch schon gezielt Angriffe durchgeführt werden. Es ist somit nur noch eine Frage der Zeit, wann Verantwortliche, die von der Lücke betroffen sind, einen Schaden feststellen. Nicht nur wirtschaftlich, sondern auch datenschutzrechtlich ist ein solches Szenario mit schwerwiegenden Konsequenzen verbunden. Letztendlich drohen Verantwortlichen insbesondere ein Abfluss personenbezogener Daten, eine Nicht-Verfügbarkeit wichtiger Systeme und Dienste oder eine Einrichtung von Backdoors für spätere Cyberattacken. Selbst Angriffe mit Ransomware zur Erpressung der betroffenen Betriebe sind wahrscheinlich. Verbraucherinnen und Verbraucher sind im Normalfall

zwar nicht direkt von der Schwachstelle betroffen, könnten aber Auswirkungen spüren, etwa wenn Dienste wie Apps oder Webservices nicht mehr erreichbar sind oder eigene persönliche Daten durch Angriffe gestohlen werden.

Bayerische Verantwortliche müssen aufgrund der erhöhten Gefährdungslage zur Einhaltung datenschutzrechtlicher Verpflichtungen unverzüglich prüfen, ob deren IT-Systeme und Anwendungen von der Java-Sicherheitslücke Log4Shell betroffen sind. Hierzu steht unter www.lda.bayern.de/log4shell eine Checkliste zur Verfügung. Ist bereits eine Sicherheitsverletzung eingetreten, z. B. weil die Sicherheitslücke aktiv ausgenutzt wurde und IT-Systeme mit personenbezogenen Daten betroffen sind, besteht nach Art. 33 DS-GVO für Verantwortliche regelmäßig eine Meldeverpflichtung bei der zuständigen Datenschutzaufsichtsbehörde.

Michael Will
Präsident des Bayerischen Landesamts für Datenschutzaufsicht
