Log4j Schwachstelle

Updates allein reichen nicht – was ist jetzt konkret zu tun?

Anwender müssen schnellstmöglich auf die Schwachstelle reagieren – aber wie? Pierre Büttner von Farmpartner-tec gibt erste Handlungsempfehlungen.

Ganz allgemein gilt auch hier: „Halten Sie Ihre Systeme sowie die darauf operierende Software mit Hilfe der verfügbaren Updates auf dem aktuellsten Stand“. Aber reicht dies schon aus? Leider nein! Nicht jeder Softwareanbieter hat in den wenigen Tagen seit Bekanntwerden der Schwachstelle mit einem Hotpatch oder Update reagieren können. Ebenso befinden sich auf vielen Anwendungscomputern Programme, die einst installiert wurden und später in Vergessenheit gerieten. Es empfehlen sich daher ergänzende Maßnahmen.

Im ersten Schritt gilt es in Erfahrung zu bringen, ob eine oder mehrere der auf Ihren Systemen eingesetzten Softwarelösungen die Log4j Bibliothek (vor Version 2.17) der Java Programmiersprache verwenden.

Leider ist dies für Betreiber und Anwender häufig nicht zu erkennen. Hier hilft ein Blick in die Dokumentationen der von Ihnen eingesetzten Software-Werkzeuge oder eine gezielte Anfrage gegenüber dem Softwareentwickler. Um keine wertvolle Zeit während der Recherche zu verlieren, können Sie die für die Angriffe genutzte „Lookup“ Funktion der Log4j Bibliothek durch Ihren Systemadministrator oder Ihren EDV-Dienstleister temporär deaktivieren lassen und im Nachgang den Sicherheitsempfehlungen der Hersteller betroffener Programme folgen.

Um die kritische Funktion zu deaktivieren, kann Ihr Systemadministrator die Java Umgebungsvariable „LOG4J_FORMAT_MSG_NO_LOOKUPS“ auf den Wert „True“ setzen oder die CLI Anweisung „–Dlog4j2.formatMsgNoLookups=True“ ausführen.

Bitte beachten Sie, dass diese Anpassungen nur von IT Fachkräften ausgeführt werden sollte. Programme, die Sie nicht nutzen und daher auch nicht regelmäßig updaten, sollten Sie vorsorglich deinstallieren.

Über diese konkreten Maßnahmen hinaus können Sie Ihren IT Sicherheits-Experten bitten, die Erreichbarkeit Ihrer Systeme von extern zu prüfen und zu bewerten. In vielen Fällen ist eine direkte Erreichbarkeit von außen nicht notwendig und auch nicht empfehlenswert.