LOG4J-LÜCKE : BSI gibt vorschnell Entwarnung für Verbraucher

Verbraucher seien von der Server-Sicherheitslücke Log4Shell nur indirekt betroffen, sagt das BSI. Diese Behauptung könnte gefährlich werden.

Boris Mayer 14. Dezember 2021, 15:06 Uhr

Kaffee verschüttet: Vorschnelle BSI-Entwarnung für Verbraucher (Bild: Manos/CC-BY 2.0)

BSI-Präsident Arne Schönbaum sagte am Montag, dass die deutsche IT-Sicherheitsbehörde keine unmittelbaren Folgen durch die Log4J-Sicherheitslücke für Verbraucher sehe. *"Handys und iPads sind davon bisher nicht*

betroffen, das muss man ganz klar sagen," erklärte er. Verbraucher treffe das Problem nur, wenn sie Dienste von Unternehmen und Behörden nutzten, die betroffen sind.

Das ist eine sehr aparte Sicht der Dinge. Richtig ist, Handys und iPads sind nicht betroffen. Bei den Java-Versionen für Android ist kein JNDI-Paket enthalten, was Angriffe über die Lücke in Log4J unmöglich macht. Und die Software für iPads und iPhones ist nun einmal nicht in Java geschrieben. Zudem ist kaum eine App auf einem Handy dafür vorgesehen, sich aus der Ferne mit dem Mobiltelefon zu verbinden. Für diese Geräte ist deshalb die Gefahr durch die Log4J-Lücke de facto nicht vorhanden.

Allerdings besteht die IT-Infrastruktur in den wenigsten privaten Haushalten der vom BSI-Präsidenten so vollmundig entwarnten Verbraucher lediglich aus ein paar Tablets und Smartphones. Computer und Notebooks sind nach wie vor sehr beliebt, hinzu kommen häufig ein Router für den Internetanschluss und vielleicht auch noch das ein oder andere Network-Attached-Storage-System (NAS) oder eine einfache Netzwerkfestplatte. Ganz zu schweigen von einer Menge IoT-Gadgets.

Und all diese Technik, von der der BSI-Präsident offenbar denkt, dass sie nur Unternehmen oder Behörden verwenden, kann sehr wohl Software beinhalten, in denen die Log4J-Bibliothek Verwendung findet.

Mehr als nur Tablets und Smartphones

Gerade Router, Netzwerkfestplatten und NAS-Systeme verfügen in den meisten Fällen über eine Webschnittstelle zwecks Konfiguration, an der man sich über Username und Passwort authentifiziert. Zwar dürfte es sich in den meisten Fällen nicht um eine Java-Applikation handeln, auszuschließen ist dies jedoch nicht.

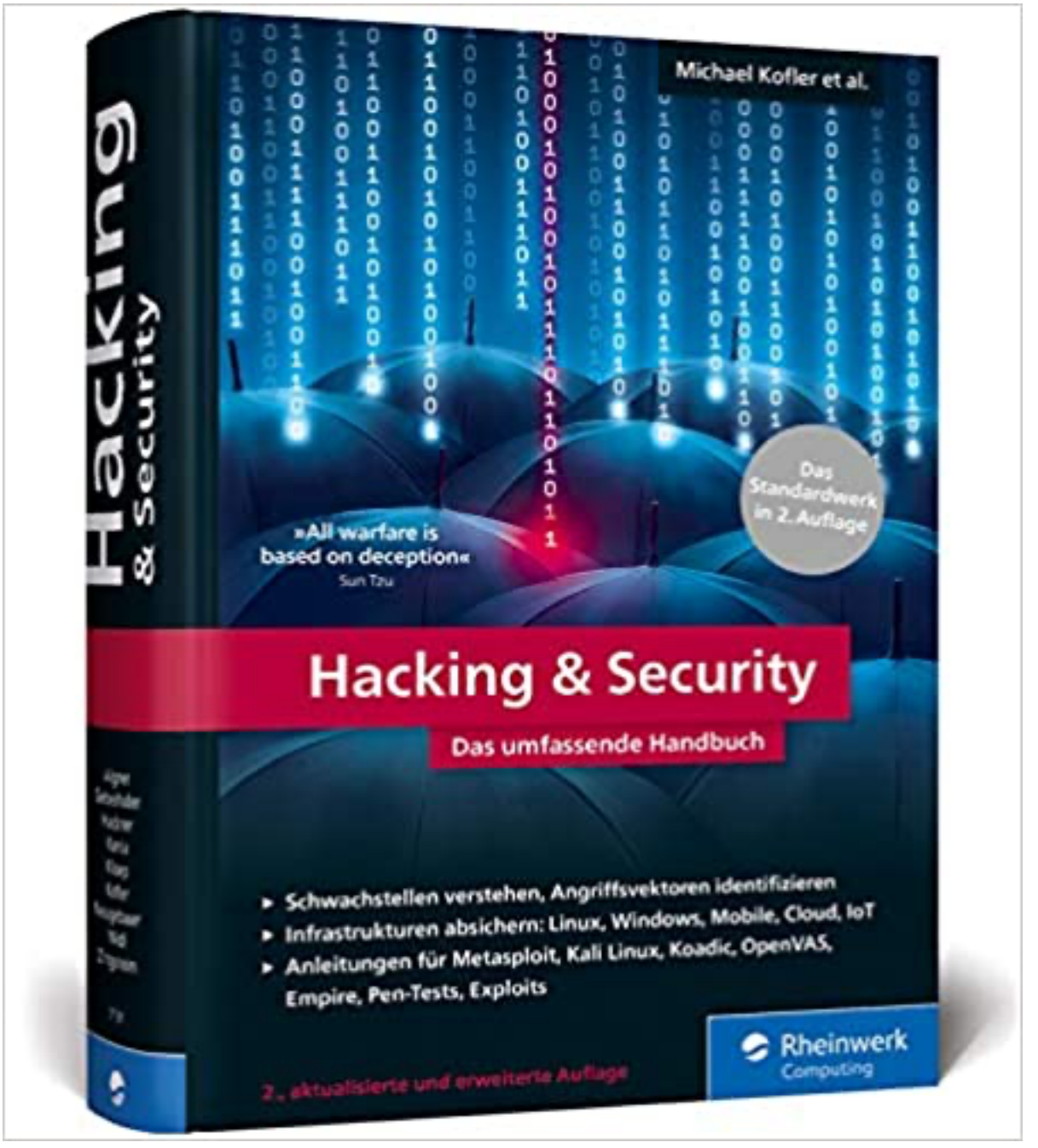
Ist es eine, könnte darin die Log4J-Bibliothek durchaus enthalten sein - manchmal sogar ohne Wissen des Herstellers oder der Programmierer, denn Log4J ist eine der Java-Bibliotheken, die gerne auch innerhalb von anderen Java-Bibliotheken eingesetzt wird. Und da kann es durchaus sein, dass eine Java-Bibliothek eine Bibliothek verwendet, die wiederum eine andere Bibliothek mit Log4J-Verwendung mitbringt.

Nicht jeder schaut sich im Packaging an, was alles genau mit eingepackt wird - genauso wenig, wie man sich beim Autokauf dafür interessiert, wer genau die Schrauben und Muttern produziert hat, die die Rad-Aufhängung zusammenhalten. Im Übrigen ist das auch ein Grund, wieso so viele Hersteller sich bisher nicht dazu geäußert haben, ob in ihren Produkten Log4J drin ist oder nicht: Sie wissen es im Moment noch nicht genau oder können es zumindest derzeit nicht völlig ausschließen.

Doch eine recht simple Admin-Webseite ist nicht das Einzige, was auf den Geräten mit der Möglichkeit zu

einem Remote-Zugriff läuft. Auf NAS-Geräten und Netzwerkfestplatten sind meistens Media-Server aktiviert, damit von Fernsehern oder anderen Geräten unkompliziert Videos oder Musik abgerufen werden kann.

Subsonic ist zum Beispiel so ein Medienserver, der in Java geschrieben ist; im Linux-Paket sind Log4J-Klassen enthalten, in welcher Version, ist noch nicht bekannt. Und Subsonic kann definitiv auf einer WD-ext4-Festplatte laufen.



Hacking & Security: Das umfassende Handbuch. 2. aktualisierte Auflage des IT-Standardwerks (Deutsch) Gebundene Ausgabe

Auf NAS-Lösungen von beispielsweise Synology oder QNAP lassen sich allerlei Apps installieren, inklusive Zugriff von irgendwo im Internet auf das System im Heimnetz, weil man ja nie weiß, wann man von unterwegs Zugriff auf die Dateien zu Hause braucht. Bei vielen dieser Geräte ist das Betriebssystem ein Linux, damit sind die darauf installierten Anwendungen lediglich durch die normalerweise ziemlich geringen Leistungsreserven der einzelnen Geräte begrenzt. Das gilt ebenso für viele Router.

Doch genau diese geringen Leistungen von in fertigen NAS-Servern integrierten Prozessoren führen dazu, dass eigene Systeme gebaut werden. Ein alter Computer oder einfach nur ein Raspberry Pi versieht inzwischen in so einigen Haushalten einen Dienst als Heimserver. Verwendet wird dann ein Linux oder ein professionelles System wie Unraid - inklusive der Möglichkeit zum Betrieb von Webservern mit allerlei Java-Applications mit Log4J darin oder gleich dem einen oder anderen Docker-Container mit einem solchen Dienst.

Jeder sollte das Heimnetz prüfen

Offenbar sind Menschen, die sich ein bisschen für Computer interessieren und mehr als nur ein iPad zu

Hause benutzen, für BSI-Präsident Schönbaum keine Verbraucher mehr, sondern Firmen und Behörden. Anders lässt sich seine Behauptung kaum erklären.

Deshalb gilt aus meiner Sicht: Auch wenn man sich nicht als Behörde oder Firma sieht, sollte man doch im Zuge der Log4J-Sicherheitslücke die Zeit investieren, das Heimnetz auf laufende Dienste zu überprüfen und abzuschalten, was eigentlich nicht benötigt wird, den Zugriff aus dem Internet zu deaktivieren, wo es möglich ist, und dann Updates für alles, was noch übrig ist, durchzuführen.

Im Übrigen gehört das BSI nicht immer zu den allerschnellsten, wenn es darum geht, auf Neuigkeiten zu reagieren. Es hat beispielsweise Jahre gebraucht, häufige Passwortänderungen aus seinen Empfehlungen zu nehmen, obwohl sich gezeigt hatte, dass häufige Änderungen zu schwachen Passwörtern führen. Da wundert es nicht, wenn es ein wenig dauert, auch an andere Geräte als Tablets und Handys zu denken.

Java könnte noch mehr Probleme machen

Und dann gibt es noch eine völlig andere Seite an der Sicherheitslücke selbst: Sowohl die JNDI-Mechanismen wie Lookup von Daten als auch die Möglichkeiten, Klassen von einem fremden Server herunterzuladen, sind keine Features von Log4J, sondern von Java selbst. In Log4J ist es nach acht Jahren nur aufgefallen, dass so etwas möglich ist, weil Softwareentwickler gerne

Nutzereingaben ins Logfile schreiben wollen, um sehen zu können, welche Eingaben vielleicht Probleme ergeben könnten. Und selbst hier hat es diese acht Jahre gedauert, bis jemand darauf aufmerksam wurde. Es ist durchaus denkbar, dass in anderen Programmen oder Bibliotheken ebenfalls Usereingaben so einfließen, dass ein JNDI-Lookup durchgeführt wird.

Und das kann wieder jede Menge Firmen und Behörden, aber auch Verbraucher treffen.

IMHO ist der Kommentar von Golem.de [IMHO = In My Humble Opinion (Meiner bescheidenen Meinung nach)]