Log4Shell – für die Finanzbranche weiterhin gefährlich

Von Sebastian Brabetz

Den richtig großen Schadenfall hat es im Zusammenhang mit der im vergangenen Jahr aufgedeckten Java-Sicherheitslücke „Log4Shell" bei Banken dank ihrer meist guten IT-Sicherheitsarchitektur nicht gegeben. Dennoch sollte sich auch die Finanzbranche nicht in Sicherheit wiegen, warnt Sebastian Brabetz – und sei es nur mit Blick auf den Kunden als Schwachstelle. So erlebt im Kontext mit Log4Shell der Banking-Trojaner Dridex eine Renaissance und sorgt für eine Phishing-Welle. Auch für Banken sind deshalb ein Schwachstellenmanagement und die Identifikation von Anwendungen mit Log4j im eigenen Netzwerk deshalb unerlässlich. Red.

Mitte Dezember des vergangenen Jahres rief das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Warnstufe „Rot" aus. Verantwortlich dafür war die Veröffentlichung einer neuen Sicherheitslücke, die als die gravierendste der letzten Jahre eingestuft wird. Bekannt ist sie unter der gängigen Bezeichnung „Log4Shell". Der Fehler befindet sich in der Open-Source-Java-Codebibliothek namens Log4j (Logging for Java), die weltweit viel genutzt wird. Die IT-Abteilungen von Banken und Unternehmen waren von Beginn an im Dauereinsatz, um das Problem zu verstehen und die nötigen Lösungsschritte umzusetzen.

Doch auch Laien haben schnell zu spüren bekommen, dass dieser Fall durchaus außerhalb der IT-Abteilungen ein Thema sein kann. Denn binnen kurzer Zeit mussten Amazon Web Services (AWS) sowie Apple Cloud an die Öffentlichkeit gehen. Zwei der größten und mitunter die am weitesten hochgerüsteten Cloud-Modelle der Welt meldeten, dass ihre Server betroffen waren.

Der schlafende Riese

Die Codebibliothek Log4j ist ein Framework, also ein Programmiergerüst zum Loggen von Anwendungsmeldungen in der weltweit meistgenutzten Programmiersprache Java. Somit handelt es sich hierbei um einen äußerst praktischen Baustein. Denn er bietet automatisiert und standardisiert eine hochwertige Protokollierung von Prozessen.

Im Laufe der Zeit hat sich Log4j darüber hinaus als globale Standardanwendung zum Loggen von Java Programmen etabliert. Anstatt selbst den Code für das Loggen zu schreiben, wird Log4j installiert. Laut Oracle wird Java weltweit von drei Milliarden Mobiltelefonen und 97 Prozent aller Unternehmensdesktops genutzt. In Rechenzentren und Spielekonsolen findet Java ebenfalls Verwendung.

Auch nachgelagerte Systeme gefährdet

Log4Shell ist tatsächlich einfach auszunutzen. Deshalb birgt es ein enormes Potenzial, weltweit immense Schäden anzurichten. Cyberkriminelle nutzen die Lücke aus, indem sie manipulierte Anfragen an verwundbare Server oder angreifbare Anwendungen senden. Anschließend sind sie in der Lage, einen beliebigen Code auszuführen. Auf diese Weise können IT-Systeme übernommen oder es kann beispielsweise Ransomware eingeschleust werden. Darüber hinaus handelt es sich hierbei um eine sogenannte „Second-Order-Attack". Das bedeutet: Nicht nur mit dem Internet verbundene, sondern ebenfalls nachgelagerte Systeme im Netzwerk können erreicht werden.

Das Softwareunternehmen Check Point verzeichnete nach weniger als einer

Sebastian Brabetz,
Leiter Professional Security Solutions,
mod IT Services GmbH,
Kassel

Woche bereits 1,8 Millionen Versuche, Log4Shell auszunutzen. Mehr als die Hälfte der Firmennetzwerke in Deutschland sollen attackiert worden sein. Darüber hinaus stellte Check Point fest, dass die Finanzbranche weltweit zu 53 Prozent betroffen war und somit in den oberen Rängen rangierte.

Nicht leicht zu beheben

Zwar ist die Sicherheitslücke einfach auszunutzen, jedoch gestaltet sich die Behebung des Problems umso komplizierter. Vielen Administratoren ist vor der Veröffentlichung gar nicht bewusst gewesen, dass sie Log4j verwenden. Die Software-Bibliothek ist in unzähligen Anwendungen vorhanden und befindet sich unter Umständen in einem von mehreren Unterordnern. Somit wird die Codebibliothek oftmals unbemerkt von Administratoren installiert.

Damit ist ein zentrales Problem identifiziert. Nach Bekanntwerden der Schwachstelle verbrachten die IT-Sicherheitsexperten viel Zeit damit, die betroffenen Anwendungen und Server in ihrem Netzwerk zu suchen. Im Gegensatz dazu konnten Cyberkriminelle schon vor der Veröffentlichung damit beginnen, die Sicherheitslücke auszunutzen. Doch auch danach war die Angriffsfläche immer noch recht groß, da sich nicht alle Unternehmen der enormen Gefahrenlage bewusst waren.

Schwachstelle Onlinebanking-Nutzer

Auch wenn die Angriffszahl auf Finanzhäuser im Branchenvergleich recht hoch war, blieb der große Schaden bislang aus. Besonders größere Banken zeichnen sich durch eine solide IT-Security aus. Da die Sicherheit der sensiblen Daten ihrer Kunden oberste Priorität genießt, wird dementsprechend viel Geld und Know-how in diesen Bereich investiert. Dies ist der Grund dafür, dass Log4j bislang nicht zu einem Leak bei einer großen Bank geführt hat. Jedoch kam es Ende Dezember vergangenen Jahres zu einem breit angelegten Cyberangriff auf die weniger gut vorbereitete vietnamesische Kryptowährungsplattform Onus. Über Log4Shell gelang es den Angreifern in den Sandbox-Server einzudringen, der die kritischen Daten der Organisation enthält. So konnten rund zwei Millionen Kundendatensätze gestohlen werden, darunter Informationen wie Benutzernamen, E-Mail-Adressen, Telefonnummern, Anschriften sowie verschlüsselte Passwörter. Die Kunden wurden vom Unternehmen dazu angehalten, ihre Kontodaten zu aktualisieren.

Im Zuge der Digitalisierung ist der Stellenwert des Onlinebankings stetig gestiegen. Damit verbunden ebenfalls die Bedeutung der Security. IT-Experten beobachten immer wieder das Auftreten von Trojanern, die Endgeräte von Benutzern befallen und falsche Überweisungen tätigen. So etwas kann zum Beispiel über hochkomplexe, auf Banken zugeschnittene Trojaner geschehen, die im Browser am Computer die Webseite live umschreiben. Für den Benutzer sieht alles normal aus, jedoch werden komplett andere Kontonummern und Beträge an die Bank übermittelt.

Da die IT-Security von Banken äußerst widerstandsfähig ist, konzentrieren sich Cyberkriminelle in dieser Branche in erster Linie auf die Benutzer. Emotet ist zum Beispiel ein Schadprogramm für Windows-Systeme, welches diese Ziele ins Auge fasst. Zuerst im Jahr 2014 entdeckt, spähte das Programm zunächst Kontozugangsdaten von deutschen und österreichischen Banken aus. Bankkunden bekamen E-Mails mit Anhängen zugeschickt. Klickten sie diese an, lud Emotet Schadsoftware aus dem Netz nach, um an die Kontozugangsdaten und im Nachgang an das Geld zu gelangen. Neben Bankkunden wurden auf diese Weise ebenfalls die Netzwerke von Behörden und Unternehmen ins Visier genommen.

Dridex-Banking-Trojaner nutzt Log4j

Die von der Schadsoftware geöffneten Türen ermöglichten die Verbreitung von Ransomware. Das englische Wort „Ransom" bedeutet auf Deutsch „Lösegeld". Ransomware ist die Bezeichnung für eine schädliche Software, die Daten auf einem Computer verschlüsselt. Diese sind für die Administratoren anschließend nicht mehr zugänglich. Für die Entschlüsselung werden letztlich hohe Lösegeldsummen gefordert.

Im Zusammenhang mit der Log4j-Schwachstelle ist ein altbekannter Trojaner erneut auffällig geworden. Im Laufe des Dezembers vergangenen Jahres konnte das Ausnutzen der Lücke durch den Banking-Trojaner „Dridex" beobachtet werden. Dieser machte schon im Jahr 2015 auf sich aufmerksam. Damals warnten die Volks- und Raiffeisenbanken vor einer stattfindenden Phishing-Welle durch den Trojaner. Phishing bezeichnet den Versuch von Cyberkriminellen, durch den Versand gefälschter E-Mails Menschen dazu zu verleiten, sensible Daten preiszugeben. Diesmal wurde Log4Shell genutzt, um Windows sowie Linux-Geräte mit Dridex Malware oder dem bekannten Meterpreter aus dem Metasploit-Baukasten zu infizieren. Gelingt dies, können Onlinebanking-Anmeldedaten gestohlen werden. Ransomware-Angriffe können ebenfalls die Folge sein.

Anwendungen mit Log4j identifizieren

In erster Linie gilt es, sich ein Bild davon zu machen, in welchen Anwendungen im eigenen Netzwerk Log4j vorhanden ist. Dieser Schritt ist unter Umständen langwierig und kostet großen Aufwand. Ist dies jedoch erledigt, können die identifizierten Lücken mit Patches oder Workarounds gestopft werden. Generell ist es notwendig, alle Anwendungen zu aktualisieren. Die durchgeführten Updates sollten den neuesten Versionen entsprechen. Ein Patch für die Sicherheitslücke steht dafür mit dem Update der aktuellen Log4j-Version 2.17.1 der Apache Software Foundation seit geraumer Zeit bereit.

Darüber hinaus ist es besonders für kleinere Banken und Finanzplattformen wichtig, sich hinsichtlich der IT-Security gut auszurüsten und keine Kosten zu scheuen. Bei Beobachtung der derzeitigen Lage wird deutlich, dass der Trend in Richtung einer steigenden Zahl jährlicher Cyberangriffe geht. Deshalb ist die Etablierung verschiedener Prozesse zur Verbesserung des Schutzes eigener Netzwerke von großer Bedeutung. Langfristig gesehen zahlt sich ein solches Investment mit Sicherheit aus.

Kontinuierliches Schwachstellenmanagement

Mithilfe des Schwachstellenmanagements können in erster Linie Sicherheits-

lücken erkannt, bewertet und behandelt werden. Sämtliche Anwendungen eines Netzwerkes werden automatisiert kontinuierlich geprüft. Gefundene Bedrohungen werden einem Risiko-Grad zugeordnet und eine entsprechende Problemlösung wird anschließend bereitgestellt. Herzstück des Schwachstellenmanagements ist der Schwachstellenscanner, der neben der kompletten Software eines Netzwerkes ebenfalls die Hardware überprüfen kann. Die Schwachstellenmanagement-Lösung schützt Unternehmen und Organisationen vor den sich ständig ändernden Bedrohungen und Herangehensweisen der Cyberkriminellen, mit denen es Schritt halten kann.

Log4Shell wird die IT-Welt und alle in dieser Branche tätigen Menschen noch in den nächsten Monaten oder sogar Jahren beschäftigen, so die Prognose. In den kommenden Wochen und Monaten könnte in den Medien weiterhin von Cyberangriffen die Rede sein. Besonders dann, wenn Cyberkriminelle bei der Ausnutzung der Sicherheitslücke Hintertüren eingebaut haben sollten und diese bislang unentdeckt geblieben sind. Betroffene Unternehmen und Behörden werden gleichermaßen in eine schwierige Situation hineingeraten, sollten sie nicht entsprechende Sicherheitsvorkehrungen getroffen haben. Die Bedeutung der Cybersicherheit wird letztendlich auch künftig beim Voranschreiten der Digitalisierung stetig wachsen. ■