audatis
Datenschutz und Informationssicherheit | CONSULTING

Whitepaper

Sicherheitslücken (Hafnium) im Microsoft Exchange-Server

Zusammenfassung

Anfang März 2021 verkündete Microsoft, dass Microsoft Exchange-Server bestimmter Versionen von Sicherheitslücken betroffen sind und diese von Angreifern ausgenutzt werden können. Dabei rief das BSI die höchste Alarmstufe aus und stufte die Sicherheitslücken als kritisch ein. Mehr als 10.000 Exchange-Server in Deutschland waren oder sind davon betroffen. Die Sicherheitslücken existierten bereits länger, sind nach bisherigen Erkenntnissen von Sicherheitsforschern wohl erst seit März in großem Umfang aktiv ausgenutzt worden. Einzelne Angriffe erfolgten bereits Anfang Januar 2021.

Problemstellung

Microsoft veröffentlichte am 3. März 2021 außerplanmäßige Sicherheitsupdates für seine Exchange-Server, welche vier Schwachstellen schließen sollen, mit denen es Angreifern möglich ist, Daten abzugreifen oder weitere Schadsoftware in den IT-Systemen der Angriffsopfer zu installieren. Es ist möglicherweise jede Organisation betroffen, die Exchange von Microsoft verwendet. Die Cloud-Produkte von Microsoft sind von dem Sicherheitsvorfall nicht betroffen.

Für folgende Versionen der Software stehen Sicherheitsupdates zur Verfügung:

- Microsoft Exchange Server 2010 (SP 3 RU)
- Microsoft Exchange Server 2013 (CU 23, CU 22, CU 21)
- Microsoft Exchange Server 2016 (CU 8 – CU 20)
- Microsoft Exchange Server 2019 (RTM, CU 1 – CU 9)

Auch einige Tage nachdem die Sicherheitslücken entdeckt wurden und Microsoft das Sicherheitsupdate in die Wege geleitet hatte, sind noch immer viele Server nicht geupdatet und daher gefährdet. Dies erlaubt Angreifern nach wie vor auf die Server und somit auf die Daten zuzugreifen. Ein großes Problem in der Praxis ist laut Aussage vieler IT-Administratoren, dass Updates am Microsoft Exchange-Server häufig mit Problemen und entsprechenden Ausfallzeiten behaftet sind, weshalb diese bei laufendenen Systemen nur ungern durchgeführt werden.

Lösungsansatz

Mit folgenden 7 Schritten sollten Organisationen, die einen eigenen Microsoft Server betreiben, zunächst prüfen, ob sie Opfer eines Angriffs durch Ausnutzung der Sicherheitslücken wurden, anschließend das System absichern und schlussendlich Vorkehrungen für zukünftige Sicherheitsvorfälle treffen.

1. Netzwerk Lockdown → Die Netzwerkkommunikation des Exchange-Servers unterbinden (diese nicht nur durch Firewalls einschränken, sondern „Netzwerkstecker ziehen“).
2. Analyse betreiben → Prüfen, ob Sie einem Angriff zum Opfer gefallen sind und dabei ein meldepflichtiger Datenschutzvorfall gem. Art. 32 DS-GVO entstanden ist. Hierzu stellt Microsoft ein Skript zur Überprüfung zur Verfügung.

   a. Laden Sie das Skript herunter unter https://github.com/microsoft/CSS-Exchange/tree/main/Security.
   b. Führen Sie das Skript aus und scannen Sie damit Ihr Netzwerk. Das Skript scannt ihr Netzwerk nach typischen Angriffsmerkmalen für ProxyLogon, eine Kombination von Schwachstellen CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 und CVE-2021-27065 miteinander. Das Skript scannt Exchange-Logs, Exchange-HttpProxy-Logs und Windows-Application-Event-Logs.
   c. Eine weiterführende forensische Analyse (z.B. der Logfiles) ist gerade bei positivem Befund notwendig und wird auch bei negativem Prüfergebnis empfohlen, da Angreifer teilweise ihre Spuren in den Systemen verwischen können. Eine absolute Sicherheit bietet dieses Vorgehen jedoch nicht.
3. Risikoanalyse und datenschutzrechtliche Bewertung → Planen des weiteren Vorgehens z.B. Melden eines Datenschutzvorfalls in Abstimmung mit dem Datenschutzbeauftragen.
4. Die betroffenen Microsoft Exchange-Server updaten (Bereitgestellte Updates von Microsoft installieren. Falls keine Updates installiert werden können, sollten unbedingt die Zugriffe auf den Exchange-Server über https/OWA deaktiviert werden).
5. Falls eine Kompromittierung festgestellt wird, müssen über Exchange hinaus manuell auch andere Systeme im Netzwerk überprüft werden, da sich beispielsweise eine mögliche Schadsoftware ausgebreitet hat. In diesem Fall ist es wichtig, sich mit dem Datenschutzbeauftragten oder einem Cybersecurity Experten in Verbindung zu setzen und das weitere Verfahren und Vorgehen zu planen.
6. Regelmäßige Updates etablieren → Einen Patch Managementprozess einführen, um zukünftig sicherzustellen, dass stets aktuelle Software eingesetzt wird und im Falle von kritischen Sicherheitsupdates a) diese bekannt sind und b) schnell umgesetzt werden können.
7. Thema IT-Sicherheit im Unternehmen forcieren und prüfen ob die eigenen Systeme sicher vor Angriffen von außen sind (Cyber-Security Assessments)

Wenn durch das oben genannte Skript keine Kompromittierung festgestellt wurde, kann allerdings eine Kompromittierung nicht ausgeschlossen werden. In diesem Fall muss der Vorfall dementsprechend weiter und tiefer untersucht werden, da der Angreifer vielleicht auf Daten zugegriffen hat, die vom Skript nicht automatisiert gefunden wurden.

Über diesen Vorfall hinaus, sollten Sie sich für die Zukunft absichern. Um zukünftig Sicherheitsvorfälle zu vermeiden oder notfalls bei Vorfällen schnell genug handeln zu können, sollten Sie bereits jetzt vorausplanen und Gegenmaßnahmen einleiten. Stehen Sie in jedem Fall in engem Kontakt mit ihren Informationssicherheits- und Datenschutzbeauftragten und besprechen Sie mit diesen den weiteren Verlauf.

Autor und Ansprechpartner

Marcel Albrink
Consultant Informationssicherheit

Schwerpunkte: IT-Schwachstellenanalyse, Sichere Softwareentwicklung

Mail: m.albrink@audatis.de
Fon: 05221 87292-06
XING **Linkedin**

Haben Sie noch Fragen?

Wir haben versucht alle wichtigen Aspekte in unserem Whitepaper möglichst verständlich aufzubereiten.

Sollten Sie dennoch Fragen oder Beratungsbedarf haben, nehmen Sie gerne mit uns Kontakt auf.

Die audatis Consulting GmbH ist als Beratungsunternehmen auf die Bereiche Datenschutz und Informationssicherheit spezialisiert und betreut Kunden im In- und Ausland bereits seit 2011.

Neben der Stellung des externen Datenschutzbeauftragten begleiten und beraten wir Unternehmen, öffentliche Stellen und kirchliche Einrichtungen bei der Umsetzung des Datenschutzes, der Informationssicherheit und der Digitalisierung.

Als Teil der audatis Group hat die audatis Consulting GmbH Ihren Sitz im ostwestfälischen Herford und betreibt eine Niederlassung in Potsdam.

audatis Datenschutz und Informationssicherheit CONSULTING

audatis Consulting GmbH
Luisenstr. 1
32052 Herford
Deutschland

Fon: 05221 872 92-0
Fax: 05221 872 92-49

Mail: info@audatis.de
Web: www.audatis.de