1 Dringender Handlungsbedarf: Sicherheitslücken Exchange Server

Sehr geehrte Mandantin,
sehr geehrter Mandant,

in diesem Schreiben möchten wir Sie auf die aktuellen Sicherheitslücken beim Betrieb des Microsoft Exchange-Servers hinweisen. Aufgrund der akut hohen Bedrohungslage informieren wir Sie deshalb außerhalb unseres regulären Newsletters, da an dieser Stelle schnelles Handeln erforderlich ist.

Warnmeldung von Microsoft

Sicherheitslücken Exchange Server

In der Mitteilung des Bundesamts für Sicherheit (BSI) vom 08. März 2021 wird darauf hingewiesen, dass mehrere Schwachstellen des Microsoft Exchange Servers identifiziert wurden.

Nach den uns vorliegenden Informationen wurden die Schwachstellen in Kombination bereits für zielgerichtete Angriffe verwendet. Ziel der Angreifer ist es mit Hilfe der Schwachstellen weiterführende Schadsoftware im Unternehmensnetzwerk zu verbreiten oder Daten direkt abzugreifen.

Durch die bisher nicht bekannten Schwachstellen bei dem Microsoft Produkt können sich Kriminelle oder staatliche Hacker von außen Zugriff auf die E-Mails des Unternehmens verschaffen und von dort aus möglicherweise in weitere Hardwarekomponenten eindringen.

Über weitere Schwachstellen können beliebige Daten auf die Server geschrieben werden, was im schlimmsten Fall bedeuten könnte, dass von dort aus weitere Systeme angegriffen werden könnten.

Die Warnung wurde vom BSI mit der **Warnstufe vier** versehen, welche für **„extrem kritisch“** steht. Hintergrund ist nicht allein die Schwere der Sicherheitslücke, sondern die hohe Anzahl der potenziellen Opfer.

Zudem ist bereits bekannt, dass Angreifer die Lücke bereits mehrfach ausgenutzt haben. Laut BSI existieren zum jetzigen Zeitpunkt auch schon Hinweise darauf, dass neben Unternehmen auch einige Bundesbehörden betroffen sind. Eine genaue Zahl liegt zurzeit noch nicht vor.

Die Angreifer selbst stammen laut Microsoft hauptsächlich von einer chinesischen Hackergruppe, die von Sicherheitsforschern Hafnium genannt wird. Hauptangriffsziel der Gruppe sind unteranderem Forschungseinrichtungen, Hochschulen, Verteidigungsunternehmen und Nichtregierungsorganisationen. Es lässt sich jedoch nicht ausschließen, dass auch andere Unternehmen betroffen sind.

Die Sicherheitslücken selbst betreffen laut Microsoft nicht das Produkt Microsoft Exchange Online, sondern **nur lokal gehostete Exchange Server**. Aufgrund der Schwere der Sicherheitslücken hat das BSI selbst bereits 9.000 Unternehmen kontaktiert, um auf die Sicherheitslücken hinzuweisen.

Microsoft selbst hat bereits am 3. März 2021 ein Update bereitgestellt, welches die Sicherheitslücken des Exchange Servers schließt. Das Update schließt folgende Schwachstellen:

CVE-2021-26855 ist eine Schwachstelle, die es dem Angreifer erlaubt HTTP-Requests zu senden und sich am Exchange Server zu authentisieren.

CVE-2021-26857 ermöglicht es beliebigen Programmcode als System auf dem Exchange Server auszuführen.

CVE-2021-26858 und **CVE-2021-27065** die es ermöglichen beliebige Dateien auf den Exchange Server zu schreiben.

Durch das von Microsoft bereitgestellte Update werden alle vier genannten Schwachstellen geschlossen. Das Update steht für folgende Versionen zur Verfügung:

- Exchange Server 2010 (SP 3 RU)
- Exchange Server 2013 (CU 23)
- Exchange Server 2016 (CU 19, CU 18)
- Exchange Server 2019 (CU 8, CU 7)

Dringender Handlungsbedarf

Um die Sicherheitslücken umgehend zu beseitigen empfiehlt das Bundesamt für Sicherheit unter anderem folgende Maßnahmen:

- Prüfung ob bereits ein Angriff auf das eigene Netzwerk stattgefunden hat. Dies kann beispielsweise über Skripte und Protokolldateien nachvollzogen werden.
- Bereitgestellte Updates von Microsoft umgehend installieren.
- Sofern eine Aktualisierung nicht sofort möglich ist, muss ein nicht ausschließlich mittels VPN aus dem Internet erreichbarer Outlook Web Access (OWA) Zugang sofort deaktiviert werden.
- Weitere Maßnahmen finden sich im Abschnitt „Maßnahmen“ der BSI Mitteilung.

Weiterführende Links

Update Microsoft Security Response Center:

https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

Meldung Bundesamt für Sicherheit:

https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-197772-1132.pdf;jsessionid=229CC6FFA7DA792E3F218E7AB4B406D3.internet471?__blob=publicationFile&v=5

Dringender Handlungsbedarf - Sicherheitslücken Exchange Server

Kontakt

Sollten Sie Fragen haben, können Sie sich jederzeit an uns wenden. Wir helfen Ihnen gerne weiter. Unsere Kontaktdaten finden Sie auf der abschließenden Seite.

Kontakt

RFS IT GmbH
Depotstraße 5 1/2
86199 Augsburg

Telefon: 0821 40879393
E-Mail: info@rfs-it.de

Widersprechen

Wir möchten Sie ausdrücklich darauf hinweisen, dass Sie der Verwendung Ihrer E-Mail-Adresse jederzeit widersprechen können. Weiterführende Hinweise zum Datenschutz finden Sie auf unserer Homepage www.rfs-it.de

RFS IT GmbH
Depotstraße 5 1/2
86199 Augsburg

Telefon: +49 821 40879393
E-Mail: info@rfs-it.de
Internet: www.rfs-it.de

Sitz: 45133 Essen, Am Alfredusbad 8
Registergericht Essen, Reg-Nr. HRB 28543
USt-IdNr. DE 314393389

Geschäftsführung:
Andreas Schneider