Microsoft Exchange Lücken schnell schliessen!

Gerne möchten wir Sie auf eine wichtige Bedrohungslage hinweisen, die Schwachstellen in Microsoft Exchange Server betrifft. Diese werden aktuell auch von den Medien und Sicherheitsbehörden intensiv thematisiert:

- Kritische Lücken in Microsoft E-Mail-Plattform „Exchange Server“
- Zehntausende Unternehmen und Behörden betroffen
- BSI: Durch Microsoft bereitgestellte Sicherheitsupdates möglichst sofort installieren

Wegen einer Sicherheitslücke in Microsoft Exchange Server (Outlook, Mails, Kalender, Handy in Zusammenhang mit Synchronisation von Mails, etc.) sind laut US-Medienberichten Zehntausende E-Mail-Server von Unternehmen, Behörden und Bildungseinrichtungen Opfer von Hacker-Attacken geworden. Vier der kürzlich bekannt gewordenen Microsoft-Sicherheitslücken sind von Hackern ausgenutzt worden. Weltweit könne es mehr als 250`000 Opfer geben, so das «Wall Street Journal». Es sind rund 170`000 Serverumgebungen betroffen. Die Schweiz ist dabei besonders stark betroffen. Der Hersteller Microsoft stuft speziell das Problem im Bereich Exchange äusserst kritisch ein, namentlich Stufe 9.1 von 10. Die meisten Exchange-Server, welche zum Beispiel den Dienst OWA anbieten und direkt im Internet erreichbar sind (zum Beispiel, aber nicht nur, bei Synchronisation von Ihren Mails auf dem Handy), sind davon betroffen

Was ist genau passiert?

Erste Hinweise auf diese Schwachstellen hatte bereits am 28. Februar das IT-Sicherheitsunternehmen Volexity aus dem US-Bundesstaat Virginia gegeben. Analysten hatten mehrere Angriffe gefunden, die über sogenannte Web-Shells, also Eingabe-Werkzeuge für Systembefehle, ausgeführt worden waren. Schon Ende Februar begannen die Angreifer offenbar damit, automatisiert Hintertüren in verwundbare Exchange Server von Microsoft einzubauen. Tausende Server pro Stunde wurden so attackiert. Für die Schwachstellen gibt es seit 4. März ein Sicherheitsupdate. Bis Updates von allen betroffenen Firmen installiert sind, dauert es jedoch erfahrungsgemäss eine ganze Weile.

Wer steckt dahinter?

Einem Bericht von Microsoft zufolge steckt die staatlich gesponserte chinesische Hacker-Gruppe HAFNIUM hinter den Attacken. Die Hacker sollen es vor allem auf US-Firmen beispielsweise aus dem Industriesektor, Bildungseinrichtungen und NGOs abgesehen haben. Nach erfolgreichen Attacken sollen sie sich laut Microsoft oft dauerhaft in Systemen festsetzen und Daten kopieren.

Wie sollte man reagieren?

Führen Sie die aktuellen Sicherheitsupdates aus!
Für die folgenden verwundbaren Exchange-Server-Versionen haben die Entwickler abgesicherte Ausgaben veröffentlicht:

- Exchange Server 2010 (RU 31 for Service Pack 3)
- Exchange Server 2013 (CU 23)
- Exchange Server 2016 (CU 19, CU 18)
- Exchange Server 2019 (CU 8, CU 7)

Damit Admins ihre installierten Exchange-Server-Versionen zügig prüfen können, stellt Microsoft ein Skript zum Download bereit. Mit den Sicherheitsupdates schliessen die Entwickler noch drei weitere Schwachstellen (CVE-2021-26412, CVE-2021-26858, CVE-2021-27078), auf die es derzeit aber keine Angreifer abgesehen haben sollen. Microsoft zufolge ist Exchange Online nicht von den Lücken betroffen.

Wir empfehlen dringend, die Software auf dem neuesten Stand zu halten. Darüber hinaus wird empfohlen, Prüfungen auf die verfügbaren „Indicators of Compromise“ (IoC) durchzuführen, die sich auf die mit diesem Vorfall verbundenen Sicherheitslücken beziehen. Die Liste ist hier verfügbar:

- Microsoft: HAFNIUM targeting Exchange Servers with 0-day exploits [Englisch, 02.03.2021]
- Microsoft/GitHub: The Exchange Server Health Checker – Prüftoolscript für Administratoren, um den Exchange Server auf „Indicators of Compromise“ (IoC) hin zu untersuchen, die ein erfolgreicher Angriff hinterlässt [Englisch, Update 10.03.2021]

Setzen Sie alle Nutzer-Passwörter zurück!
Sollten die „Indicators of Compromise“ (IoC) auf eine Ausnutzung der Schwachstellen hinweisen.

Sensibilisieren Sie Ihre Mitarbeitenden fortlaufend auf das Thema. Je mehr die Thematik sensibilisiert wird in Ihrem Unternehmen, je stärker steigt die Sicherheit markant an. Selbst Kurzgespräche in den Pausen können helfen.

Prüfen Sie die von Microsoft bereitgestellten Skripte und nutzen Sie weitere Analysetools, um zu sehen, ob Ihr Unternehmen kompromittiert wurde. Unternehmen, die ihre Exchange Server nicht extra abgesichert haben, können aber im Prinzip davon ausgehen, betroffen zu sein.

Prüfen Sie, ob datenschutzrechtliche Meldeverpflichtungen bestehen!
So gehen Sie sicher, die geltenden Fristen nicht zu verpassen.

Quellen: Newsletter 03/21 HDI Global SE und Neo One Breaking News Commercial vom 11.3. und 16.3.2021