Achtung!
Sicherheitslücken bei Microsoft Exchange Servern

Das Bundesamts für Sicherheit in der Informationstechnik (BSI) und Microsoft informierten Anfang März 2021, dass vier Sicherheitslücken (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065) in verschiedenen Versionen von Microsoft Exchange Servern gefunden wurden.
Das BSI stuft 3 dieser Sicherheitslücken als kritisch ein – Microsoft hat bereits „außer der Reihe" Sicherheitspatches veröffentlicht.

Was kann passieren?

Wenn selbst betriebene Exchange Server der Versionen 2010, 2013, 2016 und 2019 auf dem Port 443 mit nicht vertrauenswürdigen Verbindungen erreichbar sind, kann über diese Sicherheitslücke eine Schadsoftware (z.B. eine Webshell) installiert und somit Zugriff zum Unternehmensnetzwerk erlangt werden. Es können dann E-Mail-Postfächer, Adressbücher und Termine ausgelesen und manipuliert werden.

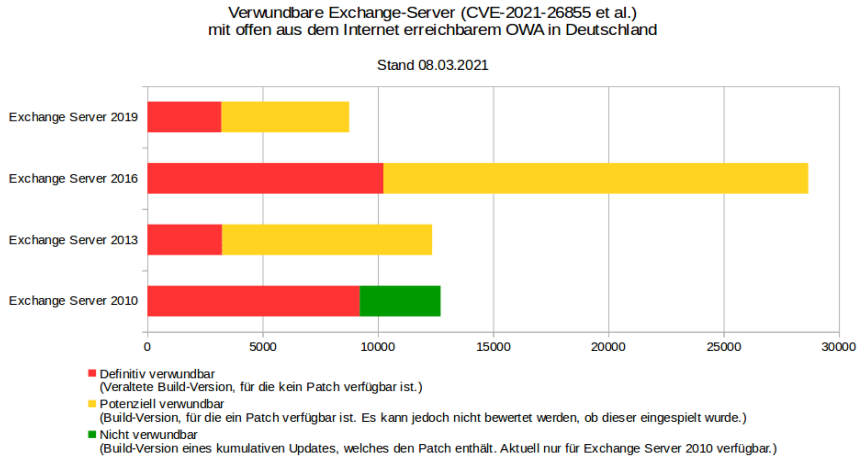
Dies soll nicht für Exchange Server gelten, die nur per VPN erreichbar sind und nicht-vertrauenswürdige Verbindungen blockieren.

Welche Server Versionen sind betroffen?

Betroffen sind folgende Server Versionen:

- Exchange Server 2010 (RU 31 – kann auch RU32 sein - for Service Pack 3)
- Exchange Server 2013 (CU 23)
- Exchange Server 2016 (CU 19, CU 18)
- Exchange Server 2019 (CU 8, CU 7)

Die Exchange Online Version soll hiervon nicht betroffen sein.



Was ist jetzt zu tun?

- Version und Patch Level des Microsoft Exchange Servers prüfen
- Alle Update-Lücken bis zur aktuellsten Version schließen
- Logfiles des Exchange Servers auf die „Indicators of Compromise" prüfen.
- Es können folgende von Microsoft bereitgestellte Links helfen:
  a) Hafnium-targeting-exchange-servers
  b) Exchange-healthchecker
  c) Older cumulative updates (falls kumulative updates nicht eingespielt werden können)
- BSI-Link zu weiteren Maßnahmen
- Prüfen, wie weit Angreifer ins Netz vordringen konnten (Active Directory des Exchange Servers überprüfen)

Nur ausnahmsweise stellt Microsoft jetzt auch Sicherheits-Updates bereit, die sich direkt installieren lassen.
(Bild: Microsoft)

Welche Folgen hat dies in Bezug auf die DSGVO?

Da sich das Schließen der Lücken nicht auf bereits vergangene Kompromittierungen auswirkt (das Kind ist bereits in den Brunnen gefallen), muss im Einzelfall geprüft werden, ob es zu einer Verletzung der Sicherheit personenbezogener Daten gekommen ist und eine Meldung (gem. Art 33 DSGVO) an die zuständige Aufsichtsbehörde zu erfolgen hat.

Auch eine Information der betroffenen Personen ist in Abhängigkeit von den Datenarten und der jeweiligen Sicherheitsverletzung im Einzelfall zu prüfen (Art 34 DSGVO).

Bitte sprechen Sie mich hierauf an!

Die komplette Untersuchung des Exchange-Servers muss auf jeden Fall umfassend dokumentiert werden.