Diese Sendung wird aufgezeichnet!

GWS

Webtalk: Exchange kritische Hafnium Lücke

Patrick Bärenfänger, Marco Klenner im März 2021

Ausgangslage

Kritische Sicherheitslücken in Exchange Servern on-Premises

- Am 03. März 2021 veröffentlichte Microsoft Notfall Patches für eine an dem Tag (0-day) bekannt gewordene Sicherheitslücke
- Chinesische Hacker der Hackergruppe Hafnium (daher der Name der Lücke) hatten Exchange-Server bereits über das Webinterface angegriffen
- Am 04. März informierten wir zusätzlich im Syskoportal und über einen Sonder-Newsletter
- Einige Kunden führten Patches selbst aus oder mit unserer Unterstützung

- 09. März 2021: Die Datenschutzbehörden schalten sich ein. Wer seinen Exchange-Server bis zu diesem Tag nicht gesichert hat UND dokumentiert, dass keine Angriffe erfolgt sind, muss Meldung machen.

- 16. März 2021: Microsoft stellt ein erweitertes Dokumentations-Werkzeug (Powershell) auf GitHub, das mehr Protokolle analysiert, als das Ursprungswerkzeug von Anfang März

- Alle Kunden mit Exchange On-Premises sollten das Werkzeug auch im Nachgang zur Dokumentation ausführen bzw. jemand damit beauftragen, dies zu tun

Gefahren

Nachwirkungen

- Das Installieren der Patches ist dann nicht trivial, wenn der Exchange-Server nicht schon einen aktuellen Patch-Stand von Februar 2021 hatte. Es müssen zahlreiche Updates nachinstalliert werden, bevor der Notfallpatch angewendet werden kann
- Auch wenn zeitnah gepatcht wurde, können sich die Hacker eine „Hintertür“ installiert haben.
- Die Hintertür kann auf dem Exchange-Server oder auf anderen Servern oder Geräten in Ihrem Netzwerk sein
- Forensische IT-Analysen können nur Spezialfirmen durchführen: (z. B. über **@-yet GmbH, Köln**)

Erforderliche Maßnahmen

- Wenn sie noch nichts unternommen haben:

- 1) Exchange Server sofort vom Internet und Netzwerk trennen
- 2) Letzte Sicherung des Exchange Servers VOR DEM 03. März 2021 aussondern und zu Dokumentationszwecken aufbewahren
- 3) Neues Microsoft Powershell-Script nach Anleitung im Web-Artikel ausführen (FULLSCAN), Ergebnis dokumentieren und ggf. Schritte 3 und 4 ausführen
- 3a) Server auf den aktuellen Stand bringen und die notwendigen Patches installieren
- 3b) alle Passwörter von Postfach-Inhabern und administrativen Domänen-Konten ändern
- 4) das testproxylogon.ps1 auszuführen (da werden die URLS / Verzeichnisse genau aufgeführt, die Änderungen haben).
- 5) erneut das Microsoft Powershell-Skript laufen lassen und Ergebnis dokumentieren und auswerten
- 6) Sicherstellen, das Sie ihr Updatekonzept optimieren

- Schritt 2ff. zu Dokumentationszwecken ausführen (FULLSCAN)
- Wenn Sie bis 09. März nichts unternommen haben und das Skript Angriffe feststellt, ist eine Meldung (Selbstanzeige) bei den Datenschutzbehörden erforderlich. Bitte stimmen Sie diese Schritte mit Ihrem Anwalt/Datenschutzbeauftragten ab.

Quellen-Nachweise

Microsoft, GWS Blog und Syskoportal

- Systemkoordinatoren-Portal: https://tech-nachrichten.de
- GWS Blog: https://erpsystem.de/category/produkt-news/
- Microsoft Dokumentations- und Prüf-Tool: https://github.com/microsoft/CSS-Exchange/tree/main/Security
- Lücken-Patches:
  - 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)
- Technische Unterstützung über einen kostenpflichtigen Vorgang in unserem Extranet

Fragen

Zeit für Ihre Fragen

Stellen Sie uns nun gern Ihre Fragen