Information Sicherheitslücken an Microsoft Exchange Servern

Sehr geehrte Damen und Herren,

am 02.03.2021 veröffentlichte Microsoft Informationen zu schwerwiegenden Sicherheitslücken an Exchange Servern (Mailserver):

- CVE-2021-26855:
  Ermöglichung des Zugriffs auf Zugangsdaten (z. B. für spätere Angriffe) ohne Anmeldung
- CVE-2021-26857:
  Ermöglichung des Ausführens von Code im Systemkontext
- CVE-2021-26858 / CVE-2021-27065:
  Ermöglichung des unerlaubten Schreibens von Daten

Diese hier festgestellten Sicherheitslücken wurden bereits im Dezember 2020 erstmalig entdeckt. Wie weit sie dabei in diesem Zeitraum genutzt wurden, ist nicht bekannt. Es ist davon auszugehen, dass dieses Angriffsszenario innerhalb dieses Zeitraums gegen ausgewählte Ziele eingesetzt wurde, um zunächst unentdeckt zu bleiben.

Aus diesen Sicherheitslücken hätten u. a. folgende Schadensszenarien entstehen können:

- Zugriff für Unbefugte auf Inhalte sämtlicher Mailboxen (Mail, Kalender, Kontakte, Notizen, etc.) mit hieraus resultierendem Datenverlustrisiko
- Möglichkeit, dass ein Unbefugter Daten ins Dateisystem des Exchange-Servers schreiben konnte und damit langfristig Schadcode ins System einschleust
- Möglichkeit, dass ein Unbefugter Befehle als System- oder Exchange Trusted Subsystem ausführt

In der Nacht zum 03.03.2021 hat Microsoft Updates für Exchange Server veröffentlicht mit denen die genannten Sicherheitslücken sofort geschlossen wurden. In der Folge wurde die Exchange Umgebung des St. Josefshaus nochmals umgehend mit den durch Microsoft bereitgestellten Testmöglichkeiten geprüft und die Installation weiterer Sicherheitsupdates eingeleitet.

Die Sicherheitslücken wurden durch die Installation geschlossen. Checks der bekannten Angriffsüberreste blieben bisher negativ, so dass es bis dato keine Hinweise auf weitere Beschädigungen oder noch vorhandene Einfallstore gibt.

Auch wenn dahingehend keine Anzeichen nachgewiesen werden konnten, kann dies nicht vollständig ausgeschlossen werden. Aufgrund dessen ist nach § 33 KDG die Meldung an die zuständige Datenaufsicht erfolgt. Des Weiteren sind wir verpflichtet, Sie als Betroffene hierüber zu informieren, was wir hiermit tun. Wir bitten evtl. damit verbundene Umstände zu entschuldigen.

Mit freundlichen Grüßen,

Vorstand St. Josefshaus Herten Betriebs-gGmbH