Katholisches Datenschutzzentrum

Brackeler Hellweg 144
44309 Dortmund
www.katholisches-datenschutzzentrum.de

Kath. Datenschutzzentrum | Brackeler Hellweg 144 | 44309 Dortmund

Empfänger

Tel.: 0231/138 985-0
Fax: 0231/138 985-22

Aktenzeichen:

Dortmund, 26. April 2021

Prüfung zum Umgang mit der Sicherheitslücke Microsoft Exchange Server SSRF Vulnerability (CVE-2021-26855, „Hafnium“)
Aufforderung zur Stellungnahme gem. § 5 Abs. 1 KDS-VwVfG

Sehr geehrte Damen und Herren,

nach der Veröffentlichung der o.g. Sicherheitslücke sind beim Katholischen Datenschutzzentrum im Zeitraum März und April 2021 Meldungen von Datenschutzverletzungen und Anfragen zum Umgang mit der Sicherheitslücke eingegangen.

Wir gehen davon aus, dass nicht alle Verantwortlichen, deren Exchange Server von der Sicherheitslücke betroffen war, eine Meldung abgegeben haben, zumal die bloße zeitweise Existenz einer Sicherheitslücke für sich genommen nicht unbedingt eine meldepflichtige Datenschutzverletzung nach § 33 KDG darstellt.

Wir haben den Vorfall zum Anlass genommen, uns den Umgang mit der Sicherheitslücke in einer Prüfung der uns bekannten Fälle sowie stichprobenhaft in weiteren Einrichtungen anzuschauen.

Ihre Einrichtung wurde als Teil der Stichprobe ausgewählt.

Nach den uns vorliegenden Informationen sind aus unserer Sicht für eine adäquate Behandlung der Sicherheitslücke mindestens drei Schritte erforderlich:

1. Schließen der Sicherheitslücke durch Installieren der verfügbaren Sicherheits-Patches, die für die Versionen MS ExchangeServer 2013, 2016 und 2019 verfügbar sind. Dazu hat der Hersteller Microsoft entsprechende Hinweise und Tools bereitgestellt: Microsoft Security Information "HAFNIUM targeting Exchange Servers with 0-day exploits"[1]

[1] https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

2. Überprüfen, ob in der Zeit bis zur Behebung der Sicherheitslücke durch Schritt 1 die Sicherheitslücke durch Angreifer genutzt wurde, indem Schadsoftware eingebracht wurde. Hierzu stellt der Hersteller Detektionswerkzeuge zur Verfügung: Microsoft Detektionsskript[2] und Microsoft Safety Scanners (MSERT)[3]
3. Kontinuierliches Überwachen der ein- und ausgehenden Datenströme, besonders zu ungewöhnlichen Zeiten. Hintergrund: Oft wird eine Schadsoftware erst nach einer längeren Wartezeit aktiv.

Bei einer festgestellten Infektion oder einer unklaren Situation zur Infektion sollte im Zweifelsfall überlegt werden, den Exchange Server neu aufzusetzen. Bei der Nutzung von Backups sollte geprüft werden, ob das Backup auch von der Infektion betroffen ist oder betroffen sein könnte. Die Wiederherstellung aus einem Backup ist dann vor Produktivstart mit den neuesten Sicherheitsupdates zu aktualisieren.

Ausführliche Beschreibungen der notwendigen Aktivitäten finden Sie z.B. auf der Seite des Bundesamtes für Sicherheit in der Informationstechnik BSI "Detektion und Reaktion bei Microsoft Exchange Schwachstellen"[4].

Als erste Phase der Prüfung haben wir uns „von außen“ (nicht invasiv) durch gezieltes Ansprechen von Protokollen und IP-Ports angeschaut, ob die Sicherheitslücke auf einem Exchange Server (noch) besteht. Dazu wird mit Hilfe des frei verfügbaren Tools „nmap“ („network mapping“) ein vom Hersteller zur Verfügung gestelltes Script (Microsoft Detektionsskript[5]) mit der Zieladresse des zu prüfenden Servers ausgeführt. Im Ergebnis wird festgestellt, ob die kritischen Zugriffe über den Port 443 (noch) möglich sind. Zusätzlich können eventuell über das Telnet-Protokoll Erkenntnisse gewonnen werden.

Im Rahmen unserer Prüfung haben wir die öffentlich verfügbaren Informationen zu Ihrem Mailserver ausgewertet:

Ihre Mail-Domäne:	domänenname.de
Ihr E-Mail-Server:	domänenname-de01i.mail.protection.outlook.com
IP-Adresse Ihres E-Mail-Servers:	999.99.9.99
Provider-Information:	Microsoft Corporation (AS8075)
Ergebnis des nmap-Scriptes:	i.O.
Gesperrte TCP-Ports	none
Freigegebene TCP-Ports	25
Ergebnis des telnet-Zugriffs:	MS365
Datum der Auswertung:	4/22/2021

[2] https://github.com/microsoft/CSS-Exchange/tree/main/Security
[3] https://docs.microsoft.com/de-de/windows/security/threat-protection/intelligence/safety-scanner-download
[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Vorfaelle/Exchange-Schwachstellen-2021/MSExchange_Schwachstelle_Detektion_Reaktion.pdf
[5] https://github.com/microsoft/CSS-Exchange/tree/main/Security

Dieses Ergebnis zeigt, dass die Sicherheitslücke in Ihrem System zum Zeitpunkt der Auswertung nicht besteht, bzw. bereits geschlossen wurde (Schritt 1 der obigen Aufzählung).

Als zweite Phase der Prüfung bitten wir Sie zur Verifizierung der oben genannten Schritte 2 (Scannen des Servers auf eingebrachte Schadsoftware) und 3 (Monitoring der Datenströme) um Ihre Stellungnahme:

- Welche Maßnahmen haben Sie zu welchem Zeitpunkt ergriffen, um nach dem Schließen der Sicherheitslücke den Befall Ihres MS Exchange Servers mit Schadsoftware zu erkennen und diese zu beseitigen? Bitte erstellen Sie eine chronologische Abfolge der Aktivitäten, einschließlich des Einspielens der Sicherheitspatche.
- Welche Maßnahmen haben Sie ergriffen bzw. planen Sie, um über einen längeren Zeitraum ungewöhnliche ein- und ausgehende Datenströme zu erkennen?

Da uns in Ihrem Fall keine Meldung vorliegt, ist uns das von Ihnen oder Ihrem Mail-Provider installierte E-Mail-Server-System nicht zweifelsfrei bekannt. Sollten Sie **keine** Version von MS ExchangeServer (lokal oder gehostet) nutzen, bitten wir um entsprechende Nachricht. Ansonsten beantworten Sie bitte unsere Fragen.

In Ihrem Fall können wir anhand des ersten Prüfschritts erkennen, dass Sie Ihre Postfächer über Microsoft 365 betreiben und damit keine Notwendigkeit bestand, die Sicherheitslücke durch eigenes Handeln zu schließen. Wir bitten um Bestätigung.

Die der Aufsicht des Katholischen Datenschutzzentrums unterliegenden Einrichtungen sind verpflichtet, der Aufsicht auf Nachfrage gemäß § 44 Abs. 2 lit. b) KDG Auskunft zu erteilen. Die innerhalb der Stelle handelnden Personen können allerdings die Auskunft auf solche Fragen verweigern, deren Beantwortung sie selbst oder einen der in § 383 Abs. 1 Nr. 1-3 Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Dabei sind die Tatsachen, auf welche die Auskunftsverweigerung gründet, darzulegen und glaubhaft zu machen.

Wir bitten um Übersendung Ihrer Stellungnahmen bis zum 31. Mai 2021.

Um unserer gesetzlichen Verpflichtung nach §§ 15, 16 KDG nachzukommen, informieren wir Sie, dass wir Ihre personenbezogenen Daten im erforderlichen Umfang verarbeiten.
Weitere Informationen finden Sie unter: https://www.katholisches-datenschutzzentrum.de/informationspflichten/.

Mit freundlichen Grüßen
Im Auftrag