Schon wieder: Kritische Schwachstelle in Exchange-Servern

Dortmund, 15.04.2021 (Ergänzung des Artikels vom 10.03.2021): Nach Bekanntwerden einer schweren Sicherheitslücke in Microsoft Exchange-Servern hat das BSI eine umfangreiche Handlungsempfehlung für Unternehmen und Einrichtungen jeder Größe herausgegeben. Das Katholische Datenschutzzentrum empfiehlt allen Einrichtungen, die einen Exchange-Server selbst oder bei einem Dienstleister gehostet betreiben, sich über die empfohlen Abwehr- und Abhilfemaßnahmen zu informieren und die notwendigen Maßnahmen einzuleiten. Dazu gehört neben der sofortigen Schließung der Sicherheitslücke durch die vom Hersteller bereitgestellten Patches, eine sorgfältige Analyse, ob die Lücke bereits durch Installation von schädlichem Code (Webshells, Skripte etc.) ausgenutzt wurde. Sollten Zweifel bleiben, ob das System kompromittiert wurde, ist notfalls – nach Überprüfung und Sicherung der Postfach-Inhalte – der Server komplett neu aufzusetzen.

Im Fall von gehosteten Exchange-Servern sollte zunächst der Dienstleister kontaktiert werden.

Link zur Informationsseite des BSI

Neben dieser durch das BSI empfohlenen Analyse- und Maßnahmenkette, steht die datenschutzrechtliche Bewertung des Vorfalls. Hierzu vertritt das Katholische Datenschutzzentrum die folgende Ansicht:

1. Alleine die Tastsache, dass ein MS Exchange-Server betrieben wird, der eine Zeit lang die beschriebene Sicherheitslücke hatte, führt NICHT zu einer Meldepflicht nach § 33 KDG, wenn diese Sicherheitslücke schnellstmöglich geschlossen wurde und es keinen Hinweis gibt, dass das System kompromittiert wurde, .
2. Wird eine Kompromittierung festgestellt, aber gleichzeitig nachgewiesen (z.B. durch Auswertung von Protokoll-Dateien), dass es im fraglichen Zeitraum keine unberechtigten Abflüsse personenbezogener Daten gegeben hat, liegt ebenfalls keine Meldepflicht einer Datenschutzverletzung an die Datenschutzaufsicht vor. Hier reicht die interne Dokumentation nach § 33 Abs. 5 KDG. Sollte es später doch noch zu einem unberechtigten Datenabfluss durch bis dahin unerkannte Schadsoftware kommen, wäre zu dem späteren Zeitpunkt eine Meldung abzugeben.
3. Wird eine Kompromittierung festgestellt und kann nicht zweifelsfrei ausgeschlossen werden, dass es einen unberechtigten Abfluss personenbezogener Daten gegeben hat, ist eine Meldung nach § 33 Abs. 1 abzugeben, wenn ein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht.
4. Wird ein unberechtigter Abfluss personenbezogener Daten zweifelsfrei festgestellt, ist selbstverständlich ebenso eine Meldung nach § 33 Abs. 1 abzugeben, wenn ein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht.

In den beiden letztgenannten Fällen sind also auch immer die Art, der Inhalt und der Umfang der Daten und die Anzahl der betroffenen Personen zu berücksichtigen

Von der – vorsorglichen – Meldung einer Datenschutzverletzung nach § 33 KDG bitten wir solange abzusehen, bis eine konkrete Verletzung entsprechend der Fälle 3 oder 4 diagnostiziert wurde.

Eine etwas ausführlichere Darstellung in Form einer 8-seitigen Praxishilfe mit Checklisten zu Sofortmaßnahmen und zukünftiger Prävention wurde vom Bayerischen Landesbeauftragten für den Datenschutz und dem Bayerischen Landesamt für Datenschutzaufsicht veröffentlicht:

Link zur Praxishilfe des LDA Bayern

Ergänzung 15.04.2021:

Am 13. April 2021 hat Microsoft weitere Sicherheitslücken im MS Exchange Server einräumen müssen und einen erneuten Patch zur Schließung dieser Lücken veröffentlicht. Betroffen sind Server-Versionen aus 2013, 2016 und 2019. Der Vorgang zeigt, dass eine kontinuierliche Beobachtung der verfügbaren Sicherheitspatche und deren unmittelbare Installation nötig ist, um IT-Systeme sicher zu betreiben. Das Katholische Datenschutzzentrum ruft alle Verantwortlichen auf, die vom Software-Anbieter bereitgestellten Analyse-Tools einzusetzen, eventuelle Sicherheitslücken zu schließen und potentiell befallene Systeme längere Zeit auf ungewöhnliche Datenübertragungen zu monitoren.