Sehr geehrte Damen und Herren,

wir müssen Ihnen leider mitteilen dass wir, das St. Jakobus Hospiz, am 08.03.2021 Opfer des sogenannten Hafnium-Angriffs geworden sind. Wir möchten Sie auf diesem Wege über den Datenschutzvorfall informieren, auch wenn nach unserem Kenntnisstand keine schwerwiegenden Folgen für Sie zu erwarten sind.

Was ist geschehen?

Zahlreiche Unternehmen sind von dem großflächigen Angriff der chinesischen Hackergruppe „Hafnium“ auf Microsoft-Exchange-Server betroffen. Durch den Angriff war es den Angreifern möglich, auf dem Server Befehle wie ein Administrator abzusetzen. Grundsätzlich eignen sich die Sicherheitslücken in Microsoft Exchange für weitreichende Kompromittierungen des Schutzes personenbezogener Daten.

Es gibt eindeutige Anzeichen, dass Unbekannte sich unerlaubterweise Zugang zum Exchange Server verschafft haben. Weitere Auswirkungen sind derzeit nicht bekannt. Eine Analyse des Datenverkehrs des Servers legt nahe, dass keine großen Datenmengen abgeflossen sind. Das Abgreifen von einzelnen Emails oder kleinen Postfächern, Adressbüchern o.ä. sowie von einzelnen kleineren Dateien kann nicht ausgeschlossen werden. Auf dem betroffenen Server lagen zum Zeitpunkt des Zugriffs lediglich Daten aus dem Jahr 2016 und älter.

Was wurde unternommen?

Nachdem der Angriff identifiziert wurde, wurden unverzüglich alle erforderlichen Maßnahmen ergriffen, um die Sicherheit der von uns genutzten Systeme wiederherzustellen. Microsoft selbst stuft diese Schwachstelle als höchst kritisch ein und hat am 03.03.2021 ein Update zur Behebung der Sicherheitslücke bereit gestellt. Dieses Update wurde unverzüglich installiert. Der Vorgang wurde zudem der zuständigen Datenschutzbehörde gemeldet. Somit konnten weitere Angriffe durch das Schadsystem verhindert werden.

Welche Folgen sind möglich?

Über die missbräuchliche Verwendung von E-Mail-Adressen hinaus könnten Dritte auch die ggf. vom Exchange-Server bezogene Kommunikation (beispielsweise

scheinbar belanglose Einzelheiten aus dem Nachrichtenverlauf oder Termine) verwenden, um Identitätsmissbrauch zu begehen. Daher kann jeder betroffen sein, mit dem wir über Outlook per E-Mail oder über Termineinladungen kommuniziert haben.

Was können wir für Sie tun?

Wir bitten Sie, wachsam zu sein und mit erhöhter Aufmerksamkeit auf Auffälligkeiten im Zusammenhang mit den genannten personenbezogene Daten zu achten.
Antworten sie nicht auf verdächtige E-Mails und öffnen Sie in verdächtigen E-Mails keine Anlagen oder Hyperlinks. Im Zweifelsfall empfehlen wir Rücksprache mit der IT-Abteilung zu halten oder den Absender auf anderem Wege zu kontaktieren um die Kommunikation zu verifizieren. Bitte achten Sie auf auffällige Zahlungen und Kontobewegungen. Wenden Sie sich sofort an uns, wenn ihnen verdächtige Vorkommnisse auffallen.

Wir bitten vielmals um Entschuldigung für die Umstände, die Ihnen durch diesen Angriff bei uns entstehen. Sollten Sie Rückfragen haben, stehen wir Ihnen gemeinsam mit unserer Datenschutzbeauftragten gerne jederzeit zur Verfügung!

Unsere Datenschutzbeauftragte erreichen Sie unter:
netvocat® GmbH – Externer Datenschutz und Seminare
Großherzog-Friedrich-Str. 40
D-66111 Saarbrücken
Tel.: +49 (0) 681 5909798 50
Fax: +49 (0) 681 5909798 30
E-Mail: info@netvocat.de