„Hafnium“: Das sagen die Aufsichtsbehörden zu Melde- und Benachrichtigungspflichten nach der DSGVO

Eine Übersicht von Dr. Carlo Piltz und Stefan Hessel

Im Kontext mehrerer kritischer Schwachstellen in Microsoft Exchange-Servern weisen derzeit mehrere Datenschutzaufsichtsbehörden auf Melde- und Benachrichtigungspflichten nach der DSGVO hin. Mit dieser Übersicht zu den divergierenden Ansichten möchten wir Verantwortliche und Auftragsverarbeiter bei der rechtlichen Bewertung der Schwachstellen unterstützen.

Bundesland	Quelle	Stellungnahme der Datenschutzaufsichtsbehörde
Baden-Württemberg	Pressemitteilung vom 10.03.2021: „Aktive Ausnutzung der Microsoft Exchange Schwachstelle“	*„Wird bei der Überprüfung der Systeme die Ausnutzung der Schwachstelle festgestellt, so ist grundsätzlich von einer Meldepflicht an die Aufsichtsbehörde auszugehen. Nur in atypischen Konstellationen wird kein Risiko für die Rechte und Freiheiten von betroffenen Personen bestehen (vgl. Artikel 33 Absatz 1 DS-GVO). Ein Verzicht auf die Meldung sollte begründet und dokumentiert werden.“*
Hamburg	Meldung vom 10.03.2021: „Schwachstelle bei Microsoft Exchange-Servern“	*„Im Fall eines festgestellten Datenabflusses muss ein Data Breach bei der zuständigen Datenschutz-Aufsichtsbehörde gemeldet werden. Darüber hinaus kann in einem solchen Fall zudem eine Benachrichtigungspflicht an betroffene Personen bestehen.“*
Mecklenburg-Vorpommern	Pressemitteilung vom 10.03.2021: „Kritische Sicherheitslücken im Microsoft Exchange Server“	*„Werden bei den Überprüfungen etwaige Kompromittierung der Systeme festgestellt, weist Heinz Müller ausdrücklich darauf hin, dass diese mindestens zu einer Benachrichtigungspflicht durch den Verantwortlichen an seine Behörde, gem. Art. 33 Abs. 1 der DS-GVO führt (siehe hierzu auch „Weiterführende Links“). Inwieweit sogar ein hohes Risiko für die betroffene Personen besteht und damit eine Benachrichtigung derer nach Art. 34 DS-GVO notwendig ist, ist letztendlich abhängig vom Einzelfall. Hierfür ist eine*

		Individualprüfung durch den eigenen Datenschutzbeauftragten erforderlich.“
Niedersachsen	Meldung vom 10.03.2021: „Kompromittierte Exchange Server meldepflichtig“	*„Die LfD Niedersachsen geht davon aus, dass in jedem Fall einer Kompromittierung des Exchange Servers sowie eines nicht rechtzeitigen Updates eine Meldung gemäß Art. 33 DS-GVO abzugeben ist. […] Im Falle einer Kompromittierung ist zudem zu prüfen, ob die betroffenen Personen nach Art. 34 DS-GVO über die Verletzung ihrer personenbezogenen Daten zu unterrichten sind.“*
Rheinland-Pfalz	Pressemitteilung von 11.03.2021: „Vermehrte Datenpannen-Meldungen in Rheinland-Pfalz wegen Sicherheitslücke auf Microsoft Exchange-Servern“	*„Sofern unbefugte Personen Zugriff auf personenbezogene Daten erhalten haben, stellt dies einen meldepflichtigen Vorfall im Sinne des Artikels 33 der Datenschutz-Grundverordnung dar. […] Sollte Ihr System nicht kompromittiert worden sein und Ihnen keine Erkenntnisse über eine unbefugte Einsichtnahme bzw. Abfluss personenbezogener Daten vorliegen, so ist eine Meldung an den LfDI RLP nicht erforderlich. Sofern von dem Vorfall sensible personenbezogene Daten i.S.d. Art. 9 DS-GVO betroffen sind, so möchten wir Sie darauf hinweisen, dass eine Unterrichtung des betroffenen Personenkreises durch den Verantwortlichen nach Artikel 34 DS-GVO unverzüglich zu erfolgen hat.“*
Bayern (BayLDA)	FAQ vom 09.03.2021: „Sicherheitslücken bei Microsoft Exchange-Mail-Servern“	*„Kommt man nach der Überprüfung der eigenen Systeme zu dem Schluss, dass die Sicherheitslücke (mit hinreichender Wahrscheinlichkeit) ausgenutzt wurde bzw. die Server über den 9. März 2021 hinaus ungepatcht waren und deshalb ein Risiko für die betroffenen Personen nicht auszuschließen ist, ist der Vorfall bei der jeweils zuständigen Datenschutzaufsichtsbehörde zu melden. […] Falls aufgrund der Sicherheitslücke von einem hohen Risiko für die betroffenen Personen ausgegangen wird, müssen diese gemäß Art. 34 DS-GVO umgehend benachrichtigt werden.“*

Nordrhein-Westfalen	Meldung vom 11.03.2021: „Kritische Schwachstellen in Exchange-Servern“	*Zur Prüfung einer Meldepflicht an die LDI NRW nach Artikel 33 Abs. 1 Datenschutz-Grundverordnung müssen Verantwortliche im Falle eines festgestellten erfolgreichen Angriffs auf Exchange-Server neben der Wahrscheinlichkeit, dass personenbezogene Daten unbefugt verändert, gelöscht oder abgegriffen wurden, auch die möglichen Schäden, die hiervon für die Rechte und Freiheiten der betroffenen Personen ausgehen, bewerten. Sollten beispielsweise nach intensiver Untersuchung der Systeme keine Hinweise für einen Datenabfluss und eine Manipulation von personenbezogenen Daten vorliegen und keine besonders sensiblen personenbezogenen Daten in den betroffenen Systemen verarbeitet worden sein, liegt zumeist ein eher geringes Risiko für die Rechte und Freiheiten natürlicher Personen vor. In diesen Fällen genügt eine interne Dokumentation der Verletzung beim Verantwortlichen gemäß Artikel 33 Abs. 5 Datenschutz-Grundverordnung. Sollte ein mehr als geringes Risiko festgestellt werden, besteht die Meldepflicht an die zuständige Aufsichtsbehörde gemäß Artikel 33 Abs. 1 Datenschutz-Grundverordnung. Sofern ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen festgestellt wird, kann nach Artikel 34 Datenschutz-Grundverordnung auch eine Benachrichtigung der betroffenen Personen erforderlich sein.*

Diese Auflistung hat einen Stand vom 11.03.2021 – 17:00 Uhr. Nicht erwähnte Behörden haben zu diesem Zeitpunkt noch keine öffentliche Stellungnahme abgegeben. Unsere ausführliche Analyse finden Sie unter www.reuschlaw.de.

Unternehmenskontakt: Dr. Carlo Piltz I Teamleader Cybersecurity & Datenschutz I T > +49 30 / 2332895 0 I E carlo.piltz@reuschlaw.de