„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.“* ***Ergänzung vom 12.03.2021:*** *„Verantwortliche, die bereits nach den Handlungsempfehlungen des BSI geprüft haben, ob die Sicherheitslücke ausgenutzt wurde und keine Kompromittierung festgestellt haben, können von einer Meldung absehen. In diesem Fall liegt voraussichtlich kein Risiko für die Rechte und Freiheiten der betroffenen Personen vor. Aber auch dann ist die Dokumentation nach Art. 33 Abs. 5 DS-GVO zu erstellen.“* ***Ergänzung vom 23.03.2021****: „Die LfD Niedersachsen geht davon aus, dass in jedem Fall einer Kompromittierung des Exchange Servers* ***oder*** *eines nicht rechtzeitigen Updates eine Meldung gemäß Art. 33 DS-GVO abzugeben ist.“*
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.“*
Bayern (BayLDA und BayLfD)	Praxishilfe vom 12.03.2021: „Exchange Security Check & Incident Response“	*„Folgende Fallkonstellationen (A bis F) sind im Hinblick auf personenbezogene Daten wesentlich:* • *Keine Meldepflicht nach Art. 33 DS-GVO* *A) Eine Verwundbarkeit des Exchange Servers war zwar gegeben, jedoch kann eine Kompromittierung nach umfangreichen Analysen ausgeschlossen werden. In diesem Fall liegt keine meldepflichtige Datenschutzverletzung vor, da die Schwachstelle mit hinreichender Wahrscheinlichkeit nicht ausgenutzt wurde (vgl. Art. 4 Nr. 12 DS-GVO).* *B) Trotz festgestellter Kompromittierung kann ausgeschlossen werden, dass personenbezogene Daten betroffen sind. Es liegt demnach keine meldepflichtige Datenschutzverletzung vor, da keine personenbezogenen Datenbetroffen sind (vgl. Art. 4 Nr. 12 DS-GVO).* *C) Trotz festgestellter Kompromittierung und der Betroffenheit personenbezogener Daten kann ein Risiko für die betroffenen Personen nach DS-*

		GVO ausgeschlossen werden. Es liegt somit keine meldepflichtige Datenschutzverletzung vor, da der Vorfall voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (vgl. Art. 33 DS-GVO). • *Meldepflicht nach Art. 33 DS-GVO* *D) Für den Fall, dass eine Verwundbarkeit gegeben war, aber man bislang nicht ausreichend nach prüfen konnte, in welchem Umfang eine Kompromittierung stattfand, ist von einer meldepflichtigen Datenschutzverletzung auszugehen, da den Sicherheitsbehörden Erkenntnisse vorliegen, dass verwundbare Server massenhaft und teils automatisiert angegriffen wurden.* *E) Für den Fall, dass Updates sehr spät eingespielt wurden: Hier ist von einer meldepflichtigen Datenschutzverletzung auszugehen, da das Zeitfenster für einen erfolgreichen Angriff ausreichend groß war. Es wäre untypisch, wenn verwundbare, an das Internet angeschlossene Server längere Zeit trotz derart öffentlichem Bekanntwerden des Angriffsweges ohne Kompromittierung blieben. Hinsichtlich eines möglichen hohen Risikos können zu einem solchen Zeitpunkt keine nachhaltigen Aussagen getroffen werden. Daher muss der Sachverhalt weiter aufgearbeitet und die Meldung nach Art. 33 DS-GVO durchgeführt werden.* *F) Falls eine Kompromittierung des verwundbaren Exchange Servers erkannt wurde: In den aller meisten Fällen hatten unbefugte Dritte*

		(Angreifer) potentiell Zugriff auf Systeme und Dienste, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Eine Meldeverpflichtung bei der zuständigen Datenschutzaufsichtsbehörde besteht. Des Weiteren ist zu prüfen, ob betroffene Personen nach Art. 34 DS-GVO über die Verletzung ihrer personenbezogenen Daten zu unterrichten sind. Dies hängt u. a. entscheidend (aber nicht nur) von der Sensitivität der betroffenen personenbezogenen Daten ab. Folglich erfordert dieser Schritt eine äußerst sorgfältige, datenschutzrechtliche Bewertung und Vorgehensweise.“
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.“
Sachsen-Anhalt	Pressemitteilung vom 11.03.2021: „Landesbeauftragter für den Datenschutz warnt vor Sicherheitslücken bei Microsoft Exchange-Mail-Servern und mahnt die Meldung von Datenpannen an.“	*„Der Landesbeauftragte weist daraufhin, dass aufgrund der Verpflichtung zur Gewährleistung der Sicherheit ihre Verarbeitungstätigkeiten gem. Art. 32 DSGVO von den Verantwortlichen gefährdeter Systeme die umgehende Installation der verfügbaren Sicherheits-Patches erwartet werde. „Angesichts des hohen Schadenspotentials ist nach erfolgtem Update zusätzlich zu prüfen, ob die Maßnahme zu spät erfolgt ist und bereits Schadcode installiert wurde. Festgestellte Datenschutzverletzungen sind der Aufsichtsbehörde gemäß Artikel 33 der Datenschutz-Grundverordnung zu melden. Hierfür steht ein elektronisches Meldeformular auf unserer Homepage bereit. Des Weiteren ist zu kontrollieren, ob die betroffenen Personen zu benachrichtigen sind.“ sagte Albert Cohaus, der den Landesbeauftragten vertritt.“*
Hessen	Pressemitteilung vom 12.03.2021: „Unmittelbarer Handlungsbedarf wegen Schwachstellen in Microsoft Exchange-Server“	*„Weiterführende Maßnahmen sind dann zu ergreifen, wenn erfolgreiche Angriffe identifiziert beziehungsweise nicht mit hinreichender Sicherheit ausgeschlossen werden können. Hierzu gehört auch, unabhängig davon ob ein konkreter Datenabfluss identifiziert werden konnte, eine Meldung gemäß Art. 33 DS-GVO an die zuständige Datenschutzaufsichtsbehörde.“*
Saarland	Mitteilung vom 12.03.2021: „Kritische Sicherheitslücken bei Microsoft Exchange-Mail-Servern“	*„Stellen Betreiber nach erfolgter Selbstprüfung der Exchange-Server Anhaltspunkte für eine Kompromittierung oder einen Datenabfluss und somit eine Verletzung des Schutzes personenbezogener Daten fest, besteht nach Art. 33*

		Datenschutz-Grundverordnung (DSGVO) die Pflicht, den Sachverhalt der zuständigen Datenschutzaufsichtsbehörde zu melden.“
Sachsen	Mitteilung vom 12.03.2021: „Datenpannen-Meldungen wegen Sicherheitslücken auf Microsoft Exchange-Servern“	*„Sofern eine Kompromittierung des Exchange-Servers nach sachkundiger Prüfung mittels der vom BSI empfohlenen Vorgehensweise nicht ausgeschlossen werden kann, stellt dies einen meldepflichtigen Vorfall im Sinne des Art. 33 DSGVO dar.“*
Thüringen	Pressemitteilung vom 15.01.2021: „Der TLfDI warnt vor Sicherheitslücken in der weit verbreiteten Mailinfrastruktur „Microsoft Exchange Server“ – Datenpannen sind umgehend zu melden –„	*„Festgestellte Datenschutzverletzungen sind dem TLfDI gemäß Artikel 33 der DS-GVO zu melden.“*
Bremen	Pressemitteilung vom 23.03.2021: „Meldepflicht?! – Aktuelle kritische Sicherheitslücken in MS Exchange“	*„Zudem weist sie auf die Pflicht der Verantwortlichen (Betreiber) hin, nach Artikel 33 der Datenschutzgrundverordnung (DSGVO) Verletzungen des Schutzes personenbezogener Daten zu melden. Dies gilt bereits dann, wenn eine Kompromittierung erfolgt ist – auch dann, wenn kein Abfluss personenbezogener Daten erfolgt ist oder noch nicht festgestellt werden konnte.“*

Diese Auflistung hat einen Stand vom 24.03.2021 – 08:30 Uhr. Nicht erwähnte Behörden haben zu diesem Zeitpunkt noch keine öffentliche Stellungnahme abgegeben. Unsere ausführliche Analyse finden Sie unter www.reuschlaw.de.

Über reuschlaw Legal Consultants
reuschlaw Legal Consultants gehört zu den führenden wirtschaftsberatenden Kanzleien im Produkthaftungsrecht und berät seit 2004 national und international tätige Unternehmen mit Schwerpunkt Produktsicherheitsrecht, Produkthaftungsrecht, Cyber & Data Security, Rückrufmanagement, Versicherungsrecht, Compliance Management und Vertragsrecht.

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