**Die Landesbeauftragte für Datenschutz und Informationsfreiheit**

**Freie Hansestadt Bremen**

Bremen/Bremerhaven,
23. März 2021

# P R E S S E M I T T E I L U N G

## Meldepflicht?! – Aktuelle kritische Sicherheitslücken in MS Exchange

Am 5. März 2021 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) in einer Pressemitteilung darüber informiert, dass zehntausende Microsoft Exchange Server verschiedener Versionen in Deutschland durch Sicherheitslücken angreifbar und mit hoher Wahrscheinlichkeit bereits mit Schadsoftware infiziert sind. Ursache sind vier Schwachstellen in der Software. Microsoft hatte in der Nacht zum 3. März 2021 überraschend außerhalb des gewohnten Update-Zyklus Sicherheitsupdates zum Schließen der Sicherheitslücken bereitgestellt.

Das BSI geht davon aus, dass Microsoft Exchange Server, welche bis zum 5. März 2021 nicht mit den bereitgestellten Sicherheitsupdates aktualisiert wurden, kompromittiert sind. Durch die Nutzung der Schwachstellen kann es zu Zugriffen auf E-Mail-Konten und der Installation von Malware kommen. Da die Sicherheitslücken relativ einfach ausgenutzt werden können, kam es spätestens seit Bekanntwerden der Schwachstellen zu massenhaften, weltweiten Angriffen gegen Microsoft Exchange Server-Ziele weltweit.

Auf der Webseite des BSI sind unter dem folgenden Link umfangreiche Informationen und Handlungsempfehlungen, insbesondere auch zur Detektion von entsprechenden Angriffen bereitgestellt:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Server/Microsoft-Exchange_Schwachstelle/schwachstelle_exchange_server_node.html

### Meldungen bei den Datenschutz-Aufsichtsbehörden

Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (LfDI) hat bereits eine signifikante Anzahl entsprechender Meldungen zu Verletzungen des Schutzes personenbezogener Daten erhalten. Sie weist alle Betreiberinnen und Betreiber von Microsoft Exchange Server-Infrastrukturen darauf hin, dass – soweit noch nicht geschehen – umgehend Maßnahmen zum Schließen der Sicherheitslücken und zur Prüfung auf Kompromittierung der Systeme erfolgen müssen. 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. Die Meldung muss unverzüglich und möglichst binnen 72 Stunden nach Kenntnisnahme erfolgen, ein entsprechendes Meldeformular ist auf der Datenschutzwebseite der Landesbeauftragten für Datenschutz und Informationsfreiheit unter https://www.datenschutz.bremen.de/detail.php?gsid=bremen236.c.15665.de zu finden.

Verstöße gegen Artikel 33 DSGVO können nach Artikel 83 Absatz 4 DSGVO mit einer Geldbuße geahndet werden.

Kontakt/Rückfragen:

Dr. Imke Sommer, Telefon 0421 361-18004, office@datenschutz.bremen.de