Vermehrte Datenpannen-Meldungen in Rheinland-Pfalz wegen Sicherheitslücke auf Microsoft Exchange-Servern

Donnerstag, 11 März 2021

https://www.datenschutz.de/vermehrte-datenpannen-meldungen-in-rheinland-pfalz-wegen-sicherheitsluecke-auf-microsoft-exchange-servern/

Die vergangene Woche bekannt gewordene Sicherheitslücke auf Exchange-Servern von Microsoft betrifft Unternehmen und Behörden in ganz Rheinland-Pfalz.

Pressemitteilung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz vom 11.03.2021

Beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) Rheinland-Pfalz sind seit Ende vergangener Woche ein Dutzend Nachfragen sowie Meldungen von Verletzungen des Schutzes personenbezogener Daten (sogenannte Datenpannen-Meldungen) nach Artikel 33 Datenschutz-Grundverordnung (DS-GVO) eingegangen. Der LfDI appelliert an Nutzerinnen und Nutzer von Exchange-Servern, sofort zu prüfen, ob sie von der Schwachstelle potenziell betroffen sind. Betroffene sollten die durch Microsoft bereitgestellten Sicherheitsupdates („Patches“) unverzüglich installieren.

Vergangene Woche hatte Microsoft kurzfristig neue Sicherheitsupdates für Exchange-Server veröffentlicht, mit dem die bislang bekannten vier Schwachstellen geschlossen werden können. Diese Schwachstellen werden derzeit aktiv von Angreifergruppen attackiert, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) mitteilte. Den Angreifern wurde der Name „Hafnium“ gegeben. Das BSI sprach unter Verweis auf einen IT-Dienstleister davon, dass zehntausende Exchange-Server in Deutschland über das Internet angreifbar und mit hoher Wahrscheinlichkeit bereits mit Schadsoftware infiziert seien. In diesem Zusammenhang sprach das BSI von einem „sehr hohen Angriffsrisiko“ für Unternehmen. Es bestehe die Gefahr, dass neben dem Zugriff auf die E-Mail-Kommunikation auch der Zugriff auf das komplette Unternehmensnetzwerk erlangt werden könne.

Erfolgreiche Attacken setzen unter anderem voraus, dass eine nicht-vertrauenswürdige Verbindung zu einem Exchange Server etabliert werden kann, zum Beispiel über Outlook Web Access. Laut Informationen des BSI sind Server, welche nur per VPN erreichbar sind oder eben solche nicht-vertrauenswürdige Verbindungen blockieren, nicht betroffen. Das BSI weist zudem daraufhin, dass Nutzerinnen und Nutzer – auch nach Einspielen der Updates – die Systeme überprüft sollten. Hierfür stellt Microsoft ein Prüfskript bereit. 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 Unternehmen oder Ihre Behörde einen Microsoft Exchange Server einsetzen, so gehen Sie bitte wie folgt vor:

1. Spielen Sie unverzüglich die von Microsoft zur Verfügung gestellten Sicherheitspatches zur

Schließung der Sicherheitslücke auf. Von der Sicherheitslücke betroffene Serverversionen finden Sie auf der Seite des BSI.

2. Prüfen Sie, ob der von Ihnen eingesetzte Exchange-Server kompromittiert wurde. Hierfür stellt Microsoft ein eigenes Prüfskript zur Verfügung. Dieses finden Sie unter dieser Adresse.
3. Sofern Ihr System kompromittiert wurde, so stellt dies eine meldepflichtige Datenschutzverletzung dar. Um die nach Art. 33 der DS-GVO vorgeschriebene Meldepflicht auszulösen, reicht ein potenzieller Zugriff aus, der mit einer Kompromittierung des eingesetzten Servers einhergeht. Losgelöst von einem möglichen Abfluss personenbezogener Daten, der womöglich erst nach einer gewissen Zeit zur Kenntnis gelangt oder festgestellt wird, empfiehlt der LfDI deshalb – bei Kompromittierung des Servers – eine vorläufige Meldung einer Verletzung des Schutzes personenbezogener Daten vorzunehmen, um Konflikte mit der Meldefrist nach Art. 33 Abs. 1 DS-GVO zu vermeiden. Für die Meldung der Datenschutzverletzung verwenden Sie bitte das hierfür bereitgestellte Online-Formular.

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.

Weitere Informationen:

- Pressemitteilung des BSI
