

Der TLfDI warnt vor Sicherheitslücken in der weit verbreiteten Mailinfrastruktur "Microsoft Exchange Server" - Datenpannen sind umgehend zu melden -

Montag, 15 März 2021

<https://www.datenschutz.de/der-tlfdi-warnt-vor-sicherheitsluecken-in-der-weit-verbreiteten-mailinfrastruktur-microsoft-exchange-server-datenpannen-sind-umgehend-zu-melden/>

Pressemitteilung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit vom 15.03.2021

Trotz aktueller Presseveröffentlichungen auf Initiative des [Bundesamtes für Sicherheit in der Informationstechnik \(BSI\)](#) und sofortiger Hilfestellung durch [Microsoft](#) steigt die Zahl der von einem Massenhack betroffenen Microsoft Exchange Server stündlich. Mehr als zehntausend lokale Server sind allein in Deutschland kompromittiert. Das Bundesamt für Sicherheit in der Informationstechnik sieht die IT-Bedrohungslage folglich als „extrem kritisch“. Betroffen seien Organisationen jeder Größe, so das BSI. Auch sechs Bundesbehörden gehören zu den Opfern des Angriffs. Das BSI „empfiehlt allen Betreibern von betroffenen Exchange-Servern, sofort die von Microsoft bereitgestellten Patches einzuspielen.“ Lesen Sie hierzu:

https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2021/210305_Exchange-Schwachstelle.html.

Am 3. März 2021 wurde offiziell eine Zero-Day-Schwachstelle von Microsoft bekanntgegeben. Durch diese Sicherheitslücke können Angreifer auf die lokalen „Microsoft Exchange Server“ (Version 2013, 2016 und 2019) zugreifen. Lediglich solche Server, die ausschließlich über vertrauenswürdige Verbindungen erreicht werden können (VPN), sollten von solchen Attacken nicht betroffen sein. Microsoft stellt Updates bereit, die umgehend von den Exchange-Administratoren angewendet werden sollten. Darüber hinaus stellt Microsoft ein eigenes Prüf-Script zur Verfügung, anhand dessen Systemadministratoren Anhaltspunkte für Angriffe auf Ihre Systeme erhalten können:

<https://techcommunity.microsoft.com/t5/exchange-team-blog/march-2021-exchange-server-security-updates-for-older-cumulative/ba-p/2192020>

und

<https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/>

Der TLfDI bittet darum, die umgehende Installation der verfügbaren Sicherheits-Patches vorzunehmen. Dieser dringliche Hinweis beruht auf der Verpflichtung zur Gewährleistung der Sicherheit der Verarbeitungstätigkeiten gemäß Artikel 32 DS-GVO von den Verantwortlichen gefährdeter Systeme.

„Bitte prüfen Sie auch, ob bereits Schadcodes installiert wurden. Festgestellte Datenschutzverletzungen sind dem TLfDI gemäß Artikel 33 der DS-GVO zu melden. Hierfür steht ein elektronisches Meldeformular auf unserer Homepage bereit:

https://www.tlfdi.de/mam/tlfdi/datenschutz/meldung_einer_datenpanne_nach_artikel_33_ds-gvo.docx.
Des Weiteren ist zu kontrollieren, ob die betroffenen Personen zu benachrichtigen sind.“, sagt Dr. Lutz Hasse, Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (TLfDI).

Die Pressemitteilungen des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit [können hier abgerufen](#) werden.

PDF generated by Kalin's PDF Creation Station