MicrosoftExchange

Immediate action required due to vulnerabilities in Microsoft Exchange Server

03/12/2021

The Hessian Commissioner for Data Protection and Freedom of Information (HBDI) provides information on the need for action due to vulnerabilities in Microsoft Exchange servers.

Fotolia_90394392_S.jpg

Due to the publications by Microsoft, the Federal Office for Information Security (BSI) and the resulting media echo, the HBDI is receiving more inquiries from Hessian responsible persons and reports of violations of the protection of personal data in accordance with Article 33 of the General Data Protection Regulation (GDPR). The background to this are critical vulnerabilities in Exchange servers from Microsoft, which can be exploited over the Internet, provided the specific framework conditions are in place. The vulnerabilities have been and continue to be widely exploited. Those responsible must therefore assume a real and immediate threat.

Eliminating the vulnerabilities by importing the appropriate patches provided by Microsoft alone is not sufficient here. In addition, those responsible must check whether there have already been successful attacks on the affected systems. Correspondingly available assistance from Microsoft and other companies and organizations can be used to support this, e.g. instructions, indicators of compromise or detection scripts. IT forensic investigations should always consider the possibility of a lateral movement.

Further measures must be taken if successful attacks can be identified or cannot be ruled out with sufficient certainty. This also includes, regardless of whether a specific data outflow could be identified, a report in accordance with Art. 33 DS-GVO to the responsible data protection supervisory authority. The corresponding period of 72 hours for a report must be observed. For Hesse, information on submitting such reports is available at https://datenschutz.hessen.de/service/sendungen-von-Hurt-des-schutzes-personaler-daten-durch-responsible. The availability of complete and comprehensive information is not a prerequisite for submitting a report. Missing information can be submitted later in accordance with Art. 33 Para. 4 GDPR. The need to inform data subjects in accordance with Art. 34 GDPR must also be examined.

All in all, those responsible must take action now at the latest in order to meet their obligations under Art. 32 DS-GVO and to

ensure the security of processing (again). The HBDI reserves the right to review this in due course.

Further information from the Federal Office for Information Security (BSI)

Critical vulnerabilities in Exchange servers

Multiple vulnerabilities in MS Exchange

Microsoft Exchange Vulnerabilities - Detection and Response

Contact for press representativesPress spokeswoman: Ms. Maria Christina RostPress and public relations: Telephone: +49 611 1408 119The Hessian Commissioner for Data Protection and Freedom of InformationP.O. Box 316365021 Wiesbaden