Press release from the state commissioner for data protection and freedom of information in Mecklenburg-Western Pomerania

Critical vulnerabilities in Microsoft Exchange Server

No.20210310_2

|

03/10/2021

|

DSMV

|

datenschutz-mv.de

As early as March 5th, 2021, the Federal Office for Information Security (BSI) informed about a new and extremely critical threat situation that affects the Microsoft Exchange Server, which is also very widespread in Mecklenburg-Western Pomerania. The risk situation is classified as the highest "IT threat situation red" and therefore requires immediate action by all affected companies and institutions (see also "Related links").

The combined application of the known Exchange vulnerabilities enables code execution for remote attackers. The BSI assumes that there is a high probability that the systems that are vulnerable in this way have already been attacked and infected with malware. However, successful attacks require, among other things, that an untrustworthy connection to an Exchange server can be established, e.g. B. via Outlook Web Access. According to information from the BSI, servers that can only be reached via VPN or that block such untrustworthy connections are not affected. Nevertheless, according to previous publications, the BSI assumes a five-digit number of affected systems in Germany alone.

Heinz Müller, State Commissioner for Data Protection and Freedom of Information for Mecklenburg-Western Pomerania, expressly points out that those responsible for affected and thus highly endangered systems are initially obliged to immediately install the security updates or patches provided by Microsoft for their systems. This is the only way they can meet their legal obligation to ensure the security of their processing activities, in accordance with Art. 32 of the General Data Protection Regulation (GDPR).

Furthermore, in view of the high potential for damage when exploiting the security gap that has existed for a long time and the resulting significantly increased probability of attacks that have already taken place, there are still further investigation

obligations for those responsible. In order to rule out that the Microsoft updates were installed too late and malicious code has already been installed in the meantime, all affected systems must be checked to see whether they still guarantee the protection required under Art. 32 GDPR. For this purpose, Microsoft has now made its own test script available for those affected (see also "Related links"). If any compromise of the systems is found during the checks, Heinz Müller expressly points out that this leads to at least a notification obligation by the person responsible to his authority, in accordance with Article 33 (1) of the GDPR (see also "Related links "). The extent to which there is even a high risk for the persons concerned and thus notification of them is necessary according to Art. 34 DS-GVO ultimately depends on the individual case. This requires an individual check by your own data protection officer.

Related Links:

BSI press release: https://www.bsi.bund.de/DE/Service-Navi/Presse/Press Releases/Presse2021/210305_Exchange-Schwachstelle.html

BSI cyber security warning: https://www.bsi.bund.de/SharedDocs/CyberSicherheitswarningen/DE/2021/2021-197772-1132.pdf?__blob=publica-tionFile&v=8

Microsoft Security Information "HAFNIUM targeting Exchange Servers with 0-day exploits": https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers

Form for reporting a data breach in accordance with Article 33 (1) GDPR: https://www.datenschutz-mv.de/kontakt/meldung-einer-datenpanne/

Back to overview