DetailHomeNewsDetail

03/11/2021

Increased data breach reports in Rhineland-Palatinate due to vulnerabilities on Microsoft Exchange serversThe vulnerabilities on Microsoft Exchange servers that became known last week affect companies and authorities throughout Rhineland-Palatinate since the end of last week, a dozen inquiries and reports of violations of the protection of personal data (so-called data breach reports) in accordance with Article 33 of the General Data Protection Regulation (GDPR) have been received. The LfDI appeals to users of Exchange servers to check immediately whether they are potentially affected by the vulnerability. Those affected should immediately install the security updates ("patches") provided by Microsoft.

Last week, Microsoft released new security updates for Exchange servers at short notice, which can be used to close the four previously known vulnerabilities. These vulnerabilities are currently being actively attacked by attacker groups, as reported by the Federal Office for Information Security (BSI). The attackers were given the name "Hafnium". Referring to an IT service provider, the BSI said that tens of thousands of Exchange servers in Germany could be attacked via the Internet and were very likely already infected with malware. In this context, the BSI spoke of a "very high risk of attack" for companies. There is a risk that, in addition to accessing e-mail communication, access to the entire company network could also be obtained.

Successful attacks require, among other things, that an untrustworthy connection to an Exchange Server can be established, for example 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. The BSI also points out that users should check the systems - even after installing the updates. Microsoft provides a test script for this. If unauthorized persons have gained access to personal data, this constitutes a reportable incident within the meaning of Article 33 of the General Data Protection Regulation.

If your company or agency uses a Microsoft Exchange Server, please proceed as follows: Immediately apply the security patches provided by Microsoft to close the security gap. The server versions affected by the security gap can be found here on the BSI website. Check whether the Exchange server you are using has been compromised. Microsoft provides its own test script for this purpose. You can find it at this address. If your system has been compromised, this represents a data protection violation that must be reported. In order to trigger the reporting obligation prescribed by Article 33 of the GDPR, potential access is sufficient, which is accompanied by a compromise of the server used. Detached from a possible outflow of personal data, which may only become known or detected after a certain time, the LfDI therefore recommends - in the event of the

server being compromised - that a preliminary notification of a violation of the protection of personal data be made in order to avoid conflicts with the reporting deadline according to Art 33 paragraph 1 GDPR to avoid. To report the data protection violation, please use the online form provided for this purpose. If your system has not been compromised and you have no knowledge of unauthorized access or outflow of personal data, it is not necessary to report it to the LfDI RLP. If sensitive personal data within the meaning of Article 9 GDPR is affected by the incident, we would like to point out that the group of persons affected must be informed immediately by the person responsible in accordance with Article 34 GDPR.
Further information:Press release from the BSIPress release from the Bavarian data protection supervisory authorities of March 18, with references to an FAQ and a practical guide

return