

Due to weaknesses in Microsoft Exchange servers, the department is currently receiving increasing reports of violations of the protection of personal data in accordance with Article 33 GDPR.

Last week, Microsoft released new security updates for Exchange servers at short notice, which should be installed immediately by those affected in order to close the security gaps. In a press release on March 5, the Federal Office for Information Security (BSI) informed about the new, extraordinarily critical risk situation, which requires immediate action by the companies concerned.

This immediate action not only includes the immediate installation of the available security updates, but also the unconditional verification of whether the responsible person's Exchange server has actually been compromised. The BSI has compiled information on Microsoft Exchange servers on the procedure required for this and published an approximately one-hour video on YouTube on the background and the necessary activities. The result of this check is of essential importance for the further evaluation of the incident by the person responsible as well as the data protection supervisory authority.

When is an incident related to these Exchange Server vulnerabilities reportable? When are those affected to be informed?

If a compromise of the Exchange server after expert examination using the recommended by the BSI