Press release from the State Commissioner for Data Protection and Freedom of Information Mecklenburg-West Pomerania

Still acute data protection risks due to security gaps in Microsoft Exchange servers

No.20210323

|

03/23/2021

|

DSMV

|

datenschutz-mv.de

The security gaps in the software of the Microsoft Exchange server, known as the hafnium hack, have led to a global wave of cyber attacks in recent weeks, which have also left their mark on Mecklenburg-Western Pomerania (see press release of March 10, 2021). . The security gaps enabled a targeted attack on the mail servers of public authorities and companies worldwide via the Internet. The target of the attacks was primarily stored and sometimes highly sensitive data from e-mails, address books or calendars. However, there is a serious risk that the existing gaps will also be used to prepare further and more in-depth attacks, e.g. to penetrate downstream IT systems and malicious code, e.g. B. Encryption Trojans to place. The first attacks of this type have now been observed worldwide.

Heinz Müller, the State Commissioner for Data Protection and Freedom of Information in Mecklenburg-Western Pomerania, has stated in the past few days that many operators of affected Exchange servers have fulfilled their obligations in an exemplary manner. "In many reports and consultations, we have noticed that many responsible persons are aware of their obligation to process personal data securely and have therefore done their best to restore the security of the processing as quickly as possible. It is also noteworthy that many actors dealt with the data leak very transparently and proactively informed those affected, even if it was not yet finally clear whether and which data leaked at all." Nevertheless, it should be noted that according to current reports from the Federal Office for Security in of Information Technology (BSI), the necessary security updates have still not been installed on all servers. “Anyone who has not acted yet is acting with gross negligence. All email traffic could be accessible to the attacker, which in many cases includes large amounts of sensitive data, such as information about a person's financial or health situation. Such a situation is not tolerable and will be punished accordingly by us.”

The "Practical help on Microsoft Exchange security gaps", which was published by the Bavarian data protection supervisory authorities and which explains in detail which test steps and measures can support the work-up, is also an aid to processing the data breach.

Back to overview