

press release

The TLfDI warns of security gaps in the far

widespread mail infrastructure "Microsoft Exchange Server"

– Data breaches must be reported immediately –

Erfurt, March 15, 2021

Despite current press releases on the initiative of the Federal Office for Security

in information technology (BSI) and immediate assistance from Microsoft®

Hourly number of Microsoft Exchange servers affected by a mass hack.

More than ten thousand local servers are compromised in Germany alone. That

The Federal Office for Information Security sees the IT threat situation

consequently as "extremely critical". According to the BSI, organizations of all sizes are affected.

Six federal agencies are also among the victims of the attack. The BSI

"Recommends all operators of affected Exchange servers to immediately

apply patches provided by Microsoft."

<https://www.bsi.bund.de/DE/Service->

[Navi/Press/Press Releases/Presse2021/210305_Exchange-Wachstelle.html](https://www.bsi.bund.de/DE/Service-Navi/Press/Press Releases/Presse2021/210305_Exchange-Wachstelle.html).

On March 3, 2021, Microsoft® officially identified a zero-day vulnerability

announced. This vulnerability allows attackers to access the local

"Microsoft Exchange Server" (versions 2013, 2016 and 2019). Only

such servers, which can only be reached via trusted connections

(VPN) should not be affected by such attacks. Microsoft®

provides updates that are immediately applied by the Exchange administrators

should be. In addition, Microsoft® provides its own test script

based on its system administrators clues for attacks on your systems

can get:

Postal address :

*The specified email address is only used to receive simple messages without signature/encryption and for messages encrypted with PGP.

Telephone: 0361 57 3112900

Fax: 0361 57 3112904

Email*: poststelle@datenschutz.thueringen.de

Internet: www.tlfdi.de

PO Box 900455

99107 Erfurt

Office building: Hässlerstraße 8

99096 Erfurt

<https://techcommunity.microsoft.com/t5/exchange-team-blog/march-2021-exchange->

- 2 -

[server-security-updates-for-older-cumulative/ba-p/2192020](https://techcommunity.microsoft.com/t5/exchange-team-blog/march-2021-exchange-server-security-updates-for-older-cumulative/ba-p/2192020)

and <https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/>

The TLfDI asks for the immediate installation of the available security

make patches. This urgent notice is based on the obligation to

Ensuring the security of processing activities in accordance with Article 32 GDPR

by those responsible for vulnerable systems.

"Please also check whether malicious code has already been installed. ascertained

Data protection violations must be reported to the TLfDI in accordance with Article 33 of the GDPR.

An electronic reporting form is available on our website for this purpose:

https://www.tlfdi.de/mam/tlfdi/datenschutz/meldung_einer_datenpanne_nach_artikel_

33_ds-gvo.docx. Furthermore, it must be checked whether the persons concerned

notify." says Dr. Lutz Hasse, Thuringia State Commissioner for the

Data Protection and Freedom of Information (TLfDI).

dr Lutz Hasse

Thuringia State Commissioner for Data Protection

and freedom of information

Hässlerstrasse 8

99096 Erfurt

www.tlfdi.de