The Bavarian State Commissioner for Data Protection

Bavarian State Office for Data Protection Supervision

Microsoft Exchange Server Vulnerabilities:

Still acute data protection risks

Joint assistance of the two Bavarian

published by data protection authorities

Munich and Ansbach, March 18, 2021

By exploiting critical vulnerabilities in Microsoft Exchange server software

there has recently been a massive, global wave of cyber attacks, which also took place in Bavaria

Bavaria has triggered considerable data protection risks (see the press release of the Baye

Austrian State Office for Data Protection Supervision of March 9, 2021). Cyber criminal attackers can

target vulnerable mail servers of companies and

access authorities. Since then, there has been an increased risk of unauthorized access to vulnerable systems

stored data such as e-mails, address books or calendars are accessed. In addition,

these gaps can be further used to prepare downstream attacks, deeper into internal

to penetrate IT systems and malicious code, e.g. B. Encryption Trojans to be placed there.

What is unusual about this incident is the high number of victims worldwide and also in Germany.

attacked systems. A large number of Bavarian companies and public,

in particular state and municipal authorities. Only in the period from March 9th to 17th

In 2021, the two Bavarian data protection supervisory authorities registered in this

more than 750 reports received about data protection violations under Art. 33 data protection

General Protection Regulation (GDPR).

Prof. Dr. Thomas Petri, the Bavarian state commissioner for data protection, emphasizes:

A successful attack on the Microsoft Exchange server can destroy all e-mail traffic

be accessible to the attacker. Especially in the case of public authorities, this can be done on a large scale

Scope even internal e-mails with possibly particularly sensitive data, such as with
medical or tax content, but also data from the youth welfare office,
be accessible to authorized persons.” Even though many Bavarian public authorities have meanwhile
gaps have been closed and not every Exchange server has necessarily been attacked
nonetheless to note that the wave of attacks is not yet over. "The sole
playing the patches is far from enough. There is already sufficient knowledge
suggests that various groups of attackers are still trying to exploit other malware such as
to install encryption Trojans and data for extortion or other abuse
pick up purposes. Increased vigilance is also important after performing the
Safety measures are essential,” says Prof. Dr. Thomas Petri.
Michael Will, President of the Bavarian State Office for Data Protection Supervision, adds: "The
Previous reports show us that in the vast majority of cases it is not just the abstract suspicion
of unauthorized access to one's own Exchange server, but actually concrete
there are indications of a compromise. A data outflow is not always necessary
recognized and thus the confidentiality of the relevant data is called into question, in numerous

In some cases, the integrity of the data processing is no longer affected by manipulation
guaranteed." However, the first successes of the intensive warnings and reconnaissance
measures taken by the security and data protection authorities. Michael Will states:
"Last week's alerts seem to have resonated with most operators
to be men We also notice in numerous consultations that many
those responsible are aware of their legal obligation to ensure secure data processing
worries. Nevertheless, some people remain uncertain as to the extent of damage such
che attack will have at the end.”
Due to the still acute threat situation, the two Bavarian data protection
supervisory authorities a joint "practical guide to Microsoft Exchange security gaps"

public, which explains in detail which test steps and measures are taken during processing
can support. In addition, it explains when the obligation to report according to Art. 33 DSGVO at the
competent data protection supervisory authority exists. In particular, the two Bavarian
data protection supervisory authorities to the following points:

 Bavarian companies and public bodies that received the March 3 security patches
2021 not promptly or not yet imported and their Exchange server from the
Internet without additional protective measures (such as VPN) must be accessible
assume that due to the time that has now passed, there is a high probability that
are likely to be compromised and thus pose massive security and data protection risks
stand. You urgently need to take the remedial measures presented in the practical help
fen. They also have the scope of exploitation of the vulnerability and the obligation to report it
to be checked according to Art. 33 GDPR.
If the necessary measures are still not taken and access to special
whose personal data worthy of protection takes place, the Bavarian data protection
regulators take regulatory action.

 Affected Bavarian public authorities and private companies, the risks for the at
cannot reliably rule out the personal data stored on them,
immediately comply with their obligation to report under Art. 33 GDPR. The presence
of the web shells mentioned by the BSI or other malware is on your own server
in this case a clear indication of an existing reporting obligation, since not only the trust
quality of the personal data, but also the integrity and, if applicable, the
Availability of the system important for data processing can be jeopardized.

The two Bavarian data
safety supervisory authorities also have a common question-and-answer area (FAQ) online
made available.

Prof. Dr. Thomas Petri

The Bavarian State Commissioner for Data Protection

Michael Will

President of the Bavarian State Office for Data Protection Supervision

supervisory authority

street address

mailing address

Telephone fax

email / web

The Bavarian State

commissioned for the

protection

Wagmüllerstrasse 18

80538 Munich

PO Box 22 12 19

80502 Munich

089/212672-0

089/212672-50

poststelle@datenschutz-

bayern.de; https://www.daten-

schutz-bayern.de

Bavarian State Office

for data protection supervision

boardwalk 18

91522 Ansbach

PO Box 1349

91504 Ansbach

0981/180093-0

0981/180093-800

poststelle@lda.bayern.de;

https://www.lda.bayern.de