Bavarian State Office for

data protection supervision

Ansbach, March 9, 2021

press release

Microsoft Exchange Mail Server Vulnerabilities:

Acute need for action for Bavarian companies

- BayLDA recommends: patch, check, report! -

According to the current press release of the Federal Office for Security in the information

mationstechnik (BSI) one thing is clear: The newly discovered vulnerabilities in

Microsoft Exchange mail servers also affect a large number of German companies. One

Ad hoc online investigation of the BayLDA has in the first test run alone a three-

identified a large number of companies whose systems were also several days after the

initial security warnings are still acutely endangered. BayLDA President Will:

"We see with great concern that despite urgent warnings from the security

safety authorities and immediate assistance from Microsoft is still

bare mail servers can be found on the net. For the companies we have identified

there is now an acute need for action. The affected systems must be

patched and then thoroughly checked. For companies that have been idle until now

remained, we believe it has been a reportable data breach."

Vulnerabilities as an IT component

Dealing with security gaps professionally should have been part of everyday IT operations for a long time. Independently

Depending on the type and size of the company, it is mainly for IT systems that can be reached via the Internet

are, in addition to a correct configuration of crucial importance, known vulnerabilities

to be rectified as soon as possible. Automated scans across the Internet otherwise allow attackers

remotely, to get an overview of vulnerable servers at the touch of a button and cyberat-

tack to start. The time window for fixing security gaps is therefore usually very small.

BSI informs about new critical vulnerabilities in Microsoft Exchange

With the press release of March 5th, 2021, the BSI informed about a new, extraordinarily critical hazard

situation, which requires immediate action on the part of the Exchange servers, which are also very widespread in Germany.

affected companies requires. The combined application of the new Exchange vulnerabilities is one

Remote code execution possible for attackers. The BSI assumes that the vulnerable systems

are very likely to have already been attacked and infected with malware.

However, successful attacks require, among other things, that an untrustworthy connection to

can be established on an Exchange Server, e.g. B. via Outlook Web Access. According to information from the BSI

Servers that can only be reached via VPN or block such untrustworthy connections,

address

Bavarian State Office for Data Protection Supervision

boardwalk 18

91522 Ansbach

Telephone +49 (0) 981 180093-0

Fax +49 (0) 981 180093-800

e-mail

Website www.lda.bayern.de

presse@lda.bayern.de

Public transportation

Schlossplatz bus stops

or train station of the city and

regional lines

not affected. Nevertheless, according to previous publications, the BSI assumes a five-digit number of

affected systems in Germany alone.

Apply Microsoft patches

Exchange administrators should install the updates provided by Microsoft immediately

be performed. Microsoft now also provides its own test script for affected companies.

addition (see below in "Related links"). With this, the system administrators of the companies can

Find clues as to whether your own Exchange Server was successfully attacked.

Data protection assessment of the Exchange security problem

Many companies are unsure of the extent to which their own operations and personal data are at risk

have actually been tapped. According to Microsoft, while at the beginning it was primarily research institutions with pan-

demie-focus, universities, law firms and defense sector organizations were attacked,

there is now the assumption that attacks occur regardless of the industry.

Irrespective of a more precise assessment of possible data protection damage from a cyber attack

cke, those responsible with endangered systems are initially obliged to immediately apply the patches provided

to install for their systems and thus to fulfill their obligation according to Art. 32 DS-GVO, the security

to ensure the integrity of their processing activities. Those responsible who have not yet performed this task

are coming, given the central role of Exchange Servers

in the

Communication system of the company extraordinarily increased security risk regardless of further

Found the obligation to report the vulnerability as a breach within 72 hours. This represents

ensure that the further steps to restore the security of the overall system are under the supervision of the

BayLDA are carried out.

In view of the high damage potential when exploiting the security gap and the significantly increased

There is also a likelihood of such attacks for those responsible who have already made the required update in a timely manner

have carried out further investigation duties: In order to rule out that importing the Microsoft

updates succeeded too late and malicious code has been installed in the meantime, all affected system

to check whether they still meet the requirements of Art. 32 GDPR.

ensure. If protection violations occur, such as so-called back doors in the system, in these cases

also to report to the data protection supervisory authority, since then for the persons concerned

there is a risk.

To what extent, in some cases, there is even a high risk for data subjects and a notification

which is necessary according to Art. 34 DS-GVO ultimately depends on the individual case. Here is an individual test

by the company's own data protection officer.

Data protection check by the BayLDA in Bavaria

Since the press release from the BSI last week, the BayLDA has received requests for advice and reports

Data breaches by various companies. Therefore, the BayLDA has the test capacities of its own

ned cyber labs to inform affected Bavarian companies of the acute risk situation.

One of the goals of the test is to identify vulnerable Exchange servers in Bavaria and their operators

to contact.

In a first test run on March 8th, 2021, the BayLDA randomly checked 16,502 Bavarian systems on their

potential vulnerability examined. For organizations that rely on a Microsoft Exchange communications

set structure, it was checked whether the necessary patch level to close the gaps was available. loading

A three-digit number of potentially vulnerable servers was already identified in the first test run

Those responsible are now informed immediately about the data protection obligations and consequences

will.

Due to the large number of companies affected, no individual advice can usually take place. Therefore established

The BayLDA has a question-and-answer (FAQ) section on its website for companies that are interested in this

have privacy issues. This can be reached at the following address: www.lda.bayern.de/exchange

After the companies have been informed, the BayLDA intends to carry out further test runs. For violations of

the requirements of the General Data Protection Regulation then threaten those responsible who do not react appropriately

greed, supervisory procedures up to fines.

Michael Will

president

Related Links:

- BSI press release:

https://www.bsi.bund.de/DE/Service-Navi/Presse/Press Releases/Presse2021/210305_Exchange-Schwach-place.html

- BSI Cyber Security Alert:

https://www.bsi.bund.de/SharedDocs/CyberSicherheitswarningen/DE/2021/2021-197772-1132.pdf?__blob=publicationFile&v=8

- Microsoft Security Information “HAFNIUM targeting Exchange Servers with 0-day exploits”

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

- BayLDA Patch Management Checklist:

https://www.lda.bayern.de/media/checkliste/baylda_checkliste_patch_mgmt.pdf