press release

TLfDI

"Log4Shell":

BSI: on the Java vulnerability

&

BayLDA: Checklist for data protection

need for action

Erfurt, December 16, 2021

The critical vulnerability (Log4Shell) in the widely used Java library Log4j

according to the BSI, leads to an extremely critical threat situation.

The BSI has therefore published a red warning level cyber security warning.

Please note the link of the Federal Office for Security in the

Information Technology (BSI): BSI - Federal Office for Information Security -

Version 1.4: Critical vulnerability in log4j released

The Thuringian state commissioner for data protection and freedom of information

(TLfDI), Dr. Lutz Hasse would also like to thank you today for the attached

press release

of

presidents

of

Bavarian

state office

for

Data Protection Authority (BayLDA) of December 14, 2021:

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

Email*: poststelle@datenschutz.thueringen.de

Internet: www.tlfdi.de

PO Box 900455

99107 Erfurt

Office building: Hässlerstraße 8

99096 Erfurt

press release

Ansbach, December 14, 2021

Bavarian State Office for Data Protection Supervision

-press office-

Email: presse@lda.bayern.de

Java vulnerability "Log4Shell":

Serious cyber threats for Bavarian companies!

LDA checklist on the need for action under data protection law

The Java logging library "Log4j" is widely used. She is part of many

commercial as well as from open source software products, but also themselves

developed Java applications. Due to the recently discovered vulnerability

"Log4Shell"

(CVE-2021-44228) attackers can use the

internet own

Execute program codes and thus a beachhead for further cyber attacks

to install. As a result, there is also a long-term risk of many services being compromised

and in many cases even restrictions on the regular operation of important systems.

Michael Will, President of the BayLDA, assesses the situation from a data protection perspective as alarming: "The threat potential of the Log4Shell vulnerability can hardly be serious enough to be taken. Those responsible must now take immediate action to to check their own systems and eliminate the vulnerability. Already in the recent past, cyber attacks have other security vulnerabilities too resulted in enormous damage. Log4Shell has the potential to surpass these risks and to massively disrupt numerous companies in their everyday work across all sectors. We are therefore monitoring developments closely and with the greatest concern. Our first Attention is paid to effective remedial measures, for which we have a check list provide. Our experiences with the negligence of numerous responsible persons despite serious cyber threats - most recently the vulnerability in Exchange servers in the spring of this year - but also show that follow-up checks for ensuring data protection is essential. Therefore, we are already examining how Bavarian responsible persons subjected to an automated data protection control which will reveal omissions in the Java vulnerability.

Violations of the security requirements of the General Data Protection Regulation

can be punished by us with heavy fines." To what extent the Java vulnerability Log4Shell for Bavarian companies, associations and associations, doctors, lawyers etc. will have, is despite all-round Reconnaissance efforts are far from foreseeable. However is already to the present Time announced that comprehensive scans for vulnerable systems take place and targeted attacks are already being carried out. So it is only

it's a matter of time before those responsible who are affected by the gap will agree

detect damage. Not only economically, but also in terms of data protection

such a scenario with serious consequences. At long last

In particular, those responsible are threatened with an outflow of personal data

Non-availability of important systems and services or establishment of

Backdoors for later cyber attacks. Even ransomware attacks for blackmail

of the affected establishments are probable. consumers are

normally not directly affected by the vulnerability, but could

Feel the effects, for example when services such as apps or web services are no longer available

reachable or personal data is stolen by attacks.

Due to the increased risk situation, those responsible in Bavaria must

Compliance with data protection obligations immediately check whether their IT

Systems and applications are affected by the Java vulnerability Log4Shell.

A check list for this is available at www.lda.bayern.de/log4shell. is

a security breach has already occurred, e.g. B. because the vulnerability is active

was exploited and IT systems with personal data are affected,

According to Art. 33 DS-GVO, there is a regular reporting obligation for those responsible

at the responsible data protection supervisory authority.

Michael Will

President"

dr Lutz Hasse

Thuringia State Commissioner for Data Protection

and freedom of information

Hässlerstrasse 8

99096 Erfurt

www.tlfdi.de