press release

Ansbach, December 14, 2021

Bavarian State Office for

data protection supervision

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. It is part of many commercial products

as well as from open source software, but also from self-developed Java applications. Through the recently

The discovered vulnerability "Log4Shell" (CVE-2021-44228) can be used by attackers via the

internet own

Execute program code and thus install a beachhead for further cyber attacks. This threatens

also in the longer term the compromise of many services and often even restrictions of regular operation

important systems.

Michael Will, President of the BayLDA, assesses the situation as alarming from a data protection perspective: "The

The threat potential of the Log4Shell vulnerability can hardly be taken seriously enough. responsible

must now take immediate action to check their own systems and eliminate the vulnerability. Already

in the recent past, cyber attacks have caused enormous damage via other security gaps.

Log4Shell has the potential to surpass these risks and has numerous operations in their business across industries

disrupting everyday work. We are therefore monitoring developments closely and with the greatest concern. Our first

Attention is paid to effective remedial measures, for which we provide a checklist. Our experiences with the

Negligence of numerous responsible persons despite serious cyber risks - most recently, for example, the vulnerability

on Exchange servers in the spring of this year - but also show that follow-up checks to ensure the
data protection are essential. We are therefore already examining how Bavarian managers can implement an automated
privacy scrutiny that will reveal failures in the Java vulnerability.
Violations of the security requirements of the General Data Protection Regulation can be used by us with sensitive
fines will be imposed."
To what extent the Java security gap Log4Shell for Bavarian companies, clubs and associations, doctors,
Lawyers, etc., is far from foreseeable, despite all efforts to clarify the situation. However
it is already known at this point in time that comprehensive scans are taking place for vulnerable systems
and targeted attacks can also be carried out. So it's only a matter of time when
Those responsible who are affected by the gap notice damage. Not only economically, but
Such a scenario is also associated with serious consequences in terms of data protection law. At long last
In particular, those responsible are threatened with an outflow of personal data, a non-availability of important ones
Systems and services or setting up backdoors for later cyber attacks. Even attacks with
Ransomware to blackmail the affected establishments are likely. consumers
are normally not directly affected by the vulnerability, but could feel the effects, for example

due to the
increased risk
if services such as apps or web services are no longer accessible or your own personal data due to attacks
been stolen.
Bavarian leaders must
observance
data protection obligations immediately check whether their IT systems and applications from the
Java vulnerability Log4Shell are affected. A checklist is available for this at www.lda.bayern.de/log4shell
Disposal. Has a security breach already occurred, e.g. B. because the vulnerability was actively exploited
and IT systems with personal data are affected, according to Art. 33 DS-GVO for those responsible

regularly an obligation to report to the competent data protection supervisory authority.

Michael Will

president

to the