press release

Ansbach, December 1st, 2021

Bavarian State Office for
data protection supervision

Bavarian State Office for
data protection supervision

- press office -

Email: presse@lda.bayern.de

Prepared for emergencies? - Privacy check against wave of ransomware attacks on Bavarian companies

Starting signal for random examinations by the data protection supervisory authority

Bavarian companies - from small medical practices to large corporations - are becoming increasingly international attacked by acting cybercriminals. In addition to encrypting files, including exorbitant Ransom demands often lead to the theft of sensitive health data, account data or Application documents combined with the threat of refusing to pay them online publish. Within the last year alone, the Bavarian State Office for Data Protection Supervision Several hundred ransom attacks have been reported by Bavarian companies, with ransoms ranging from 10 TSD to up to 50 million euros were demanded. President Michael Will: “It is in our own interest to have Bavarian companies protect their data against attacks by cybercriminals. Compliance with data protection law creates a security wall for the data of the persons concerned, which can often be achieved with simple measures can be built. With our testing campaign, we take up basic tasks that are common in every company can and should be guaranteed.”

The high number of reported cases, which increased significantly again from September after a summer break reflects the risk for any company of becoming a victim of a cyber attack. Especially Medium-sized companies are disproportionately affected and thus refute the misleading feeling that not to be the focus of attackers.

If data and the IT system are encrypted, operations often come to a standstill. Even a working one

However, before the trend of attackers stealing personal data (ransomware

2.0), no protection and shifts the damage to the affected workforce and customers. It can be serious

if sensitive information such as the contents of a medical patient file, account details or

application documents

appear in the so-called Darknet to there

in marketplaces

for others

Cybercriminals being put up for sale.

Due to the very high threat level of attacks with ransomware, the BayLDA decided to

to devote a whole series of tests to this topic. The aim is to use five targeted test questions to

to query the most important security areas and other information for comprehensive protection

to offer. “IT security to protect against ransomware is one of the mandatory tasks for all companies that

process personal data. Our exam shows just for small and medium-sized companies

Simple and effective measures to help you maintain your data protection needs and be at your best

At the same time successfully defend the case against the attacks of cybercriminals,” says Will.

01.12.2021

Newly established department for test methods

With the "ransomware" test, the newly established BayLDA test procedures department gave the go-ahead for

a series of unprovoked focused checks. In the future, standardized written and

tests with a clear focus are also carried out automatically via the Internet.

The test questions and information on the respective test complex are also available at https://

www.lda.bayern.de/de/kontrollen_stabsstelle.html published. Future subject areas are already being

preannounced.

The goal of the regular, focused audits is, on the one hand, the data protection controls of the non-

to expand public bodies in Bavaria. On the other hand, the accompanying provision of

Information also draws the attention of the data protection officer to the respectively checked or to be checked pending topics are steered. “We would like the operational data protection experts as Win multipliers to jointly increase the protection of Bavarian companies. Our Focused test catalogs offer them simple tools for internal controls and training.”, explains President Michael Will.

01.12.2021