press release

Ansbach, June 2nd, 2022

Bavarian State Office for

data protection supervision

Bavarian State Office for

data protection supervision

- press office -

Email: presse@lda.bayern.de

Email accounts targeted by cybercriminals – Assistance for Bavarian companies

The Bavarian State Office for Data Protection Supervision (BayLDA) often reports successful attacks reported to e-mail accounts of Bavarian companies. The BayLDA therefore has in May 2022 in Another preventive test as part of its strategy of random sample tests initiated to sensitize those responsible and to provide specific assistance to protect against to expose this form of cybercrime.

BayLDA President Will explains the objective: “E-mail accounts are still the most vulnerable spot for many Companies that cybercriminals like to use. Your protection will only succeed if up-to-date technical Protective measures are in place and at the same time a high level of education and awareness-raising among users users are ensured. Our random check is also for those companies we this time do not check more closely, an important impetus to review and update their protective measures."

Cyber attacks on email accounts

E-mail communication is still one of the central interfaces in the majority of companies business communication with internal and external partners. Due to the large number of electronic Messages Criminals often use e-mail services for cyber attacks using carefully prepared e-mails to induce the addressed to take certain actions, for example changed payment details consider clicking on the links contained therein or opening a file attachment.

Damage from a cyber attack via e-mail

If the recipients follow the instructions from such emails, there is a risk of very different types of damage. a far

A widespread phenomenon is the manipulation of payment data, so that the money is not transferred to orders, for example

is transferred to the correct addressee. Classic phishing attacks, in which

the addressee's password should first be obtained in order to access the e-mail account

to win. This means that not only can all the information contained be accessed, but also in the name

of the victim through identity theft targeted messages are sent to all contacts. malicious codes

spread rapidly as a result. Ultimately, this is how ransomware can also nest, the one

Encryption of data and increasingly before to increase the potential for blackmail

Server copied by the attackers. For the companies that fall victim to such a malicious code infestation, the

data protection and economic damage is particularly high.

Prevention through privacy controls

By far the most important measure for active protection against such cyber attacks is raising awareness

of its own staff. The BayLDA's Test Procedures department has therefore relocated due to the acute

threat situation in cyberspace, after the area of ransomware now also the protection of e-

To control mail accounts over a large area in Bavaria. As part of the prevention check, basic

Safety measures at the audited companies queried. At the same time to them as well as that will not be

The companies involved in Bavaria are provided with information material that

Make it easier to check the key components of a security concept, such as a checklist for the

most important fields of action phishing awareness and security awareness, passwords, two-factor

Authentication and user management, maintenance and configuration of accounts, verification of

Data traffic as well as device and patch management including backup concept.

Will, President of the BayLDA, is currently appealing to small and medium-sized companies to use these new

Carefully evaluate information offers on data protection and cyber security for yourself: “Cyber threats

are no longer just a risk for large, prominent companies. Getting better organized and

equipped criminal organizations use all too precisely that small and medium-sized ones in particular

Companies are often far too careless when it comes to protecting their own systems – this is reflected in the current ones

reports of data breaches to us. We have therefore made it our mission to focus on the prevention aspect

to further expand our data protection controls and to broaden them through targeted offers.”

05/09/2022