DetailHomeNewsDetail

06/03/2020

New wave of malware - increase in data breaches these days due to phishing mailsIn the past few days, numerous organizations and companies in Rhineland-Palatinate have been infected with a new type of malware comparable to the Emotet malware. Eight corresponding data breaches have been reported to the State Commissioner for Data Protection and Freedom of Information in Rhineland-Palatinate (LfDI) since May 20. Both companies and public authorities are affected by the attacks. The current wave of attacks involves malicious software in which the malware usually reads not only the e-mail contacts but also the existing e-mail communication and then spreads further along the e-mail path. Once the malware has penetrated IT systems, it may be able to download other malware. It is currently unclear whether and to what extent further data was lost in the most recent attacks in Rhineland-Palatinate, in addition to the data from e-mail communication still open. According to the first information provided by those responsible for the companies and institutions concerned, no further leaks of data have been identified so far; however, this is subject to further investigation. Attacks with the new type of malware are problematic in terms of data protection, because personal data becomes known to unauthorized third parties as a result of the e-mails being leaked. Depending on the context, these e-mails can contain sensitive data from the sender. The attacks usually follow the following pattern: The malware reads contact relationships and e-mail content from the mailboxes of already infected systems. Then authentic-looking spam mails are sent to the recipients from the contact list. They therefore receive bogus e-mails from senders with whom they have recently actually been in contact, which increases the risk that the e-mails will be trusted. The descriptions of those affected in Rhineland-Palatinate in the past few days are similar in this sense: E-mails with the addresses of the companies and institutions affected were sent to people who consisted of two elements. At the top of the email was a short sentence with a link that could potentially lead to infection. In the lower part of the e-mail, an older e-mail was attached that the person had previously sent to the company or institution. In the event of an attack with the new type of malware, there is a data protection violation under Article 33 DS-GVO at the to be reported to the competent supervisory authority within 72 hours. After an attack, all affected people, i.e. all e-mail senders who are in the mailbox of the infected company, should be informed about the incident according to the motto "Sharing is caring" (prevention by sharing information) in order to prevent the virus from spreading 9 GDPR, a high risk for the rights and freedoms of the persons concerned must be assumed.In these cases, the Responsible for an obligation to notify the persons concerned according to Art. 34 Para

Prevention of an attack Further information is available from the Federal Office and the Bavarian State Office for Da ten protection supervision.

The Bavarian State Commissioner for Data Protection and the Bavarian State Office for Data Protection Supervision provide a checklist with best-practice measures to ensure availability with regard to cyber attacks in medical facilities.

return