Bavarian State Office for

data protection supervision

Ansbach, December 18, 2019

press release

Christmas mail from the hacker – Warning of new Emotet infection wave

According to the findings of the Bavarian State Office for Data Protection Supervision (BayLDA)

Numerous organizations are currently dealing with the Emotet Trojan. The malware caused

has already caused considerable economic and data protection damage. That

BayLDA therefore warns all those responsible - whether company, doctor, craftsman etc. -

urgently and recommends paying particular attention to incoming e-mails. This

also applies to Christmas greetings from supposedly well-known communication partners.

Links or attachments should not be opened carelessly. Should an infection occur,

a report to the data protection supervisory authority is mandatory.

Explanation: What is Emotet?

Emotet is malware that is currently considered one of the most dangerous threats on the Internet

is to be classified. The reason for this is that, in the event of an infection, the malware not only destroys the e-mail contacts,

but also the

Communication reads and then spreads on the e-mail path. Once Emotet is in the IT

Systems penetrated, other malicious programs are reloaded. This includes, for example, malware that

Spying out access data and granting cybercriminals access to the IT infrastructure. Also will

further spreading throughout the victim's network is possible. Often an encryption Trojan

reloaded, so-called ransomware, which encrypts all files after a certain time in order to

to blackmail sail to restore the files. Emotet causes enormous damage as a result.

Symptoms: how to recognize Emotet?

The Trojan is able to send authentic-looking emails. Emotet acquires the appropriate ones

Information by reading the e-mail correspondence. In this way, e-mails are sent in a targeted manner that apparently come from already known contacts and also excerpts from an earlier communication contain. The recipient is addressed directly. Linguistically, such e-mails are in a relatively incorrect written free German.

One distinguishing feature is that the name in the sender field does not match the email address displayed. conspicuous lend is also a very short text as well as file attachments or inserted links with the request to to open. The malware then hides itself either in the attached document or on the linked web site. If you recognize such a message in your own inbox, the specified sender is ideally to inform. Often the said contact does not know that they are infected with Emotet and malware is distributed via email on its behalf.

address

Bavarian State Office for Data Protection Supervision

boardwalk 18

91522 Ansbach

Telephone +49 (0) 981 180093-0

Fax +49 (0) 981 180093-800

e-mail

Website www.lda.bayern.de

presse@lda.bayern.de

Public transportation

Schlossplatz bus stops

or train station of the city and

regional lines

Prevention: how to protect yourself from Emotet?

An important component of protection against Emotet file attachments is disabling macros in Office applications.

ments. All security aspects that are required in any case in the digital environment should also be taken into account.

den: Installation of security updates for the operating system and the applications, regular backups of the

Data, restriction of administrative user rights and, if necessary, additional security software.

Ultimately, the decisive safety factor remains the human being, i. H. the user for whom the attack

right arrives. For this reason, raising the awareness of all employees for those responsible is not only

in their own interest, but also an organizational obligation. This is the only way to avoid that

file attachments are opened carelessly or links are clicked on by supposedly known senders.

Response: How do you behave in the event of an infection?

Computers in networks must first be isolated. It can be assumed that an infected system

must be completely reinstalled to ensure that all malicious components are removed

became. As a rule, all access data used in the affected system must be changed, as these

could be grasped, e.g. B. also the passwords used via the web browser.

In the case of an Emotet infection, there is a security breach from the point of view of data protection law, which, according to

Art. 33 DS-

GMO must be reported to the competent supervisory authority within 72 hours. Bavarian responsible persons

from the non-public area can submit their report via an online service at the BayLDA:

 www.lda.bayern.de/datenschutzviolation

In order to stop the spread of Emotet, it is important that those around you know about your own infection

becomes. Existing contacts or communication partners are very likely to be lost due to the

accessed data is attacked and can only be targeted to the personalized through such information

prepare attack. According to Art. 34 DS-GVO there is even an obligation to notify

ment of those affected if they are at high risk – this can be assumed in the case of an Emotet infection.

The BayLDA provides general information on the appropriate handling of malicious code on its own website

available and also refers to the websites of the Federal Office for Information Security (BSI):

 www.lda.bayern.de/schadcode

 www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Themen/Emotet/emotet.html

 www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Information/Article/emotet.html

The President of the BayLDA, Thomas Kranig, assesses the current risk situation as follows:

“Emotet has been on our minds as a data protection supervisory authority for many months, but at the moment we are particularly intense. At regular intervals we receive almost instantaneous reports from infected people Organizations in which not only the daily routine is mixed up, but also partly the whole operation is at a standstill. It doesn't matter whether it's a law firm, a doctor's office or a large company - the damage was so far mostly classified as serious. So Emotet threatens every user, both professionally and privately. Unfortunately the fake emails and the attack scam are getting better and better. That the attackers now shortly before Christmas night even send the pest disguised as a Christmas greeting, many people like the anticipation of the Christmas season cloudy. There is hope that the protective measures and the warning against Emotet spread at a faster pace than Emotet itself.”

Thomas Kranig

president