media information

Saxon data protection officer

Secure digitization:

More protection against cyber attacks needed

 Saxony's data protection officer advocates more prevention.

 Each cyber attack costs more than 21,000 euros on average.

In view of the recent hacker attacks against German companies

the Saxon data protection officer pleads for significantly more prevention.

"Saxony's companies shouldn't wait until they fall victim to

hacker attacks," says Andreas Schurig. On the contrary:

"Prevention is more effective and more important than ever to keep data from customers

and employees do not fall into the wrong hands."

Increase in reported data breaches

According to the General Data Protection Regulation, companies must just as

organizations and managing data breaches at the

report to the competent supervisory authority. The trend in Saxony shows this

clearly upwards: In 2018, those responsible reported to the Saxon

Data Protection Officer 227 cases. In 2019 there were 450 reports. 2020

the authority recorded an increase of 40 percent to 635 reports.

And this continuous increase will continue in 2021: in the past

ten months, 750 reports have already been registered. About one of them

third attributed to cybercrime – a noticeable increase in the

Work of the Saxon data protection officer. "I'm assuming, though

that in reality there are many more people affected. The dark figure should

be very high," says Andreas Schurig. And these hacking attacks are for them

affected companies and organizations expensive: A cyber attack

costs an average of EUR 21,818 per incident (source: Statista). The number of attacks

and the extent of the damage increases sharply. In total, the

Your contact person

Andrew Schneider

extension

Telephone 0351/85471-120

Fax 0351/85471-109

saechsdsb@

slt.sachsen.de*

File number

SPR-0121/11/52

Dresden,

November 5, 2021

Street address:

Saxon

Data Protection Officer

Devrientstrasse 5

01067 Dresden

www.saechsdsb.de

Transport connection:

Accessible by road

train line 4

(bus stop Am Zwingerteich)

*Information about the

processing of your

personal data and

to access for encrypted

Emails can be found at

https://www.saechsdsb.de/

Data protection.

Costs for digital attacks on the German economy to around 24.3 billion in 2020 alone

Euro. That was four times more than in 2019 (source: Bitkom study).

Even more serious are those caused by ransomware

Damage: The companies average total cost to fix a

Attacks by blackmail software are around one million euros; about 46 percent

of German companies are affected (source: Sophos State of Ransomware 2021).

“This development is very worrying. Poor data security revealed

usually also weaknesses in data protection. It's not just for those affected

Companies threatening their existence, but also for people whose data is in the

possessed by criminals. Identity theft is one of the worst

Consequences. Those affected are at risk of a total financial and social loss,” warns Andreas

Schurig.

Prevention is the best way

At the same time, the top Saxon data protection officer makes it clear that prevention and

precautions are the right means against hacker attacks and cyber blackmail. "The

The best protection is to be well prepared for an emergency.” The following precautions are

to recommend:

 Back up data! The data of companies and organizations must absolutely

be secured. These backups should not themselves be caught by cyberattacks

can become.

 Configure the firewall correctly! The firewall should only be required

Allow data connections. Also an early warning system about abnormally high

Data traffic can help system managers avoid greater damage

turn off

 Observe the emergency plan! For cases of cyber blackmail or hacker

Attacks should have an emergency plan that is to be worked through in an acute case. In addition

also includes a regulation as to when the IT administrator, data protection officer

or the employees, company management and customers are to be informed.

 Reserve technology! Another urgent recommendation is reserve technology

to hold up. Investigators can forensically examine the attacked IT system,

while the company is quickly able to work again despite the cyber attack.

 Communicate early! Those responsible should be data subjects or

Inform departments quickly about the incident even if not yet sure

is whether and which personal data is affected.

 Further training! IT managers and all those who work in companies and

Organizations responsible for IT security require regular

further education.

"Prevention is a right and wise investment that pays off significantly in the event of an attack

pays off", says Saxony's data protection officer Andreas Schurig. The alternative to

In the case of cyber blackmail, prevention is often just an expensive ransom.

Notification and notification to the competent data protection authority

In the event of a personal data breach, the

Responsible according to Article 33 of the General Data Protection Regulation immediately and

if possible within 72 hours after he became aware of the violation

to report to the Saxon data protection officer. The authority offers this on its

website an online form with which those responsible can submit all relevant

information can be transmitted quickly and easily.

What information does the Saxon Data Protection Officer need?

In the event of a hacker attack, data theft or other attacks, companies should

or responsible persons report to the police as soon as possible. Parallel should

communicated the data protection violation to the Saxon data protection officer

become. Important information for such a report under Article 33 data protection

Basic regulations are:

 Information on the person responsible (name of the company/association concerned etc.)

incl. telephone and e-mail contact;

 Period of breakdown and time of incident;

 Details of the area and category of the incident (e.g. hacking, theft, etc.);

 Information on the data concerned (e.g. addresses, e-mail addresses, bank or

credit data, passwords, health)

 Details of the incident and actions taken and/or intended.

On the notification of the data breach

follows the examination by the Saxon

Data Protection Officer. Of particular interest here is: what damage could occur

people are caused by the incident or what damage has already occurred? How

Could this happen and what precautions can be taken in the future to avoid it

Repetition

to

seize? Provided

necessary,

stands

the saxon

Data protection officer in clarifying these questions with the person responsible in

Exchange and advise on the measures to be taken. The goal is always

Inform citizens of high risks and get them through the right ones

measures to prevent damage.

About the Saxon data protection officer

The Saxon data protection officer is the independent data protection supervisory authority for Saxony

according to Article 51 paragraph 1 of the General Data Protection Regulation (GDPR). This arises with regard to non-

public bodies (eg companies and associations) from § 14 paragraph 2 of the Saxon

Data Protection Implementation Act; with regard to public bodies (e.g. authorities) from § 14 paragraph 1

same law.

Andreas Schurig has held the office since 2004 and is managed by more than 30 people in his office in Dresden

employees supported. The Saxon data protection officer controls the

compliance with data protection rules and investigates complaints from citizens. To the

other tasks

includes advice

responsible for Saxony

data protection issues.

More information: www.saechsdsb.de