INTERNATIONAL SOCIAL SECURITY ASSOCIATION

issa

Section on Machine and System Safety

Cyber Security

in Small Enterprises

Factsheet Nº 1

issa INTERNATIONAL SOCIAL SECURITY ASSOCIATION

Section on Machine and System Safety

Cyber Security

in Small Enterprises

Factsheet Nº 1

A real-life example

The bakery-confectionary named "Sweet and Crispy" with 10 employees is producing chocolate among other things. One day the foil wrapping unit of the packaging machine catches fire during a break without any prior warning. Fortunately, the fire is promptly noticed by an employee and can be extinguished in the early phase. Nevertheless, the damage is serious.

What happened?

Investigations of the cause of fire showed that the required temperature of the wrapping unit was set to a value which was considerably too high – above the inflammation temperature of the foil which caused the fire. After an electrical failure could be excluded, an expert found out that the machine was permanently connected to the internet. An employee of "Sweet and Crispy" had connected the machine to the router since he wanted to use the recommended remote maintenance. The manufacturer had advertised this feature and promised a repair within 24 hours. But the entrepreneur forgot to change the default password.

Conclusion

The bakery "Sweet and Crispy" has become a victim of a hacker attack. Obviously, the required temperature was altered via the internet. This story sounds incredible? Such or similar incidents happen more and more often. Current reports of the "Bundesamt für Sicherheit in der Informationstechnik" (BSI = Federal office for security in the information technique) show the growing importance. According to these reports, machines and devices with internet connection in German companies still have a high number of security gaps.
And more than 350.000 new malware programs are detected daily.

Are you sure that such an incident cannot happen in your company?

A fault or failure of IT-systems can quickly lead to a loss of reputation, to a production failure or massive damages. A reasonable IT-protection can, however, be reached with relatively simple measures.

That's the reason why you have to take important basic measures!

Basic measures for machines or devices with internet connection

Pull the plug

The simplest measure is to pull the plug to disconnect the internet if it is not needed. As it is mostly not so easy in real life, admission to the internet has to be secured in another way.

Choose a strong password

A strong password is in many cases often the decisive measure in order to protect oneself against unauthorized accesses. Character sequences such as “0000”, “12345” or “qwerty” are of course not appropriate.

The latest recommendations for a good password are not based on small and capital letters, digits and special signs. But complete individual sentences with a lot of characters are recommended. A good password could be, for example:

IfTheWeatherIsNiceTomorrowIWillTakeTheDogForAWalk

It’s important that these sentences are individual and easy to remember, as a password which you cannot remember will lead to cheating. The password will then stick on the monitor or lay in the drawer. Also, the regularly forced, annoying password change is not required anymore.

There are “blacklists” with passwords which are favorized by hackers to get an illegal access. If you want to test your own password, you can do this under the following link:
https://haveibeenpwned.com/Passwords

§§

Who is responsible?

The manufacturers and users are responsible for the security of machines and devices in the internet

Please note that you as an operator have to take the usual precautions to protect your own network of viruses and other threats. This includes the choice of a correct password and also the use of a virus scanner with current virus signatures, a fire wall and especially the correct adjustment of the router. It is also important to keep the operating system and the application programs regularly up-dated.

The manufacturer of devices and machines with internet connection has to secure the internal network as well. When purchasing a machine, you should pay attention that this has been implemented. This can be recognized by the following feature:

There are conditions for entering passwords that cannot be guessed easily. The length of the password does not say anything about the security.

A so called 2-factor authentication is also possible. There are several methods. The most common is the use of a relatively simple password and a dynamic code that can only be used once. This code is sent by SMS, e-mail or by an appropriate app on the mobile device (for example smartphone) at every login attempt.

A further method is the delayed entry of a password after an incorrect entry. In this case the program blocks the password entry after an incorrect entry for some seconds. After the second incorrect entry the waiting time doubles after each password-attempt. After only a few attempts the hacking of even simple passwords will be so time-consuming for the hacker that he gives up.

The use of biometric data (fingerprint, automatic face recognition) is also possible, but not offered in this field so far.

Further information

1 **Small Business Guide: Cyber Security:**
https://www.ncsc.gov.uk/collection/small-business-guide

2 **U.S. Small Business Administration:**
https://www.sba.gov/managing-business/cybersecurity/top-ten-cybersecurity-tips

3 **Canadian Centre for Cyber Security:**
https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

6 Tips to improve cyber security in your enterprise

1. Keep the operating system, application programs, router and firewall updated as far as possible and use the virus scanner with updated virus signatures.

2. Replace the standard passwords at the first use by own, strong passwords.

3. Protect your passwords against access by unauthorized persons.

4. Instruct and sensitize your employees for the proper handling with computers and networked machines.

5. An effective rights management should be implemented by defining which employees get access to which systems and machine functions.

6. Pay attention that the precondition for a secure network is provided when purchasing machines and devices with internet connection.

issa | INTERNATIONAL SOCIAL SECURITY ASSOCIATION

Section on Machine and System Safety

ISSA-Section
Machine and System Safety

Dynamostrasse 7–11
D-68165 Mannheim
Germany
Phone: +49 (0) 621 4456 2213
Fax: +49 (0) 621 4456 2190

www.safe-machines-at-work.org