issa | INTERNATIONAL SOCIAL SECURITY ASSOCIATION

Section on Machine and System Safety

Safe Passwords

in Small Enterprises

Factsheet
Nº 2

issa | INTERNATIONAL SOCIAL SECURITY ASSOCIATION

Section on Machine and System Safety

Safe Passwords

in Small Enterprises

Factsheet Nº 2

A real-life example

The confectionery manufacturer „Cookies and Chocolate“ is a small enterprise with 16 employees. Among other things, chocolate bars with a biscuit filling are produced in two shifts. One day, the internal quality assurance department discovers that the bars produced have an unusual discoloration. A further examination reveals that the bars produced contain too much salt. The production of the chocolate bars is stopped immediately. Nevertheless, the production of the day is affected and the machine can no longer be used for several days due to further investigations.

What happened?

Investigations of the cause of the error revealed that the recipe was changed during ongoing production. The machine that weighs the ingredients has „remote maintenance“ access. This access was not deactivated after the machine was installed, so the machine was permanently connected to the internet. Furthermore, the responsible operator forgot to change the default password for the maintenance access.

Conclusion

Obviously, the recipe has been manipulated via the internet. The company has become a victim of a hacker attack.

This story sounds incredible?

Such or similar incidents happen more often. Current reports of the “Bundesamt für Sicherheit in der Informationstechnik“ (BSI = Federal office for security in the information technique) underline the increasing importance of the topic Cyber Security. According to these reports, machines and devices with internet connection in German companies still have many security gaps. And daily more than 350.000 new malware programs are registered. Nobody can still afford to neglect the topic of cyber security when developing or operating a machine.

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 damage including injury of a person cannot be excluded. 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

Choose a strong password

The simplest measures would be to deactivate all unused ports, as USB, Bluetooth or W-LAN, and only connect the machine to the Internet if this is necessary.
An appropriate password instead of the preset standard password is in many cases often the decisive measure in order to protect oneself against unauthorized accesses.

The latest recommendations for a good password are not based on small and capital letters, digits and special signs. Complete individual sentences with a lot of signs are recommended.

One way to generate a random password is to use so-called hash generators.
The sentence „I‘m going home.“ becomes the password with the SHA-256 method:

„93594b335fca7586fa204f63f750d79c85406bd59d54790bde1e9adbb09e2d4f“

Since the hash method contains a defined algorithm, the password is identical for all hash generators when the same word or phrase is entered.

Since such passwords cannot be remembered, it is recommended to store the passwords in so-called password safes (e.g. KeePass 2). The advantage is that only one master password for the safe needs to be remembered to access all passwords stored.

Passwords that hackers prefer to test in order to gain illegal access are known in the meantime. If you also want to test your own password, you can do this e.g. at the following link:

https://haveibeenpwned.com/Passwords

§§

Who is responsible?

The manufacturers and operators 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, 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. A separation between the office and production network is also very useful.

The manufacturer of devices and machines with internet connection also has to secure the machine’s own network and to provide the possibility to disable unused ports.

There are conditions for entering passwords that cannot be guessed easily. The length of the password is not the only decisive factor for 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

8 Tips to improve cyber security in your enterprise

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

2. Replace the default passwords at the first use by own and secure passwords.

3. Protect your passwords against access by unauthorized persons.

4. Instruct and sensitize your employees for the proper handling of computers, networked machines and passwords.

5. An effective authorization management should be implemented by defining which employees have 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.

7. Deactivate unused ports.

8. Make it possible for your employees to save passwords securely.

issa INTERNATIONAL SOCIAL SECURITY ASSOCIATION

Section on Machine and System Safety

ISSA-Section
Machine and System Safety

Project Group Digital Manufacturing

Dynamostrasse 7–11 · D-68165 Mannheim
Germany
Phone: +49 (0) 621 4456 2213
Fax: +49 (0) 3212 1419 443

www.safe-machines-at-work.org

AUVA

BGN
Berufsgenossenschaft
Nahrungsmittel und Gastgewerbe

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

INAIL
ISTITUTO NAZIONALE PER L'ASSICURAZIONE
CONTRO GLI INFORTUNI SUL LAVORO

suva

TECHNICAL UNIVERSITY
OF KOŠICE

UNIVERSITY *of* GREENWICH