IT-SECURITY COMPLIANCE FOR HOME OFFICES

CHRISTOPH HAAR, Erik Buchmann
Hochschule für Telekommunikation Leipzig
E-Mail: haar@hft-leipzig.de

CHRISTOPH HAAR

- 2010-2015 Business Informatics (Bachelor) Martin-Luther-University Halle/Wittenberg, Germany

- 2015-2017 Business Informatics (Master) Martin-Luther-University Halle/Wittenberg, Germany

- Since 2018 Scientific Assistant Hochschule für Telekommunikation Leipzig, Chair for Data Privacy and Security in Information Systems

AGENDA

- 1. Motivation
- 2. Method
- 3. Result
- 4. Conclusion

1. MOTIVATION

- The ongoing COVID-19 pandemic increases the need to transfer employees into home offices.
- The BSI Grundschutz, ISO 2700x, NIST 800-53 or ISIS12 do not focus on approaches to secure the IT-infrastructure on the employee's private network.
- The reason is that private networks are not considered as part of the companie's infrastructure.
- We want home offices to become part of a certification.
- This is necessary to ensure that employees can perform their daily business without any restriction..

2. METHOD

1. We introduced a basic home-office scenario.

2. On the basis of the BSI, we have defined the role "Home Office User" for the employees.

Tasks	Execute business tasks on business data at home
Operations	Use work equipment and software applications at home
Qualification	Knowledge of the application domain and the IT-system used
Eligibility	Every employee whose function can be performed in a home office

Table 1: The Role „Home Office User“

- The home office user is an employee of a health insurance company, who is using customer data.

2. METHOD (CONT‘D)

3. We performed the BSI Basic Protection, to identify all relevant security requirements for the home-office scenario.

4. We used the role „Home Office User", to identify, all security requirements, that could be implemented by the employee.

   - All other security requirements has to be implemented by the employer.

3. RESULT

- We identified a total of 103 security requirements for our home office scenario.
- 92 security requirements must be implemented by the employer.
- Table 2 shows the 11 security requirements, that must be implemented by the employee.

ID	Description
APP.1.1. A2	Limiting Active Content
APP.1.1. A3	Opening Dcouments from External Sources
APP.1.2. A4	Version Checking and Uptdates for (...)
NET.3.2. A2	Installing Updatdes and Patches
OPS.1.1.4. A5	Operating Virus Protection Programs
OPS.1.1.4. A6	Updating Virus Protection and Signatures
SYS.2.1. A1	User Authentication
SYS.2.1. A3	Activation of Automatic Update Mechanisms
SYS.2.1. A6	Use of Antivirus Programs
SYS.3.1. A2	Laptop Access Protection
SYS.3.1. A3	Use of Personal Firewalls

Table 2: Security Requirements for the Employee

3. RESULT (CONT‘D)

- Our home office scenario is a minimum scenario.
  - These 103 security requirements must be implemented in any home hoffice scenario.
- For a more complex home office scenario, additional security requirements must be identified in the Basic Protection.
- The role „Home Office User“ must be used to identify all additional security requirements that must be implemented by the employee.

4. CONCLUSION

- Our goal was to make home offices part of a certification for companies.
- Home offices must not be considered as external workplaces.
- They are part of the infrastructure of a company.
- Home offices must be integrated into the IT-security policy to ensure
  - data security in the home office.
  - that employees can perform their daily business without any restriction.
- Our scenario introduced a minimal example for a home office.
- This scenario can be expanded to include more elements.

THANK YOU FOR YOUR ATTENTION