# IT-Security Compliance for Home Offices

Christoph Haar
Hochschule für Telekommunikation Leipzig
Leipzig, Germany
email: haar@hft-leipzig.de

Erik Buchmann
Hochschule für Telekommunikation Leipzig
Leipzig, Germany
email: buchmann@hft-leipzig.de

***Abstract*—The ongoing COVID-19 pandemic increases the need to transfer employees into home offices. Securing a home office is challenging. Approaches, such as BSI Grundschutz, ISO 2700x, NIST 800-53 or ISIS12 focus on company premises, and the data carried outside must be strongly restricted. The focus of such approaches is to secure the IT-infrastructure on company premises but not on the employee's private network. In this paper, we explore how the IT-Grundschutz Compendium, a standardized IT-security framework from the German Federal Office for Information Security, can be carried into a home office. Our objective is to extend the scope of protection of the BSI Grundschutz from company premises into the private areas of an employee in a home office. To this end, we apply the BSI Basic Protection to a basic home-office scenario. For each security requirement, we investigate whether it can be implemented by the employee, or by the employer.**

***Keywords – IT-Grundschutz; Home Office Security; Compliance; Basic Protection***

## I. Introduction

The IT-Grundschutz Compendium [1] maintained by the German Federal Office for Information Security (BSI) allows companies to approach pre-defined levels of IT-security in a standardized way. The security level can be audited and certified, and it is compatible with the International Organization for Standardization (ISO) 2700x series of standards [2] or the National Institute of Standards and Technology (NIST) Cybersecurity Framework [3]. Such approaches ease the definition of a security strategy, the execution of risk analyses on company assets and the implementation of a security management that considers organization, personnel, business processes, the IT-architecture, IT-operations, IT-systems and devices, networks, applications and data. Approaches for specific domains exist, e.g., the Payment Card Industry Data Security Standard (PCI DSS), the International Electrotechnical Commission (IEC) standard 62443, or the Federal Information Processing Standards (FIPS) 199 and 200. In many sectors, a certified level of IT-security is mandatory for any major enterprise. The certification confirms, that the company has achieved a reasonable level of IT-security, i.e., it is not only protected against certain attack vectors.

However, such security approaches focus on company premises. Only two of approx. 100 modules in the IT-Grundschutz Compendium directly address home offices (”INF.8 Working from Home” and ”OPS.1.2.4 Teleworking”). Other modules explain how, say, IT-operations on company grounds can be organized without security risks. In consequence, home offices are either considered insecure, or securing them requires elaborate, individual risk analyses and protection mechanisms, as required by INF.8 and OPS.1.2.4.

This is problematic. The Coronavirus-2019 pandemic increases the urge for enterprises allow working from home [4]. Work-life-balance concepts, issues, such as the reconcilability of family and working life, and flexible working-time models also foster this development. However, having obtained a certified level of IT-security means that sensible data must not leave secure areas. But today's homes are filled with networked smart-home devices that do not have security clearance from an enterprise expert, Wireless Local Area Network (WLAN) network connections can be eavesdropped from public spaces, and family members can be expected to enter the work place at home at any time. A recent (meta-)study [5] illustrates the scope of this issue.

Many existing guidelines promise to secure private networks [6]–[8]. Even the BSI has published a checklist for employees in the home office due to the ongoing Coronavirus-2019 pandemic [9]. This checklist covers some basic rules of conduct in a home office. However, none of the guidelines we are aware of reach the completeness and soundness of standardized approaches, such as the BSI Grundschutz or the NIST Cybersecurity Framework. Frequently, it also remains unclear which level of technical understanding is required from an employee to follow such guidelines at home successfully. From a company perspective, the main disadvantage of such guidelines is their incompatibility with certificates. Companies, that do not want to put their certified security strategies at risk, but send employees into home office, are forced to implement harsh measures that limit the usability of a home-office workplace.

One example for such a measure is to strictly disallow any company data on a private device, and to use screen forwarding from a remote machine at the company to the user's device via Virtual Private Networks (VPN). While this approach protects the integrity and confidentiality of the transmission and ensures the availability of the data at the company's side, it might be inadequate for many business tasks. One issue is that a malware at the user's device could interfere with the login process of the VPN or the remote machine. Another issue is that it is restricted to business processes that can be executed entirely on the remote machine. Furthermore, screen forwarding via VPN is too slow for many graphical tasks, including computer-aided design or multimedia content creation. A superior approach would be to extend the company's certified security concept to the user's home office.

ISBN: 978-1-61208-919-5

In this paper, we analyze how the certifiable security level ”Basic Protection” of the IT-Grundschutz Compendium can be executed in a home office. Furthermore, we find out whether the identified security requirements can be implemented by an employee without in-depth technical background knowledge, or need an expert from the employer. To this end, we restrict the focus of this paper on the technical parts of the IT-Grundschutz Compendium that are relevant for home offices, i.e., we only consider the module layers ”Applications” (APP), ”Concepts” (CON), ”Detection and Reaction” (DER), ”Operations” (OPS), ”Networks” (NET) and ”Systems” (SYS).

In particular, we make the following contributions:

- We model a minimal home-office scenario that contains customer data, together with respective roles for the employee in the home office and the company’s IT-security expert.
- We execute a Basic Protection approach according to BSI Grundschutz on this scenario, and we say what must be modified if the scenario changes.
- For each security requirement identified, we examine whether it can be implemented by the employee.

We found out that, from a technical point of view, it is indeed possible to apply the Basic Protection of the BSI to a home office. This means that it is technically feasible to extend the scope of a certified security policy to workplaces at home. However, only 11 of the 103 security requirements needed to implement Basic Protection in our minimal scenario can be implemented by an employee without IT-security expertise that is beyond his or her working skills. All other requirements must be implemented by the employers IT-security experts, either by bringing-in the device, by call-center support or by a security expert visiting the workplace.

Section II describes the IT-Grundschutz basic protection and the basic terms of this work. We define a minimal home-office scenario and implement the basic protection in Section III. In Section IV, we check which of the identified basic requirements the user can implement independently. We discuss our findings in Section V. Section VI concludes.

## II. Related Work

In this section, we introduce the IT-Grundschutz Compendium, related standards and fundamental concepts.

### A. BSI IT-Grundschutz

Since 1991, the German Federal Office for Information Security (BSI) maintains a structured collection of guidelines to implement IT-security in large enterprises in a standardized way. The most recent collection is the IT-Grundschutz Compendium, version 2021 [1], together with supporting standards, such as BSI-Standard 200-2 ”IT-Grundschutz Methodology” [10]. The BSI distinguishes security levels, such as ”Basic”, ”Standard” and ”Increased”. The security levels can be audited and certified, and are compatible with the ISO 2700x series of standards [2] or the NIST cyber security framework [3]. In 2017, the BSI published the ”Guide to Basic Protection based on IT-Grundschutz” [11]. It defines the steps shown in Figure 1 to secure a typical IT-infrastructure. We have aligned our research approach according to these steps. For this reason, we briefly describe them in the following.

### B. Basic Protection

The security level ”Basic” requires to specify the scope of the protection, to map the information doman to BSI modules, and to implement adequate safeguards.

*a) Specification of the Scope:* The **information domain** is defined by means of a structural analysis. Either the entire IT-infrastructure of the company can be considered, or certain departments only. That essentially depends on the size of the individual departments or the company [10]. The information domain includes business processes (e.g., production), IT-systems (e.g., PC’s, server), applications (e.g., Word, Dropbox), data (e.g., customer data), communication links (e.g., ethernet), rooms (e.g., offices), and organizational structures. The individual components of the information domain are described as a network plan.

After the information domain has been defined, it must be modeled by using the **IT-Grundschutz Compendium**. The IT-Grundschutz Compendium contains modules that map the elements of the information domain [1] to security requirements. The modules contain a clear introduction, a threat landscape and requirements on different protection levels. Furthermore the scope within each module is described. In the scope it is also pointed out in more detail which other modules should be considered when using this module.

The current version of the IT-Grundschutz Compendium [1] was released in 2021. However, this version is only available in German at the moment. We use the 2021 version as a basis for this paper, but we briefly describe the differences to the preceding version from 2019 [12], which is available in English: The module ”APP.5.1 General Groupware” is no longer included in the 2021 version. The requirements contained in this module are now contained in other modules, such as ”APP.5.3 General E-Mail Client and Server” The modules ”SYS.4.5: Removable Media” and ”APP.6 General Software” are not yet included in the 2019 version. We need to consider them in our work. The module ”CON.2” only contains one basic requirement ”Implementation of the Standard Data Protection Model”. This requirement includes all basic requirements from the 2019 version. The Standard Data Protection Model complements the IT-Grundschutz Compendium regarding data protection and is also available in english [13]. In the 2021 version, some basic requirements have been omitted. That means, we do not have to consider them in our work. In the 2021 version the following basic requirements have been added: OPS.1.1.3.A15, OPS.1.1.3.A16, SYS.2.1.A42, SYS.3.1.A9 and APP.1.1.A17. We will consider them in our work.

*b) Selection and Prioritization (a.k.a. Modelling):* After the information domain has been defined, the **modelling** must be applied in the next step. For this purpose, all elements of the information domain are mapped to the respective modules in the IT-Grundschutz Compendium [1]. The modules contain definitions of possible risks that have to be considered when

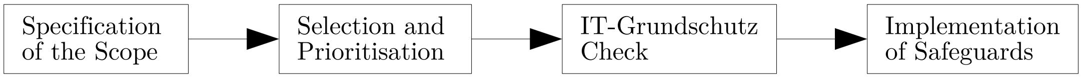
Specification of the Scope
Selection and Prioritisation
IT-Grundschutz Check
Implementation of Safeguards

Figure 1. ”Basic Protection” according to BSI Standard 200-2

securing an element. Furthermore, requirements are described in each module that must be implemented to avert potential risks. For a more detailed description of the modules, we refer to one of our previous works [14]. This step is challenging, because elements can be linked with multiple modules, and modules frequently contain cross-references to other ones.

The result of the modelling is an IT-Grundschutz model of the information domain, which consists of various modules. The requirements for averting potential risks that are described in the modules represent a checklist that must be worked through. The IT-Grundschutz Check can now be started with this checklist.

*c) IT-Grundschutz-Check:* In the preceding step, relevant modules have been identified. Each of these modules contains basic requirements that must be implemented. However, some requirements might have been already implemented in the past, or the products used allow better options to fulfill a requirement than those named in a module. For this reason, the IT-Grundschutz Check provides as a **gap analysis**. For each basic requirement, it is checked whether and to what extent it has already been implemented. The following answers to the implementation status of the basic requirement are possible [11]:

- **Unnecessary:** The requirement can be omitted, because it is not relevant in the information system under consideration or has already been met due to alternative safeguards.
- **Yes:** Appropriate safeguards have been implemented completely for the requirement.
- **Partially:** The safeguards implemented so far do not entirely fulfill the requirement.
- **No:** The requirement has not been met yet, i.e., appropriate safeguards have not been implemented yet.

The result of the IT-Grundschutz Check is a list of requirements with implementation status ”partially” or ”no”. The implementation of these requirements is the starting point for the next step in the Basic Protection. When implementing Basic Protection, the BSI stipulates that all requirements MUST be implemented. For this reason, we will not check which of the basic requirements can be waived, but consider all of them to be necessary.

*d) Implementation of the Safeguards:* Regarding the realisation of the requirements, it must be decided how and in what order the identified requirements have to be implemented. The BSI describes **implementation recommendations** for the requirements. These implementation recommendations are best practice approaches with many years of experience from experts in the field of information security.

## III. Basic Protection for Home Offices

In this section, we analyze to which extent an employee is able to implement the BSI protection level ”Basic” to secure a typical home-office scenario. We start with our research method: First, we define the role ”Home-Office User” as a person without in-depth background knowledge on IT-security. Second, We specify a home-office scenario, and we model its information domain according to BSI standard 200-2 [10]. Third, we apply the BSI protection level ”Basic” on this scenario, i.e., we derive appropriate security requirements for this scenario from the BSI Grundschutz Compendium [1]. Fourth, we use our role definition from the first step as a reference to test if an employee can execute the respective IT-security requirements, or needs help from an expert from the employer. Finally, we discuss what changes if the minimal home-office scenario is extended due to further needs of the employee’s business task.

### A. A Minimal Home-Office Scenario with Customer Data

With ”home office”, we refer to a situation where a home-office user fulfills (a subset of) his business tasks at home, in a domestic environment that is not strictly tailored for business, but also for daily (family) life, leisure, recreation, sports, etc. A room used for home office might also contain a TV or a smart speaker which could be banned on company premises. The room might be shared with other family members when it is not used for work. The PC used for work might be shared with others, with a different user account. We implement the BSI protection level ”Basic” for the following scenario:

**Scenario:** *A health insurance company sends an employee from the customer service department into home office. Since the employee manages sensible data, the company requires that the room used for home office is locked when the employee is off. Furthermore, the company provides a work laptop with an operating system, applications for opening and editing documents, an e-mail client, a web browser and anti-virus software. Furthermore, the work laptop has an USB interface. The employee’s private network has a router that acts as an Internet gateway and a personal firewall, and spans a WLAN network (WLAN0). To establish a network connection to the company, the employee connects his laptop via WLAN to the router, as shown in Figure 2.*

### B. The Role ”Home-Office User”

In the context of this paper, we assume that an employee is an adequately-trained domain expert for the business task he executes, and we also assume that the employee has been trained to use computer equipment securely. However, we do

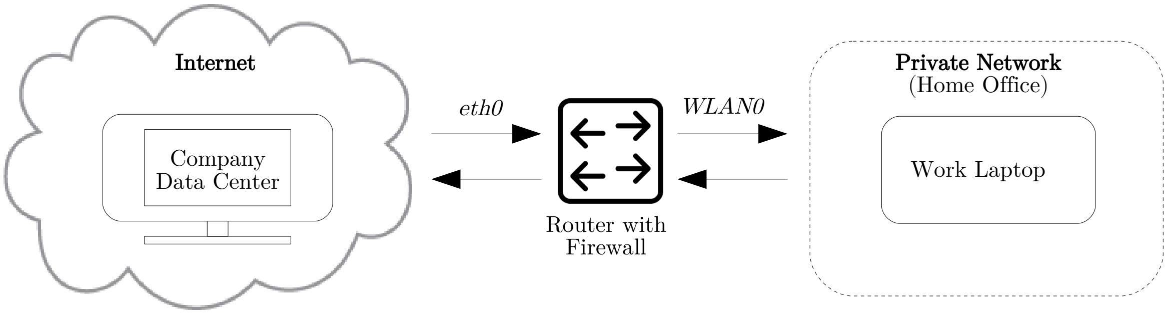

Figure 2. Network plan of a basic home-office scenario

not expect the employee to possess in-depth technical knowledge regarding IT-operations, IT-administration or IT-security. To approach a role specification for our home-office user that considers this, but is also in line with well-established best practices in industry and business, we adapt role definitions from the BSI. In standard 200-2 [10], the BSI describes a set of roles, such as ”Information Security Officer”, ”Data User”, ”Data Owner” or ”Data Creator”. For our paper, we borrow the role ”Home-Office User” from the BSI role ”Data User”.

While the BSI assumes that every employee can take the role ”Data User” [10], our role ”Home-Office User” is restricted to employees that are eligible for home office and have been trained for home office specific IT-components, e.g., how to establish a VPN connection to a company server, how to set up a video conference or how to lock the screen so that no family member gets insight into work data. Table I summarizes the properties and characteristics of this role definition. Note that the BSI defines the term ”operations” according to ISO Standard 12207 [15]. This standard describes a software lifecycle that includes the primary processes of development, operation and maintenance. The ISO standard 15288 [16] describes the same for systems. In our work, we will also use this definition. Thus, our role definition is both compatible with BSI Grundschutz and the ISO standards.

TABLE I
ROLE ”HOME-OFFICE USER”

| *Property* | *Role Characteristics* |
|---|---|
| **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 systems used |
| **Eligibility** | Every employee whose function can be performed in home office |

With our minimal home-office scenario, the role home-office user is instantiated as follows:

**Scenario User:** *The employee works in customer service, has been qualified accordingly, and has years of working experience in that domain. His daily activities include answering customer requests, assessing and settling medical invoices or providing insurance contracts. For this purposes, he uses telephone and email. To do this, he uses the work laptop provided by the employer. Furthermore, the employee has been trained to use the laptop securely at home, i.e., he is able to change passwords, to allow automatic security updates for applications and operating system, and knows how to handle the anti-virus software.*

### C. The Information Domain

To implement the BSI Basic Protection on our scenario, we need its information domain. In the context of this paper, the scope of the information domain is limited to the technical home office setup of the employee, i.e., it ends with the router that provides Internet access.

In line with the BSI Grundschutz methodology, we model the the information domain for each of the levels ”Data”, ”Communication”, ”Applications” and ”IT-Systems” from the network plan (cf. Figure 2) and our scenario description (cf. Subsection III-A). The information domain for our scenario is shown in Table II. Observe that we do not make assumptions yet on the applications or operating systems installed.

TABLE II
INFORMATION DOMAIN OF THE PRIVATE NETWORK

| *ID* | *Object* | *Description* |
|---|---|---|
| **Data** | | |
| D1 | Customer Data | Personal data from customers |
| D2 | Content Data | Data of applications and services |
| D3 | Account Data | Login and authorization data of the user |
| **Communication** | | |
| N1 | Router/Firewall | Security gateway |
| **Applications** | | |
| A1 | System Software | Operating system, drivers and utilities |
| A2 | Applications | Applications to display and edit documents |
| A3 | E-Mail Client | Application for sending/receiving emails |
| A4 | Web Browser | Application to display web content |
| **IT-Systems** | | |
| S1 | Work Laptop | Laptop provided by the employer |

Data D1 to D3 represent different kinds of information from the daily work. For example, the work laptop is secured with a username and password (D3). The same applies to the login of the work e-mail account. Customer data, such as the names, addresses and customer IDs (D1), are processed together with other information (D2) on the work laptop (S1) due to the activity as a customer service employee. The employee's private Internet router (N1) serves also as a security gateway, because it contains a firewall. The applications A1 to A4 represent the various software needed for daily business.

### *D. Implementing Basic Protection*

To implement Basic Protection, we have to identify all modules from the IT-Grundschutz Compendium that address the elements of our information domain (Table II). Observe that the modules in the IT-Grundschutz Compendium are organized in a hierarchy. To secure the web browser, not only ”APP.1.2 Web-Browser” needs to be considered, but also ”APP.6 General Software”. Furthermore, the scope definition of some modules contain cross references to others. For example, ”SYS.3.1 Laptops” refers amongst others to ”NET.2.2 WLAN usage” and ”SYS.2.1 General Client”. It is also possible that a requirement forces to implement another module. For example, basic requirement ”NET.2.1.A8 Procedures in the Event of WLAN Security Incidents” makes it mandatory to consider ”DER.2.1 Security Incident Handling”. Finally, some requirements implicitly call for other modules. For example, Basic Requirement ”SYS.2.1.A4 Regular Backups” is implicitly linked with ”CON.3 Backup Concept”. Table III shows all modules needed to model our scenario, and Table IV contains the list of all Basic requirements, we have identified. For a detailed description of the modules and its security requirements, see the IT-Grundschutz Compendium [1].

TABLE III
MODULES RELATED TO OUR INFORMATION DOMAIN

| *ID* | *Description* |
|---|---|
| APP.1.1 | Office Products |
| APP.1.2 | Web-Browser |
| APP.5.3 | General E-Mail Client and Server |
| APP.6 | General Software |
| CON.2 | Data Protection |
| CON.3 | Backup Concept |
| CON.6 | Deleting and Destroying Data and Devices |
| DER.2.1 | Security Incident Handling |
| DER.2.3 | Clean-Up of Extensive Security Incident |
| NET.1.1 | Network Architecture and Design |
| NET.1.2 | Network Management |
| NET.2.1 | WLAN Operation |
| NET.2.2 | WLAN Usage |
| NET.3.1 | Router and Switches |
| OPS.1.1.3 | Patch and Change Management |
| OPS.1.1.4 | Protection Against Malware |
| SYS.2.1 | General Client |
| SYS.3.1 | Laptops |
| SYS.4.5 | Removable Media |

Our starting point was a minimal home-office scenario with customer data. For this reason, this exhaustive list of Basic requirements must be fully implemented, in order to extend the certified security level ”Basic Protection” from company premises to the workplace of a home-office user that handles any kind of customer data, personal data or other sensitive information.

Note that tasks like telemedicine or power plant control need a higher security level than ”Basic Protection”, because any security issue might endanger the life of a person or produce very high damages. In such scenarios, the list of requirements would be much larger. However, such scenarios are less suitable for home offices anyway.

## IV. Responsibilities for requirements

To systematically approach at a distinction between requirements that can be implemented by the employee and requirements that need an expert from the employer, we define two prerequisites.

**Prerequisite 1:** The implementation of the requirement must be within the abilities defined in the role specification from Table I. In particular, for each requirement, we need the following questions answered with ”yes”:

- Has the requirement an impact on the user's professional tasks or business processes?
- Is the requirement within the user's typical activities with work equipment or software applications?
- Are the user's qualifications sufficient to appropriately meet the requirement?

**Prerequisite 2:** The requirement cannot be implemented at the employer's site.

If Prerequisites 1 and 2 are met, the user has the abilities and the responsibility to implement a requirement. If this is not the case, the requirement must be implemented by an expert.

Observe that some requirements for home-office users are among the typical tasks for an expert in the employer's IT department. It is the IT department which configures laptops, installs software or manages VPN tunnels. Thus, such tasks are addressed before the employee is sent into home office.

**Example:** *With our home-office scenario, an anti-virus application has been installed on the employee's laptop. This application is associated with Basic requirement SYS.3.1.A4 ”Use of Anti-Virus Programs”. Because the employee has been ordered to use it, it is part of his professional tasks. The employee needs to handle virus warnings or requests to accept fresh virus signatures, i.e., it is within his typical activities with the laptop. The employer has provided a training on how to use the anti-virus software. Finally, the daily use of the anti-virus application cannot take place at the employers site. Thus, Prerequisites 1 and 2 are met, and requirement SYS.3.1.A4 is within the responsibilities of the employee.*

Reconsider Table IV. All bold requirements fulfill both prerequisites and must be implemented by the home-office user in order to extend the company's security concept, level ”Basic”, to the user's home office.

To our surprise, this number of requirements is rather small. All other basic requirements must be implemented with the help of experts of the IT department, either via bringing-in the laptop, via hotline support, or by visiting the user.

TABLE IV
BASIC REQUIREMENTS FOR A MINIMAL HOME OFFICE

| *ID* | *Description* |
|---|---|
| **APP.1.1.A2** | **Limiting Active Content** |
| **APP.1.1.A3** | **Opening Documents from External Sources** |
| APP.1.1.A7 | Awareness of Specific Office Properties |
| APP.1.2.A1 | Using Sandboxing |
| APP.1.2.A2 | Encryption of Communications |
| APP.1.2.A3 | Using Certificates |
| **APP.1.2.A4** | **Version Checking and Updates for (...)** |
| APP.5.3.A1 | Secure configuration of e-mail clients |
| APP.5.3.A2 | Secure operation of e-mail servers |
| APP.5.3.A3 | Data backup and archiving of emails |
| APP.5.3.A4 | Spam and virus protection on e-mail servers |
| APP.6.A1 | Planning the software useage |
| APP.6.A2 | A requirements catalog for software |
| APP.6.A3 | Secure procurement of software |
| APP.6.A4 | Installation and configuration of software |
| APP.6.A5 | Secure installation of software |
| DER.2.1.A1 | Definition of a Security Incident |
| DER.2.1.A2 | Policy for Handling Security Incidents |
| DER.2.1.A3 | Responsibilities for Security Incidents |
| DER.2.1.A4 | Notification for Security Incidents |
| DER.2.1.A5 | Remedial Action for Security Incidents |
| DER.2.1.A6 | Recovering after Security Incidents |
| DER.2.3.A1 | Creation of a Management Committee |
| DER.2.3.A2 | Deciding on a Clean-Up Approach |
| DER.2.3.A3 | Isolation of Affected Network Segments |
| DER.2.3.A4 | Blocking and Changing Access Data (...) |
| DER.2.3.A5 | Closing the Initial Entry Route |
| DER.2.3.A6 | Returning to Production Operations |
| CON.2.A1 | Implementing the Standard Data Protection Model |
| CON.3.A1 | Determining the Factors for Backups |
| CON.3.A2 | Stipulating Backup Procedures |
| CON.3.A4 | Drawing Up a Minimum Backup Concept |
| CON.3.A5 | Regular Backups |
| CON.6.A1 | Regulations for Deleting/Destroying Information |
| CON.6.A2 | Disposal of Sensitive Resources and Information |
| CON.6.A11 | Deletion of Data by External Service Providers |
| CON.6.A12 | Minimum Requirements for Deletion |
| NET.1.1.A1 | Network Security Policy |
| NET.1.1.A2 | Documentation of the Network |
| NET.1.1.A3 | Specification of Network Requirements |
| NET.1.1.A4 | Network Separation in Security Zones |
| NET.1.1.A5 | Client-Server Segmentation |
| NET.1.1.A6 | End Device Segmentation for Networks |
| NET.1.1.A7 | Protection of Sensitive Information |
| NET.1.1.A8 | Basic Protection of Internet Access |
| NET.1.1.A9 | Communication with Untrusted Networks |
| NET.1.1.A10 | DMZ Segmentation for Internet Access |
| NET.1.1.A11 | Communication with the Internet |
| NET.1.1.A12 | Protection of Outgoing Communication |
| NET.1.1.A13 | Network Planning |
| NET.1.1.A14 | Implementation of Network Planning |
| NET.1.1.A15 | Regular Gap Analysis |
| NET.1.2.A1 | Network Management Planning |
| NET.1.2.A2 | Network Management Requirements |
| NET.1.2.A6 | Regular Backups |
| NET.1.2.A7 | Basic Logging of Events |
| NET.1.2.A8 | Time Synchronisation |
| NET.1.2.A9 | Network Management Communication |
| NET.1.2.A10 | Limitation of SNMP Communication |
| NET.2.1.A1 | Definition of a Strategy for WLAN Usage |
| NET.2.1.A2 | Selection of a Suitable WLAN Standard |
| NET.2.1.A3 | Selecting Crypto Methods for WLAN |
| NET.2.1.A4 | Suitable Location of Access Points |
| NET.2.1.A5 | Secure Basic Configuration of Access Points |
| NET.2.1.A6 | Secure Configuration of WLAN Clients |
| NET.2.1.A7 | Setting Up a Distribution System |
| NET.2.1.A8 | Procedures for WLAN Security Incidents |
| NET.2.2.A1 | Creating a User Policy for WLAN |
| NET.2.2.A2 | Awareness and Training of WLAN Users |
| NET.2.2.A3 | WLAN Usage in Insecure Environments |
| NET.3.1.A1 | Basic Configuration of a Router or Switch |
| **NET.3.1.A2** | **Installing Updates and Patches** |
| NET.3.1.A3 | Restrictive Granting of Access Rights |
| NET.3.1.A4 | Protection of Administration Interfaces |
| NET.3.1.A5 | Protection Against Fragmentation Attacks |
| NET.3.1.A6 | Emergency Access to Routers and Switches |
| NET.3.1.A7 | Logging on Routers and Switches |
| NET.3.1.A8 | Regular Backups |
| NET.3.1.A9 | Operational Documentation |
| OPS.1.1.3.A1 | Concept for Patch and Change Management |
| OPS.1.1.3.A2 | Specification of Responsibilities |
| OPS.1.1.3.A3 | Configuration of Auto-Update Mechanisms |
| OPS.1.1.3.A15 | Regular updating of IT systems and software |
| OPS.1.1.3.A16 | Searching for patches and vulnerabilities |
| OPS.1.1.4.A1 | A Concept for Protection Against Malware |
| OPS.1.1.4.A2 | System-Specific Protection Mechanisms |
| OPS.1.1.4.A3 | Virus Protection for End Devices |
| **OPS.1.1.4.A5** | **Operating Virus Protection Programs** |
| **OPS.1.1.4.A6** | **Updating Virus Protection and Signatures** |
| OPS.1.1.4.A7 | User Awareness and Obligations |
| **SYS.2.1.A1** | **User Authentication** |
| **SYS.2.1.A3** | **Activation of Automatic Update Mechanisms** |
| **SYS.2.1.A6** | **Use of Anti-Virus Programs** |
| SYS.2.1.A8 | Protection of the Boot Process |
| SYS.2.1.A42 | Use of cloud and online functions |
| SYS.3.1.A1 | Rules for Mobile Laptop Use |
| **SYS.3.1.A2** | **Laptop Access Protection** |
| **SYS.3.1.A3** | **Use of Personal Firewalls** |
| SYS.3.1.A9 | Secure remote access with laptops |
| SYS.4.5.A1 | Awareness for handling removable media |
| SYS.4.5.A2 | Loss or manipulation report |
| SYS.4.5.A10 | Volume encryption |
| SYS.4.5.A12 | Protection against malware |

## V. DISCUSSION

The focus of our work was to extend the company's security concept to the user's home office in a standardized way that is compatible with a certification from BSI. To approach at a minimal but comprehensive set of requirements, we have started with a minimal home office scenario that includes customer data. In consequence, the Basic requirements from Table IV must be fully implemented for any home-office scenario using customer data. We have found out that this includes much help from an security expert of the employer.

In some home-office scenarios, employers would equip their employees with additional devices, such as tablets or smartphones, or maybe with other categories of applications, such as database systems. The requirements for operating the company's own hardware and software in the home office can also vary greatly. In such cases, the list of requirements in Table IV must be extended. Recall that our minimal scenario did not make any assumptions on the operating systems and business applications used. Therefore, first candidates for further BSI modules are SYS.3.2.4 ”Android”, SYS.2.4 ”macOS Clients” or SYS.2.2.3 ”Windows 10 Clients”.

The procedure to extend this list of requirements is identical to the research method we have used in this paper: It starts by widening the scope of the information domain. The next step is to research further BSI modules, followed by an assessment of the implementation status of the additional requirements with the IT-Grundschutz Check. The core protection of the BSI-standard 200-3 [17] uses the same approach. Core protection means to secure the most vulnerable subset of the information domain first, and to extend this protection at a later time.

Our approach is adaptable to other certifications, e.g., based on the NIST Cybersecurity Framework [3]. The IT-Grundschutz Compendium is organized in various process layers and system layers, while the Cybersecurity Framework is organized in the categories ”Identify”, ”Protect”, ”Detect”, ”Respond” and ”Recover”. However, both approaches use a comparable methodology. The BSI role ”Data User” [10]” corresponds to the NIST role ”Information System User” [18]. Furthermore, the requirements in the modules of the IT-Grundschutz Compendium have their counterparts in the controls of the Cybersecurity Framework. For example, BSI module ”CON.3 Backup Concept” names requirements that are a subset of the imperatives in the NIST control family ”CP: Contingency Planning”. Finally, both IT-Grundschutz Compendium and NIST Cybersecurity framework can be mapped to the ISO 2700x series of standards [2].

## VI. Conclusion

With the Basic Protection from the 200-2 standard, the BSI provides companies with a comprehensive guide to implement a defined level of IT-security in a company-wide IT-infrastructure. This security level can be audited and certified, which is mandatory in many sectors of industry and business. However, the BSI considers home-office users as a risk that is external to the company’s infrastructure. In consequence, home-office users must have restricted access to company assets, which restricts the business tasks that can be carried out at home.

In this paper, we have investigated which requirements must be implemented in a minimal home-office scenario with customer data in order to obtain the BSI protection level ”Basic”. Furthermore, we have used a definition for a home-office user, to find out which of those requirements can be implemented by the user.

We have observed that the number of requirements that need a security expert from the company is manageable for a small home-office scenario, and we have discussed how to extend this scenario for more complex settings. Our findings are a first step towards creating an IT-Grundschutz profile for a home office, to simplify security management for employees in a home office, while ensuring a certified security policy at the same time.

## References

[1] Federal Office for Information Security, “BSI IT-Grundschutz Kompendium Edition 2021,” https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html [accessed: July 2021], 2021.

[2] ISO/IEC/IEEE, “The ISO/IEC 27000 Family of Information Security Standards,” https://www.itgovernance.co.uk/iso27000-family [accessed: July 2021], 2015.

[3] National Institute of Standards and Technology, “SP 800 series on Information Security and Cybersecurity Practice Guides,” https://csrc.nist.gov/publications/sp800 [accessed: July 2021], 2020.

[4] FAZIT Communication GmbH in cooperation with the Federal Foreign Office Berlin, “The Federal Government informs about the Corona crisis,” https://www.deutschland.de/en/news/german-federal-government-informs-about-the-corona-crisis [accessed: July 2021], 2021.

[5] M. Bispham, S. Creese, W. H. Dutton, P. Esteve-Gonzalez, and M. Goldsmith, “Cybersecurity in working from home: An exploratory study,” Available at SSRN 3897380, 2021.

[6] S. Cooper, “How to secure your home wireless network,” https://www.comparitech.com/blog/information-security/secure-home-wireless-network/ [accessed: July 2021], 2020.

[7] NortonLifeLock Inc., “Keep your home Wi-Fi safe in 7 simple steps,” https://us.norton.com/internetsecurity-iot-keep-your-home-wifi-safe.html [accessed: July 2021], 2020.

[8] D. Nield, “How to Secure Your Wi-Fi Router and Protect Your Home Network,” https://www.wired.com/story/secure-your-wi-fi-router/ [accessed: July 2021], 2020.

[9] Federal Office for Information Security, “IT-Sicherheit im Home Office,” https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/checkliste-home-office_mitarbeiter.html [accessed: July 2021], 2020.

[10] Federal Office for Information Security, “BSI-Standard 200-2: IT-Grundschutz-Methodology,” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.html [accessed: July 2021], 2017.

[11] Federal Office for Information Security, “Guide to Basic Protection based on IT-Grundschutz,” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/Basic_Security.html [accessed: July 2021], 2017.

[12] Federal Office for Information Security, “BSI IT-Grundschutz Compendium Edition 2019,” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-it-gs-comp-2019.html [accessed: July 2021], 2019.

[13] Conference of Independent German Federal and State Data Protection Supervisory Authorities, “The Standard Data Protection Model,” https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf [accessed: July 2021], 2020.

[14] C. Haar and E. Buchmann, “Securing Orchestrated Containers with BSI Module SYS.1.6,” in Proceedings of the 7th International Conference on Information Systems Security and Privacy, 2021.

[15] ISO/IEC/IEEE, “ISO/IEC12207:2017 Systems and software engineering Software life cycle processes,” https://www.iso.org/standard/63712.html [accessed: July 2021], 2008.

[16] ISO/IEC/IEEE, “ISO/IEC/IEEE 15288:2015 Systems and software engineering  System life cycle processes,” https://www.iso.org/standard/63711.html [accessed: July 2021], 2015.

[17] Federal Office for Information Security, “BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz,” https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html [accessed: July 2021], 2017.

[18] National Institute of Standards and Technology, “NIST Special Publication 800-100: Information Security Handbook – A Guide for Managers,” https://csrc.nist.gov/publications/detail/sp/800-100/final [accessed: August 2021], 2020.