Bachelor's thesis

Degree programme in Information and Communications Technology

2022

Philipp M. Woolaway

SECURING theFIRMA

– Creating a comprehensive Cyber Security concept for theFIRMA

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree programme in Information and Communications Technology

2022 | 31, 11

Philipp M. Woolaway

SECURING theFIRMA

- Creating a comprehensive Cyber Security concept for theFIRMA

The student-run simulated company theFIRMA is analyzed from a cyber security perspective, taking into consideration the context and needs of this Turku AMK project. Theoretical concepts such as security standards and frameworks are illustrated. Available options for security improvement within the Microsoft infrastructure used by the university are identified and defined.

The relevant findings are categorized into three pillars of action: physical security, software security and awareness training.

Physical security focuses on hardware solutions for the perimeter of the company premises and on an improvement of access control for employees and guests.

The section software security addresses key issues in the prevention of unauthorized access, in the running of unwanted or malicious software and suggests solutions to harden the company network.

The main pillar illustrates awareness training for both employees and administration. The aim is to create a persistent focus on cyber security and data protection within the company projects, shifting to a mentality of security by design and giving administration tools to better protect and supervise company employees and resources.

KEYWORDS:

Cyber security, awareness training, information and communications technology, information security management, theFIRMA

CONTENT

LIST OF ABBREVIATIONS **5**

1 INTRODUCTION **6**

2 THEORY BEHIND THE THESIS **7**

2.1 Security standards and frameworks 7

2.1.1 ISO/IEC 27000-series 7

2.1.2 NIST Cybersecurity Framework 9

2.2 Legal requirements 10

2.3 Security best practices 11

2.4 Security tools in the Microsoft environment 12

2.4.1 User device monitoring 12

2.4.2 Endpoint configuration management 13

2.4.3 Securing access 13

3 PRACTICAL WORK AND PROCESSES **14**

3.1 Physical security 14

3.1.1 Physical access control 16

3.1.2 User owned devices (UoDs) 17

3.1.3 Preventing damage through storage devices 18

3.2 Software security 20

3.2.1 Legacy boot and running Wireshark 20

3.2.2 Software Center and temporary rights 22

3.2.3 Portable Apps and network hardening 23

3.3 Awareness training 25

3.3.1 Awareness training material 25

3.3.2 Awareness and control tools for administration 26

4 RESULTS AND CONCLUSIONS **29**

5 REFERENCES **30**

APPENDICES

Appendix 1. Interviews with relevant parties at theFIRMA
Appendix 2. Awareness training presentation

FIGURES

Figure 1: adoption of ISO 27000 in Italian companies and public administration in 2016 (Statista, 2020) 8
Figure 2: usage of security frameworks in U.S. healthcare in 2018 (Statista, 2019) 9
Figure 3: screenshot of options in MIFARE Classic Tool Version 2.3.1 15
Figure 4: view of boot options on a theFIRMA workstation 21
Figure 5: view of disabled Secure Boot on a theFIRMA workstation 21
Figure 6: view of Wireshark run from a live Xubuntu USB-Stick in a theFIRMA workstation 22
Figure 7: a checklist of tasks when an employee quits at theFIRMA 27

LIST OF ABBREVIATIONS

Abbreviation	Explanation of abbreviation (Source)
AD	Active Directory (Microsoft)
CISO	Chief Information Security Officer
GDPR	General Data Protection Regulation (European Union)
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
NIST	National Institute of Standards and Technology (United States Department of Commerce)
UAC	User Account Control (Microsoft)
UoD	User Owned Device
VPN	Virtual Private Network

1 INTRODUCTION

The thesis is aimed at analysing the cyber security situation in theFIRMA and consequently developing a comprehensive security concept for theFIRMA. theFIRMA is a project within Turku University of Applied Sciences, consisting of a company that is simulated and run in the university's premises. This company is entirely run by students and it works on university tasks and external customer projects, whilst being supervised and counselled by TUAS staff members. Since the company has steadily increased in volume and takes on many external projects, it is of vital importance to create a basis to secure its operations and train its employees. The aim must be adjusted to the nature of the company, to its unique characteristics and to its budget. The suggestion and implementation of industry best-practices was divided into three main pillars: physical security, software security and awareness training. Each of these topics was analysed through interviews with parties within theFIRMA and elaborated through assessments and previous experiences in this field. The expected result was to secure theFIRMA to an acceptable degree, to suggest future optimization of the company's security approach and to create a sense of awareness and cooperation on the topic amongst the students working in the company.

2 THEORY BEHIND THE THESIS

2.1 Security standards and frameworks

Cyber security standards, often also referred to as cyber security frameworks, are collections of standardised techniques, guidelines and procedures, created by organizations, commissions or institutes as a common reference for companies within this field. They are generally used to perform evaluations on companies, to identify and mitigate risks and to define protocols to follow in order to maintain an adequate level of security. The most popular standards can be applied to companies of different sizes and are broad in scope, i.e. they are adaptable to organisations in different business areas.

The two most notable standards in the cyber security field are the ISO/IEC 27000-series (ISO27K) and the NIST Cybersecurity Framework (NIST CSF). There are also standards specific to certain industries, such as the NERC 1300 for electric systems (North American Electric Reliability Council, Effective Date: June 1, 2006) and ANSI/ISA 62443 for industrial automation and control systems (International Society of Automation, 2018). These are typically used for companies that have very specific security requirements, operate in a clearly defined field or only need to ensure security certifications and compliance for a limited part of their business operations.

2.1.1 ISO/IEC 27000-series

The ISO/IEC 27000-series was developed and is maintained by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and consists of nearly fifty different standards. It is typically referred to as an information security management system (ISMS), i.e. a comprehensive set of guidelines and security controls that forms a system aimed at managing all cyber security related operations within a company. It is becoming the de-facto standard in the European Union, as it has been given the status of European Standard by Technical Committee CEN/CLC/JTC 13 “Cybersecurity and Data Protection”. As such, it has replaced national standards of member states in this field as of August 2020. (International Organization for Standardization (ISO), 2018) This should speed up an otherwise slow adoption of this family of standards within member countries. For

example, over 60% of companies and public administration in Italy had not implemented the requirements of ISO/IEC 27000 in 2016 (Figure 1).

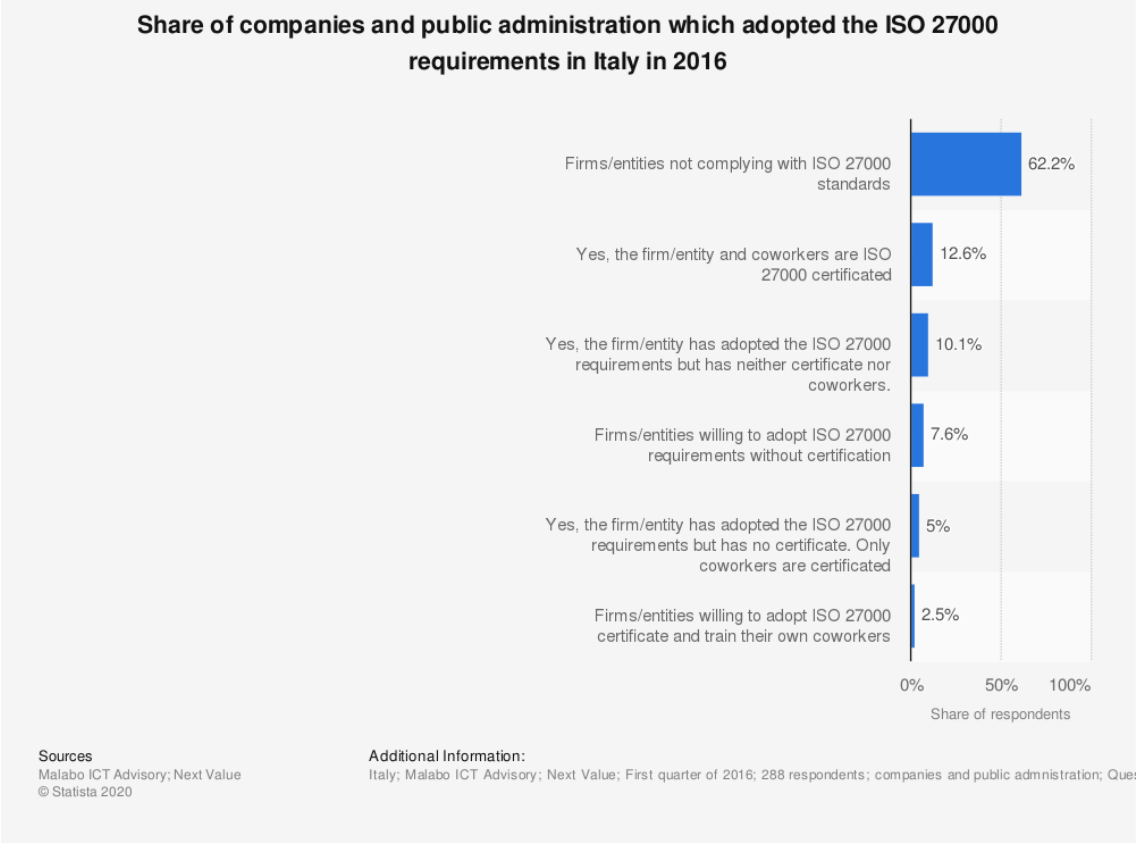


Figure 1: adoption of ISO 27000 in Italian companies and public administration in 2016 (Statista, 2020)

The first and main standard is ISO/IEC 27001, which is based on the Plan-Do-Check-Act (PDCA) cycle, defined in the standard as providing requirements for establishing, implementing, maintaining and continually improving an information security management system. (International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2017, p. 5) A more specific description of these processes is given in the subsequent standards, which are also often interlinked and contain multiple cross-references between the documents.

Some of the most adopted and detailed standards are:

1) ISO/IEC 27001: details how an information security management system is set up, supported and enhanced over time
2) ISO/IEC 27003: offers guidance on the implementation of ISO/IEC 27001

3) ISO/IEC 27004: determines tools to measure performance and effectiveness of implemented information security measures
4) ISO/IEC 27005: delivers recommendations and methods for information security through risk assessment and management

(International Organization for Standardization (ISO), 2018, pp. 19-21)

2.1.2 NIST Cybersecurity Framework

The NIST Cybersecurity Framework is a set of policies devised by the National Institute of Standards and Technology, an agency of the United States Department of Commerce. It was originally aimed at enabling the analysis and protection of critical infrastructure, i.e. supplies and facilities that ensure that a society and its economy remain operational under adverse circumstances. Nowadays it is implemented by many private businesses, as well as some foreign governments, and is mainly used in the United States of America. This is exemplified by research on U.S.A. healthcare organizations, of which nearly 60% were using the NIST framework to manage cyber security as of 2018 (Figure 2).

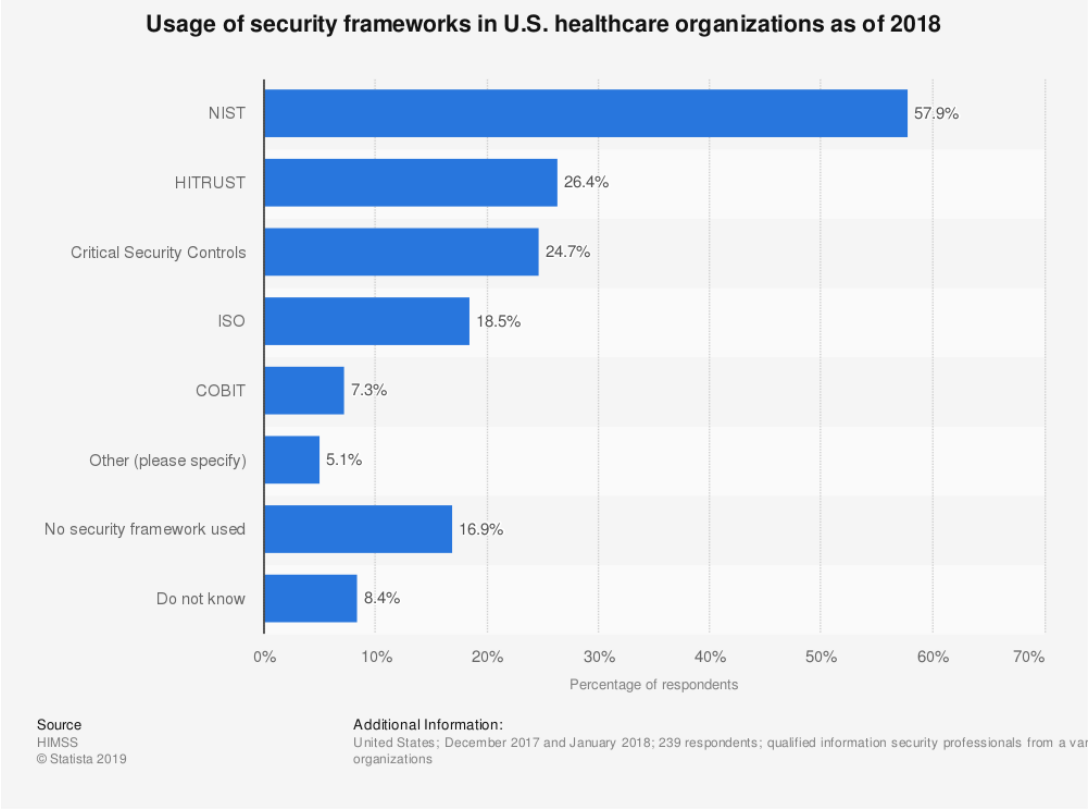


Figure 2: usage of security frameworks in U.S. healthcare in 2018 (Statista, 2019)

The NIST CSF follows the cycle Identify, Protect, Detect, Respond, Recover. These are known as concurrent and continuous Functions and they constitute the Framework Core. The framework consists of three components in total, each of which targets a specific part of the process:

1) The Framework Core: aimed at controlling and lowering information security risks present in an organization
2) Framework Implementation Tiers: helps contextualize an organization's approach to information security management and its approach to risks
3) A Framework Profile: indicates an organization's unique situation compared to aims defined through the Framework Core, showing possible areas in need of development

(National Institute of Standards and Technology, 16.04.2018, pp. 3-4)

These components can be compared with specific standards from the ISO/IEC 27000-series, as the Framework Core is similar in scope to the ISO/IEC 27001 standard. Conversely, the Framework Implementation Tiers show parallel elements to the ISO/IEC 27005 standard.

2.2 Legal requirements

It is an obligation for companies and organisations to respect and enforce local legal requirements and regulations, based on their country of registration. This can refer to legislation specific to a certain administrative area or region, as well as to national or international laws and agreements. Such laws and obligations can be specific to a certain field of business or find application in organisations throughout all industries. An example of the latter is the European Union's General Data Protection Regulation (GDPR), issued in 2016. This regulation, aimed at protecting personal data and the processing of it, applies to any organisation handling data of subjects within the European Economic Area (EEA), regardless of the country of registration of the organisation and the citizenship or residence of the data subject. In this case the law is specific to the areas of data processing and transfer, but applies to any data originating from within the EEA and any establishment wishing to deal with such data, therefore applying to any industry. (The European Parliament and the Council of the European Union, 04.05.2016)

In case of subsidiary or affiliate organisations, internal policies and regulations are often passed on by the parent company through what is known as downstreaming. This refers to passing on existing procedures to the subsidiary, typically on issues and fields that are relevant to both organisations. The subsidiary usually implements these and expands or changes them according to its specific needs, while having to comply with them at their core.

2.3 Security best practices

Best practices are non-binding suggestions on procedures that have been identified and accepted by an industry as producing the superior result. They are not legal requirements and can be subject to quick change based on the development of the industry. Best practices can be used as a basis to create policies within a company and are often grouped and described in publications by organisations or companies such as the European Union Agency for Cybersecurity (ENISA) or Norton. Examples for this are the paper *Pseudonymisation techniques and best practices report* by ENISA (European Union Agency for Cybersecurity (ENISA), 2019) and online guide *10 cybersecurity best practices that every employee should know* by Norton. (NortonLifeLock Inc., n.d.)

Best practices are sometimes integrated with due diligence. This expression refers to different notions: in legal terms it defines the care that a reasonable person exercises to avoid harm to other persons or their property; in business terms it refers to research and analysis of a company or organization done in preparation for a business transaction (such as a corporate merger or purchase of securities). (Merriam-Webster, n.d.) In cyber security the term is typically used referring to both aforementioned definitions: when assessing its security operations and improving defence systems, the company is preparing for future events. When applying legal requirements and best practices, the organisation is safeguarding its obligations and acting in a moral, sensible and accountable way.

An example for a best practice, which can be considered due diligence at the same time, is the application of least privileges. This is a procedure where users of a system are only granted the minimum of privilege, i.e. access to data, authority etc., which is necessary for them in order to be able to carry out their duties. It is best practice as it is a widespread method of making sure data is only accessed by parties that are authorized to view or use it and need the data to complete tasks; at the same time it is due diligence,

as it helps an organization ensure it has limited users' access to data to a reasonable degree and can therefore not face consequences or legal action in respect to this practice. Another similar example is the use of awareness training: it is best practice to keep employees up to date with the latest security procedures as to not fall behind the competition. However, it is also due diligence, as the employees must act within the legal framework and in compliance with the security policies of the company.

2.4 Security tools in the Microsoft environment

Within the Microsoft ecosystem there are many tools to secure a company's IT infrastructure at the endpoint level, as well as to regulate user access to functionality and applications. These tools need to be accessible to administrators and can be used to monitor and safeguard different features on an enterprise's machines.

The features can be divided into three main categories:

1. User device monitoring
2. Regulating applications and permissions
3. Securing access

2.4.1 User device monitoring

User device monitoring is used to ensure the safety and integrity of company data on devices controlled by users, especially regarding mobile devices such as smartphones, tablets or laptops which can be transported to a location outside the enterprise's premises and secured network infrastructure. Microsoft's main tool to control such endpoints is Microsoft Intune. This is a suite to manage mobile devices and applications on company systems and on user owned devices, which are used for company purposes and privately at the same time. Devices that are managed via Microsoft Intune can be configured remotely and in bulk, they can be monitored and also locked and wiped, i.e. in case of theft, as to protect the intellectual property they might contain. (Microsoft, n.d. a)

The deployment of software on, and management of, mobile devices can be handled via Microsoft Intune, which integrates with solutions available for workstations within the

company premises. These fixed endpoints are controlled via the Microsoft Configuration Manager, a tool to secure and administrate applications and operating system settings.

2.4.2 Endpoint configuration management

A solution that is part of the Microsoft Endpoint Configuration Manager is the Software Center. This tool allows system administrators to manage which software is installed on endpoints. These configurations can be set on a per machine basis or on different groups of workstations. The Software Center also allows for version control, i.e. it gives the possibility to prevent or reverse the updating of a certain application if new features have not yet been tested and approved by administrators. (Microsoft, n.d. b)

A set of security solutions that protect access to the operating system is available for mobile and fixed workstations. These solutions work on the level of the firmware running the initialization of hardware upon boot. Namely, two solutions are UEFI and Secure Boot: the first is the successor to legacy BIOS firmware and to previous EFI specifications by Intel. The latter is a security standard or protocol that prevents the execution of software that was not signed, and therefore approved, by the machine's manufacturer. (Microsoft, n.d. c)

2.4.3 Securing access

A security solution that is consequent to the deployment of UEFI and Secure Boot is BitLocker, a tool that is employed to encrypt drives on a machine. This allows a user or administrator to prevent unauthorized access to the data contained on a machine's drives, both within the company premises as outside, e.g. if the drive is removed and stolen. (Microsoft, n.d. d)

User Account Control, UAC in short, was first introduced to the Microsoft ecosystem in Windows Vista and has since become an integral part of the operating system. It manages the elevation of privileges of the user when using apps or executing tasks, thus preventing the unwanted installation of software or the access to services by unauthorized parties. (Microsoft, n.d. e)

3 PRACTICAL WORK AND PROCESSES

The initial evaluation was carried out by conducting interviews with the CISO and two system administrators, during which theFIRMA's situation was assessed and detailed. Personal tests were carried out following the evaluation, as to verify the initial findings. After that, the ISO27000 family of standards was used as a guideline to carry out a more thorough analysis of possible risks and vulnerabilities. Tests based on previous professional experience were also conducted as integration to the theoretical analysis.

After a variety of issues was identified, the proposed countermeasures were elaborated and categorized in one of three main pillars: physical security, software security and awareness training. While the first two aimed at fixing existing or likely vulnerabilities, the awareness training is primarily aimed at creating a baseline knowledge for cyber security in theFIRMA and to make the relative topics part of the development culture of the employees. An important part of this is making the employees understand that these operations are not carried out against them and that the implemented measures are set up to protect them and incentivise an early-on implementation of security, thus avoiding future incidents. This is also known as security by design, a method that is increasingly gaining in popularity. It is becoming more common knowledge that the first line of defence must be the employees, as a centralized security team is very limited in its defensive capabilities if threats occur on multiple fronts and often does not receive information on infiltration attempts early enough. This is especially true for such attacks as phishing.

3.1 Physical security

The first perimetral security feature that protects physical premises is the walls and doors around the offices. The doors securing access to theFIRMA are standard interior doors, that are unlocked by using magnetic and/or RFID key cards which contain a unique identifier (UID) of the owner. Two main issues were identified with the doors and their locks: the first issue is that the doors are mounted on normal hinges, thus they can be pried open or unhinged with ease. The second issue is that the key cards used for the locks operate using the MIFARE Classic standard, which is also implemented throughout the TUAS ICT-City building. The first issue can be solved by building security door hinges

into the frames. There are three different types of security hinges on the market: security tab hinges, non-removable pin hinges and continuous hinges. Given the surveillance system already available inside TUAS and the fact that the doors to theFIRMA are internal to the building, as well as considering the limited budget of the company, the first variant was suggested as the most effective solution at a low price point.

The second issue is one that cannot be solved, but only mitigated and addressed through awareness training, as long as the standard utilized for the key cards remains unchanged. The MIFARE Classic standard is an early implementation of this type of access key cards and it is known to be vulnerable to easy cloning. Using an Android phone with NFC enabled, a potential attacker can copy the UID of any original MIFARE Classic card and then write the same UID on a rewritable card purchased for a few Euros (Figure 3: screenshot of options in MIFARE Classic Tool Version 2.3.1). As it is the standard itself that is flawed and there are no backward methods to fix it, the only way to

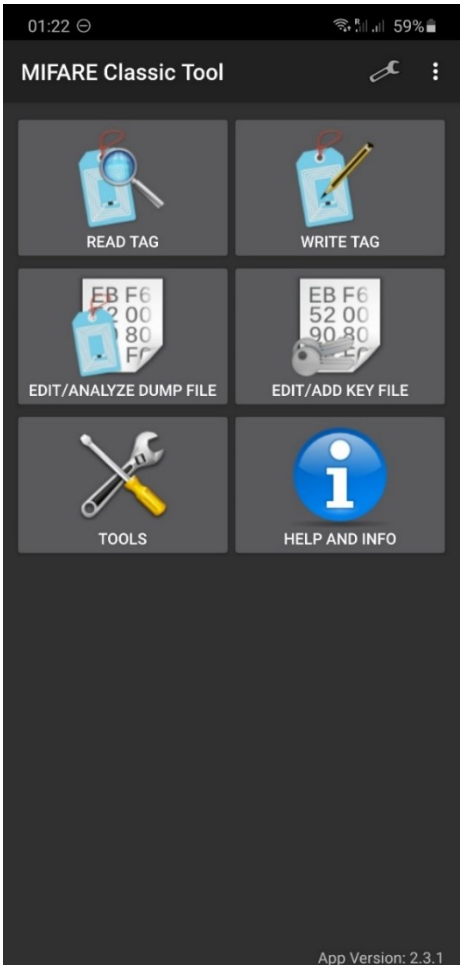


Figure 3: screenshot of options in MIFARE Classic Tool Version 2.3.1

mitigate the risks posed by this implementation is to train the card holders on how to handle their cards in a secure way.

3.1.1 Physical access control

Following the enhancement of the physical security of the premises, the access control to the premises must also be improved. Although access via personal key cards should prevent third parties from accessing theFIRMA's premises, the human element must be taken into consideration. During the assessment time at theFIRMA it was often observed that a simple knock on the door was enough to be allowed into the office by other students. Furthermore, there was no method in place to check an employee's identity or if the entrant should be allowed access to the premises. The only employees wearing an identifying badge were those in management, but their IDs were not printed with photos of the cardholders on them. This would allow a potential impersonator to easily pose as a member of management and to ask employees, especially if new to the company, to carry out certain actions for them or to reveal confidential information. The suggested solution to this risk is to implement a new badging system, where every employee obtains a badge with their name and a photo of them, along with a colour code identifying their role in the company. These badges are to be worn by employees at all times and can't be given to another person. The new badges are also necessary to gain access to theFIRMA when the employee doesn't own a key card. When this is the case, only upon presenting the badge will the student be let onto the premises. If the person trying to access the premises isn't a student, or can't be verified as one, they need to have a booked appointment with an employee of theFIRMA or have another employee verify their identity before access is granted.

The measures detailed previously are aimed at preventing unauthorized access to theFIRMA both in presence and absence of employees. However, should an unauthorized party manage to gain access to the premises and wish to steal hardware from within, it is recommended to secure valuable items such as monitors, workstations and laptops to the desks via Kensington Locks or similar tools. Those items that can't be secured in such a way or which must be mobile by nature, i.e. smartphones, presentation remotes etc., should be stored in lockable drawers or cabinets whenever not in use.

3.1.2 User owned devices (UoDs)

Another issue that needs to be addressed is user owned devices (UoDs), i.e. employees' personal devices which are brought into theFIRMA for both personal and professional use. A distinction has to be made between these use cases in regards to the security of the company, as they pose different threats to different assets.

In case of personal devices used for business purposes, these currently undergo an insufficient security verification: the user needs to present a current and alert-free scan result from their antivirus software of choice, after which the device is deemed safe to use. An in-depth analysis of the reliability of such scans would breach the scope of this work, but it can be assumed that they are insufficient to guarantee protection of both company data and theFIRMA's network. As theFIRMA provides workstations to those students actively involved in projects, it would be advisable to ban the usage of employees' private computers on the company's premises. However, in a situation where working from home or other places outside the company is necessary, this measure can't be applied and other solutions need to be identified to protect the company data being used or managed inappropriately by the employees. The possibility of using management software such as Microsoft Intune was suggested to the company for such cases, but the technical and legal implications and applicability could not fully be assessed at the time of writing this report.

In regard to personal devices that are brought onto theFIRMA's premises, but used only for personal scope, there are two main risks that need to be taken into consideration: physical damage and digital damage. The physical damage could result e.g. from an employee plugging a faulty device into a workstation or power outlet to charge it and, in a worst-case scenario, causing a fire hazard or other damage. As this is caused by a device not belonging to the company, it would likely not be covered by an insurance policy aimed at reimbursing such damages and therefore trigger major expenses for theFIRMA. Sensitisation on the implications of such actions is covered by the awareness training chapter.

3.1.3 Preventing damage through storage devices

The digital damage could result from plugging in a compromised device into a workstation, e.g. to charge it or to transfer files to and from it. In this case a further distinction has to be made between smartphones and storage devices, i.e. USB sticks, memory cards or external drives. As detailed above, personal smartphones should not be plugged into the workstations for charging because of insurance implications and they should also not be used as storage devices for company data. Furthermore, theFIRMA does not allow the use of company workstations for purposes other than the assigned projects, therefore a transfer of data from the employee's smartphone to the computer need not occur.

As far as personal or other external storage devices are concerned, they also pose the risk of a malware infection to the workstations as they have been used in an environment outside the company's control. Three possible solutions to this problem were identified, with increasing budget requirements and implementation complexity, but also growing ease of use and security. The simplest and cheapest solution is to ban all storage devices that do not belong to the company and to migrate to a cloud-only approach to file storage and sharing. The requirements for this should be covered by the Microsoft OneDrive solution included in TUAS' subscription plans with Microsoft. However, whilst this solution is simple to implement and would not cause any extra cost to the university or theFIRMA, there are three major potential problems that need to be taken into consideration. The first is that access to the files, or to their most recent version, always requires an internet connection. Whilst this should be granted in most scenarios, it is not a given e.g. during travel and could potentially have a high impact on the employees' ability to work and to comply with deadlines. The second issue with working from a cloud environment is the privacy and confidentiality of data. As theFIRMA takes on many external projects, it is not unlikely that some customers would disagree if personally identifiable information or confidential business information were uploaded to a potentially public or insecure environment. The third point is that, even if acting on the assumption of a secure environment, an easily made mistake could compromise the data. Especially in highly integrated environments such as the Office 365 suite, a click on the wrong file or failure to remember to encrypt communication could expose the handled data to the wrong receiver or even to a malicious third party.

The second solution to external storage devices could take the shape of a dedicated workstation running a Linux OS, into which the employee inserts their USB stick. The system would then transfer the contained data or selected files to a shared folder, from which the user could access it. Whilst this solution is quite economical, it is cumbersome on the end user, it implies a complex setup within the company network and can lead to bottlenecks especially at the beginning of shifts, when many employees need access to their data at the same time.

The last proposed solution is an evolution of the previous idea: instead of implementing a centralized solution, the same approach is applied to every workstation. This would mean that every desk is fitted with a single-board computer, such as a Raspberry Pi, running Linux. The user can then plug in their USB stick into this computer instead of the workstation and access the data via a local LAN connection. This would solve the potential bottleneck described above as well as granting a more secure and confidential handling of the data the employee is trying to access. The main issue with this last solution is that it requires a large one-time investment to fit every workstation with such a computer, as each of them costs an average of ca. 40-50 €. However, a further bonus of the second and third approach is that the environments are more secure, as the Linux operating system is not vulnerable to most malicious attacks and could filter infected data before it is accessed on a Windows workstation.

Experiments for these solutions also led to the implementation of a throwaway machine, a PC equipped with a malware scanner and not connected to any device or network. What this laptop is intended for is to be used by employees if they find external drives or similar hardware of which they do not know the provenance. A simple but effective attack on companies, which has often been observed, is to leave USB sticks with malware lying in a parking lot or other area near an office building. The employees are often overcome by curiosity and will plug in the infected hardware to their workstation in order to see what it contains. The throwaway machine was set up for such cases, i.e. to safely access an unknown device without the risk of infecting or compromising theFIRMA’s network and workstations.

3.2 Software security

3.2.1 Legacy boot and running Wireshark

Starting at the firmware level of the workstations, the BIOS settings on various systems were analysed. The findings confirmed what was suggested during the initial interviews with relevant parties, i.e. that most systems were running with a legacy setup of the BIOS, with no UEFI or Secure Boot enabled. (Figure 4, Figure 5) This is relevant from a security perspective for two main reasons: to ensure there has been no tampering with the boot process e.g. by malware and to prevent booting from an external device, such as a live USB stick. The latter was tested on different machines by inserting a live USB stick running Xubuntu. Since the BIOS was not locked down, booting from the external device didn't require any further setup and the system could be used to access the network and the local workstation's drive. This would potentially allow unwanted access to locally stored data and it wouldn't prevent a malicious third party from downloading and installing tools such as Wireshark, ZenMap or Metasploit that could then be used against the company.

A running instance of Wireshark, installed as detailed above, was run on one of the workstations. (Figure 6) This was configured not to have access to the network peripherals of its host, as snooping traffic on a common network constitutes a major privacy violation. The reason the attack used above is successful in accessing the local hard drives without any further setup is that the workstations are not using any encryption on the installed drives. If the drive is therefore mounted to another operating system through a live medium or removed from the housing and installed in a different computer, nothing prevents access to the data it contains, which can be tampered with or shared without the owner of the drive present.

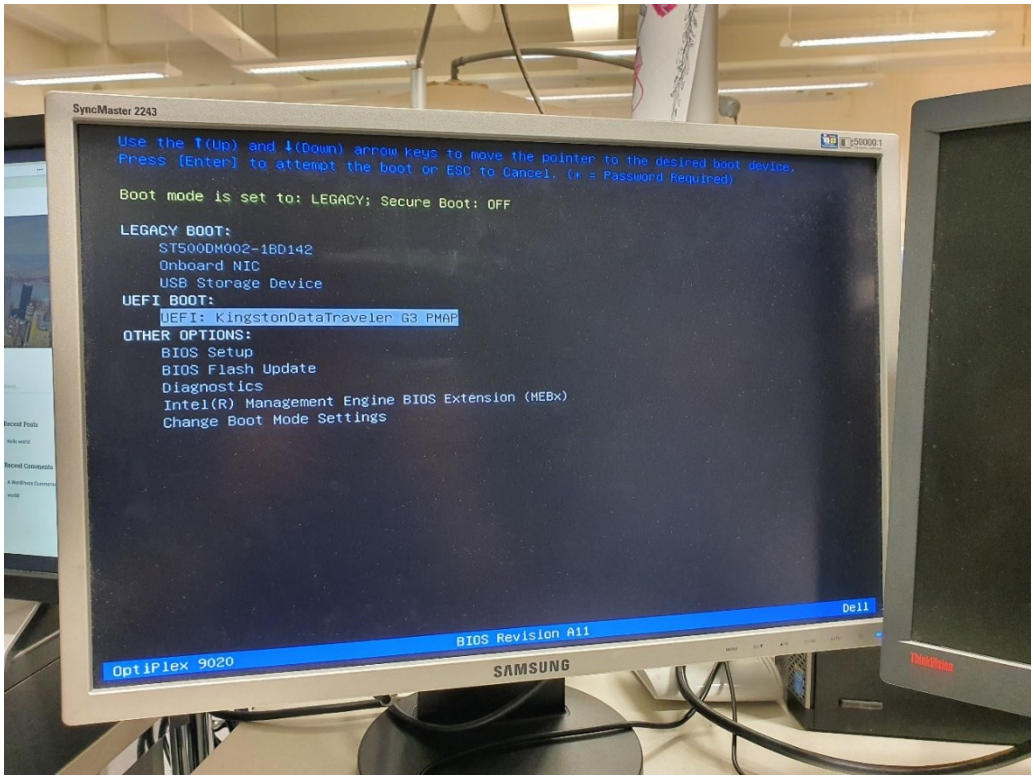


Figure 4: view of boot options on a theFIRMA workstation

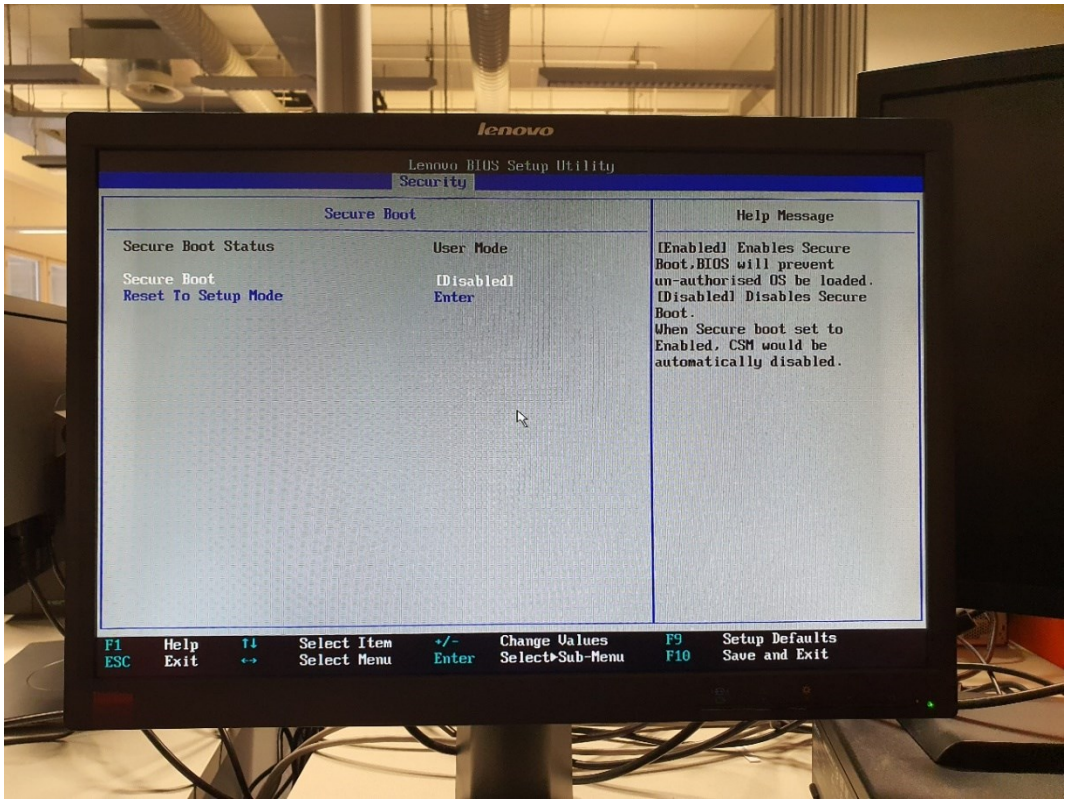


Figure 5: view of disabled Secure Boot on a theFIRMA workstation

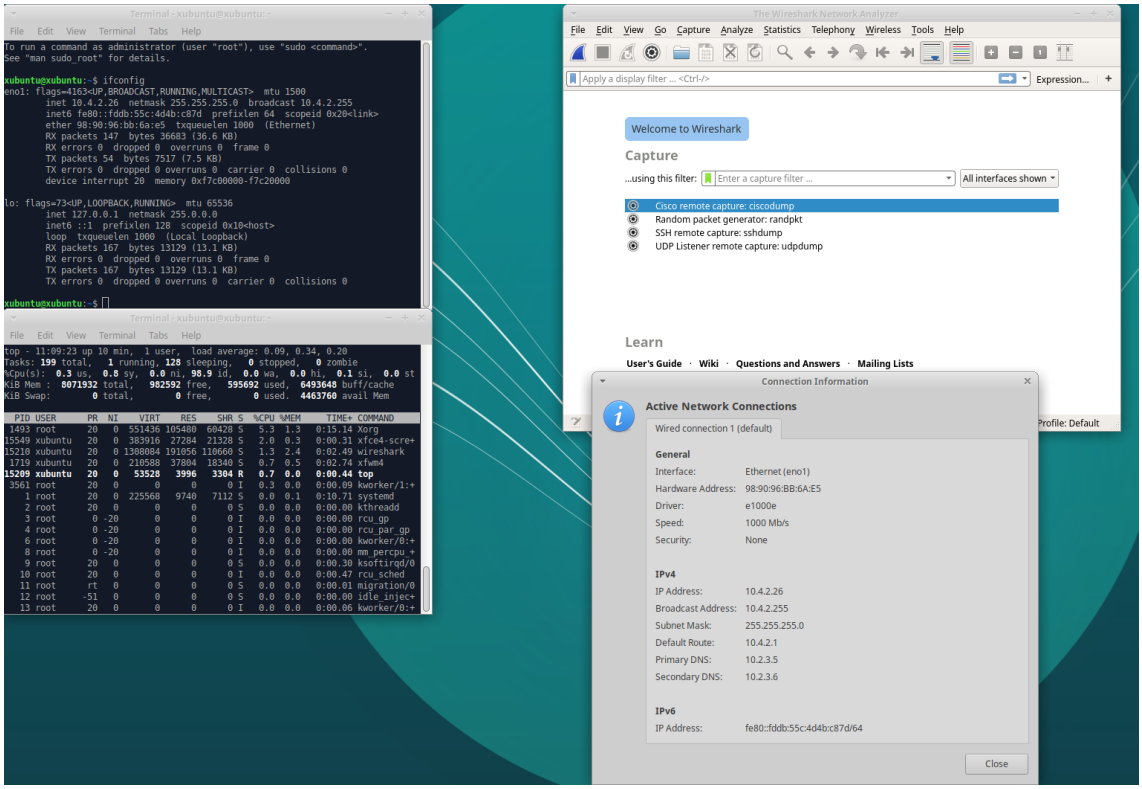


Figure 6: view of Wireshark run from a live Xubuntu USB-Stick in a theFIRMA workstation

A simple solution to this would be to ensure the encryption of all drives in the workstations through the activation of BitLocker. As Microsoft Windows' native solution to encrypt drives or volumes it can be easily set up, but only after the BIOS has been configured to UEFI and Secure Boot has been enabled. A further advantage of using BitLocker is that its key management and verification system can be directly implemented into the Active Directory of theFIRMA. This would ensure the encryption of the drives whilst removing the necessity for users to set up local passwords for their drives, which they might not remember or forget to share with their successor, thus preventing any further access to the drive.

3.2.2 Software Center and temporary rights

A useful feature that comes with the AD integration is implementing the Software Center, an administrative tool to centrally manage and trigger installations of software on Microsoft Windows endpoints, i.e. the workstations in theFIRMA's case. This allows the company's administration to have control over what software is installed on each system and makes it possible to remove local administrative rights from end users, as most of

them do not require such broad authority for their typical work routine and processes. It should be made possible to grant temporary rights and to unlock features for a limited time through scripting or more elaborate account management. This would allow a user that requires administrative privileges for their current project to dynamically request them from administration, giving precise information as to why these rights are needed and for which timeframe. The same request procedure could be used for features that have been, or will be, disabled on workstations, such as PowerShell or Hyper-V. Not only would this grant access to rights only when they are needed, but it would also provide a log of who had access to them and when, facilitating incident management should they knowingly or unknowingly be abused. Such an implementation would help theFIRMA improve its abiding by the principle of least privileges, i.e. that each user is only granted rights and access to what is indispensable for them to carry out their work.

Features such as PowerShell and Hyper-V needed to be disabled for users: PowerShell had already been deactivated prior to this research, but Hyper-V was still accessible to all users. This is an issue as most end users do not have a need for Hyper-V on their system, but it is available and could be abused by a malicious third party, as it is a significant source of information on theFIRMA's network and workstations. For instance, a non-administrative user could access a view of the entire folder structure of the current AD by opening the *Locations* option. Likewise, Hyper-V allows to browse through a list of all available machines and related information, such as OS version, host name, status etc. This data could be useful to an attacker to know which vulnerabilities a given system might have and how it could be accessed.

3.2.3 Portable Apps and network hardening

Removing administrative rights is not an effective enough way to prevent access to valuable resources or data. This is further undermined by applications that can actively circumvent User Account Control (UAC). This type of applications has become known as *Portable Apps*, applications that do not require any installation and run from a single folder, which contains all the necessary data to run the program. This is convenient for users that often change systems and want to have their preferred programs at hand, but it poses a considerable risk from an enterprise security perspective. Firstly, they can be run from a removable drive, allowing non-traceable use. Secondly, a malicious user could run applications such as e.g. Wireshark directly in the workstation, without having

to enter any credentials. An irregularity in the UAC is given by the Mozilla Firefox installer, which, can bypass the request for administrative rights in Microsoft Windows. This was observed already before research at theFIRMA and still works at the time of writing: by clicking on the *Close* button (X) when the UAC is prompted during installation, the process should be aborted immediately. However, the Firefox installer carries out the installation without interruption. As Firefox is a recognized browser and the use of such software is allowed and essential in theFIRMA, this is not a direct threat to the company. However, if the installer was adapted to malicious software, as the code is publicly available, this would again pose a significant security risk which needs to be addressed.

There are multiple possible solutions to prevent the use of Portable Apps, but the suggested one is to implement Application Control policies. These rules allow to define or whitelist only the software that the company wants to permit to be run on its systems. As the inventory of programs in use at theFIRMA is limited, this implementation would not require constant updating and is a very effective solution to prevent unwanted services and applications. A further minor measure that can be taken to prevent users from tampering with settings on their workstations is to use *Canonical Names* to hide functionality. This can be used to prevent the end user from accessing settings such as the HomeGroup, Windows Defender settings etc. and intentionally or unintentionally modifying them.

In regards to software management specific to theFIRMA's network, two suggestions were made to the administration. The first is to reconfigure the firewall to prevent port scanning by services such as ZenMap. The second suggestion was to remove any unused remote access methods in place at theFIRMA. During the interviews with relevant parties, it was noted that a VPN server was active on theFIRMA's network, but that the administration was not aware of its scope nor of whether it was actively being used. The administrators were therefore urged to remove the VPN connection and to prevent the future implementation of such software, especially if undocumented.

3.3 Awareness training

Solving practical matters is important, but to create a persistent recognition and understanding of issues related to cyber security in a company is essential. Employees are the weakest link in any given business and the cause behind most of the major breaches in recent years. However, if trained accordingly, they can become the company's broadest and most important line of defence, both in case of external and internal threats to theFIRMA's assets. Awareness is used in this paper as terminology referring to two pathways to securing theFIRMA, through theoretical understanding of security topics: the first is an awareness training session written for new entrants to the company; the second refers to the management and administration developing a deeper understanding of theFIRMA's current status in any given situation concerning security issues.

3.3.1 Awareness training material

Training material was developed for new employees of the company to make them aware of security topics and to inform them of expected or mandatory behaviour regarding their tasks. This will be integrated with the current practice of having new entrants play a "Security game", a video game simulation of theFIRMA which challenges players with typical cyber security related situations. These include, but are not limited to, receiving a phishing e-mail, using a password manager etc. The game was developed by students at theFIRMA on request of the CISO and was a good starting point to make new employees think about how to react to situations of compromised security. However, the average student has often not been faced with such challenges before and has not been taught basic best practices of cyber security. As a result of this, the game on its own might result in a frustrating experience that could put off students from interacting with it or stop them from internalizing the conveyed topics, which would be in contrast with its desired purpose. The idea for a more comprehensive training is to give students a short and simple presentation on topics such as correct use of devices, password security, suspicious activity, data protection and more. After this presentation they will then play the "Security game", putting their newly acquired knowledge to the test in realistic situations. At the end of the game they will be reminded of the topics once more via the *10 commandments of security*:

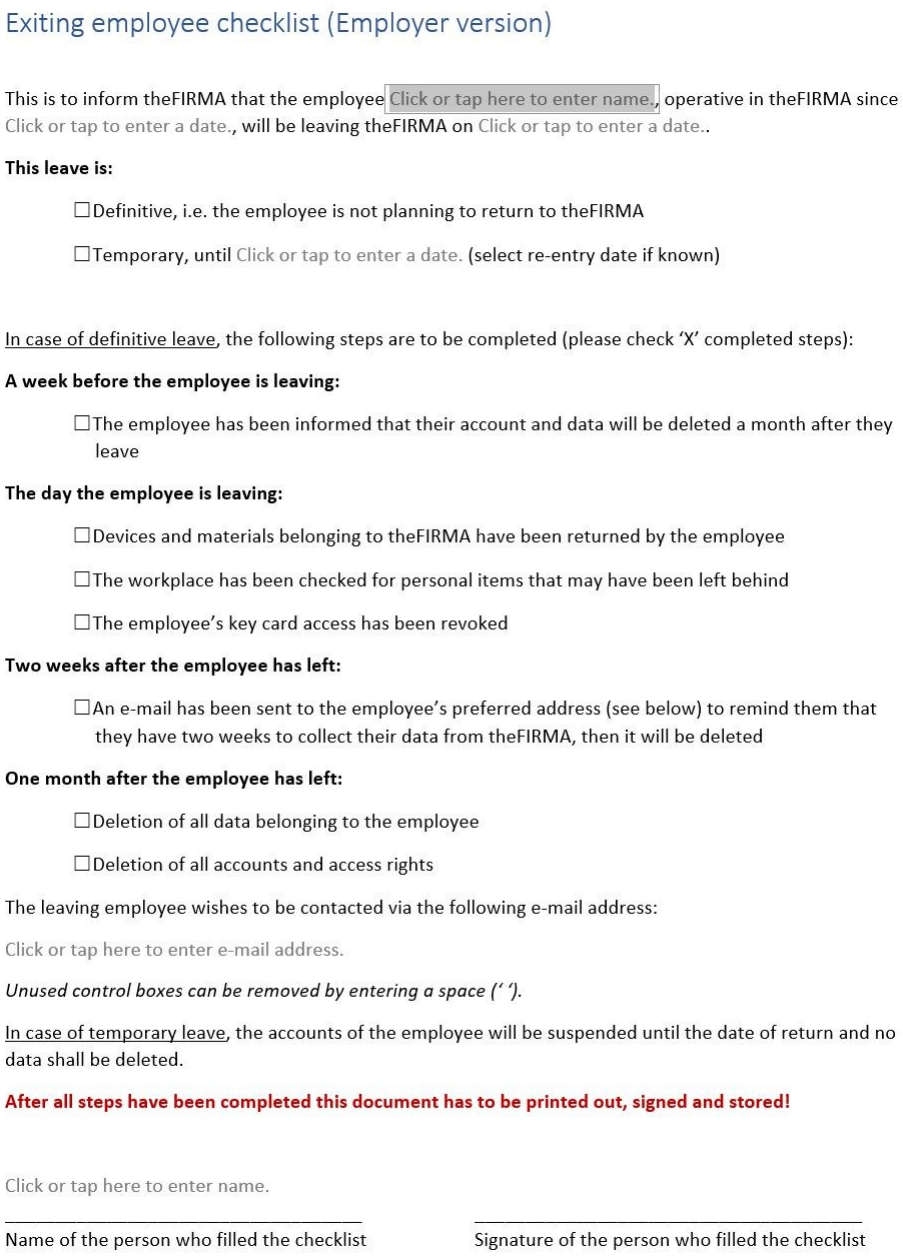
1. Do not allow others to access your computer or accounts
2. Do not share your password(s) with anyone, not even admins
3. Lock your PC (⊞ + 'L') whenever leaving your desk, even if just for coffee
4. Use different passwords for different services
5. Use strong passwords (minimum 12 characters, mix letters/numbers/symbols/ upper and lowercase, no dictionary words, no obvious substitutions)
6. Be aware of spam mail: if an e-mail seems suspicious, don't click on any links/images/attachments. Report the e-mail to admins or security
7. If you find external media such as USB-sticks, hard drives etc. don't plug them into any computer. Give them to an admin or security person for inspection
8. Be suspicious of files that you don't know, even if they come from a seemingly trustworthy person/source
9. If you notice suspicious activity on your computer, please report it immediately
10. Don't hoard data/information. Only save information that is strictly necessary to you and delete it after it has fulfilled its purpose

Once their training is completed, the new employees will sign a document acknowledging that they have received the awareness guidance and vowing to comply with the given recommendations to the best of their knowledge. The training material is also made available on theFIRMA's Optima page to be accessed again at a later time or by students already employed in the company. One aspect that is mentioned in the presentation is that all employees must comply with the GDPR. This is because when working on projects for customers, they transition from being data subjects to being data processors and are therefore subject to legally defined responsibilities and must comply with measures defined by the data controller, typically their commissioner.

3.3.2 Awareness and control tools for administration

Whilst the training routine is aimed at conveying basic security knowledge to the employees, the management and administration teams need awareness of the situation of the company, as they should already master best practices, but need to make informed decisions. A series of checklists and control tools was developed to provide them with this information. The first checklist is for new hardware being deployed in the company and it details steps to configure it according to theFIRMA's requirements and policies. It defines actions such as installing the company's Microsoft Windows image or setting up a different operating system, configuring user accounts and passwords, documenting the BIOS configuration and assessing existing damage to the machine. All this information is stored in the administration's databank as an addition to the current

list of machines and should be expanded and updated wherever necessary. The need for such a checklist became clear after the CISO found an unconfigured Apple laptop in theFIRMA, which he could then set up with a personal account and use to access the company network. Another important control measure that was suggested is the use of an exit plan. This is a timeline with checkpoints that must be fulfilled when an employee leaves the company, even if only for a short period. (Figure 7) This exit plan serves two main purposes: the first is to keep track of which employees have left theFIRMA, as on average they only stay for up to 6 months.



Exiting employee checklist (Employer version)

This is to inform theFIRMA that the employee Click or tap here to enter name., operative in theFIRMA since Click or tap to enter a date., will be leaving theFIRMA on Click or tap to enter a date..

This leave is:

☐Definitive, i.e. the employee is not planning to return to theFIRMA

☐Temporary, until Click or tap to enter a date. (select re-entry date if known)

In case of definitive leave, the following steps are to be completed (please check 'X' completed steps):

A week before the employee is leaving:

☐The employee has been informed that their account and data will be deleted a month after they leave

The day the employee is leaving:

☐Devices and materials belonging to theFIRMA have been returned by the employee

☐The workplace has been checked for personal items that may have been left behind

☐The employee's key card access has been revoked

Two weeks after the employee has left:

☐An e-mail has been sent to the employee's preferred address (see below) to remind them that they have two weeks to collect their data from theFIRMA, then it will be deleted

One month after the employee has left:

☐Deletion of all data belonging to the employee

☐Deletion of all accounts and access rights

The leaving employee wishes to be contacted via the following e-mail address:

Click or tap here to enter e-mail address.

Unused control boxes can be removed by entering a space (' ').

In case of temporary leave, the accounts of the employee will be suspended until the date of return and no data shall be deleted.

After all steps have been completed this document has to be printed out, signed and stored!

Click or tap here to enter name.

Name of the person who filled the checklist

Signature of the person who filled the checklist

Figure 7: a checklist of tasks when an employee quits at theFIRMA

The second, more important function is to allow administration to disable unused accounts and to remove data belonging to students that are no longer employed by the company. Not only will this free space on theFIRMA's servers, but it has a positive impact on security too. Old accounts could potentially be used to impersonate an employee or to gain unauthorized access to theFIRMA's resources.

A further tool to verify if theFIRMA e-mail addresses or account credentials have been added to account databases for unauthorized access would be the AD integration of haveibeenpwned. (Dyke, 2018) This tool can be used to verify if a given address is part of any account lists found on the web and when integrated with the Active Directory, would allow users to see directly if their accounts have been compromised in some way.

Screening of prospective employees in administrative roles is already taking place in the form of job interviews, but it was noted that there is a way to be appointed to such a role without background checks. Students coming from the *Projects and Services* course are appointed to the chosen administrative role directly, without being interviewed, according to a system administrator. This is unacceptable from a security perspective, as possibly untrained or even malicious actors could gain access to many of theFIRMA's most important assets without having been checked. It was therefore strongly suggested that all applicants for a position in administration should undergo the same selection and screening process, regardless of their background. This will not only allow fair opportunities for all candidates, but it will also grant better selection possibilities for recruiters, as the technical skills and role compatibility could be assessed clearly.

4 RESULTS AND CONCLUSIONS

All the suggested solutions had to be adapted to the special context and needs given by theFIRMA. As a company run by students and with no turnover, the two main issues when implementing solutions were the budget and the constant rotation of the workforce. The latter especially makes it very difficult to create a persistent cultural awareness that will last longer than the average 6 months most students spend working in theFIRMA. The given awareness training was therefore skimmed down to a short PowerPoint presentation, highlighting the most important best practices and giving a guideline on how to behave when confronted with potentially hazardous situations. Some policies in theFIRMA are inherited from those applying to the entirety of Turku AMK. Whilst this takes workload off the company, it poses some significant constraints too. Policies like password changes every 90 days are heavily debated in the cyber security field but are mandated to theFIRMA by the university rules. Another example is the usage of the MIFARE Classic protocol for key cards, which is implemented by Turku AMK and directly impacts the security of theFIRMA.

Suggested future developments: implement solutions that are currently only theoretical (e.g. AD integrations), target specific material and training at the various employee groups (secure coding, GDPR compliance in websites etc.), expand budget to allow for more enterprise-like solutions, develop and implement a solution for secure file access such as a Raspberry Pi on each desk and SMB folder access, define clearer backup policies.

5 REFERENCES

Dyke, J. V. (2018, 02 25). *Checking for Breached Passwords in Active Directory – Using k-Anonymity!* Retrieved 09 13, 2022, from JacksonVD: https://jacksonvd.com/checking-for-breached-passwords-ad-using-k-anonymity/

European Union Agency for Cybersecurity (ENISA). (2019). *Pseudonymisation techniques and best practices.* European Union Agency for Cybersecurity (ENISA).

International Organization for Standardization (ISO). (2018). *EN ISO/IEC 27000:2020 (E).* CH-1214 Vernier, Geneva, Switzerland: ISO/IEC.

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). (2017). *EN ISO/IEC 27001:2017:E.* Avenue Marnix 17, B-1000 Brussels: CEN.

International Society of Automation. (2018). *ANSI/ISA-62443-4-2-2018, Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components.* Research Triangle Park, NC 27709: International Society of Automation.

Merriam-Webster. (n.d.). Retrieved September 12, 2022, from Merriam-Webster Dictionary: https://www.merriam-webster.com/dictionary/due%20diligence

Microsoft. (n.d. a). *Microsoft Intune is an MDM and MAM provider for your devices*. Retrieved 09 13, 2022, from Microsoft Docs: https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Microsoft. (n.d. b). *Software Center user guide*. Retrieved 09 13, 2022, from Microsoft Docs: https://docs.microsoft.com/en-us/mem/configmgr/core/understand/software-center

Microsoft. (n.d. c). *Secure boot and device encryption overview*. Retrieved 09 13, 2022, from Microsoft Docs: https://docs.microsoft.com/en-us/windows-hardware/drivers/bringup/secure-boot-and-device-encryption-overview

Microsoft. (n.d. d). *BitLocker*. Retrieved 09 13, 2022, from Microsoft Docs: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview

Microsoft. (n.d. e). *User Account Control*. Retrieved 09 13, 2022, from Microsoft Docs: https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-overview

National Institute of Standards and Technology. (16.04.2018). *Framework for Improving Critical Infrastructure Cybersecurity - Version 1.1.* National Institute of Standards and Technology.

North American Electric Reliability Council. (Effective Date: June 1, 2006). *Standard CIP–008–1 — Cyber Security — Incident Reporting and Response Planning.* Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731: North American Electric Reliability Council.

NortonLifeLock Inc. (n.d.). *10 cybersecurity best practices that every employee should know*. Retrieved September 13, 2022, from https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html

Statista. (2019). *Usage of security frameworks in U.S. healtchare organizations as of 2018 .* Statista.

Statista. (2020). *Share of companies and public administration which adopted the ISO 27000 requirements in Italy in 2016.* Statista.

The European Parliament and the Council of the European Union. (04.05.2016). *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.* Official Journal of the European Union.

Interview with relevant parties at theFIRMA.

In order to protect the identity of the interviewees, their names have been substituted with their role at the time of the interview. Also, to improve readability, multiple short answers or subjects with direct links have been merged into single answers. The content of the answers was not modified.

The interviewer is Philipp M. Woolaway (PW). Interviewees: Chief Information Security Officer (CISO) and two System Administrators (Sysadmin 1 and 2).

Interview A with CISO and Sysadmin 1

PW: What security tests have you carried out so far?

CISO: My main focus has been physical security testing. This includes tests through social engineering and tests on our hardware security.

PW: How would you describe your findings so far?

CISO: The company needs to improve its security substantially. Currently basically anyone who knocks on the door is let in, no questions asked. It was also possible to just ask employees to plug in a USB stick into their PCs and to open a random file, nearly all of them didn't oppose it and didn't ask for a reason.

PW: Ok, that's a bit worrying. Do you think this is due to a lack of knowledge?

CISO: Definitely. Most of the employees have never even been lectured on security best practices.

PW: So, some kind of awareness training is necessary. How about other physical security aspects: are the computers secured by Kensington locks or similar?

CISO: No, there are no locks securing any hardware. Generally speaking there's a lack of lock security, as drawers are often left unlocked and the doors don't have security hinges.

PW: Did you ever find any sensitive material in an unlocked drawer?

CISO: I once found a printout of the entire administrative password manager. That shouldn't even exist, but to find it in an unlocked drawer was even more concerning.

PW: I agree. Is there anything else on the physical security side that I should know about?

CISO: New hardware is usually configured before being handed out to employees. However, I once found a MacBook that had not yet been set up and was just lying on a desk. Also, some employees leave their badges lying on their desk or elsewhere.

PW: Ok, thank you. Let's talk about software security now. What security solutions have been implemented so far?

CISO: It was possible to run PowerShell on Windows computers, that has now been disabled. Also, Hyper-V allows non-administrative users to view the AD structure, all available machines and information about them such as OS version, name etc. That needs to be changed.

Sysadmin 1: It was also possible to install software without administrative rights, that should be fixed by now. Unauthorized access to folders should also be prevented since recently.

PW: Do you know of any other major problems?

CISO: ZenMap can be used to read information such as OS version and open ports on devices, but it's hard to prevent that. I have asked for security measures on the BIOS, such as secure boot and passwords, to be implemented.

Sysadmin 1: Although the access to folders has been restricted, we still have lots of old folders and files that would need to be archived or deleted, but we don't know if we are allowed to do that. Our main issue currently is that we should be migrating to a new AD, but progress has been slow and it is stopping us from implementing further measures.

PW: I understand. What can you tell me about possible remote access and disk encryption, e.g. with BitLocker?

Sysadmin 1: To my knowledge remote access is only available to system administrators and it is secured by certificates.

CISO: There is no disk encryption such as BitLocker or others.

PW: Ok, thank you both for your time.

Interview B with Sysadmin 2

PW: Is there some kind of management of UODs (user owned devices)? Possibly via Intune or similar software.

Sysadmin 2: No, there isn't. The only check we carry out on employee devices so far is for them to show us a successful (i.e. with no positives) scan of their system with an antivirus software of their choice. I don't think we can ask the students to install management solutions on their devices.

PW: Did you research so-called PortableApps or other software that circumvents installation controls?

Sysadmin 2: No, we're waiting for the implementation of the new AD without local administrative rights to see what we need to prevent separately.

PW: Hyper-V seems to give users access to a lot of information. If not many employees use it, could you disable it on the systems like it was done with PowerShell?

Sysadmin 2: To my knowledge only the administrators use it, so that should be possible.

PW: Good. I was thinking about a solution like temporary administrative rights and temporary access to locked software, maybe upon request.

Sysadmin 2: Once we have the new AD, we are planning to use Software Center to control application installation on the endpoints, so that should be a feature we could look into.

PW: Is there some kind of screening for those who want to work as system administrators?

Sysadmin 2: If they apply for the job then they must take part in an interview where their skills and motives are assessed. Unfortunately, we sometimes get students from the "Projects and Services" course who are not checked in any way and are just given the role directly.

PW: What about external access to theFIRMA's network, is it possible? And how is it secured?

Sysadmin 2: Windows remote desktop is used but secured by certificates. There is a VPN setup, but it's not used.

PW: If it's not used by anyone it should be closed.

Sysadmin 2: I agree, I'll look into it.

PW: What policies are in place for backups?

Sysadmin 2: We have 10-day backups of all servers, including the file server.

PW: That's good. It should allow to implement centralized BitLocker once the new AD is running.

Sysadmin 2: Yes, that should be possible. We'll have to wait until it's ready though.

PW: Sysadmin 1 mentioned that there is a lot of old material that might no longer be needed. Have you thought of some solution to archive or delete it?

Sysadmin 2: We are planning to only migrate files and other data from the last two to three years once the new AD is set up, that should help remove some of it.

PW: One more thing. The CISO mentioned that he had made sure for all BIOSs to be locked down some time ago. I have found this not to be implemented on at least two machines. Is this the situation with all PCs?

Sysadmin 2: To my knowledge none of the machines has a locked BIOS, I don't know why CISO was under that impression.

PW: Ok, thank you for your time.

Interview C with CISO

PW: I have found out from talking to Sysadmin 2 that none of the PCs have security measures on the BIOS level. Sysadmin 2 also didn't know why you were under the impression that this would be implemented.

CISO: I had discussed and agreed on this solution with the predecessor to Sysadmin 2. However, we were supposedly going to change all hardware at the time. Probably it lost priority because of this and was then forgotten entirely. We only ended up getting a few new PCs, so it's sad to see this simple security solution was never applied.

PW: Ok, thank you for clarifying on this issue.

SECURITY AWARENESS TRAINING FOR theFIRMA

Why and how you should take care of cyber security in theFIRMA

Topics covered in this presentation

- Why is cyber security important to us?
- Badging and access
- Using your own devices
- Best practices for your desk
- Unauthorized access
- Secure passwords
- Spam mail
- External media and files
- Suspicious activity
- Data protection
- Feedback

Why is cyber security important to us?

- Anyone who works with electronic devices and computers is potentially affected by cyber security issues
- Cyber security policies allow for theFIRMA to run smoothly without internal or external interference
- We care about your work and data and try to protect it as best we can
- Cyber security is a community effort: the more employees know and care about it, the better the overall security of theFIRMA
- We have legal requirements on cyber security, such as complying with data protection laws

Badging and access

- As an employee of theFIRMA you should request a key card to access the premises. You can find more information under: https://messi.turkuamk.fi/english/Faculties/1/Pages/joukahaisenkatu.aspx
- You will receive a paper badge with your name on it and a colour code, based on your task within theFIRMA. Please always have this on/with you during working hours
- You can only allow access to the premise to someone presenting a badge, to someone who has a verified appointment with an employee or to someone whose identity can be verified by another employee

Using your own devices

- You are allowed to bring your own devices (smartphone, tablet, laptop etc.) to theFIRMA and to use them for project work
- If you intend on using your own devices, each of them has to be scanned with your antivirus scanner of choice. A report showing your device as clean/safe has to be presented to the administrators before you are allowed to access theFIRMA network with it
- You will typically be assigned a workstation with a fully equipped computer within theFIRMA, so there should be no need for you to use your own devices on premise
- You can find a list of available antivirus software under https://en.wikipedia.org/wiki/Comparison_of_antivirus_software

Best practices for your desk

- Make a habit of locking your PC whenever leaving your desk by using the combination ⊞ + 'L', even if you're just going to grab a coffee or to talk to someone
- Keep your desk clear of important/confidential documents unless you are working on them
- Any items that are not being used should be stored in your bag or in a lockable drawer, especially if they contain sensitive information
- Do not leave key cards and badges lying on your desk in your absence, as they can easily be stolen or copied
- When leaving work: make sure that you haven't left anything behind, that all items or documents staying in theFIRMA have been stored in a secure location and that you have logged out of or turned off your PC

Unauthorized access

- You are not allowed to share your key card, badge, username(s) and password(s) with anyone. These are all intended for personal use only
- Nobody inside or outside theFIRMA is allowed to ask you for your password(s)
- Administrators do not need your password(s) to carry out their tasks, so they would never ask for it
- You are not allowed to grant anyone access to a computer owned by theFIRMA whilst you are logged in. You should also avoid doing this with personal devices
- You are not allowed to give access to shared drives or similar to any third party, unless there are contractual grounds for doing so
- You are not allowed to set up or grant remote access to theFIRMA's systems and premise in any form

Secure passwords

- Minimum length of 12 characters
- Use a mixture of letters (upper and lower case), numbers and symbols (@, !, ? etc.)
- Avoid using any dictionary words
- Avoid obvious substitutions, such as p4ssw0rd
- Use a unique and different password for every service/account
- Try to use two-factor authentication (2FA) wherever possible
- Consider using a password manager (e.g. KeePass) to generate and store randomized and secure passwords
- Consider changing your password(s) every three months (TUAS: https://id.turkuamk.fi)
- Regularly check if any of your accounts have been compromised, for example by entering your e-mail address in https://haveibeenpwned.com/

Spam mail

- If an e-mail seems suspicious, do not open any attachments, don't click on any links and avoid downloading images within the message
- If an e-mail contains a lot of spelling errors or refers to a topic you have no business with, it's probably spam
- Never share personal or identifying information via e-mail. Any serious company has a secure method to access your data and would never ask for it via mail
- Make a habit of looking at the sender's e-mail address. If it seems odd, unknown or doesn't match the content of the message, it's probably spam
- Make a habit of looking at the "Must See Students" section on the front page of Messi, as it often contains warnings about ongoing spam campaigns
- As a general rule, avoid opening any unsolicited or weird looking e-mails

External media and files

- If you find external media such as USB-sticks, hard drives etc. don't plug them into any computer. Give them to an admin or security person for inspection
- Avoid plugging in your devices to theFIRMA computers via USB to charge them. Please bring and use an external charger
- Be suspicious of files that you don't know or didn't expect, even if they come from a seemingly trustworthy person/source
- Avoid sharing and accepting data/files on personal USB-sticks. Use e-mails or a shared drive instead

Suspicious activity

- If you notice suspicious activity on your computer, please immediately report it to the administrators or security
- Report spam mail if it has some kind of connection with theFIRMA
- Report anyone who asks you for your accounts and passwords
- If you notice someone acting (intentionally or unintentionally) in a way that is not compliant with security best practices, please consider advising them
- If you notice an external party trying to access theFIRMA's network or premise in a forceful way, report them immediately

Data protection

- By signing a contract with theFIRMA/TUAS you have vowed to comply with the European General Data Protection Regulation (GDPR)
- By violating this agreement, both you and the company/university may incur in significant legal and financial consequences
- As a general rule, only collect data that is strictly necessary for your work (i.e. needed for a specific task) and delete it as soon as you don't need it anymore
- Try to anonymize data whenever possible, e.g. mention a person in a document by their held position and not their name
- Don't hoard personal data because "you might need it later". This is both counterproductive for your work and a data protection issue

Feedback

- Our cyber security measures are not meant to get in your way while working, but please understand that sometimes comfort and easy usability can open the way to security issues and must therefore be regulated
- If you have any complaints or suggestions about the security measures don't hesitate to contact the admins or security about them
- As an employee of theFIRMA you are a valuable source of information about possible security issues, so please don't be shy and contact us whenever you have questions or notice something suspicious

The game

Yay! You have made it to the end of theFIRMA's awareness presentation ☺

You will now play our cyber security game to put what you have learned to the test.

If you feel unsure about any of the topics, please feel free to come back to this presentation to refresh your knowledge. The slides will be available on theFIRMA's Optima page.

After playing the game, you will be asked to sign a paper confirming that you have received this training.

Keep an eye on security during your work and stay safe!