



FH Salzburg

## BACHELOR THESIS

# Managing the Risk of Cyber Threats for an Enterprise and Securing its Workstations

Carried out in the study program  
Business Informatics and Digital Transformation  
University of Applied Sciences Salzburg GmbH

Submitted by  
Franz-Karl Schachinger

Program Director: FH-Prof. MMag. Dr. Manfred Mayr  
Supervisor: FH-Prof. Priv.-Doz. DI Mag. Dr. Dominik Engel

Puch/Salzburg, Juni 2022

---

## **Affidavit**

I hereby declare under penalty of perjury that I have written this bachelor thesis independently and without outside help and that I have not used any sources or aids other than those indicated. Furthermore, I hereby affirm that I have taken verbatim or in substance from the sources used. I hereby certify that I have marked as such the passages taken verbatim or in content from the sources used.

The work has not been submitted in the same or a similar form to any other examination board, neither at home nor abroad, nor has it been published.

June 8, 2022

Franz-Karl Schachinger

## **Abstract**

This thesis addresses the question of what steps need to be taken in a systematic risk management process. The core topics of defining the scope, methods and processes to identify potential risks, how identified risks can be weighted and practical approaches to eliminate these risks are addressed. An outlook on further risk mitigation options, monitoring and control of the risk situation is dealt with in the concluding part. The focus of the thesis is mainly on threats to computers of company employees, but general cyber risks are also addressed. The result of this work includes basic information technology security measures based on a Microsoft Windows client/server environment, where the server is the domain controller with an Active Directory service and the client is an employee's computer. Furthermore, a concept of risk management measures is established, which is represented by a cyclical process at the end.

**Keywords:** *Client Security; Cyber Threats; Risk Management*

## **Acknowledgement**

First of all, I would like to thank my supervisor, Dominik Engel, for guiding and supporting me in the process of writing this thesis.

I also want to thank my colleagues from SPAR ICS for proofreading and giving me directions on certain topics.

Special thanks to Benjamin Petermaier and Robert Lamprecht from KPMG for supporting me in the draft for the practical part of the thesis.

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Scope of thesis . . . . .	1
1.2	Structure of thesis . . . . .	2
<b>2</b>	<b>Introduction to Risk-Management</b>	<b>3</b>
2.1	What is risk? Definition and delimitation . . . . .	3
2.1.1	Cyber threats . . . . .	4
2.2	Situation of Risk-Management . . . . .	6
<b>3</b>	<b>The Process of Managing Risk</b>	<b>8</b>
3.1	Risk Appetite . . . . .	8
3.2	Risk Identification . . . . .	11
3.3	Risk Analysis and Measurement . . . . .	13
<b>4</b>	<b>Client Risk Assessment</b>	<b>17</b>
4.1	Definition of Clients and Scope Delimitation . . . . .	17
4.2	Identification of Risk on Clients . . . . .	17
4.2.1	Physical Risks: . . . . .	17
4.2.2	Immaterial Risks: . . . . .	18
<b>5</b>	<b>Countermeasures and Mitigation</b>	<b>20</b>
5.1	Mitigation Strategys: . . . . .	20
5.2	Virtual Machine Environment: . . . . .	20
5.3	Access and Theft mitigation: . . . . .	22
5.4	Securing BIOS/UEFI: . . . . .	24
5.5	Setting up Encryption: . . . . .	25
5.6	Secure Firmware: . . . . .	26
5.7	Permission separation: . . . . .	27
5.8	Password Policy: . . . . .	28

---

5.8.1 Mitigations: . . . . .	29
5.9 Microsoft Defender Antivirus: . . . . .	30
5.10 Execution and Installation Rules: . . . . .	31
5.11 Local Firewall: . . . . .	32
5.12 Protocols and Services: . . . . .	33
5.13 Applications: . . . . .	34
5.14 Conclusion to the Security Measures . . . . .	35
<b>6 Risk controlling</b>	<b>37</b>
6.1 Conclusion the Risk Management process: . . . . .	38
<b>7 Conclusion and Outlook</b>	<b>40</b>
<b>8 Used Tools</b>	<b>45</b>

## List of Figures

1	The risk management process [2]	8
2	Risk preference [18]	9
3	Effects of risk awareness and attitude on costs in risk-management [19]	10
4	Dependencies of Risks [19]	13
5	Risk Evaluation Matrix	16
6	Lab Environment	21
7	Chassis Intrusion	23
8	Disable Automatic Hotspot connection	24
9	Encryption in Progress	26
10	Restricting Driver Installation	27
11	Exemplary restrictions	27
12	Domain Password Policy	29
13	Defender Scan Configuration	30
14	Script Redirection to Notepad through GPO	31
15	Applocker Script Execution Policy	32
16	Local Firewall Settings	32
17	Auditing Settings	38
18	Illustration of an information security risk management process [20]	39

## List of Tables

1	Table based and designed on ISO27005 [20]	15
2	Used Tools	45

# 1 Introduction

Disruptive events like the corona-virus pandemic, the war in Ukraine, changes in the economy like supply chain issues or rising inflation demonstrate, that companies need to plan for unforeseen risks in order to meet corporate objectives. Risk-Management is a process to systematically prepare for these very obstacles and can decrease business disruption through unexpected impediments.

This thesis discusses the question of what a systematic approach to the various phases of risk management might look like, starting with the identification of a company's position on risk. Furthermore, methods to analyse emerging risks and their impact on an enterprise will be covered.

With the wave of digitization, not only a new way of working and new possibilities of value creation open up for enterprises, but also risks of the cyberspace are introduced. The trend to work from home and the associated information technology risks increase the need for secure computer workstations for employees. Therefore, this thesis focuses on providing an overview of risks in the cyberspace, specifically on those computer workstations, also referred to as "clients". The goal is to create an overview of given settings enhancing security on a Microsoft Windows 10 operating system, and to compile a configuration baseline for employee computers in an enterprise environment. This baseline will be created in a mostly automated way to mitigate the possibility of human error. This configuration serves as a guideline for possible mitigation options in some of the various areas of risks, and should encourage to further expand security measures.

After covering the steps identification, analyzing, and mitigation of risks regarding clients, an introduction on the following risk-controlling and monitoring tasks will be given.

This work aims to propose a guideline for managing and mitigating IT risks on computers in an enterprise environment and gives an introduction to possible attack vectors for threat actors.

## 1.1 Scope of thesis

This thesis aims on giving insight on how to identify, analyze and mitigate Information technology risks for employee workstations, so called clients, in an enterprise. An overview of the process of managing risk in a company with focus on cyber threats will be given. This process consists of scope defining for the assessment, the attitude regarding risk of a company and furthermore the identification of possible risks and applicable methods to perform this task.



The following steps of weighting identified risks on clients, will provide the basis for the practical implementation of mitigation measures on a Microsoft Windows 10 operating system in an enterprise environment. The focus of these practical implementations will lie on the client, even though the laboratory environment consists of other components. Starting from the hardware of the computer workstation, these measures will cover issues up to the operating system and application level and will be carried out in automated form whenever possible.

For the last step in the risk management process, controlling and auditing measures are addressed in order to present a comprehensive overview of the cyclical process.

The motivation of this thesis is to provide insight on how to approach securing a client system based on an identified and weighted risk factor, however a complete comprehensive guidance exceeds the scope.

## 1.2 Structure of thesis

This thesis is structured in the way a risk assessment would be conducted. To introduce the reader into the subject, a definition of risk and an overview of possible threats is given in the beginning of Chapter 2. In the following Chapter 3, the different attitudes towards risk are explained with the purpose of establishing a scope and the depth of the risk assessment. With the scope defined, the first step in the process of risk-management, the identification of threats and potential methods for this step are explained in Chapter 3.2. After introducing the topic of weighting and prioritizing the identified risks, the mentioned methods are applied to a client workstation.

In Chapter 5, possible mitigation options are discussed and implemented, covering different areas of a computer workstation. To complete the risk-management process, the topic of risk controlling is addressed in Chapter 6.

## 2 Introduction to Risk-Management

“The growing complexity and dynamics of the context in which companies nowadays operate has caused a relentless increase in the level of risk in all areas of corporate management and business activities. As a result, the discipline and practice of risk management has enforced itself gradually in various sectors and industries, as well as across different company sizes.”<sup>1</sup> This statement is further supported by the most recent events at the time of writing this thesis in 2022. International influencing factors, such as pandemics, political factors or supply chain disruptions have shown to affect everyone in our globalized economy [2].

If such events happen, it is naturally that those, who have prepared a strategy will have an advantage and better chances to come out on top – “Denn die Fähigkeit, Chancen und Gefahren (Risiken) adäquat abzuwägen, ist ein zentraler Erfolgsfaktor des unternehmerischen Erfolgs.”<sup>2</sup> (The ability to adequately weigh up opportunities and threats (risks) is a key factor for entrepreneurial success.)

### 2.1 What is risk? Definition and delimitation

A commonly used definition of risk is based on possible damage or the potential loss of a net asset position, with no potential gains to offset it [2]. According to the Cambridge Dictionary, risk management is “the job of deciding what possible financial risks are involved in a planned activity and how to avoid or deal with them” [4].

The goal of a profit-oriented company in our capitalistic economy is to be financially successful, maximize profit and minimize losses as well as risks in their actions. This also partly applies to non-profit organizations, which need to be financially stable as well, to keep the business alive. Different risks and events can disrupt this and other business goals. Therefore, companies need to identify, understand, and manage the risks they are facing in order to continue doing business.

These risks can vary, depending on the size of the company, geographic factors, reputation and also on the economy sector the company is operating in. However, different statistic reports have identified the biggest global risks and threats for businesses in today’s world, independent of economic sector.

---

<sup>1</sup> Enterprise Risk Management, Stefan Hunziker, Page 2 [1]

<sup>2</sup> Frank Romaine - Risikomanagement, Page 14 [3]

The following listed topics pose as the biggest threats to a companies success, according to various reports<sup>3</sup>:

**Force Majeure** Superior force or extraordinary event which extends beyond the control of the company, such as war, epidemic, flood, earthquake and similar events.

**Climate Change** Risks coming with global warming for example extreme weather conditions or effects of Force Majeure.

**Business Interruption** Risk that the business is halted, for example supply chain disruption.

**Legislation/Regulation** Changes and introduction of rules or laws that hinder the business of a company.

**Cyber Attack/Incidents** Risks relating to the information-technology infrastructure, for example Ransomware, Data Loss and Denial of Service

### 2.1.1 Cyber threats

Since this thesis is with client-security in mind, current information technology threats and techniques businesses are facing are explained in more detail. This list covers some of the most common attack techniques and is based on the MITRE ATT&CK framework<sup>4</sup>, which can be consulted for more insight and other techniques.

**Phishing:** Phishing is a type of cybersecurity threat, that targets users directly through communication means. The threat actor<sup>5</sup> can pose as a trusted contact to steal data like login credentials, account numbers or will make other demands to gain insight into the targeted environment [9]. Phishing can occur through E-Mail, text or direct messages (Smishing), telephone or Voice over IP communication (Vishing) and other communication tools. Phishing is often used as an initial attack vector<sup>6</sup>, to access a network or IT-infrastructure of an entity for further exploitation. A phishing attack can be broadly

<sup>3</sup> Alliance Global Risk Barometer[5]

AmTrust Financial - 2021 Small Business Risks[6]

The One Brief - Top 10 Risks [7]

Visualcapitalist - The Biggest Business Risks around the world [8]

<sup>4</sup> MITTRE ATT&CK is a global knowledge base of adversary tactics and techniques: <https://attack.mitre.org/>

<sup>5</sup> A person or entity responsible for an event that has been identified as a security incident or as a risk.

<sup>6</sup> “An attack vector is pathway or method used by a hacker to illegally access a network or computer in an attempt to exploit system vulnerabilities [10]”.

spread with generic messages or very precisely tailored to a specific individual. In case of a phishing campaign targeting a specific person, the tactic is called spear-phishing. If this person is a high profile target, such as the Chief Executive Officer or another senior member, it is called “Whaling”.

**Malware:** Malware is software developed with malicious intent, which can be classified as ransomware, spyware, trojans, worms, adware, viruses, or as another type. Depending on the classification, this software is designed to extract and encrypt data or inflict other kinds of damage to a system. Malware is often used as part of a larger scale attack, as once access to a network or shared server is gained, multiple endpoints<sup>7</sup> can be infected. Ransomware, which has risen in popularity in recent years, usually tries to spread to multiple clients and encrypt data. The decryption can only be performed with cryptographic keys, which are in possession of the threat actors, which will demand a ransom in exchange for these keys. Sophisticated attacks will first exfiltrate the data before encrypting it, to gain even more leverage over the target [11]. This data can subsequently be sold or used for blackmail (threat of publication). This is often referred to as double extortion. Another recent rising form of malware, so called “Wipeware” is deployed with the only intent to “destroy” its host system.

**Insider Threats:** An insider threat can be an employee, external consultant or any person, who has been given access or permissions deliberately, but misuses this authorizations for malicious actions[12].

**Missing or Weak Encryption:** Encryption is the cryptographic transformation of plaintext into ciphertext. Encryption can be applied to data in motion or to data at rest. A security risk occurs, if an unauthorized actor can access confidential data and information because of missing encryption (plaintext) or can reverse the encryption (decrypt) the ciphertext to get hold of the data<sup>8</sup>.

**Vulnerable Systems and Applications:** Software (Application, Operating System, Kernel, ...) may have flaws due to human errors, rushed development, incorrect configuration or technical weaknesses. Detected flaws in the software code are fixed through updates and patches. If these flaws stay unpatched, they could be exploited by a threat actor and therefore pose a security risk. Thus, it is indispensable to update systems and

---

<sup>7</sup> Endpoints can be Client Personal Computers, Mobile Devices or other Servers.

<sup>8</sup> See MITRE Common Weaknesses ID 311.  
<https://cwe.mitre.org/data/definitions/311.html>

applications regularly to the newest standard. The MITRE Corporation hosts a list of Common Vulnerabilities and Exposures (CVE)<sup>9</sup> for popular software, which should be consulted in regular cycles through a standardized process, to ensure safety of systems. Systems can also be vulnerable because of wrong or weak configuration. Since employees working in information technology often require more permissions and have higher privileged accounts, the possibility and impact of miss-configuration is higher. Training, education and frequent reviews can help mitigate this errors.

**Denial of Service:** A (Distributed-) Denial-of-Service (DOS) occurs, when an attacker interrupts the intended functionality of a system or application through their action. For example a web-server could be flooded with illegitimate traffic, so that its resources are exhausted [13]. Often, this attack technique is used to distract from another ongoing attack.

**Human Errors:** People are prone to errors, therefore it is important to implement guidelines and practices to mitigate named above or other risks. Possible steps are to train non-technical employees cyber security principles or have a review system for technical work.

## 2.2 Situation of Risk-Management

Risk can also be described by costs, which appear from nowhere and occupy monetary reserves, which were planned elsewhere. Risk also depends on how variable costs and revenues are. To manage this, it should be researched by businesses, how likely it is that they encounter a big enough pitfall or financial loss, to disrupt their business plans [14].

Often, companies with a certain business size are required by law to implement a control system to ensure the continued existence of the business. However, in the example of the Austrian laws as the “*AktG - Aktiengesetz § 70 AktG Leitung der Aktiengesellschaft Absatz 1*”<sup>10</sup> for stock corporations and for limited liability companies in the law “*GmbHG - GmbH-Gesetz §22 Absatz 1*”<sup>11</sup>, this is rather loosely specified, so no explicit obligation to establish a risk-management-system can be derived from these paragraphs. For public

---

<sup>9</sup> MITRE CVE <https://www.cve.org/>

<sup>10</sup> “Der Vorstand hat unter eigener Verantwortung die Gesellschaft so zu leiten, wie das Wohl des Unternehmens unter Berücksichtigung der Interessen der Aktionäre und der Arbeitnehmer sowie des öffentlichen Interesses es erfordert.”

<sup>11</sup> “Die Geschäftsführer haben dafür zu sorgen, daß ein Rechnungswesen und ein internes Kontrollsystem geführt werden, die den Anforderungen des Unternehmens entsprechen.”

companies it is required to have an internal control system, as for example specified in “AktG - Aktiengesetz §82”<sup>12</sup>, however this is not aimed at information technology threats. A study by *Delloite*<sup>13</sup> finds, that only 13% of surveyed businesses have implemented a Risk Management System.

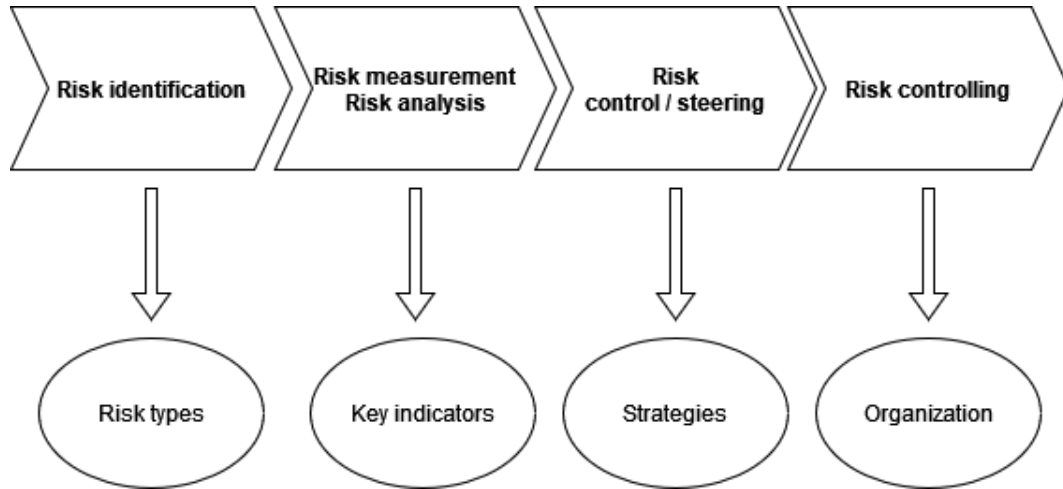
Implementing a risk-management-system or risk-management-framework in a company builds on identifying and evaluating multiple factors. Beginning from identifying and classifying the multiple risks a corporation is exposed to, up to mitigating these risks, risk-management is a complex task. Thus, a systematic process needs to be put in to place.

---

<sup>12</sup> “Der Vorstand hat dafür zu sorgen, daß ein Rechnungswesen und ein internes Kontrollsystem geführt werden, die den Anforderungen des Unternehmens entsprechen.”

<sup>13</sup> Delloite Benchmarkstudie Risikomanagement 2020[15], N=64

### 3 The Process of Managing Risk



**Figure 1:** *The risk management process [2]*

Before an assessment of risk, a scope and the objective of the risk-management process needs to be defined. It is important to align this objective of the risk-management to the relevant objectives of the business. Furthermore, risk assessments can be applied to the areas legal, technical, regulatory, reputation and financial. These areas may change in priority and have interdependencies, depending on the operating sector of the business. For the sake of simplifying the risk assessments, it is recommended to categorize risks, according to their origin and effect [2].

#### 3.1 Risk Appetite

By the definition of COSO<sup>14</sup>, risk appetite can be defined as “The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value [16].” Risk appetite can be classified into three preferences[17]:

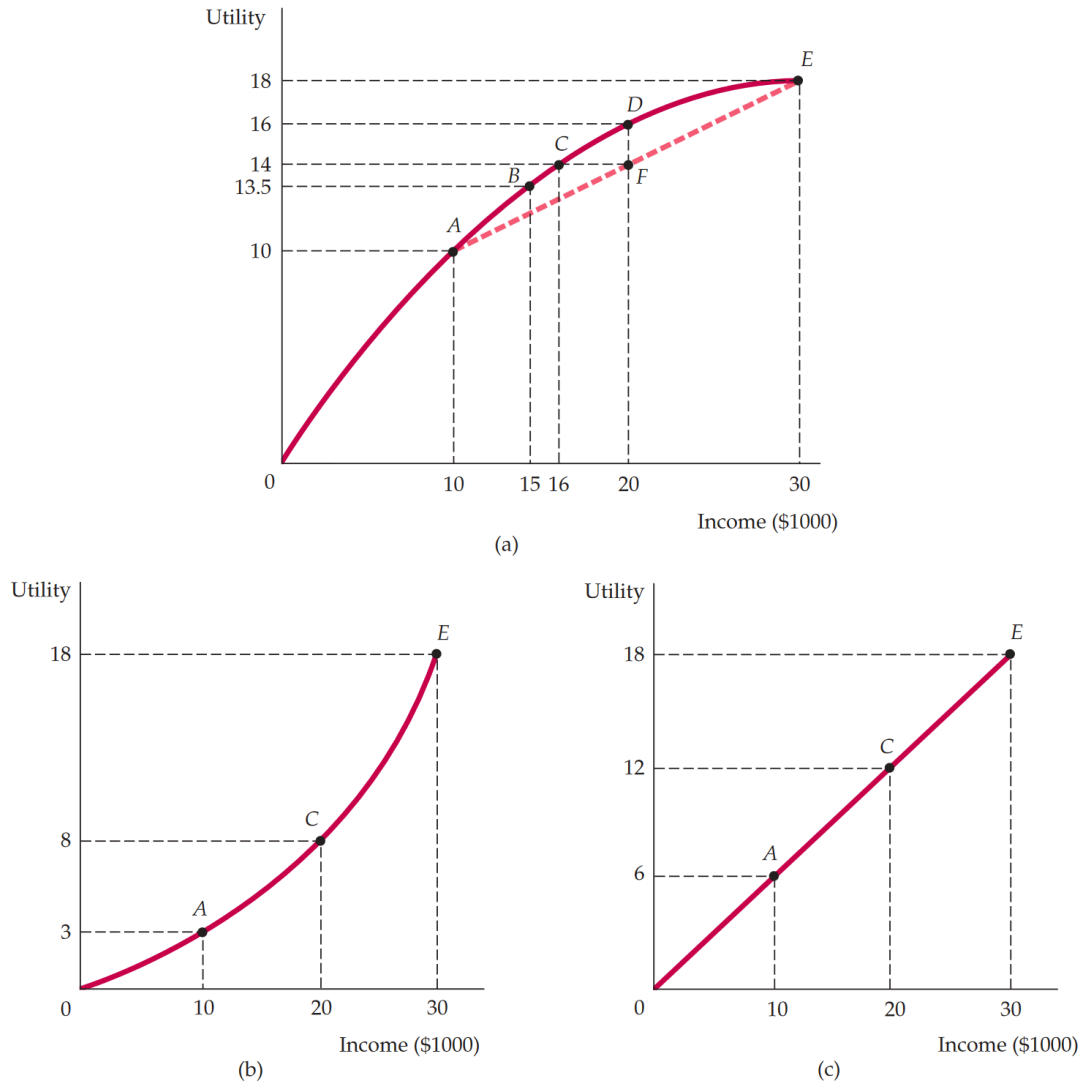
**Risk-aversion** The condition of preferring a certain income to a risky income with the same expected value.

**Risk-neutral** The condition of being indifferent between a certain income and an uncertain income with the same expected value.

**Risk-seeking** The condition of preferring a risky income to a certain income with the same expected value.

<sup>14</sup> COSO: Committee of Sponsoring Organizations of the Treadway Commission

The three types of risk appetite can be further explained and visualized by the following example:



**Figure 2:** Risk preference [18]

**Utility:** “A numerical score representing the satisfaction that a consumer gets from a given market basket” [17]. The value of the utility depends of the risk preference of the individual. We can calculate the utility with the function of the *Expected utility*<sup>15</sup> [17].

The graphic displays the individual behaviours of risk preferences. Figure (a) shows the behaviour of (a) **risk-avers** type, figure (b) shows **risk-seeking** and, figure (c) displays

<sup>15</sup> “sum of the utilities associated with all possible outcomes, weighted by the probability that each outcome will occur.”



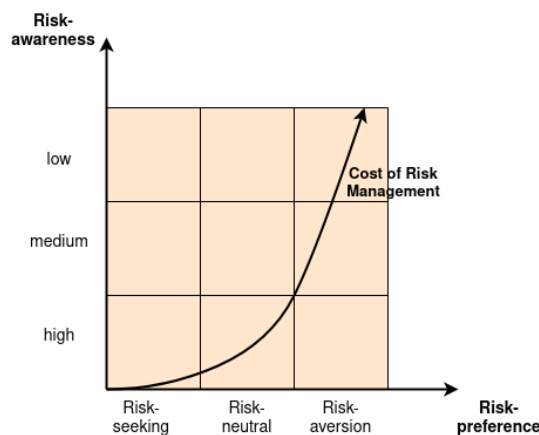
the behaviour of a **risk-neutral** preference. The behaviour is described through a job offer. The curve tells us the utility that can be gained. In the example (figure (a)), a person currently earns \$15,000 ( $u=13.5$ ), and has the offer for a new job, with an potential maximal income of \$30,000 ( $u=18$ ) and a minimum income of \$10,000 ( $u = 10$ ), each with the possibility rated at 0.5. To evaluate the job offer, we calculate the expected utility.

$$E(u) = (1/2)u \$10,000) + (1/2)u \$30,000) = ((0.5) u10) + ((0.5) u18) = 14$$

The new job offer with an expected utility score of 14 and an income of maximum \$30,000 is thus preferred to the original job with an expected utility rating of 13.5 .

To put this into context, a business has the investment options cyber-security and operations. While the expected utility of the investment in operations is rated higher by the business, there is the risk of a security incident/hacking attack, which could be reduced by investing into the cyber-security. Hence, it is down to the risk-preference of the management and the risk appetite of the business, to decide on a strategy.

The risk appetite of a company is influenced by multiple factors. It depends on the strategy of the company, the business culture and the economy sector it operates in. For example, a start-up business most likely has a greater risk-appetite than an older, more-established, less agile company in the critical infrastructure sector. Another factor to consider is the risk-awareness. “Darunter versteht man das Ausmaß, in dem Personen, die sich in einer Gefahrensituation befinden, um das Gefahrenpotential wissen.” [19] - Risk awareness can be interpreted as the extent to which individuals who find themselves in a hazardous situation are aware of the potential for danger. This following graphic displays the development of costs of risk-management, depending on the risk awareness:



**Figure 3:** *Effects of risk awareness and attitude on costs in risk-management [19]*

## 3.2 Risk Identification

“The purpose of risk identification is to determine what can happen to cause a potential loss, and to gain insight into how, where and why the loss can happen” [20]. An organization needs to have an asset inventory (at an appropriate level of detail) in order to identify the risks the assets are exposed to. Generally speaking, two kinds of assets can be distinguished [20]:

**Primary assets:** Primary assets consist of business processes and activities as well as information and data. These are usually the core processes and information, whose loss or degradation hinder the business continuity of an organization. Information as a primary asset consists of strategic information, vital information for the exercise of the organization’s mission or business and also personal information, specified in the General Data Protection Regulation.<sup>16</sup>

**Supporting assets:** The supporting assets, on which the primary assets rely on, can be of various types, for example hardware (Clients), software, network, personnel, site, organizational structure, machinery and similar valuables.

Aside from the company assets, connected companies also need to assess risk from their partners and suppliers. A survey by BlueVoyant<sup>17</sup> has found that 93% of surveyed participants have suffered a cybersecurity breach because of weaknesses in their supply chain/third-party vendors [21]. An example would be the the Solarwinds breach<sup>18</sup> of 2020, which is estimated to have cost in excess of \$100 billion.

There are multiple methods to identify and collect risks a company is facing. This list compiles an overview of possible methods [3]:

### Collection Methods:

**Checklists:** Checklists can help controlling already known risks, however unknown risk may be left out. A checklist can reduce the effort needed for a risk assessment because of its reusable character. Albeit a checklist is never fully complete and has to be updated for new assets in the company and cleared from obsolete risks.

<sup>16</sup> European Data Protection Regulation: <https://gdpr-info.eu/>

<sup>17</sup> Bluevoyant review 2021: [21] N=1200

<sup>18</sup> Solarwinds breach: CVE-2020-10148 <https://nvd.nist.gov/vuln/detail/CVE-2020-10148>

**Interviews:** Interviews with technical experts and department/product leads can help exposing previously unknown risks. These interviews should also be standardized to have structural results that allow comparisons over time.

**Risk-Identification Matrix:** This matrix consists of the risk-causes and the correlating affected entities. With a scoring method from 0-10, risks can be classified.

### **Analytical Methods:**

**Event Tree Analysis:** In this analysis, it is assumed that an event has occurred, which can potentially influence risk. The potential consequences are then analyzed in a binary format, where 1 represents an intact and 0 the defect state of the influenced entity.

**Root cause analysis:** This analysis focuses on deeply understanding a problem to avoid its recurrence. This is done in four steps:

1. Identify the problem: The issue and the affect it has on the organization or system is identified.
2. Data collection: All available associated data is compiled.
3. Analysis: In this step it is researched how the problem occurred and why it was not mitigated or which factors enhanced the problem.
4. Define and implement countermeasures and solutions: Solutions or mitigations are defined and implemented, to prevent the problem from happening again.

### **Creative Methods:**

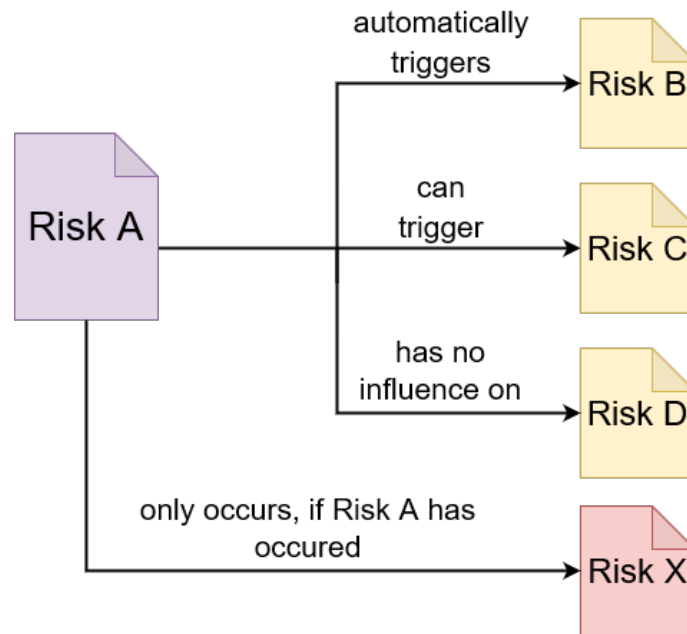
**Brainstorming:** A group of five to seven people name possible risks, their cause and possible effects. These are documented and further analyzed through complementary methods.

**6-3-5 Method:** This method is conducted by a group of six (6) people, of which every participant composes three (3) ideas, which are then passed on five (5) times, where the next participant subsequently derives three more ideas.

Regardless of the method chosen, lessons must be learned from past and other incidents. Root-causes of occurred incidents must be analyzed, to find out if the problem can reoccur

at other business assets. Likewise, incidents happening outside of the company in the industry, must be kept an eye on and preventive measures must be taken.

It is worth noting, that each of these risks has to be analyzed on dependencies, which could cause subsequently further risks. Those dependencies are illustrated in following figure:



**Figure 4:** *Dependencies of Risks [19]*

To mitigate failure and unavailability of services, which may be caused through risk-dependencies, an organization needs to put redundant systems in place. This is also specified in the industry standard ISO27001: “Information processing facilities are implemented with sufficient redundancy to meet availability requirements” [22].

In case a threat actor can exploit one vulnerability on a system, the redundant system should not have the same vulnerability. Ideally, the redundant system differs from the original system, because if a common mode of failure is known on a given device, it is simple the matter to bypass all redundant controls by using the same attack method [23].

### 3.3 Risk Analysis and Measurement

The risks detected in the risk identification process may be distorted, biased, not of relevance or mitigated by controls out of the process scope. Therefore, the need for the risks to be sorted, analyzed and classified by certain characteristics is given. In risk analysis, factors like risk sources, consequences, likelihood, scenarios, controls and

their effectiveness are considered in order to determine a prioritization of tasks in a risk treatment plan [24]. “The purpose of risk analysis is to understand the causes and sources of risk, the effectiveness of existing risk controls, the likelihood of the event, and the consequences - both negative and positive - of the event.[25]”

The most typical way to calculate risk in its easiest form is to use the two factors impact and likelihood, which results in the formula:

$$Risk = Impact * Likelihood$$

The weighting of the factor “Impact” is naturally very individual for every business entity, depending on their current business state, economical sector, risk appetite and other influencing variables. The factor “Likelihood” can be derived from mathematical models, current statistics, experience or estimated values from the risk assessment team or the responsible person of the respective concerned asset. It is important for the quality of the results, that these factors are rated with the same level of information and stripped of cognitive biases like personal preferences [25]. To reach an acceptable level of consistency in this ratings, the scope of the risk assessment must be considered as mentioned in Section 3 and the rating should follow clear rules. The optimal result achieved would be if two different bodies in charge of risk assessment come to the same assessed value of risk, while having identical level of information.

To initially compile a simple risk-matrix, the following table can be used. This table has been filled with exemplary possible risks for better insight.

<i>ID Nr.</i>	<b>Identification</b>		<b>Risk Rating</b>		
	<i>Asset</i>	<i>Threat</i>	<i>I*</i>	<i>P**</i>	<i>E***</i>
1	Apache Server	Log4j	3	2	6
2	Windows Clients	Printer Spooler Priv. Esc	2	2	4
3	Employees	Phishing	3	3	9
4	Windows Clients	Trojan	3	1	3
5	Active Directory	User Enumeration	2	2	4

<b>Risk Mitigation</b>	
<i>ID Nr.</i>	<i>Possible Countermeasures</i>
1	Update Software
2	Change GPO
3	Awareness Training
4	Disable Software installation
5	Adapt GPO settings

<i>ID Nr.</i>	<b>To Do</b>		
	<i>Actions (What)</i>	<i>Responsibility (Who)</i>	<i>Urgency (When)</i>
1	Upgrade to newest Version	System Administrators	1 Week
2	Disable unsigned Driver installation	System Administrators	1 Day
3	Hire Consulting Agency	Security Department	A.S.A.P.
4	Implement Softwarecenter	Application Team	2 Months
5	Disable Enumeration	System Administrators	1 Day

**Table Key:**

Asset	Affected Inventory
Threat	Exploitable Weakness
I*	Impact (1 – 3)
P**	Probability (1 – 3)
E**	Exposure / Risk = I * P

**Table 1:** Table based and designed on ISO27005 [20]

This matrix serves as a basis to calculate a simple rating of exposure. The variables used are covered and explained in Chapter 3.3 which addresses the topics Risk Analysis and Measurement . It is advised to immediately assign a responsible person for the treatment of each single risk, to ensure the treatment and removal of risk.

With the derived information from the risk calculation table and other insights from the risk-management process, a risk-evaluation-matrix as described in Section 2 can be created:

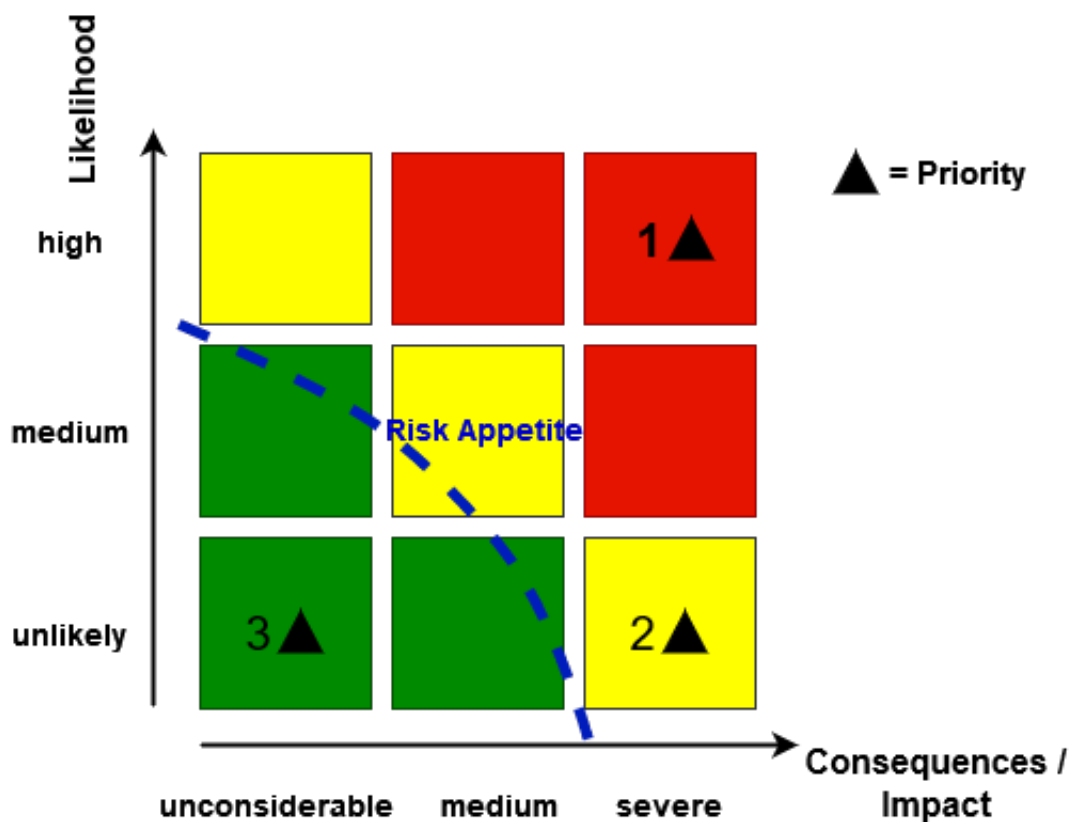


Figure 5: *Risk Evaluation Matrix*  
[26]

## 4 Client Risk Assessment

### 4.1 Definition of Clients and Scope Delimitation

In the context of this thesis, clients are understood as computer workstations for employees. Since Microsoft Windows is currently the most widespread operating system<sup>19</sup>, especially in enterprise environments, technical discussions and recommendations focus on this operating system. Despite this focus, some recommendations and risks are technically independent and universally applicable. The assets addressed consist of aforementioned clients. Although in an enterprise environment are many more different assets like servers and network inventory, the risk identification on this assets would exceed this thesis scope.

**Risk appetite applied to clients:** Risk appetite can hardly be constituted by a single asset type like clients, however as a similar metric, usability can be chosen. Security measures tend to decrease the freedom of the user in his or her actions on the computer. For example, providing a non-administrative user account to the employee, may limit his or her actions but improves the security by applying the concept of least-privilege. The goal is to implement “usable security” in the sense that users are not restricted in their daily tasks, thus decreasing productivity, but that the workstation has solid baseline security against the most common security risks. This baseline should be updated and improved over time, with the usability for the user in mind.

### 4.2 Identification of Risk on Clients

As addressed in Chapter 3.2, there are multiple ways of conducting a risk-assessment. This assessment is structured in a “Checklist” (Section 3.2) style, starting at the physical layer up to the software.

#### 4.2.1 Physical Risks:

Physical risks concern the hardware of a client, such as the different connecting ports, as well as the computer as a whole. There is also the possibility that the device contains unknown or unwanted modifications by the manufacturer.

---

<sup>19</sup> Microsoft Windows has a market share of 76% Worldwide according to GlobalStat [27]



**Access and Theft:** Physical access to the devices by unauthorized entities needs to be prohibited. Threat actors may enter the company site and try accessing or stealing devices. Therefore physical access control policies need to be put in place [28].

**Hardware Risks:** Hardware faces of course the risk of destruction, either through signs of aging, improper handling or by force. Therefore, it is important to advise users of the correct hardware handling and ensure, that the relevant data always resides on assets that are backed up.

**Hardware additions:** Adversaries may introduce computer accessories, like peripheral devices to gain initial access. This should be mitigated by Access control, as stated in the section *Access and Theft*. These devices can be also be introduced on accident by employees, who acquired these devices in good faith. A fully established asset management, can reduce this risk, as well as advising employees, not to introduce foreign hardware into the business<sup>20</sup>. Further mitigation, for example disabling the auto-run feature for auxiliary devices and limiting hardware installation should be implemented [30].

#### 4.2.2 Immaterial Risks:

**Firmware Risks:** Firmware, like the UEFI<sup>21</sup> (BIOS)<sup>22</sup> or drivers, are responsible for booting the device and runs before the operating system is initialized. The risk of vulnerabilities and weaknesses in the code of the firmware can be applied here. Malware could leverage weak BIOS security controls or vulnerabilities in the system to persistently stay on the host. Therefore the firmware needs to be updated regularly and security options like “Secure Boot”, “Hardware Virtualization (Virtualization-based Security)” and “Device Guard” should be enabled. To keep this settings safe from modification a BIOS password needs to be set.

**Operating System Risks:** The operating system serves as the interface of the client-hardware for the user. With the huge functionality provided by modern operating systems, there is a very broad range of potential attack vectors and accompanying risks. Risks arising from the operating system-software itself can be exploitable vulnerabilities in the code, outdated and unsupported versions, wrong or weak configuration and modified, unofficial

---

<sup>20</sup> Employees introducing foreign hardware without the knowledge and management of the IT-Department is also called “Shadow IT” [29].

<sup>21</sup> Unified Extensible Firmware Interface

<sup>22</sup> Basic Input-Output System

versions of the operating system-software.

**Risk of missing or weak encryption:** Data-at-rest and data-in-motion both pose risks, if it is not encrypted, also discussed in Section 2.1.1. Encryption ensures the core security fundamentals of *Confidentiality*<sup>23</sup> and *Integrity*<sup>24</sup>.

**Software and Application Risks:** As mentioned in Section 2.1.1, software versions need to be kept up to date and patches for vulnerabilities need to be applied, to keep a system secure. Vulnerabilities, that have been discovered and made public pose the risk of exploitation by threat actors. Other risks of software and applications are outdated or unsecure engineering practices, where the application uses for example outdated protocols or does not encrypt data. A general principle for security is, to only install software by trusted sources, scan files for malicious contents and compare hashes or signatures from the file with the ones published by the manufacturer.

**Risk of User Privileges:** The operating system often provides different user account types with different set of privileges and permissions. The Microsoft Windows Operating System provides three types, the “Standard-User”, “Administrator Account” and, the “Guest Account”. Generally speaking, providing a user with more privileges than needed for his or her tasks poses an unnecessary risk. A guideline is, to provide a standard user for each employee and sparingly provide administrative accounts when necessary. These administrative privileges should not stay permanently and have to be provided and revoked in a life-cycle process, for example LAPS<sup>25</sup>. LAPS provides the possibility of granting temporary administrative privileges for a person[32].

**Scripts and Executables:** Scripts and other executable files can be used for automation, however they inherit the risk of malicious use. If the execution of such files is necessary, it should be restricted to administrative users, which in turn should be restricted as described above. Only allowing execution of signed scripts is a further restriction option. [33]

**Risk of Data Loss:** The loss of important data is not only present in data-centers, but also on clients. Losing data can lead to losses in money and reputation. Thus, a central, automated back-up solution for relevant data needs to be put in place. Additionally, locally stored data (data-at-rest) needs to be encrypted.

---

<sup>23</sup> Confidentiality: Certain information must only be known and accessible to certain people.[31]

<sup>24</sup> Integrity: The data is trustworthy and free from tampering. It is authentic, accurate and reliable. [31]

<sup>25</sup> Local Administrator Password Solution

## 5 Countermeasures and Mitigation

### 5.1 Mitigation Strategys:

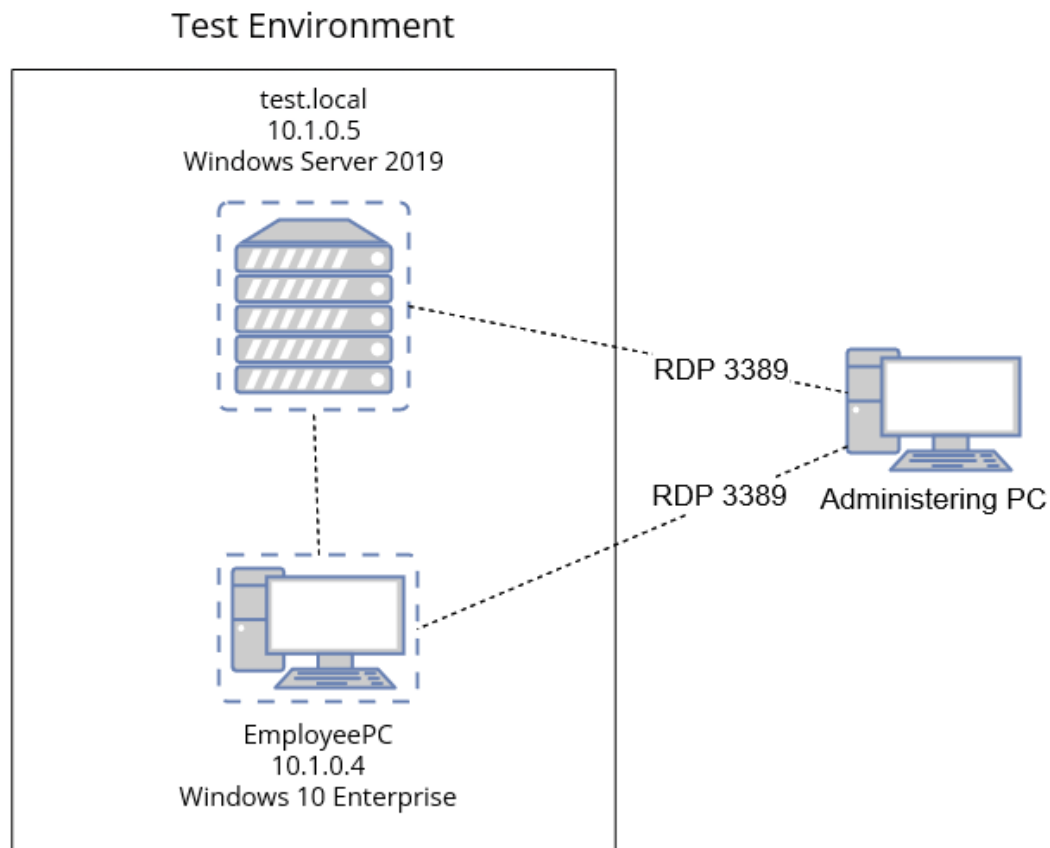
The main approaches to risk management can be separated into four categories [34]:

- **Risk-avoidance:** The risk-avoidance strategy is, to work with such foresight that, on the one hand, the probability of the risk occurring is close to zero and, on the other hand, almost all measures to be taken in the event of the risk occurring have already been planned in detail. This means, that strategic planning is done in a way, to avoid actions which involve risk.
- **Risk-acceptance:** When following this strategy, a certain risk is accepted. Possible reasons for this strategy are negligible effects, unsustainable costs or redundancies to compensate for the impact of the risk.
- **Risk-minimization:** This strategy aims to reduce the previously analyzed risk to a minimum. Actions and measures are actively taken to reduce the impact and the probability of a risk.
- **Risk-transfer:** The aim of this strategy is not to reduce risk, but to transfer the resulting consequences of an occurred risk to a third party. The possibilities here are to transfer the risk to an insurance company, to the customer or to a contractor.

After investigating several risks for clients, possible basic mitigation and risk reducing options will now be demonstrated.

### 5.2 Virtual Machine Environment:

For the practical implementation, a Domain, created in Microsoft Azure, will be used. The environment consists of one Microsoft Windows 10 workstation, which will represent a regular employee, and one Microsoft Windows Server 2019 server, which operates as Domain Controller, hosts the Active Directory Services and is illustrated in the following figure.



**Figure 6:** *Lab Environment*

The details of the deployment can be found on the GitHub repository<sup>26</sup> in the compressed zip-file "VM\_win10.zip" and VM\_Server2019.zip. The access to the Workstation and the Server is handled through the Remote-Desktop-Protocol (RDP)<sup>27</sup> on the default TCP and UDP port 3389. For most of the provided scripts, the Microsoft Windows Remote Server Administration Tools for Windows 10 must be installed<sup>28</sup>.

**Preface:** The following steps are done with an administrative account. It is recommended for convenience reasons, to use an account with administrative privileges for the initial setup of the security measures. After implementing the measures, the default workstation user must not have administrative privileges and the administrative account should only be used for explicit reasons and must be additionally secured. This process of user segregation will be described later on.

<sup>26</sup> GitHub Repository link: [https://github.com/fkarlSchachinger/BAC2\\_ClientSecurity-Practical](https://github.com/fkarlSchachinger/BAC2_ClientSecurity-Practical)

<sup>27</sup> RDP Protocol allows encrypted, wrapped and framed packet exchange [35].

<sup>28</sup> These tools can be added to Windows by downloading them from following link: [www.microsoft.com/en-us/download/details.aspx?id=45520](http://www.microsoft.com/en-us/download/details.aspx?id=45520)

As for the server administration, an administrative account was also used, however user and permission segregation on the Domain Controller and in Active Directory are out of the scope of this thesis.

### 5.3 Access and Theft mitigation:

**Physical Device Protection:** Securing your devices physically by putting them behind access control measures, is an important step to deny unauthorized persons access, as discussed in access control in Section 4.2.1. Controlling the business site through access controls like requiring keys or key cards (which should only give absolutely necessary access according to the *Least Privilege* Principle<sup>29</sup>).

Locking your devices physically to a table, for example with a Kensington Lock, may be an impracticable policy for mobile working employees, however for privilege access workstations (PAW)<sup>30</sup> it is recommended.

Some motherboard manufactures provide the BIOS Option "Chassis Intrusion", which monitors the physical opening of the Workstation chassis. If available, this should be enabled:

Implementation Chassis Intrusion detection:

1. In the boot-process of the workstation hit the (depending on the system) F10 or DEL key.
2. Follow the settings to Security and set *Chassis Intrusion* to enabled.

This setting is shown in Figure 7.

<sup>29</sup> "The Principle of Least Privilege states that a subject should be given only those privileges needed for it to complete its task." [36]

<sup>30</sup> PAW: A Privileged Access Workstation is a dedicated computing environment for sensitive tasks that is protected from Internet attacks and other threat vectors [37]

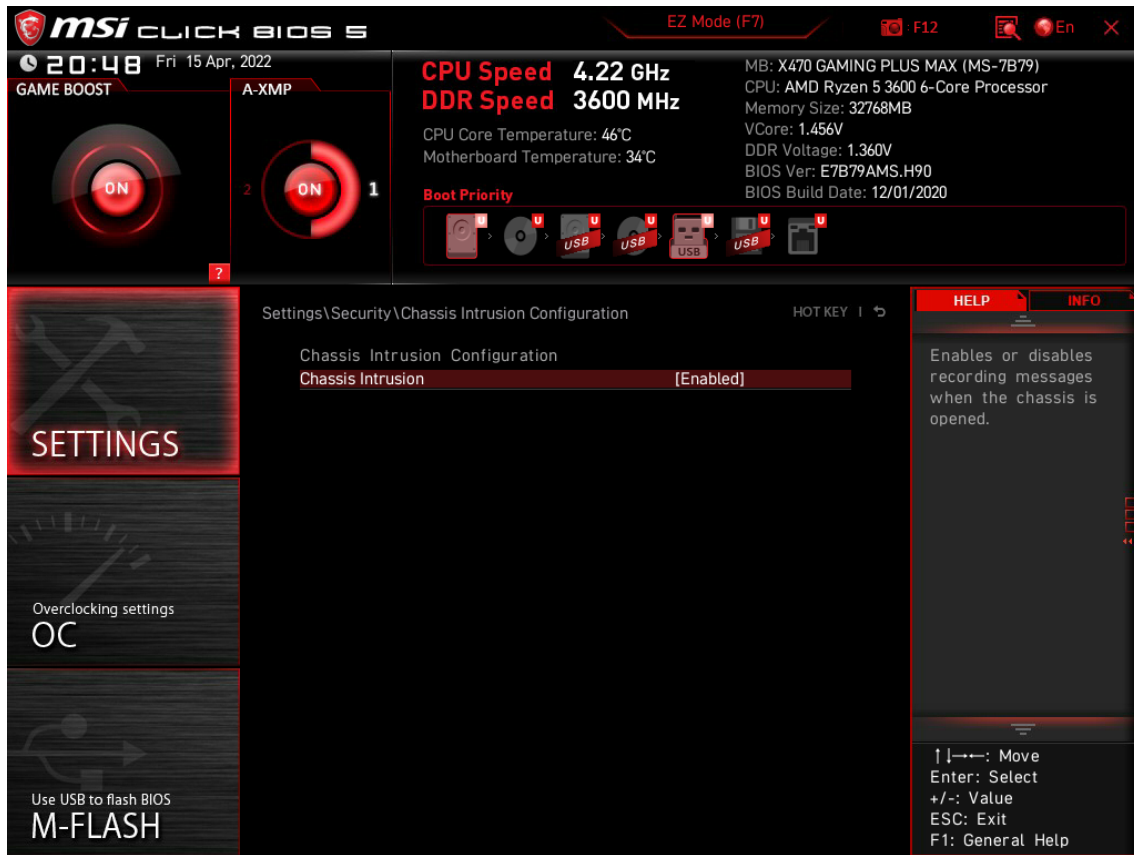


Figure 7: Chassis Intrusion

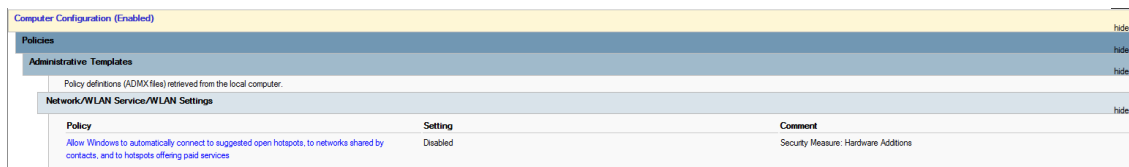
**Automatic Lock:** Whenever an employee leaves the workstation temporary, the access must be locked and require a password, to prevent actions by unauthorized persons. This should be automated, every time there is a certain time of inactivity on the workstation. This can be done by setting the group policy object “Interactive logon: Machine inactivity limit”. This setting among others will be set later automated with the provided script “SecurityScript.ps1”.

**Hardware Additions:** As previously mentioned, hardware-additions (Section 4.2.1) can pose a risk. Security measures are, disabling the auto-run feature and limiting hardware installation by the user via GPO<sup>31</sup>. These measures are also implemented in the provided script “Security\_Skript.ps1”. Disabling automatic connection to open hotspots is an additional measure, which can be manually set in the GPO:

*“Computer Configuration/Policies/Administrative Templates/Network/WLAN Services/WLAN Settings”*

In an enterprise environment a network and endpoint monitoring system should be put

<sup>31</sup> Group Policy



**Figure 8:** *Disable Automatic Hotspot connection*

in place additionally, to detect and mitigate unauthorized hardware installation. For extraordinary secure environments, an asset inventory of allowed device ID's can be put in place, to limit installation only to the allowed list. However, this is connected with great effort and may still allow other devices to be installed, as the device ID could be spoofed by an adversary. The practical implementations can be found in the “Access.Mitigations” group policy object after running the provided script.

**Encryption:** In case an attacker has obtained a storage-drive of the business, damage can be mitigated, if the drives of the business are always fully encrypted. In the Microsoft Windows 10 operating system this can be implemented through the “Bitlocker” feature. Before setting up this feature, certain options must be configured in the BIOS/UEFI.

## 5.4 Securing BIOS/UEFI:

The following settings must be set in the BIOS:

- **Enabling TPM 2.0:** The activation of the TPM<sup>32</sup> unlocks various security related functions. It is designed to carry out cryptographic operations, is tamper resistant and enables the generation, storing and limitation of cryptographic keys for device encryption. The TPM can also serve as a replacement for smart cards [38].
- **Enable Secure Boot:** Secure Boots makes sure that a device boots using only software that is trusted by the original equipment manufacturer (OEM) [39].
- **Enable Virtualization:** Enables CPU virtualization technology.
- **Set a BIOS Password:** To hinder adversaries from changing settings a BIOS Password must be set.

Reference figures for this settings are provided on the GitHub repository<sup>33</sup>.

<sup>32</sup> Trusted Platform Module

<sup>33</sup> [https://github.com/fkarlSchachinger/BAC2\\_ClientSecurity-Practical/tree/master/BiosScreenshots](https://github.com/fkarlSchachinger/BAC2_ClientSecurity-Practical/tree/master/BiosScreenshots)

## 5.5 Setting up Encryption:

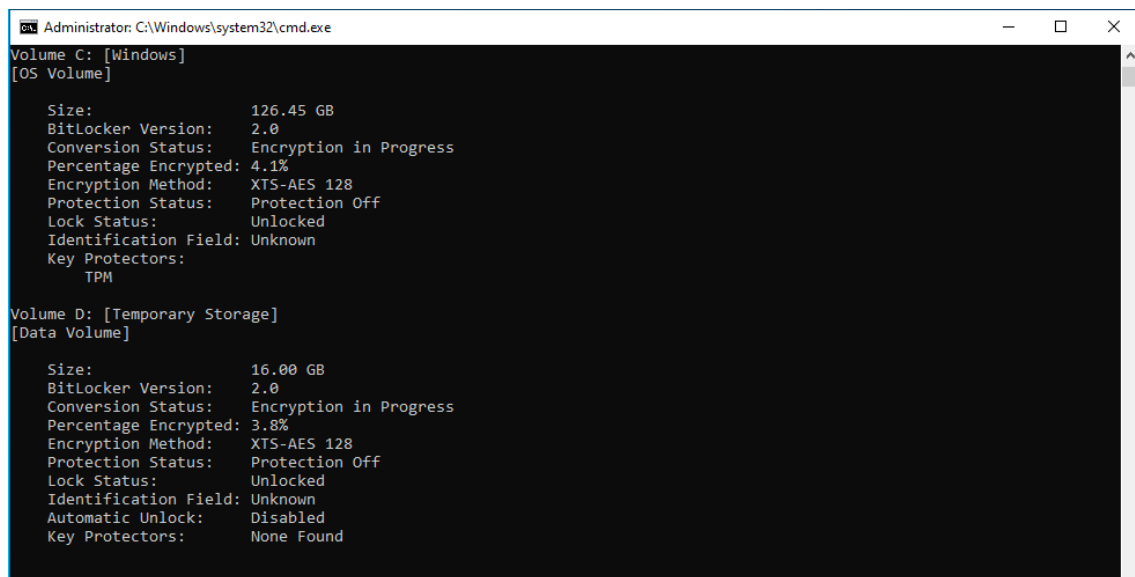
The Microsoft Windows 10 operating system provides a data protection feature called “BitLocker”, which encrypts the operating system drive. Data stored on systems must be encrypted by using a modern, secure encryption algorithm, in case the storage drive is physically stolen or the data on the drive is extracted by an malicious actor. To harm the business or extract information from the stolen data, it must be decrypted first. Depending on the algorithm used, this is very time consuming. In the provided script “StartUp\_BitLocker.ps1”<sup>34</sup>, which is called automatically by the initial script, the BitLocker feature will be enabled by calling the BitLockerDriveEncryption feature of the Windows 10 operating system. The BitLocker feature uses by default the *XTS-AES 128-bit* encryption standard. The code of the implemented script ‘StartUp\_Bitlocker.ps1’:

```
1      $var = manage-bde.exe -status | Out-String
2      $test = select-string -pattern "Protection Off" -InputObject $var
3      $test
4
5  if($var.contains('Protection Status:      Protection Off')){
6      manage-bde.exe -on C:
7      Write-Host 'Bitlocker: Beginning Encryption of C: Drive after reboot'
8      $title = 'Reboot for BitLocker Required:'
9      $question = 'Reboot now (Y) or later (N)?'
10     $choices = New-Object Collections.ObjectModel.
11         Collection[Management.Automation.Host.ChoiceDescription]
12     $choices.Add((New-Object Management.Automation.Host.
13         ChoiceDescription -ArgumentList '&Yes'))
14     $choices.Add((New-Object Management.Automation.Host.
15         ChoiceDescription -ArgumentList '&No'))
16     $decision = $Host.UI.PromptForChoice($title, $question, $choices, 1)
17     if($decision -eq 0){
18         Write-Host 'Rebooting now'
19         Restart-Computer
20     }else{
21         Write-Host 'Reboot in 5 mins'
22         Start-Sleep -Seconds 300
```

<sup>34</sup> [https://github.com/fkarlSchachinger/BAC2\\_ClientSecurity-Practical/tree/master/Skripts/StartUp\\_BitLocker.ps1](https://github.com/fkarlSchachinger/BAC2_ClientSecurity-Practical/tree/master/Skripts/StartUp_BitLocker.ps1)



```
23 Restart-Computer
24 }
25 }else{
26 Write-Host 'Already Encrypted'
27 }
```



```
Administrator: C:\Windows\system32\cmd.exe
Volume C: [Windows]
[OS Volume]

Size: 126.45 GB
BitLocker Version: 2.0
Conversion Status: Encryption in Progress
Percentage Encrypted: 4.1%
Encryption Method: XTS-AES 128
Protection Status: Protection Off
Lock Status: Unlocked
Identification Field: Unknown
Key Protectors: TPM

Volume D: [Temporary Storage]
[Data Volume]

Size: 16.00 GB
BitLocker Version: 2.0
Conversion Status: Encryption in Progress
Percentage Encrypted: 3.8%
Encryption Method: XTS-AES 128
Protection Status: Protection Off
Lock Status: Unlocked
Identification Field: Unknown
Automatic Unlock: Disabled
Key Protectors: None Found
```

Figure 9: *Encryption in Progress*

## 5.6 Secure Firmware:

“Firmware is a form of microcode or program embedded into hardware devices to help them operate effectively[40]”. This can range from the Workstation itself (BIOS), to peripherals or external supporting hardware like printers. Firmware is a form of software, which may contain vulnerable code and therefore needs to be patched regularly. Besides regular updates, important steps for security are also making sure the software updates come from a trusted source (the hardware manufacturer), avoiding and limiting the installation of untrusted hardware (which was implemented in Section 4.2.1) and finally setting up firmware-security (in example Secure Boot). Some practical measures implemented can be found in the group policy objects “FirmwareSecurity” and “StandardUser” after running the initial script.

By setting registry keys, features like “System Guard” and “VirtualizationBasedSecurity”, a more secure boot process is enabled. Through group policies, the installation of drivers can be limited.

Computer Configuration (Enabled)				hide
Policies				hide
Windows Settings				hide
Security Settings				hide
Local Policies/Security Options				hide
Devices				hide
Policy		Setting		hide
Devices: Allow undock without having to log on		Disabled		
Devices: Allowed to format and eject removable media		Administrators		
Devices: Prevent users from installing printer drivers		Enabled		
Devices: Restrict CD-ROM access to locally logged-on user only		Enabled		
Devices: Restrict floppy access to locally logged-on user only		Enabled		
System/Driver Installation				hid
Policy		Setting	Comment	
Code signing for driver packages		Enabled		
When Windows detects a driver file without a digital signature:			Warn	
Policy		Setting	Comment	
Configure driver search locations		Enabled		
Do not search floppy disk drives			Enabled	
Do not search CD-ROM drives			Enabled	
Do not search Windows Update			Enabled	

**Figure 10:** *Restricting Driver Installation*

## 5.7 Permission separation:

As described by the principle of Least Privilege in Section 5.3, a user should only have permissions he truly needs. Therefore, user accounts should only be equipped with the privileges and permissions, the employee assigned with the user-account absolutely requires for the designated tasks. By default, newly created users are added to the “Domain Users” security group in the active directory. This group can be split up further into user groups, in my example “StandardUsers”, and privileges can be accordingly managed by group affiliation. The “StandardUsers” user group represents my typical office worker, which is in no need of special privileges. To further increase security for these standard users, their permissions are restricted by the automatically linked group policy object “StandardUser”. This Group Policy Object (GPO) consists of multiple restrictions regarding software installation and the modification of settings in the operating system. Exemplary implemented restrictions:

Prevent access to registry editing tools	Enabled	
Disable registry from running silently?	Yes	
Policy	Setting	Comment
Prevent access to the command prompt	Enabled	
Disable the command prompt script processing also?	No	

**Figure 11:** *Exemplary restrictions*

The use of administrative privileges must also be further split into different account types. For example would a first-level help-desk support engineer not need domain administrative privileges. However, since these account types have to be specified in the active directory and are individual for businesses, this implementation will be limited to the standard user account and the automatic disabling of the initial administrative account used for the setup, through following code snippet:

```
1      #End of Measures, disable the admin account
2      $user = whoami.exe | Out-String
3      $userTrimmed = $user.Split("\")
4      net user $userTrimmed /active:no
```

When setting up a new workstation with the Microsoft Windows Operating System, the default local administrator account must be deactivated specifically. This should be automated at the operating system deployment to mitigate human errors.

## 5.8 Password Policy:

Secure passwords are an important security measure to protect accounts from unauthorized access. Threat actors can utilize different types of attacks to get hold of the password or gain knowledge about it. Common attack procedures are:

**Plaintext/unencrypted passwords:** A severe risk exists, when passwords are stored in plaintext. By default, most modern applications require complex passwords and store them encrypted. However, this risk has to be continuously monitored in the business, to make sure, passwords in for example API<sup>35</sup> or remote connection tools are not stored unprotected or un-hashed.

**Phishing and OSINT:** Malicious emails, Browser-in-the-Browser attacks or fake phone calls also pose a great risk, since it involves the end-user. This can be mitigated by training the employees of a business regularly and conduct a phishing assessment. OSINT<sup>36</sup> is information, which is openly available. Threat actors may use open source intelligence to derive a password combination for a specific user (maybe the user used a combination of his name together with his birth date). Further explanation of phishing can be found in section 2.1.1.

---

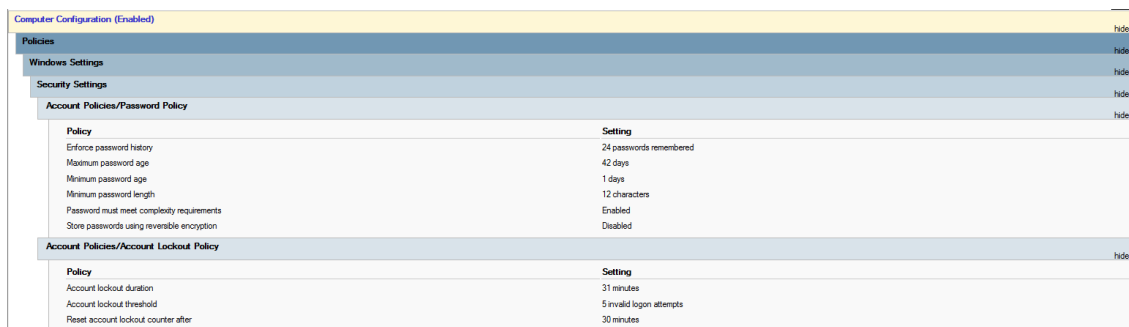
<sup>35</sup> Application Programming Interface

<sup>36</sup> Open Source Intelligence

**Rainbow tables and dictionary attacks:** A rainbow table consists of plaintext passwords and the associated password hash. A dictionary attack consists of a previously leaked or decrypted combination of username and password, which is used in a brute-force attack [41].

### 5.8.1 Mitigations:

**Group Policy Object:** In the active directory, the “Default Domain Policy” can be used to configure the default password policy for domain users. **Note:** As this Policy can not be extracted, the settings have to be defined manually, accordingly to the enterprise guidelines.



Computer Configuration (Enabled)	
Policies	
Windows Settings	
Security Settings	
Account Policies/Password Policy	
Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	12 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Account Policies/Account Lockout Policy	
Policy	Setting
Account lockout duration	31 minutes
Account lockout threshold	5 invalid login attempts
Reset account lockout counter after	30 minutes

**Figure 12:** *Domain Password Policy*  
[42]

The employees can be supported when choosing complex passwords by implementing a password manager solution. Additionally, multi-factor-authentication needs to be put in place, to even further reduce the risk of unauthorized access. In a Microsoft Windows environment, this can be done by utilizing Microsoft 365 features. For storing passwords, secure hash algorithms, such as SHA3<sup>37</sup> must be used with an adequate key length and the hashes must be salted<sup>38</sup>, this way rainbow table attacks can be mitigated.

**Microsoft Credential Guard:** In the Microsoft Windows 10 operating system, stored credentials and authentication is managed by the LSASS (Local Security Authority Subsystem Service) Service. This service can be further protected by using virtualization-

<sup>37</sup> Secure Hash Algorithm 3 Standard, specified by NIST in Federal Information Process Standard 202 in august 2015.

<sup>38</sup> Hash salting is a mechanism in which a randomly generated string is added as input to the hashing algorithm in addition to the password. A different hash is thus always generated for one and the same password.[43]

based security. Virtualization-based security isolates this service from the rest of the operating system and is implemented by following PowerShell CMDlet:

```

1      #Implement Credential Guard
2      $key = "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa"
3      Set-GPRegistryValue -Name "FirmwareSecurity" -Key $key
4      -ValueName "LsaCfgFlags" -Value 1 -Type DWord

```

## 5.9 Microsoft Defender Antivirus:

The Microsoft Windows 10 operating system comes with a built in antivirus software solution, the “Microsoft Defender”. As this software has great capabilities it naturally should be utilized. In the “SecuritySkript.ps1” a configuration is automatically added through registry keys and a group policy object. The advantages of the Defender are scanning of files on the workstation and identification of known malware by signatures which get updated by Microsoft regularly. The defined settings are as followed:

Windows Components/Windows Defender Antivirus/Scan			hide
Policy	Setting	Comment	
Check for the latest virus and spyware definitions before running a scheduled scan	Enabled		
Run full scan on mapped network drives	Enabled		
Scan network files	Enabled		
Scan packed executables	Enabled		
Scan removable drives	Enabled		
Specify the interval to run quick scans per day	Enabled		
Specify the interval to run quick scans per day	5		
Policy	Setting	Comment	
Specify the maximum percentage of CPU utilization during a scan	Enabled		
Specify the maximum percentage of CPU utilization during a scan	40		
Policy	Setting	Comment	
Turn on catch-up full scan	Enabled		
Turn on email scanning	Enabled		

**Figure 13:** *Defender Scan Configuration*

Among other settings defined, registry keys for the feature “Attack Surface Reduction Rules” are defined. These are rules created by Microsoft to harden the workstation and block common attack vectors<sup>39</sup>. The rules have options to be enabled to “Audit Mode” or “Block Mode”. Depending on the business use cases, these options have to be defined individually, however a strict start with “Block Mode” is recommended. Rules can be softened to “Audit Mode” if business use cases exist. Following settings are implemented with “Block Mode” by the script:

<sup>39</sup> Further explanation can be found in the official Microsoft documentation:  
<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide>

Block abuse of exploited vulnerable signed drivers
Block Adobe Reader from creating child processes
Block all Office applications from creating child processes
Block credential stealing from the Windows local security authority subsystem (lsass.exe)
Block executable content from email client and webmail
Block executable files from running unless they meet a prevalence, age, or trusted list criterion
Block execution of potentially obfuscated scripts
Block JavaScript or VBScript from launching downloaded executable content
Block Office applications from creating executable content
Block Office applications from injecting code into other processes
Block Office communication application from creating child processes
Block persistence through WMI event subscription
Block untrusted and unsigned processes that run from USB
Block Win32 API calls from Office macros
Use advanced protection against ransomware

## 5.10 Execution and Installation Rules:

To additionally implement security measures, execution of script files with the standard user must be further prohibited. This can be done by redirection certain script file extension to the notepad executable, to mitigate the execution of the script. This can be either implemented locally through a batch file, or through a group policy object.

Batch command:

```
1  ::Redirect Files to notepad
2  ftype htfile="%SystemRoot%\system32\notepad.exe" "%1"
```

Group Policy Object for User Configuration:

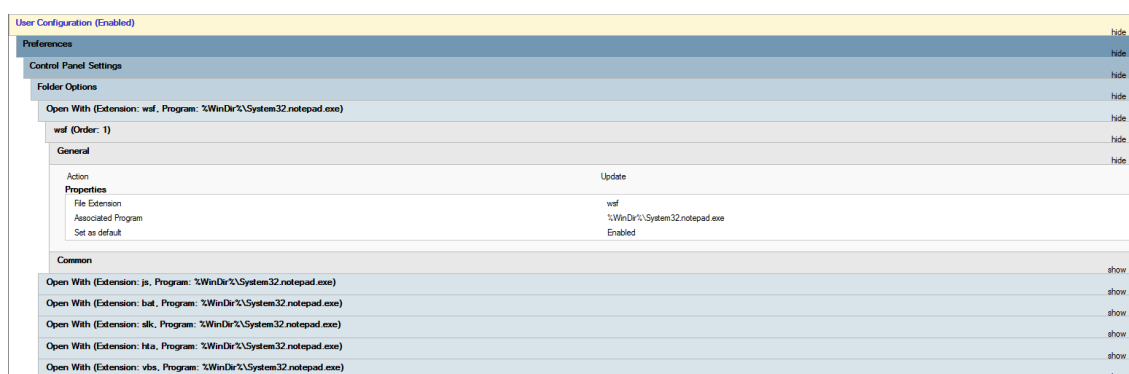





Figure 14: Script Redirection to Notepad through GPO

Microsoft Windows also offers more specific settings for restricting scripts, executables or Windows Installer files, which are grouped in the “Application Control Policies”, also called “Applocker”.

With these adaptable settings, it is possible to define different rules based on the active directory group membership of the user. Some of the defined settings are as followed:









Action	User	Name	Condition	Exceptions
 Deny	Everyone	All scripts located in the Program Files folder	Path	
 Deny	Everyone	All scripts located in the Windows folder	Path	
 Allow	BUILTIN\Administrators	(Default Rule) All scripts	Path	

**Figure 15:** *Applocker Script Execution Policy*

This policy can be customized to the needs of the company, for example enabling only installation of signed applications by certain publishers. A predefined set of rules is created through the provided script in the “Applocker GPO”, linked to the “CMPEmployees” organizational unit.

## 5.11 Local Firewall:

The Windows Defender Firewall is the local or host-based firewall implemented in the Microsoft Windows operating system. As this provides an additional layer of security, it should be turned on and configured accordingly to the business needs. Possible configurations can be done for the public, private and domain profile for inbound and outbound connections with the ability to allow or block traffic. For highest security, but also highest restriction, the approach should be to allow only specific traffic and block everything else. The, in the github repository included batch file<sup>40</sup> can be included in a group policy object as a start-up script which runs only once for the initial setup. Due to the differences in paths on different domains, the script path in the group policy object has to be adapted.

Outbound Rules												
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port	Authorized Computers
 Block calc.exe netconns		All	Yes	Block	No	C:\Wind...	Any	Any	TCP	Any	Any	Any
 Block cscript.exe netconns		All	Yes	Block	No	C:\Wind...	Any	Any	TCP	Any	Any	Any
 Block hh.exe netconns		All	Yes	Block	No	C:\Wind...	Any	Any	TCP	Any	Any	Any
 Block mshta.exe netconns		All	Yes	Block	No	C:\Wind...	Any	Any	TCP	Any	Any	Any
 Block Notepad.exe netconns		All	Yes	Block	No	C:\Wind...	Any	Any	TCP	Any	Any	Any
 Block regsvr32.exe netconns		All	Yes	Block	No	C:\Wind...	Any	Any	TCP	Any	Any	Any
 Block runscripthelper.exe netconns		All	Yes	Block	No	C:\Wind...	Any	Any	TCP	Any	Any	Any
 Block wscript.exe netconns		All	Yes	Block	No	C:\Wind...	Any	Any	TCP	Any	Any	Any

**Figure 16:** *Local Firewall Settings*

<sup>40</sup> [https://github.com/fkarlSchachinger/BAC2\\_ClientSecurity-Practical/blob/master/Skripts/Hardening.bat](https://github.com/fkarlSchachinger/BAC2_ClientSecurity-Practical/blob/master/Skripts/Hardening.bat)

## 5.12 Protocols and Services:

The operating system comes with a wide range of default protocols and services running, which often are not used or required in an enterprise environment. To reduce the attack surface and mitigate attack vectors of vulnerable protocols and services, those unused should be disabled. An implementation of this measure is done in the PowerShell script “ServicesAndProtocols.ps1”, also provided on the GitHub repository. Important measures are the disabling of the “Server Message Block” (SMB) protocol version 1, as it has multiple security vulnerabilities<sup>41</sup> and setting the “Transport Layer Security” protocol to version 1.3 for similar reasons.

```
1 Write-Host 'WinRM Services must be enabled on the Remote PC'
2 Write-Host 'Input Computer Name:'
3 $name = Read-Host
4 $cred = Get-Credential
5 $temp = 'XblAuthManager','XboxNetApiSvc','XblGameSave','XboxGipSvc',
6         'AxInstSV','PimIndexMaintenanceSvc_1a34cb0c','MapsBroker',
7         'lfsvc','NcbService','PhoneSvc','PcaSvc','RmSvc',
8         'SensorDataService','WalletService','wisvc';
9
10 $list = [System.Collections.ArrayList]$temp
11
12 Invoke-Command -ComputerName $name -Credential $cred -ScriptBlock{
13     #Disable Unecessary Services
14     foreach($item in $list){
15         $new = Get-Service $item
16         Set-Service -InputObject $new
17             -StartupType Disabled -Status Stopped
18     }
19     #Disable SMBv1 on Client
20     Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
21
22     #Set TLS to 1.2 Version
23     [Net.ServicePointManager]::SecurityProtocol =
24         [Net.SecurityProtocolType]::Tls13
25 }
```

<sup>41</sup> <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SMBv1>



```
26 #Disable SMBv1 on server  
27 Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

### 5.13 Applications:

As previously mentioned in Sections 4.2.2 and 2.1.1, installed Software and Applications may introduce vulnerabilities to the system, for example through open network ports, manipulated code or weak input sanitization. It is indispensable to regularly update and apply patches to the installed software, to reduce vulnerabilities and mitigate potential threats. Additionally, these software assets should be secured and hardened where possible.

With the Microsoft Windows 10 operating system, the Microsoft Edge Browser is installed on client workstations by default. As a browser is a highly utilized tool by office employees, it must be hardened additionally. Microsoft offers domain wide configuration settings for the Edge Browser through group policies. The settings for the Microsoft Edge group policy object have already been defined by specialists of the “Center for Internet Security (CIS)”. Therefore the Microsoft Edge Browser settings will be configured by utilizing these recommendations as a baseline. It must be noted, that predefined standards can be a good baseline for configurations, however they should not be blindly important but have to be revised and adapted accordingly to the IT-environment of the business. The settings defined by CIS can be found in the provided GPO as the object “29D42EA1-A2E0-46D9-AEC4-9913624497BE” and the latest official version from CIS can be found on the official website<sup>42</sup>. An exemplary setting of this policy is enabling the “TyposquattingChecker”. This setting warns the user, when he or she is trying to visit an illegitimate site, set up by threat actors for phishing purposes, which has a near identical URL<sup>43</sup> to the legitimate original website.

Other common applications of office employees are the Microsoft Office application collection. These applications provide features, which can be used for productivity but also from threat actors for nefarious purposes. Such a feature may be the option of using makros or visual basic executable content in a Microsoft Excel or Microsoft PowerPoint file.

---

<sup>42</sup> <https://www.cisecurity.org/cis-benchmarks/>

<sup>43</sup> Uniform Resource Locator

The provided batch script “Hardening.bat” configures baseline settings to weaken those threats, exemplary settings are:

```
1 reg add "HKCU\Software\Policies\Microsoft\Office\14.0\Word\Security"  
2     /v vbawarnings /t REG_DWORD /d 4 /f  
3  
4 reg add "HKCU\Software\Policies\Microsoft\Office\15.0\Word\Security"  
5     /v blockcontentexecutionfrominternet /t REG_DWORD /d 1 /f  
6  
7 reg add "HKCU\Software\Policies\Microsoft\Office\15.0\PowerPoint\Security"  
8     /v         blockcontentexecutionfrominternet /t REG_DWORD /d 1 /f
```

To ensure only secure and approved software is in the asset inventory of the business, software for employees should only be available and distributed from one central source, for example the “Software Center” (available when the System Center Configuration Manager is set up) or “Microsoft Endpoint Manager (Intune)”.

## 5.14 Conclusion to the Security Measures

The implementations done with the provided scripts present initial measures to improve client security in an enterprise environment and is not to be seen as a complete security setup. An additional important security measure is an effective back-up strategy, which may be implemented for individual clients on the workstation itself, but is in enterprise environments more often centrally managed. This can be done by having uniform storage locations for departments which are then secured with multiple back-ups or by implementing a cloud-solution.

In an enterprise environment, security can be improved by focusing and expanding on the discussed areas, and implementing additional measures in network and server infrastructure. The goal is to not only secure the clients, but to establish a defense-in-depth<sup>44</sup> security configuration for the enterprise, where the client poses as one of the inner layers, to protect the data and values of an enterprise.

---

<sup>44</sup> “Defense in depth is a strategy that leverages multiple security measures to protect an organization’s assets. The thinking is that if one line of defense is compromised, additional layers exist as a backup to ensure that threats are stopped along the way.[44]”

For all those measures and implementations, it is important to keep the *Business Value Chain* in mind. In order for cybersecurity and IT in general, to be relevant to and communicate with the business, they must understand how the business speaks and how the value is created in the business [45]. “Many security failures weren’t due to technical errors so much as to wring incentives: if the people who guard a system are not the people who suffer when it fails, then you can expect trouble [46]”.

## 6 Risk controlling

As noted in Section 5.14, the cyber-security strategy of an enterprise should consist of multiple layers, which can be categorized in different controls.

### Security controls [47]:

- **Preventive controls:** Controls with the goal to prevent the attack from reaching the asset in the first place.
- **Detective controls:** Controls with the goal of identifying that an attack is occurring, what kind of attack and where it came from.
- **Corrective controls:** These controls are designed to minimize the damage from an attack.
- **Compensating controls:** Controls, designed to compensate for the failure of other controls and mitigate the damage from an attack.

By evaluating current control sets against cyber threats, required actions can be derived. This evaluation should be done in a continuous cycle of reporting and subsequent decisions for actions. “Risk controlling fulfills the information function through reports to corporate management as well as to individual business unit and organizational units[48]”. In the area of client security, this can be enabled through periodical, structured reports from the different IT-departments where controls are implemented. Those related areas range from network, applications, servers, hardware and data-storage responsible or departments to the IT-security responsible. In Section 3.3 the importance of consistency in this reports is discussed. These reports should consist of important measures to further strengthen and expand security controls, which may be derived from continuous monitoring and auditing the environment.

**Auditing:** Regular audits either through external professionals or internal staff is a necessary process to ensure current implemented security controls are effective and security goals are reached. External audits can take form in so called “Penetration Tests”, where external professionals try to find weak spots and vulnerabilities in the IT-environment of the system.

Other audits may target compliance topics or the fulfillment of certain industry standards, such as the ISO-27001 standard.

**Continuous Monitoring:** The continuous monitoring of actions and behaviours in the IT-environment provides the ability to react to anomalies, which may indicate the actions of a threat actor. Auditing events on client can for example be specified through group policy, which is implemented in the test environment through the GPO “Monitoring”:

Computer Configuration (Enabled)		hide
Policies		hide
Windows Settings		hide
Security Settings		hide
Advanced Audit Configuration		hide
Account Logon		show
Account Management		show
Detailed Tracking		show
Logon/Logoff		show
Object Access		show
Policy Change		show
System		show
Administrative Templates		hide
Policy definitions (ADMX files) retrieved from the local computer.		
System/ Audit Process Creation		show
Windows Components/ Windows PowerShell		show

**Figure 17:** *Auditing Settings*

For enterprises of certain size, implementing a SIEM<sup>45</sup> software to manage the information gathered, not only from clients, but also from servers, the firewall and other assets, and handle security relevant events. Establishing a SOC<sup>46</sup> may also be of worth. A SOC can be defined as ”a centralized team in a single organization that monitors the information technology environment for vulnerabilities, unauthorized activity, acceptable use/policy/procedure violations, intrusions into and out of the network, and provides direct support of the cyber incident process [45]”.

## 6.1 Conclusion the Risk Management process:

The individual steps of the risk management, beginning with the description of context and scope delimitation in Section 3.1, the implementation of security measures in part 5 to the different strategies of controlling risk have been discussed in this thesis. Summarizing, the information security risk management process can be summarized in this figure:

<sup>45</sup> Security Information and Event Management

<sup>46</sup> Security Operations Center

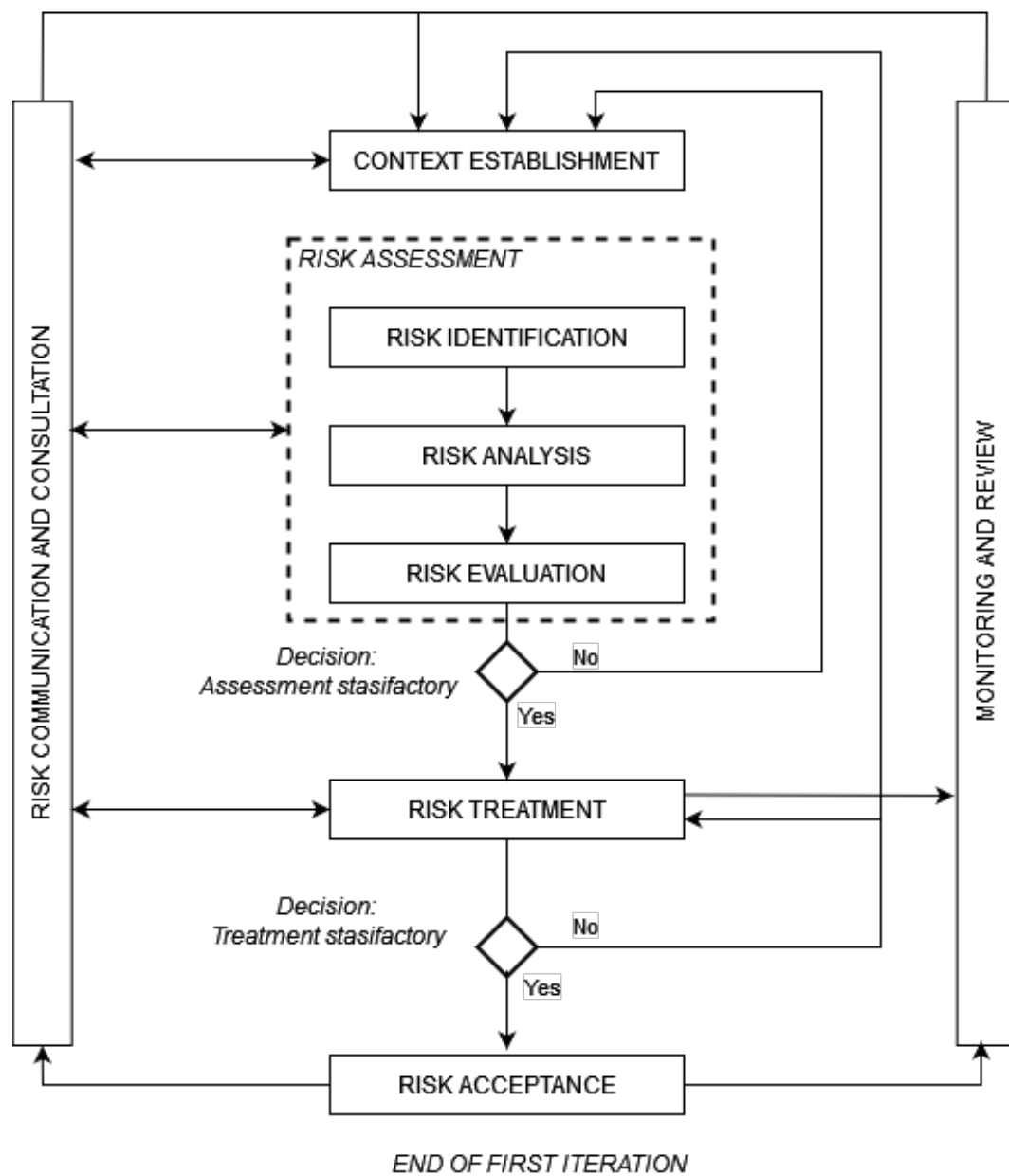


Figure 18: Illustration of an information security risk management process [20]

## 7 Conclusion and Outlook

In the introduction to the thesis, the question of systematic risk-management was raised. Before a company can begin such a process, the current situation and the risk-preference of the acting company must first be determined. The risk appetite was described by a practical example in the subject area of microeconomics. By giving an overview of the current situation of risk-management and introducing common risks in cyberspace, an outline of the duties for managing risks in information technology could be established. Methods to identify areas in need of planned measures and how the impact of events in those areas can be measured were given, to then be applied for collecting theoretical risks for computer workstations in an enterprise. With the practical implementation of countermeasures to these very identified cyber threats, the possibilities to enhance information technology security on computer workstations were introduced. By providing an overview of the topic of risk controlling, a cycling process to manage risk was completed.

**Outlook:** With faster evolving, more complex technologies being integrated into our environment, while global dependencies increase, it is indispensable for companies to put a management process for risks in place. The fundamental overview given in this thesis should motivate to further expand on security measures and decide on a strategy for handling unforeseen events.

The topic of cyber security offers the possibility to go into great detail, not only on computer workstations, but in the information technology industry as a whole. Depending on the asset inventory and the informational value of a company as well as their business strategy, it is up on the decision-makers to choose the depth and effort of security measures, recent events however show, that cyber security is not optional nowadays. The situation of digital data and its intrinsic value require an up-to-date cyber strategy for businesses, which is now and will be in the future challenged by threat actors.

## Bibliography

- [1] S. Hunziker, *Enterprise Risk Management, Modern Approaches to Balancing Risk and Reward*. Springer Gabler, 2019, p. 14, ISBN: 978-3-658-25357-8.
- [2] T. Wolke, *RISK MANAGEMENT*. Walter de Gruyter GmbH, 2017, pp. 1–10, ISBN: 9783110440539.
- [3] F. Romeike, *Risikomanagement*. Springer Gabler, 2018, pp. 2–5, ISBN: 978-3-658-13952-0.
- [4] *Risk management*. [Online]. Available: <https://dictionary.cambridge.org/dictionary/english/risk-management> (visited on 02/28/2022).
- [5] Allianz Global Corporate & Speciality, *Allianz risk barometer*, 2022. [Online]. Available: <https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html> (visited on 02/28/2022).
- [6] AmTrust Financial, *2021 small business risks*, 2022. [Online]. Available: <https://amtrustfinancial.com/blog/small-business/small-business-risks-potential-exposures> (visited on 02/28/2022).
- [7] Aon plc., *2021's top 10 risks, The pandemic shines a spotlight on interconnected risks*, Oct. 27, 2021. [Online]. Available: <https://theonebrief.com/2021s-top-10-risks-the-pandemic-shines-a-spotlight-on-interconnected-risks/> (visited on 02/28/2022).
- [8] Visualcapitalist, Iman Gosh, *The biggest business risks around the world*, 2021. [Online]. Available: <https://www.visualcapitalist.com/the-biggest-business-risks-around-the-world/> (visited on 02/28/2022).
- [9] Fortinet Inc., *Phishing definition*. [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/phishing> (visited on 03/07/2022).
- [10] —, *Attack vector definition definition*. [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/attack-vector> (visited on 03/07/2022).
- [11] —, *Malware definition*. [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/malware> (visited on 03/07/2022).
- [12] —, *Malware definition*. [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/insider-threats> (visited on 03/07/2022).
- [13] F. Inc., *Defense in depth*. [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/ddos-attack> (visited on 04/22/2022).



- [14] M. Crouhy *et al.*, *The essentials of risk management*. McGraw-Hill Education, 2014, p. 5, ISBN: 978-0-07-182115-5.
- [15] Deloitte Touche Tohmatsu Limited, *Benchmarkstudie risikomanagement*, 2020. [Online]. Available: <https://www2.deloitte.com/de/de/pages/audit/articles/risikomanagement-benchmarkstudie-2020.html> (visited on 03/05/2022).
- [16] “Risk appetite - critical to success,” Committee of Sponsoring Organizations of the Treadway Commission (COSO), 220 Leigh Farm Road, Durham, NC 27707 USA, Tech. Rep., May 2020.
- [17] R. S. Pindyck and D. L. Rubinfeld, *Microeconomics*. Pearson Education Limited, 2018, pp. 180–200, ISBN: 978-1-292-21331-6.
- [18] ———, *Microeconomics, Graphic 5.3*. Pearson Education Limited, 2018, p. 187, ISBN: 978-1-292-21331-6.
- [19] G. Verteegen, *Risikomanagement in IT-Projekten*. Springer-Verlag Berlin Heidelberg, 2003, pp. 90–110, ISBN: 978-3-642-55737-8.
- [20] “Information technology — security techniques — information security risk management,” International Organization for Standardization, Geneva, CH, Standard, Jun. 2018.
- [21] BlueVoyant, *Managign cyber risk across the extended vendor ecosystem*, Oct. 2021. [Online]. Available: <https://www.bluevoyant.com/news/bluevoyant-research-reveals-rise-in-supply-chain-cybersecurity-breaches-as-firms-struggle-to-effectively-monitor-third-party-cyber-risk/> (visited on 03/12/2022).
- [22] “Information technology — security techniques — information security risk management – requirements (iso/iec 27001:2013 + cor. 1:2014),” International Organization for Standardization, Geneva, CH, Standard, Jun. 2018.
- [23] T. Macaulay and B. Singer, *Cybersecurity for Industrial Control Systems*. Auerbach Publishers, Incorporated, 2011, p. 142, ISBN: 978-1439801963.
- [24] “International standard - risk management - guidelines,” International Organization for Standardization, Geneva, CH, Standard, Feb. 2018.
- [25] P. E. J. Green, *Enterprise Risk Management - A Common Framework for the Entire Organization*. Elsevier Inc., 2016, pp. 5–10, ISBN: 978-0-12-800633-7.
- [26] G. Verteegen, *Risikomanagement in IT-Projekten*. Springer-Verlag Berlin Heidelberg, 2003, p. 146, ISBN: 978-3-642-55737-8.

- [27] StatCounter - Global Stats, *Desktop operating system market share worldwide*, Feb. 2022. [Online]. Available: <https://gs.statcounter.com/os-market-share/desktop/worldwide> (visited on 03/25/2022).
- [28] National Institute of Standards and Technology, “Protecting controlled unclassified information in nonfederal systems and organizations,” U.S. Department of Commerce, Washington, D.C., Tech. Rep. Protecting Controlled Unclassified information, SP 800-171, Revision 2, version 2, 2020. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-171r2> (visited on 03/25/2022).
- [29] Fortinet Inc., *What is shadow it?* [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/shadow-it> (visited on 04/16/2022).
- [30] T. M. Corporation, *Replication through removable media*. [Online]. Available: <https://attack.mitre.org/techniques/T1091/> (visited on 03/25/2022).
- [31] Fortinet Inc., *Attack vector definition definition*. [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/cia-triad> (visited on 03/25/2022).
- [32] T. M. Corporation, *Rainbow table password cracking*. [Online]. Available: <https://attack.mitre.org/tactics/TA0004/> (visited on 04/25/2022).
- [33] ———, *Rainbow table password cracking*. [Online]. Available: <https://attack.mitre.org/tactics/TA0002/> (visited on 04/25/2022).
- [34] G. Verteegen, *Risikomanagement in IT-Projekten*. Springer-Verlag Berlin Heidelberg, 2003, pp. 169–210, ISBN: 978-3-642-55737-8.
- [35] Microsoft Corporation, *Understanding the remote desktop protocol (rdp)*, Sep. 24, 2020. [Online]. Available: <https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol> (visited on 04/08/2022).
- [36] M. Gegick and S. Barnum, *Least privilege principle*, May 10, 2013. [Online]. Available: <https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege> (visited on 04/25/2022).
- [37] Stanford University, *Privileged access workstation (paw), increased security for high risk systems*, Jan. 2022. [Online]. Available: <https://uit.stanford.edu/service/paw> (visited on 04/22/2022).
- [38] M. Cooperation, *Trusted platform module technology overview*, Mar. 24, 2022. [Online]. Available: <https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview> (visited on 04/16/2022).

- [39] Microsoft Corporation, *Enable secure boot on windows devices*, Dec. 21, 2021. [Online]. Available: <https://docs.microsoft.com/en-us/mem/intune/user-help/you-need-to-enable-secure-boot-windows> (visited on 04/21/2022).
- [40] Fortinet Inc., *Firmware definition*. [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/what-is-firmware> (visited on 04/17/2022).
- [41] T. M. Corporation, *Rainbow table password cracking*. [Online]. Available: <https://capec.mitre.org/data/definitions/55.html> (visited on 04/25/2022).
- [42] M. Corporation, *Password policy microsoft*, Mar. 9, 2022. [Online]. Available: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements> (visited on 04/28/2022).
- [43] Michael Kofler et al., *Hacking & Security, Das umfassende Handbuch*. Rheinwerk Verlag, Bonn 2020, 2020, p. 258, ISBN: 978-3-8362-7191-2.
- [44] Fortinet Inc., *Defense in depth*. [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/defense-in-depth> (visited on 04/22/2022).
- [45] D. Murdoch, *Blue Team Handbook, SOC SIEM and Threat Hunting Use Cases, A condensed field guide for the Security Operations team*. 2019, p. 16, ISBN: 978-1-091-493896.
- [46] R. Anderson, *Security Engineering, A Guide to Building Dependable Distributed Systems*. John Wiley & Sons Inc., 2020, p. 275, ISBN: 978-1-119-64278-7.
- [47] C. Moschovitis, *Cybersecurity Program Development for Business, The Essential Planning Guide*. John Wiley & Sons Inc., 2018, pp. 90–110, ISBN: 978-1-119-43000-1.
- [48] T. Wolke, *RISK MANAGEMENT*. Walter de Gruyter GmbH, 2017, pp. 290–310, ISBN: 9783110440539.

## 8 Used Tools

For the practical part of the thesis, following software, tools and libraries were used:

Function	Software & Version
IDE	Visual Studio Code
Extension	PowerShell by Microsoft
Extension	Run in PowerShell by Toby Shell
Development tool	Microsoft PowerShell ISE
Operating System Client Virtual Machine	Windows 10 21H2 Enterprise
Operating System Server Virtual Machine	Windows Server 2019 Version 1809
Installed Server Features and Tools	Microsoft Active Directory
Scripting language	PowerShell
Scripting language	Batch
Version Control	GitHub

**Table 2:** *Used Tools*