



University of
Zurich^{UZH}

A Gordon-Loeb-based Visual Tool for Cybersecurity Investments

Christian Omlin
Zurich, Switzerland
Student ID: 14-936-165

Supervisor: Muriel Franco, Eder Scheid
Date of Submission: January 28, 2022

Abstract

As digital dependency increases, companies are becoming more exposed to cybersecurity threats. Cybersecurity has become a critical factor for companies that depend on information systems. Therefore, companies are interested in implementing appropriate cybersecurity solutions to reduce the risk of a successful cyberattack. If these investments are done incorrectly or not at all, the consequences can be devastating. Successful attacks can lead to system failures and data theft, often resulting in financial loss and damage to the company's reputation. However, it is difficult for a company to evaluate how much money they should invest in cybersecurity and in which measures they should invest. Since budgets are often limited, companies aim for the highest level of security while keeping costs as low as possible. The goal of this thesis is therefore to develop a visual tool for cybersecurity investments. The tool supports the calculation of the optimal cybersecurity investment for different business areas. It also provides the user with suitable cybersecurity measures. Furthermore, it shows the user the calculated profitability of the various security investments.

Acknowledgments

First of all I feel the need to thank my supervisor Muriel Franco for his regular assistance, our in-depth discussions and his very helpful inputs throughout this thesis.

I would also like to thank my co-supervisor, Eder Scheid for his support.

Finally, I would also like to thank Prof. Dr. Burkhard Stiller, head of the Communication System Research Group (CSG) at University of Zurich, for giving me the possibility to write my bachelor's thesis about such an interesting topic.

Contents

Abstract	i
Acknowledgments	iii
1 Introduction	1
1.1 Motivation	2
1.2 Description of Work	2
1.3 Thesis Outline	3
2 Background	5
2.1 Cybersecurity Threats	5
2.1.1 Distributed Denial-of-Service (DDoS)	5
2.1.2 Ransomware	7
2.1.3 Phishing	8
2.2 Cybersecurity Investments	9
2.3 Gordon-Loeb Model	10
3 Related Work	13
4 Approach	15
4.1 Methodology	15
4.2 User requirements	16
4.2.1 Business Profile	16
4.2.2 Segment	17

4.2.3	Security Recommendation	17
4.2.4	Return-On-Security-Investment (ROSI)	18
4.3	Cybersecurity Investment	18
4.3.1	Segment Valuation	19
4.3.2	Cybersecurity Investment Calculation	19
4.4	Return On Security Investment (ROSI)	20
5	Prototype and Implementation	23
5.1	Technology Stack	23
5.2	Architecture Overview	24
5.3	User Interface	25
5.3.1	Home Page	25
5.3.2	Business Profile	26
5.3.3	Segments	27
5.3.4	Recommendation	30
5.4	Server	32
5.4.1	Investment Calculator	33
5.4.2	Valuation Estimator	34
5.4.3	Protection Recommender	35
5.4.4	ROSI Calculator	35
5.5	Database	36
5.5.1	Business Profiles	36
5.5.2	Optimal Investment Equation	36
5.5.3	Segment Definitions	37
5.5.4	Segments	39
6	Evaluation	41
6.1	Case Study No. 1 - Optimal Investment	42
6.2	Case Study No. 2 - Cybersecurity Recommendations	44
6.3	Case Study No. 3 - ROSI Index	46

<i>CONTENTS</i>	vii
7 Summary, Conclusions & Future Work	49
Bibliography	50
Abbreviations	55
List of Figures	55
List of Tables	58
A Installation Guidelines	61

Chapter 1

Introduction

Cybersecurity is increasingly becoming a key player in the digital age. With the ever-increasing connectivity of internet-enabled devices, the risk of cyberattacks is also increasing. As an example, Internet-of-Things (IoT) can automate and improve processes, but it also provides points of attack for attackers. Considered on a global average, a cyberattack is carried out every 39 seconds, resulting in more than 2200 attacks per day [5]. In the first quarter of 2021, the number of cyberattacks increased by 17% compared to the first quarter of 2020 and by 1.2% compared to the fourth quarter of 2020 [22]. A successfully executed attack very often leads to high costs. As an example, in 2020 an average data breach resulted in costs of \$3.86 million [17].

Further, the COVID-19 pandemic is also playing a key role, as many companies are allowing employees to work remotely. This circumstance leads to attackers taking advantage of quickly deployed systems and targeting them [9]. This has led to a sharp increase in phishing attacks, malicious mails and malware during the COVID-19 crisis [9]. It has also been noted that there is an increase in attacks on hospitals and medical research facilities. Especially for SMEs, the sudden change represents a considerable risk, as they usually do not have the same security systems, expert knowledge and budget as a large company. According to [9] the biggest challenges of a SME are low cybersecurity awareness, insufficient protection for critical and sensitive information, budget issues, lack of cybersecurity expertise and lack of suitable guidelines.

If we consider the technical side, it is possible to verify that there is a massive amount of security measures placed in the market, such as firewalls, anti-virus programs, encryption, security monitoring, physical security or backups. However, making the right choice is not a simple matter. Besides, 84% of all cyberattacks rely on social engineering [9], cybersecurity awareness training also becomes critical for companies [21]. As already mentioned, not every company has the same prerequisites to secure itself against these attacks. Large companies such as banks and insurance companies have a more generous budget which means they can afford more expensive security systems or it is easier for them to hire specialists. For SMEs, therefore, the fundamental question is how they can invest their limited budget optimally in IT security systems and how much money is worth investing in which system. The latter question will be elaborated later in this paper.

1.1 Motivation

To protect themselves against cyberattacks companies invest in Information Technology (IT) security systems. It is estimated that \$150 billion was spent on cybersecurity in 2021 [30]. This is an increase of 12.4% compared to the previous year. This shows that companies need to protect themselves more and more against the increasing number of cyberattacks. But making investments is not enough. Cybersecurity investments need to be targeted.

In order to benefit from accurate security measures, the risks must first be verified. Furthermore, it has to be considered which components of a company are more vulnerable to an attack and which ones have to be protected in the best possible way. Therefore, the different business components must be analyzed to know the value of each component and its vulnerability in order to make the right investment with this information. Another question is how much money a company should invest in cybersecurity.

This is exactly the question the Gordon-Loeb model[14] addresses. The Gordon-Loeb model is a mathematical economic model which analyzes the optimal investment in cybersecurity. The model calculates the optimal amount of investment with the help of the value of the data or service, how much the data is at risk (*i.e.*, attack probability) and the probability an attack on the data is going to be successful.

Since the Gordon-Loeb model is difficult to apply to a whole company, an extension of the model was developed which calculates the optimal investment based on information segmentation [15]. This means that the company is not considered as a whole, but is broken down into different segments. For each segment the investment is then calculated with the help of the Gordon-Loeb model. Thus, the company has the opportunity to invest more in segments that present a high value and are more vulnerable to attacks than in segments that are less important. Therefore, the Gordon-Loeb model and information segmentation are intended to show companies how much they should invest in cybersecurity per segment. However, there is still a lack of visual tools to help the users apply the model in different scenarios in an intuitive way.

1.2 Description of Work

The main goal of this thesis is to develop a visual tool that provides mechanism for decision makers to configure their business information and compute the Gordon-Loeb metric for each configured information segment. To achieve this, the user is able to create different segments. Since the value of the segment must be determined in order to calculate the optimal investment, the tool provides value estimation support for the segments. Based on the segment information, the tool then calculates the optimal cybersecurity investment. The tool presents the calculated values in a well-structured table. The table helps decision makers to understand how much they should invest in cybersecurity measures. In addition, the tool suggests suitable cybersecurity measures to the user. To fulfill this requirement, the MENTOR recommendation system [12] is integrated into

the tool to display solutions suitable for the segment and cybersecurity attack types. To simplify the user's decision between the different cybersecurity solutions the tool calculates the Return-On-Cybersecurity-Investment (ROSI).

After the prototype has been created, a series of appropriate case studies are conducted which represent real-world scenarios. The case studies demonstrate the usefulness and correctness of the designed tool and show how a decision maker can invest in cybersecurity solutions with the help of the tool.

1.3 Thesis Outline

The rest of the thesis is structured as follows. Chapter 2 provides the theoretical basis for the thesis. Chapter 3 discusses related work in this area. Chapter 4 presents the approach, highlighting the user requirements and calculations of the metrics used for the prototype. In the following chapter 5, the developed prototype is presented and the technologies used for it. The evaluation is introduced in chapter 6. Chapter 7 concludes the thesis and provides suggestions for future work to improve the tool.

Chapter 2

Background

This chapter provides the basic knowledge necessary for the understanding of the work. First, the most common types of cybersecurity threats are presented. After that the focus lies on how companies invest in cybersecurity and what the challenges are. The existing models are also briefly discussed. Finally, the Gordon-Loeb Model concepts and its different nuances are explained.

2.1 Cybersecurity Threats

Cybersecurity threats is a common term in our society and is becoming increasingly important. Not least because of the current COVID-19 pandemic, in which many companies had to have their workers work remotely at short notice, which led to cybersecurity threats. In the scope of this section, three different attacks are described in more detail.

2.1.1 Distributed Denial-of-Service (DDoS)

The goal of a distributed denial-of-service (DDoS) attack is to disrupt the normal operation of a network, service or server. This is achieved when the target or the underlying infrastructure is flooded with Internet data. To overwhelm a target with vast amounts of data requires multiple compromised Internet-connected devices [3].

These devices were previously infected with malware so that the attacker can remotely control each device. A group of infected devices is called a botnet [3]. Using the botnet, the attacker then launches the attack by flooding a target or its infrastructure with requests from all devices simultaneously [23]. The more devices there are in the botnet, the more powerful the DDoS attacks. If the target does not have DDoS protection, it will be overwhelmed by the many requests and will respond very slowly or not anymore at all, which leads to a denial of service [23]. The difference between a DDoS and a DoS attack is that a DoS attack originates from a single device, whereas a DDoS attack involves multiple devices sending simultaneous requests [7].

Unlike other types of cyberattacks, a DDoS attack does not attempt to enter the system or breach data. Rather, it aims to overload a target, such as a website or server, and thus makes it unavailable.

DDoS attacks can be divided into three general categories: volume-based attacks, protocol attacks, and application layer attacks [24].

Volume-Based Attacks: Volume-based DDoS attacks are the most common DDoS attacks of the three categories. They use a huge amount of computers, which are often distributed all over the world, to flood a website with traffic. The large amount of data overloads the available bandwidth of the website, making it inaccessible or slow [24].

UDP flood is an example of a volume-based attack. The attackers use the User Datagram Protocol (UDP), which is an essential part of the Internet Protocol (IP). In a UDP flood, the attacker sends many requests to random ports, causing the target to receive more UDP packets than it can process. The result is that the target is overwhelmed and stops responding [24].

Protocol Attacks: Unlike volume-based attacks, protocol attacks target server resources rather than bandwidth. The target of the attacks is the so-called *intermediate communication equipment*. This means the intermediate between the website and the server, which are, for example, load balancers or firewalls. By sending phony protocol requests, the attackers use up the available resources. This overloads the website and server resources [24].

An example of such an attack is Smurf DDoS. The attacker uses ICMP (Internet Control Message Protocol) packets that contain the victim's spoofed IP address. He then sends these packets to an IP broadcast address, which can be, e.g. a router or a firewall. If the network is large enough, the victim is flooded with data, resulting in a denial of service [24, 2].

Application Layer Attacks: Application layer attacks, also called *Layer 7 DDoS* attacks, use common Internet requests such as HTTP GET and HTTP POST. One reason why such attacks are particularly effective is that such an attack consumes server resources as well as network resources [1].

These attacks focus on application vulnerabilities. Also in this attack, the goal is to crash a server by overloading it with requests. The requests appear to be legitimate by imitating a normal user. The difficulty then lies in distinguishing a normal user from an attacker. Such attacks aim to disable certain features or functions of a website, such as online transactions [24].

An example of an application layer attack is Slowloris. Slowloris is a software which allows a single machine to paralyse a web server with minimal use of network resources. The software connects to the target server and then sends only partial requests, which it keeps open as long as possible. At the same time, Slowloris sends other HTTP partial requests. The goal is to send so many partial requests, which are never completed, that the server's maximum load is exceeded and it becomes unreachable [24].

In 2019, 16 DDoS attacks were recorded every minute. Which led to more than 23'000 attacks per day [36]. This example shows that a DDoS attack is not a rarity, but an essential threat that should not be underestimated. During the Corona crisis, DDoS attacks and their complexity increased. There was a 55% increase in DDoS attacks between

January 2020 and March 2021 [10].

A study by Kaspersky shows that the average cost of a DDoS attack for small and medium-sized businesses is around \$120'000. A successful DDoS attack at a large company can cause a damage of over \$2 million. As the number and complexity of attacks continue to increase, the average cost in 2021 is expected to be significantly higher than in 2017 [18].

2.1.2 Ransomware

Ransomware is a specific type of malware. Other types of malware are trojans, spyware or worms, for example, which will not be discussed further [32]. In a ransomware attack, the data on the victim's computer is locked and thus made inaccessible. After the data has been made inaccessible, which is often done by encryption, the attacker blackmails the victim. Only in case of a payment the attacker would decrypt the data and make it accessible to the victim again. Unlike other types of attacks, in this attack the victim is notified that an attack has taken place and the victim receives targeted instructions on how to recover from the attack. Since cryptocurrencies do not require identity disclosure, claims are often made in virtual currency, such as Bitcoin [31].

Ransomware malware is spread through infected malware applications, malicious attachments in emails, phishing email, infected external storage devices or compromised websites [31]. There are several types of ransomware, the three common ones are presented below.

Locker Ransomware: In this attack, devices and systems are prevented from performing their basic functions. For example, mouse and keyboard functions can be disabled or login privileges can be denied. If the victim wants to regain full use of the device or system, he has to pay a ransom. This type of attack does not destroy or encrypt any data [35].

Crypto Ransomware: The goal of this attack is to encrypt the victim's data that is as valuable as possible, such as photos, videos or documents. The data is not deleted, but access is denied to the victim. Only against payment the attacker will decrypt the data with the cryptographic key. In this attack, a countdown is often displayed, threatening to delete all data if the payment is not made on time [35].

Scareware: In this attack, a system or device is infected by a malware that pretends to have found a malicious software or other malfunction. The victim is then asked to make a payment to a fake service or company in order to fix the problem. The name of the attack was chosen because the victim often gets scared and thinks that it is a real problem without knowing that it is a scam [35].

The WannaCry attack was one of the largest and most damaging cyberattacks in history. It was a ransomware crypto worm that infected Microsoft Windows operating systems. This worm encrypted data and demanded bitcoins to decrypt the data. The worm used a vulnerability in Microsoft Windows as an entry point to access the system. Within a day, more than 23,000 computers were infected in at least 150 countries [28].

This attack had a financial impact worldwide, it is estimated that this cybercrime caused \$4 billion in damage worldwide [19].

In the first half of 2021, ransomware attacks almost doubled. During these two quarters, 1097 attacks were recorded. In contrast, in 2020, 1112 successful ransomware attacks were

recorded for the entire year. This shows that ransomware attacks have increased sharply, not least because of the current COVID-19 pandemic [4].

2.1.3 Phishing

The term phishing refers to a social engineering attack that is intended to fraudulently obtain a person's private information. Using emails or websites, fraudsters try to obtain sensitive information from potential victims. In many cases, the collected information is not used themselves, but sold to cybercriminals on the darknet [29].

The attackers try to obtain information from their potential victims, such as credit card details, login credentials, social security numbers, bank account details, tax and medical records, and sensitive business data such as customer names and contact information. With justifications such as the loss of access to the bank account or the blocking of the social media account, the scammers try to get the victims to enter sensitive data [29, 25]. The scammers try to deceive the potential victims by creating fake websites for example, that look exactly like the real ones. To make it even more believable, they use a URL that looks very similar to the original ones, which makes it even harder to spot a fake website. The goal of the scammers is to make users believe that they are on the real website and therefore enter sensitive data [29].

There are different types of phishing attacks, below are the most common ones.

Email-Phishing: This form of phishing is the most common type and has been used since the 1990s. In the process, the scammers send the phishing email to all the email addresses they can muster. Such a mail contains, for example, the information that their account has been compromised and that it is necessary to react immediately by clicking on the link. Such attacks are usually easy to identify, as they often contain spelling and grammatical errors. Often, the sender's email address differs only slightly from the original one. In this attack, quantity is prioritized over quality [33].

Spear-Phishing: A spear-phishing attack is specifically targeted at an organization or specific individual. Targeted information is collected in advance, such as company logos, email and web addresses, information about partner companies or personal information about individuals in order to appear as authentic as possible. Often, the extra effort to collect the information pays off with a high number of targets falling for the scam [26]. Often, spear phishing emails have similar layout but contain, for example, fake invoices from business partners. Further, the victim is prompted to download an important attached document, which then installs malicious software that collects personal information [29].

Whaling: The whaling attack targets a company's top management. Targeted information or problems are communicated to the executive in the hope that they will reveal sensitive information such as high-level access data to company accounts or trade secrets. As an example, an email could state that the company is facing legal consequences and that they need to click on the link to get more information. By clicking on the link, malware can be installed or the user is asked to enter sensitive data [26, 29, 33].

Phishing attacks doubled from 2019 to 2020. The FBI reported 114'702 phishing victims in 2019, then over 240'000 victims the following year. It is estimated that phishing attacks caused \$54 million in damage in 2020. Many scammers choose topics which have a connection to the current COVID-19 pandemic to reach a large target audience. As an example, unemployment insurance and disaster loans were often targeted [34].

2.2 Cybersecurity Investments

In the previous section, we discussed various types of cyberattacks that can cause enormous damage. To protect themselves against such attacks, companies and private individuals invest in cybersecurity. As already mentioned, the number of attacks and their complexity is constantly increasing, which leads to higher investment costs against such threats. In 2020, over \$121 billion was invested in cybersecurity [30]. For 2021, an increase of 12.4% is expected, not least due to the current COVID-19 pandemic [30].

Investing in cybersecurity is easier said than done. First, a company must identify the cyber threats that are most relevant to their company or industry sector. Further, not all components of a company are equally valuable. There are areas that would cause a high potential damage in case of a successful attack and on the other hand there are components that would cause less damage. Thus, it is essential to protect the areas that would cause high damage and have a high probability of becoming victim of an attack with the appropriate cybersecurity investment.

Large companies such as banks or insurance companies often have a significantly larger budget available for cybersecurity than SMEs. Thus, large companies can afford experts who implement company-specific security systems. Often, comprehensive security subscriptions are not geared towards small companies and would also exceed the budget [9].

Cybersecurity is a special topic that requires special knowledge. However, in an SME it is common for one employee to take on several tasks, consequently one employee can be responsible for cybersecurity as well as for other areas. Cybersecurity solutions often require IT expertise to implement and manage properly. If an employee is only partially involved in cybersecurity, the expertise is often not sufficient to deploy the appropriate system in the best possible way. This poses a major challenge for SMEs [9].

Another difficulty is to determine how much money to invest in cybersecurity. Two different approaches are discussed in the scope of this chapter.

Return on Security Investment (ROSI), as defined according to [6], is the calculation of the financial return on an investment in security. By comparing the financial benefit and the cost of the investment, the investment can be quantitatively evaluated. In the field of information security, there are different approaches of how the ROSI is calculated. What all approaches have in common is that the ROSI is a value that is made up for the financial benefit compared to the costs. Many approaches use concepts such as Annualised Rate of Occurrence (ARO) and Annualised Loss Expectancy (ALE) as part of the ROSI calculation [6].

Based on the ROSI calculation, conclusions can then be drawn about how much money should be invested in cybersecurity.

Another attempt to determine the level of investment is made by the Gordon-Loeb model, which is described in more detail in the next section.

2.3 Gordon-Loeb Model

The Gordon-Loeb model is a mathematical economic model that calculates the optimal level of investment in information security. Like many decisions, a cost-benefit analysis is performed for this model. An additional investment in cybersecurity makes sense if the expected additional benefits are higher than the expected additional costs. In mathematical terms, the optimal investment is at the point where the expected marginal cost is exactly equal to the expected marginal benefit [14].

The Gordon-Loeb model (GL model) contains the following basic assumptions. First, information of companies and organizations are vulnerable to cyber attacks, which is denoted with v ($0 \leq v \leq 1$). This represents the probability that an information asset will be breached under current conditions. Furthermore, the potential loss of the breached information asset is expressed as L . Here, the value of the information stock equates to the potential loss and can be expressed as a monetary value. It can be concluded that vL expresses the expected loss before the cybersecurity investment. The third and final assumption is that a cybersecurity investment, denoted as z , reduces v depending on the productivity of the cybersecurity investment. The GL Model denotes $s(z,v)$ as the security breach probability function. Or, put another way, $s(z,v)$ denotes a function that takes into account the productivity of different levels of cybersecurity investment and thus provides a measure of the probability of vulnerability of an information set after an investment in cybersecurity. The GL model assumes that the function is twofold continuously differentiable and strictly convex. This means, the benefit increases at a decreasing rate with further investments. In simple terms, this means that a further investment in cybersecurity can have a positive effect but brings diminishing returns, which illustrates Figure 2.1. Further, the GL model assumes that the probability of a possible successful cyber attack can be close to zero, but will never be zero, as there is always a residual vulnerability that cannot be covered [14].

By making the above assumptions, equations can be established. The following equations assume that the price of a unit of investment, z , is equal to one. In the following equation, the expected benefit of an investment in cybersecurity is referred to as EBIS and is equal to the reduction in an organization's expected loss attributable to the investment [14].

$$EBIS(z) = [v - S(z, v)] L$$

Since organizations have only one decision variable, the function above is referred to as a function of z . The parameters v and L are given variables which the company cannot influence. The net benefit of an investment is called ENBIS, which is equivalent to EBIS minus the cost of the investment. The equation for this is as follows [14]:

$$ENBIS(z) = [v - S(z, v)] L - z$$

Maximizing the above equation is mathematically the same as minimizing the following expression:

$$S(z, v)L + z$$

Further transformations and optimization of z show that the optimal level of investment is exactly when the marginal benefit of a cyber investment equals the expected marginal cost. In Figure 2.1, this point is denoted by z^* . Gordon and Loeb showed that the optimal investment level does not exceed vL/e or about 37% of the expected loss. This insight can be expressed as follows [14]:

$$z^*(v) < (1/e)vL$$

Companies often have several information areas at their disposal, which makes information segmentation inevitable. To find the optimal investment per segment, four steps are necessary [14]:

Step 1: Estimating the value and therefore the potential loss (L) of each segment.

Step 2: Estimate the probability of each segment's information falling victim to a successful cyberattack.

Step 3: Create a grid with all possible combinations of step 1 and step 2. Each cell of this grid represents the expected loss (L) without cybersecurity investments. The expected loss represents the potential benefit that can be gained by investing in cybersecurity.

Step 4: Derive the level of cybersecurity investment by increasing the investment as long as the benefit of the additional investment is bigger than or equal to the cost of the additional investment. Since not all investments in cybersecurity have the same productivity, the optimal amount for investments in different segments will vary.

With these four steps, it should be possible for an organization to determine the optimal cybersecurity investment level for each segment.

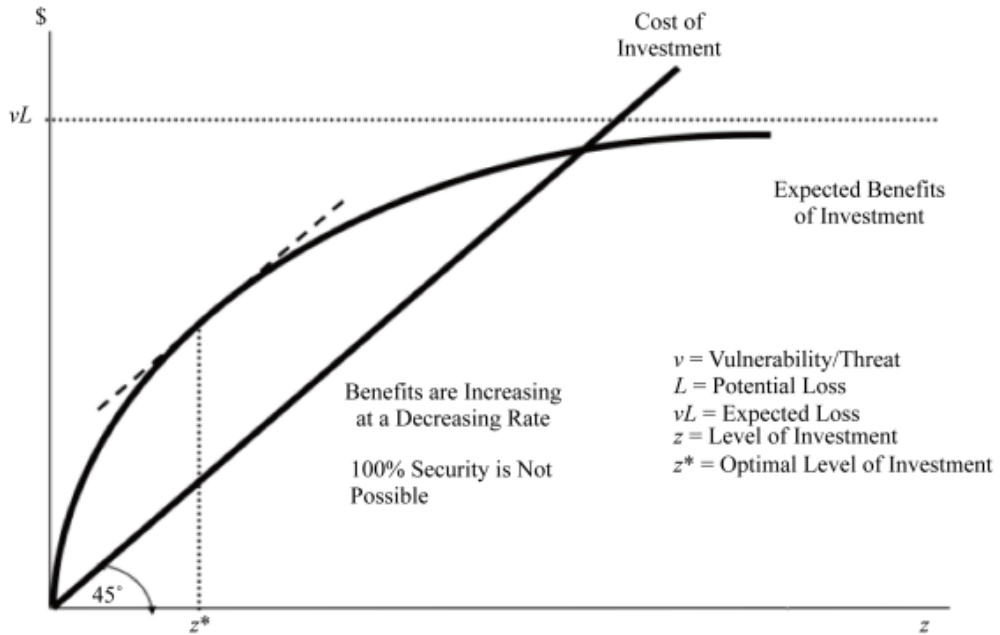


Figure 2.1: Benefits and costs of an investment in cybersecurity [14]

Chapter 3

Related Work

Due to the fact that there are more and more Internet-enabled devices and the number of cyber-attacks is increasing every year, the significance of cybersecurity investments is becoming more and more important. Therefore, a lot of research is being done in this area, trying to make it as easy as possible for a company to invest in cybersecurity. A few of these approaches will be analyzed in more detail in this chapter.

Fowler and Chen described a new method called Cybersecurity Performance Index (CsPI) [11] for evaluating cybersecurity investment decisions. With the CsPI method, the authors replace the traditionally used Return on Investment (ROI) metric. ROI is used to evaluate investments based on return on investment, which is not appropriate for cybersecurity investments because they do not generate a direct profit. Summer Fowler and Peter P. Chen suggest applying the established technique called *Earned Value* which is common in project management to the field of cybersecurity investments. Earned Value (EV) is the percentage of the total budget that is completed at a given point in time in a project. The goal is to measure the progress of cybersecurity spending against a plan. The plan should include protection, detection, response, and recovery goals to be achieved with the investment. Business objectives and threats should be considered. It should demonstrate how well current cybersecurity investments are performing against a plan.

Another approach based on an extension of the Gordon-Loeb Model is described in [20]. This model is a dynamic extension of the classical Gordon-Loeb model, where the depreciation rate of the cybersecurity assets and the return on investment is additionally taken into account. It is shown that the depreciation costs in the dynamic model are lower than implicitly assumed in the classical model, while the rate of return threshold is higher, which causes the utilization costs to decrease in general. Due to this difference, the economic efficiency of the system increases.

[16] presents an approach where the Gordon-Loeb Model is linked to the Cybersecurity Framework of the National Institute for Standards and Technology (NIST). The NIST framework is a guide for organizations to manage and reduce cybersecurity risks. It provides organization-specific activities based on standards, guidelines and practices to mitigate cyber risks. The NIST Framework describes that an organization should evaluate its cybersecurity risk management based on a cost-benefit analysis, but it does not provide

guidance on how to do so. [16] provides an approach to integrating cost-benefit analysis into the NIST Framework.

Another approach based on the Gordon-Loeb Model is discussed in [15], thus showing the benefits of information segmentation when evaluating the optimal amount of cybersecurity investment. It is an analytical model that provides conditions for segmenting information to reduce total investment costs and expected loss.

Table 3.1 compares the above works with each other. It distinguishes whether the Gordon-Loeb model is used, whether it supports information segmentation, whether it is a visual tool, and whether specific countermeasures are proposed. The last row of the table represents the tool that will be implemented in the scope of this thesis.

Table 3.1: Related Work Comparison

Work	Uses Gordon-Loeb Model	Information Segmentation	Visual Tool	Protection Recommendation
CsPI [11]	No	No	No	No
Dynamic extension of GL Model [20]	Yes	No	No	No
GL Model / NIST Integration[16]	Yes	No	Yes	Yes
Information Segmentation[15]	Yes	Yes	No	No
Cybersecurity Investment Tool (This thesis)	Yes	Yes	Yes	Yes

The data shown above represent that there are many approaches to simplify an organization's cybersecurity investment. It is also evident that the Gordon-Loeb model is an accepted approach for determining the level of cybersecurity investment, of which many extensions have been developed. However, there is no visual tool that calculates the optimal investment level based on the Gordon-Loeb model and then proposes suitable security systems. Therefore, this work is of central importance for organizations that want to calculate the optimal cybersecurity investment level based on information segmentation in a tool and then receive suggestions for cybersecurity systems in the same tool.

Chapter 4

Approach

The focus of this work is to implement a visual tool that helps decision makers to invest in cybersecurity. Decision makers can use this tool to create a business profile that represents their company. After creating the profile, the user is allowed to create different business segments and manage them. After each segment is added, the summary table is updated. This table provides information about the optimal cybersecurity investment and demonstrates the monetary advantage of information segmentation. With the integration of MENTOR[12], the user can select between appropriate cybersecurity recommendations and calculate the Return-On-Security-Investment (ROSI).

Within the scope of this thesis, a prototype was designed and developed to show the feasibility of the proposal. Details are discussed in Chapter 5. Furthermore, three case studies were carried out, which are discussed with in Chapter 6.

4.1 Methodology

Figure 4.1 illustrates the process from creating a business profile to selecting a cybersecurity solution and calculating the Return-On-Cybersecurity-Investment index. To create different business segments the user must first create a business profile, which is described in more detail in the Section 4.2.1. After creating the business profile, the user is allowed to create different business segments. Examples of segments are databases or a web server hosting a web store. To create a segment, the user must select the type of the segment, which is described in Figure 4.1 with Step 2.1. Determining the value of the segment, which is described in the figure in Step 2.2, is discussed in more detail in Section 4.3.1. Once a segment is created by the user, the system calculates the optimal cybersecurity investment. This is denoted by Step 3 in the figure below and is explained in Section 4.3.2. As a next step, the user can choose between different cybersecurity solutions. Step 4 in the figure illustrates this process. The user information required for this is described in Section 4.2.3. Step 5 in the figure describes the user's ability to calculate the Return-On-Security-Investment index of a selected cybersecurity solution. User inputs required for this calculation are described in more detail in Section 4.2.4. Section 4.4 explains the calculation of the Return-On-Security-Investment index.

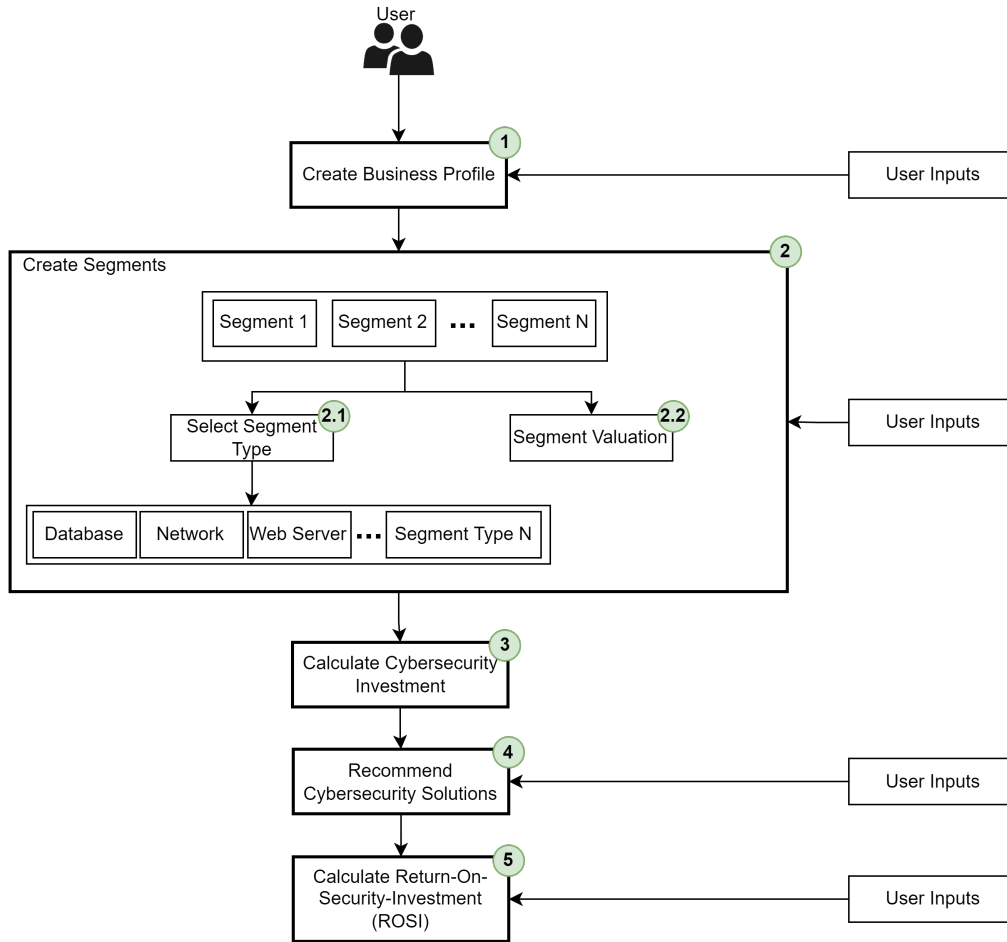


Figure 4.1: Methodology Diagram

4.2 User requirements

In order to calculate the optimal level of cybersecurity investment for the decision maker and then propose suitable cybersecurity solutions, the user has to provide a set of parameters while interacting with the tool. These available features, interactions, and information required from user are discussed in this section.

4.2.1 Business Profile

The business profile represents the company. To create such a profile, the user must submit key data of the company to the system. With this information, the determination of the segment value can be optimized and it is used for proposing appropriate cybersecurity solutions. The creation of the business profile is described in Figure 4.1 with Step 1.

- **Company Name:** This parameter represents the name of the company.
- **Number of Employees:** How many employees the company currently employs.

- **Revenue:** The annual revenue (\$) of the company.
- **Region:** This parameter provides information in which region the company operates. The user can choose between the following regions *Europe*, *North America*, *South America*, *Africa* or *Asia*.

4.2.2 Segment

A segment represents a technical business area of a company. The optimal investment amount is calculated for each segment. Creating segments is described in Figure 4.1 with Step 2. The following parameters are required for this:

- **Segment Name:** The parameter represents the name of the segment, which can be freely chosen by the user.
- **Segment Type:** In order to suggest suitable cybersecurity threats to the user and simplify the monetary valuation of the segment the system needs the type of segment. The system allows the selection between *Web Server*, *Network* or *Database*.
- **Value:** In order to calculate the optimal cybersecurity investment level, the monetary value (\$) of the segment is needed. Since it is often difficult to determine this value, the application provides an assistance for the valuation of the segment.
- **Risk:** The *Risk* parameter describes the probability of a cybersecurity attack. The user is allowed to specify a number between 0 and 100. This parameter is needed to determine the optimal investment.
- **Vulnerability:** Vulnerability is also needed to calculate the optimal cybersecurity investment. It describes the probability that a cybersecurity attack on the segment will be successful. Values between 0 and 100 are allowed.

4.2.3 Security Recommendation

After the optimal cybersecurity investment has been calculated, suitable cybersecurity solutions are proposed for the segment. The system receives the suggestions through the integration of MENTOR [12]. The parameters listed below are necessary to provide suggestions that are precisely tailored to the segment. Proposing cybersecurity solutions is described in Figure 4.1 with Step 4.

- **Region:** This parameter represents the region of the company being offered the cybersecurity solution. The default value is the region of the created business profile.
- **Investment:** The monetary amount (\$) to be raised for the cybersecurity solution. By default, the calculated optimal cybersecurity investment is displayed.

- **Attack Type:** This parameter reflects the cybersecurity threat against which the segment should be protected. The user can choose between different types of attacks which are adjusted to the segment type. Furthermore, the user is allowed to select cybersecurity solutions for all listed attack types or categories of attack types.
- **Deployment Time:** The time-frame in which the cybersecurity solution will be deployed. *Seconds, Minutes, Hours* or *Days* can be selected.
- **Leasing Period:** The length of time the cybersecurity solution would like to be leased. The user can choose between *Minutes, Hours, Days, Weeks* or *Months*.
- **Service Type:** This parameter allows the user to choose whether the segment should be protected proactively or reactively. Thus, it is possible to select between *Proactive* and *Reactive*.

4.2.4 Return-On-Security-Investment (ROSI)

For each cybersecurity solution displayed, the user can calculate the Return-On-Cybersecurity-Investment (ROSI) index. The ROSI index is discussed in more detail in Subsection 4.3. To calculate the ROSI, the parameters listed below are required. The calculation of the Return-On-Security-Investment index is described in Figure 4.1 with Step 5.

- **Mitigation Rate:** The mitigation rate refers to the reduction of risk by the selected cybersecurity solution. The default value is the number provided by MENTOR, but the user is free to enter any number between 0 and 100.
- **Cost of Incident:** This parameter represents the monetary damage (\$) caused by a successful cybersecurity attack. The default value is the monetary value of the segment. This value can be adjusted by the user.
- **Annual Rate of Incidence:** To perform the ROSI calculation, the estimated annual frequency rate of the selected attack type must be specified, which this parameter describes. The user is free to choose which frequency to submit to the system.

4.3 Cybersecurity Investment

The calculation of the optimal investment level is a core competence of the application. The user is allowed to create different segments. From each segment the system calculates the optimal amount of investment. By segmenting, the optimum of each segment can be calculated, which gives a smaller total investment amount than if all segments are merged into one first and calculate the optimum second. This financial advantage is provided also by the application.

4.3.1 Segment Valuation

To calculate the optimal investment level the value of the segment must be estimated. However, as mentioned before, it is very difficult for a user to determine the monetary value of the segment. Therefore, the application provides an aid to facilitate this decision. The system allows the user to enter parameters tailored to the segment, which are then evaluated based on research. Thus, the user receives a proposal for the value of the segment, which he can accept or change. This process is described in Figure 4.1 with Step 2.2.

Database

Based on data breach evaluations and reports, such as the one from IBM [17], the application can help determine the value of a segment. The user can specify how many records are stored in the database for different categories. The system multiplies the given number by the value of a record of this category. This allows the application to give an estimate of the total value of the database. Table 4.1 illustrates the different parameters with their corresponding values.

Table 4.1: Database Valuation Parameter

Parameter	Value
Number of Customer Data	\$175
Number of Anonymized Customer Data	\$171
Number of Employee Data	\$163
Number of Intellectual Property Data	\$151
Number of Other Corporate Data	\$150

Web Server

Estimating the monetary value of a web server that is responsible for a sales platform is not trivial. However, research has shown that the value of a website is often regarded as being between 24 and 36 times the monthly revenue of the corresponding sales platform [27]. To give an estimate of the value of the web server, the application queries the monthly profit of the web store and multiplies it by the average of 24 and 36.

4.3.2 Cybersecurity Investment Calculation

The application calculates the optimal cybersecurity investment based on an extension of the Gordon-Loeb Model. This extension combines the Gordon-Loeb Model with the idea of information segmentation. The determination of the optimal cybersecurity investment is described in Figure 4.1 with Step 3.

An important factor in this calculation is the so-called breach probability function. It is denoted as $S(z, v)$, where z describes the monetary investment and v the vulnerability of the segment. The breach probability function describes the productivity of the investment, which first increases and then decreases after a certain point. From this point on, each additional investment is higher than the resulting benefit [15]. The breach probability function for segment i ($i = 1, 2, \dots, N$) is expressed as follows:

$$S_i(z_i, v_i) = S\left(\frac{z_i}{L_i/L}, v_i\right)$$

L_i describes the value of the segment where L comprises the value of all segments.

Each segment can minimize the segment's total cybersecurity costs as below [15]:

$$\min_{z_i} [S\left(\frac{z_i}{L_i/L}, v_i\right)L_i + z_i]$$

With the resulting z^* , the optimal investment can then be calculated as follows [15]:

$$S\left(\frac{z_i^*}{L_i/L}, v_i\right)L_i + 1 = 0$$

To calculate the optimal investment in cybersecurity the application uses the following data breach function [15]:

$$S_i(z_i, v_i) = \frac{v_i}{1 + \frac{1}{L * 0.001} \frac{z}{L_i}}$$

Thanks to this Gordon-Loeb Model extension, the system calculates the optimal investment level for each segment. In addition, the monetary advantage of information segmentation is also illustrated in the application.

4.4 Return On Security Investment (ROSI)

To determine the cost-effectiveness of a cybersecurity investment, the system uses the Return On Security Investment (ROSI) index. The calculation of the ROSI index is described in Figure 4.1 with Step 5. This index is used because cybersecurity investments do not bring a direct profit but reduce a potential damage. The ROSI calculation is an extension of the Return On Investment (ROI) formula. The ROI calculation looks as follows [8]:

$$ROI = \frac{\text{Gain from investment} - \text{Cost of investment}}{\text{Cost of investment}}$$

The ROI index makes statements about how effective the investment is compared to the return. The result is expressed as a percentage. The higher this number, the higher the

effectiveness of the investment compared to the return. As mentioned before, this index can be poorly applied to cybersecurity investments, as cybersecurity investments do not yield a monetary return. Instead, the ROSI index is applied. When evaluating cybersecurity investments, the focus is on assessing how much potential loss can be prevented by an investment. Therefore, the monetary value of the investment must be compared with the monetary value of the risk reduction. The formula of the ROSI index is defined as follows [8]:

$$ROSI = \frac{ALE * \text{mitigation ratio} - \text{Cost of the solution}}{\text{Cost of solution}}$$

ALE is defined as follows [8]:

$$ALE = ARO * SLE$$

Where *ARO* stands for the estimated annual rate of a cyberattack occurrence. *SLE* represents the monetary damage caused by a successful cybersecurity attack.

Using the *mitigation rate*, which represents the percentage value of risk reduction from the cybersecurity investment, the ROSI index can be calculated. Through the ROSI index, the system provides the decision maker with valuable information on how effective his cybersecurity investment is. This makes it easier for the user to select the appropriate cybersecurity solution for segments.

Chapter 5

Prototype and Implementation

This chapter provides details of the technologies used, the architecture, and describe in details each component of the architecture necessary to implement the approach described in Chapter 4.

5.1 Technology Stack

Figure 5.1 shows the different layers of the application and the technologies used for it. The architecture represents a three-tier architecture (*cf.* Section 5.2). The first layer (*i.e.*, User Layer) consists of the user interface, which allows to capture user interactions and to visualize data. The user layer is developed with the framework Angular within its latest version. Angular was developed by Google and is a TypeScript based front-end web application framework. TypeScript is a programming language based on the JavaScript programming language.

The second tier of the architecture describes the Business Logic Layer. The task of this layer is data processing and data preparation. In addition, all complex calculations should be performed in this layer. The connection between the user interface and the business layer is ensured with the Hypertext Transfer Protocol (HTTP). Since the information should be transmitted in a programming language independent format, the JavaScript Object Notation (JSON) is used. This data format allows to send and receive data between different subsystems. The business logic layer was implemented using the NestJS framework, which is a framework based on Node.js and has a similar application structure as Angular.

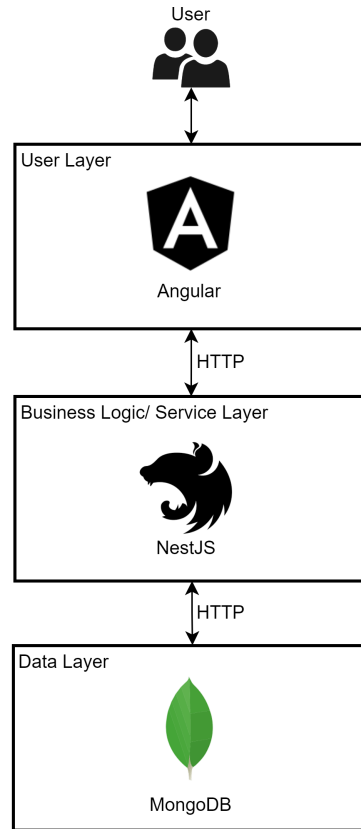


Figure 5.1: Technology Stack

The last layer of the architecture contains the databases required for storage of relevant information for the application. The database is responsible for persisting information. MongoDB was used to implement this layer. MongoDB is a document-oriented NoSQL database management system. This technology allows to save data in JSON format which is then stored in the database in documents. The data for this prototype is stored on MongoDB Atlas, which is global cloud database service and very flexible and scalable. To connect to the database the library *Mongoose*¹ is used for implementing the prototype. *Mongoose* is an object data modeling (ODM) library for Node.js. With *Mongoose*, schemas can be created which represent the data structure of the databases. The connection between the business layer and the database is also based on HTTP.

5.2 Architecture Overview

Figure 5.2 gives an overview of the three different application layers and their responsibilities. The user interface of the application is described in more detail in Subsection 5.3. The server, which is responsible for the data preparation, performs calculations and is connected to third-party applications, is discussed in Section 5.4. Subchapter 5.5 focuses on the database and its structure.

¹<https://github.com/Automattic/mongoose>

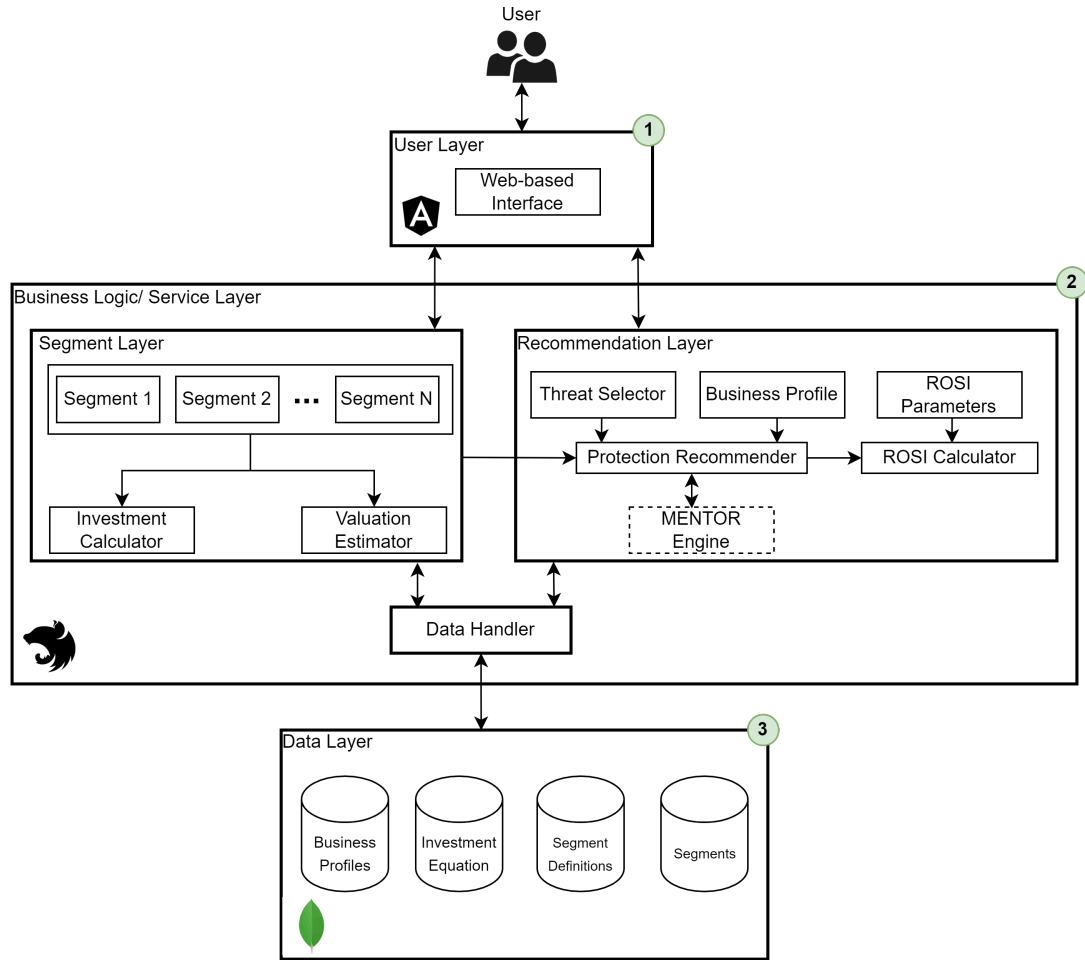


Figure 5.2: Architecture Overview

5.3 User Interface

The frontend is structured on four pages. Each of these pages focuses on a specific function of the application. The arrangement of the pages is structured in a way that reflects the logical flow of using the tool. In the following subchapters the different pages are described in detail.

5.3.1 Home Page

Figure 5.3 shows the view when the user starts the tool for the first time. On the left side it can be seen the menu with the different pages. The currently selected page is clearly signaled in the menu so that the user always knows which page he is on. It is noticeable that the *Segments* and *Recommendation* pages cannot be clicked because they are locked. To activate these pages, the user must first create a business profile, because the information of the business profile is necessary for the evaluation of segments. In the middle of the page the user is made aware of exactly that. By clicking on the *Create*

profile button, the user is then taken to the *Business Profile* page where he can create such a profile. Furthermore, a lot of emphasis was put on a user-friendly appearance for this page, as the home page should make a positive first impression.

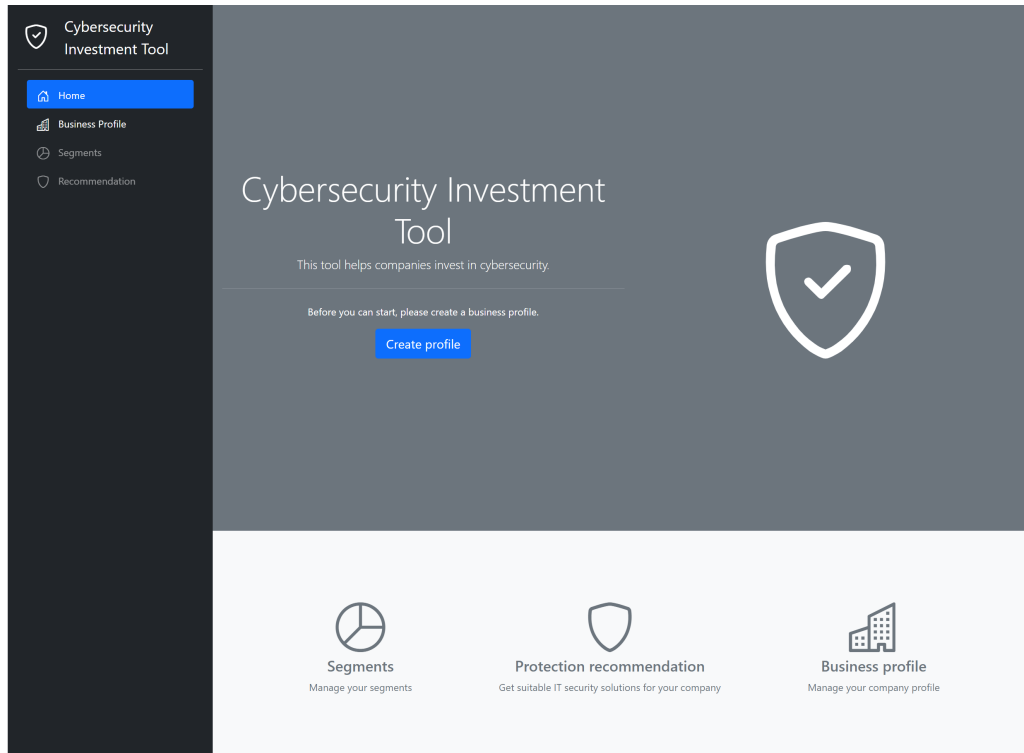


Figure 5.3: Home Page

Once the user has created a business profile, he/she has access to all features of the tool. This means that the pages *Segments* and *Recommendation* are enabled and therefore clickable. In addition, the name of the company is displayed at the bottom left of the menu and the company name is also visible in the center of the page. Furthermore, the *Create profile* button has disappeared.

5.3.2 Business Profile

The page where the user can create a business profile is illustrated in Figure 5.4. On the left of the figure the menu is shown. Further, the currently selected page is represented in the header. In addition to the menu, the user can also use the header to find out which page he is currently on. The tool was designed in such a way that it is as easy as possible for the user to operate. In the middle of the Figure 5.4 the registration form where the user can enter the information about the company is presented. Once all the fields are filled in, the *Save* button will be enabled. By clicking the button, the business profile will be created. In addition, the user is allowed to change the information provided and update the business profile.

The screenshot shows the 'Business Profile' page of the 'Cybersecurity Investment Tool'. On the left is a dark sidebar with a shield icon and the tool's name. Below it are navigation links: 'Home', 'Business Profile' (highlighted in blue), 'Segments', and 'Recommendation'. The main content area has a top header 'Business Profile'. On the left side of this area is a building icon, the word 'Welcome', and the text 'Please enter your company information.' To the right is a grey rounded rectangle titled 'Company Information' containing four input fields: 'Company Name', 'Number of Employees', 'Revenue', and 'Region' (a dropdown menu). A blue 'Save' button is at the bottom right of this form.

Figure 5.4: Business Profile

5.3.3 Segments

After creating a business profile, the user is allowed to navigate to the *Segments* page. He will be offered the view shown in Figure 5.5. On the left side of the figure the navigation menu is shown. To the right of the menu there is an action board that allows the user to add a new segment and switch between two views. If the user has not yet created a segment, the *Show segment details* button is disabled. In the center of the page, the user is notified that he has not yet created a segment and is prompted to create a new segment.

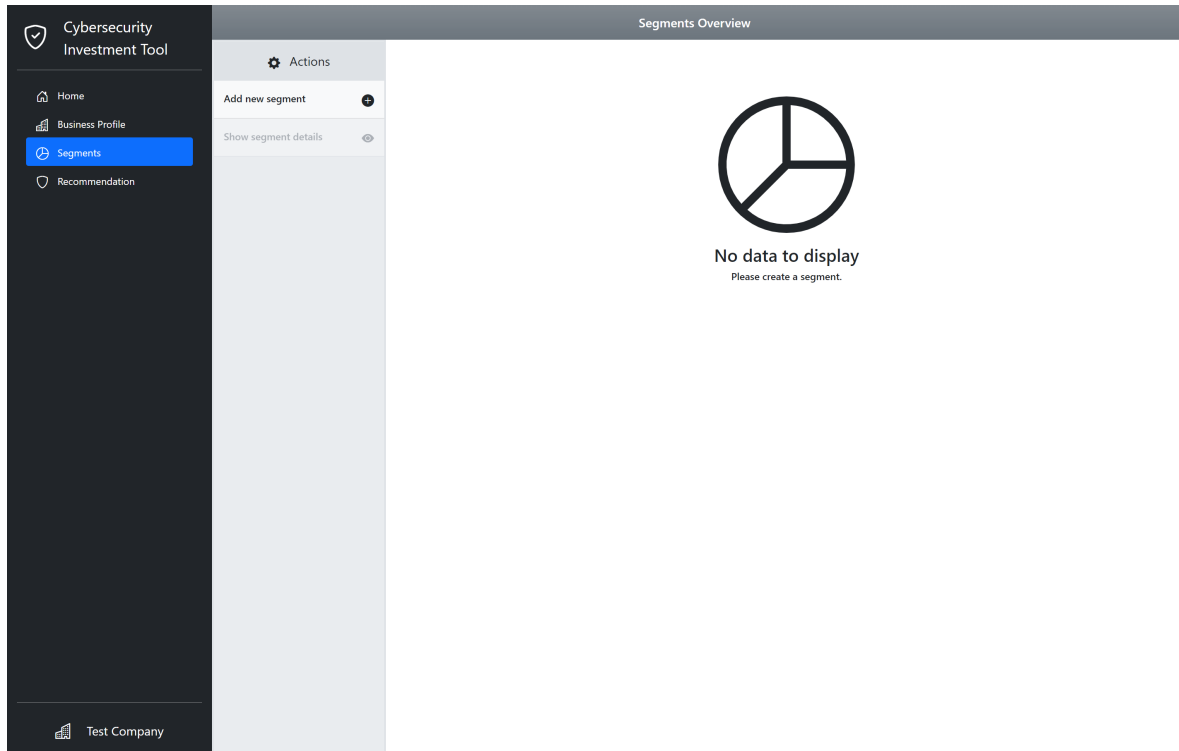


Figure 5.5: Segments Empty Page

When clicking on the *Add new Segment* button, a dialog is displayed where the user can register a segment. Figure 5.6 illustrates this dialog. Initially only two input fields are visible. The user is asked to choose between three segment types. The supported segment types are *Web Server*, *Network* and *Database*. Once the user has selected between one of these three types, the dialog is extended with more input fields. This is shown in Figure 5.7.

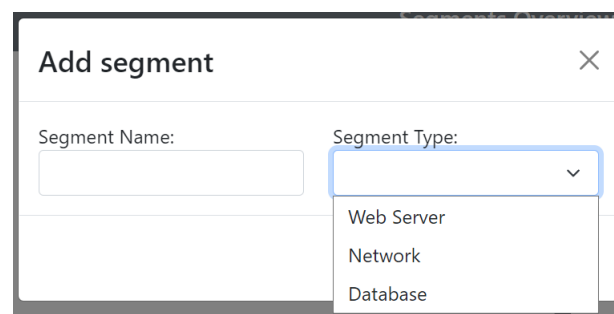


Figure 5.6: Add Segment Dialog

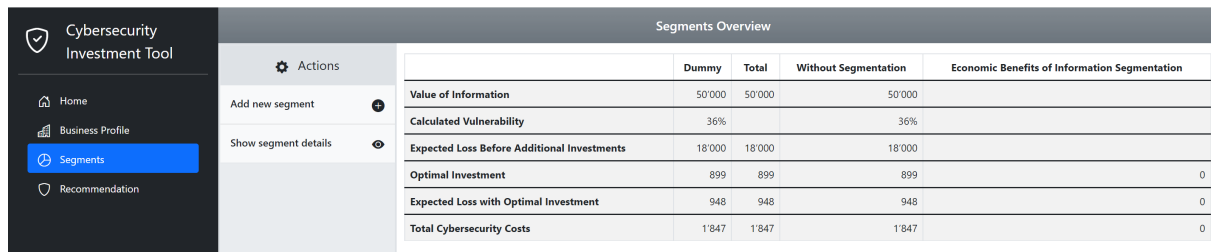
Figure 5.7 shows that the segment type *Database* has been selected for this purpose. In the middle of the dialog the value estimation is displayed, which helps the user to determine the value of the segment. The input fields for the value estimation are loaded from the database and then generically displayed in the dialog. It is up to the user which input fields he wants to fill in and which not. Once he has filled in the input fields, he can click on the *Calculate Value* button and the value of the segment will be calculated. The

calculated value is then entered in the *Value* field. The user is allowed to show and hide the value estimation help. In the lower part of the dialog, information about the value, risk and vulnerability of the segment are requested. If the user moves the mouse over the blue info icon, he will get additional information about the input field. Once the user has specified the segment name, segment type, value, risk and vulnerability, the *Save* button will be enabled and the user is able to create the segment.

Figure 5.7: Add Segment Dialog With Selected Segment Type

Figure 5.8 represents the view as it is presented to the user once he has created a segment. For this purpose, a segment was created with mock data. In the middle of the page a table is now visible, which gives information about the created segments. In the second column of the table the segment can be seen, which was created and has the name *Dummy*. The rows of the table provide information about the value of the segment, the vulnerability, the expected loss before additional investments, the optimal investment level, the expected loss with optimal investment and the total cybersecurity costs. The total cybersecurity cost can be calculated by adding the optimal investment with the expected loss with optimal investment. In the column *Total* all values of all segments are added, whereas the column *Without Segmentation* represents the values of the segments if no information segmentation would be performed. The last column shows the economic benefit of information segmentation. Since only one segment was created in Figure 5.8, there is logically no benefit from information segmentation. Chapter 6 discusses the table in more detail.

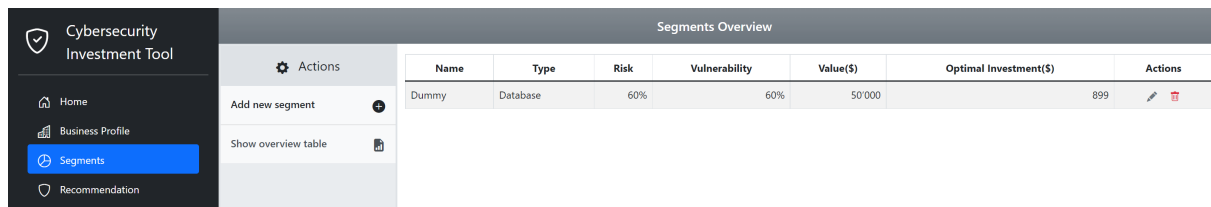
Once a segment is created, the *Show segment details* button is enabled and the user can switch between two segment views. When the user clicks on the *Show segments detail* button, the details of the created segments are displayed in a table. Figure 5.9 shows the view as it is presented to the user. In the table each segment is displayed in one row. For each segment the user can find the name, the type, the risk, the vulnerability, the value



Actions	Dummy	Total	Without Segmentation	Economic Benefits of Information Segmentation
Value of Information	50'000	50'000	50'000	
Calculated Vulnerability	36%		36%	
Expected Loss Before Additional Investments	18'000	18'000	18'000	
Optimal Investment	899	899	899	0
Expected Loss with Optimal Investment	948	948	948	0
Total Cybersecurity Costs	1'847	1'847	1'847	0

Figure 5.8: Segments Overview

and the optimal investment. In addition, the user can edit or delete the segment in the last column. By clicking on the red garbage icon, a dialog is displayed where the user must confirm that he really wants to delete the segment. When confirming, the segment will be deleted. Clicking on the gray pencil icon in the *Action* column opens a dialog where the user can edit the information about the segment. Figure 5.10 illustrates this dialog. Once the user has made a change, the "Update" button is activated and the segment can be updated.





Name	Type	Risk	Vulnerability	Value(\$)	Optimal Investment(\$)	Actions
Dummy	Database	60%	60%	50'000	899	 

Figure 5.9: Segment Details

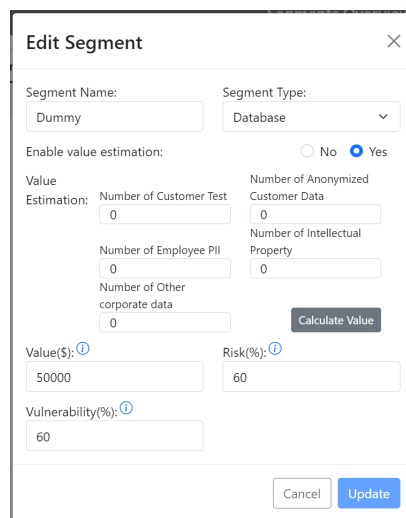


Figure 5.10: Edit Segment Dialog

5.3.4 Recommendation

Once the user has created a segment he is able to navigate to the *Recommendation* page. Figure 5.11 shows the *Recommendation* page with the created *Dummy* segment. To the

right of the menu all created segments are visible. By clicking on the segment it can be selected.

The selected segment is represented by a blue background. In the middle of the page the input fields are visible which have to be filled in to search for suitable cybersecurity solutions. The default value for the region is the region of the business profile. In addition, the *Investment* input shows the amount that the system has calculated as the optimal investment amount. This value can be changed by the user. At the *Attack Type* input the user can choose between different attack types. By default, cybersecurity solutions are searched for all supported attack types. Once the user has entered a value for all input fields, the *Submit* button is activated and the user can search for suitable cybersecurity solutions.

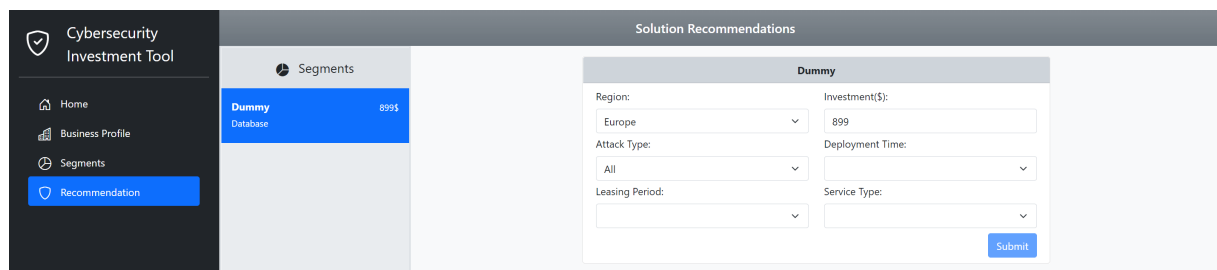


Figure 5.11: Recommendation Page

Figure 5.12 shows the view after clicking the "Submit" button and suitable cybersecurity solutions have been found. The lower half of the page lists the recommendations provided by the third-party application MENTOR [12, 13] and submitted by the server. For each recommendation, the provider of the recommendation, a short description, the deployment time, the leasing period and the cost are displayed. By clicking on the *Calculate ROSI* button, the user can calculate the Return-On-Security-Investment Index.

Once the user has clicked on the *Calculate ROSI* button, a dialog will open. Figure 5.13 (a) illustrates this dialog. To calculate the ROSI index, information about the mitigation rate, cost of incident and annual rate of incidence must be entered. The default value for the mitigation rate is the value provided by MENTOR[12]. For the cost of incident value, the value of the segment is displayed as default value. The user is free to change these values. If the user hovers over a blue info icon, he/she gets additional information about the input field.

As soon as the user has entered a value for all three input fields, the *Calculate ROSI* button is activated. After clicking on the button, the server performs the calculation and the calculated value will be displayed where the *Calculate ROSI* button was before. What can be seen in Figure 5.13 (b). Clicking on the calculated ROSI value will cause the dialog to reopen and allow the user to make adjustments.

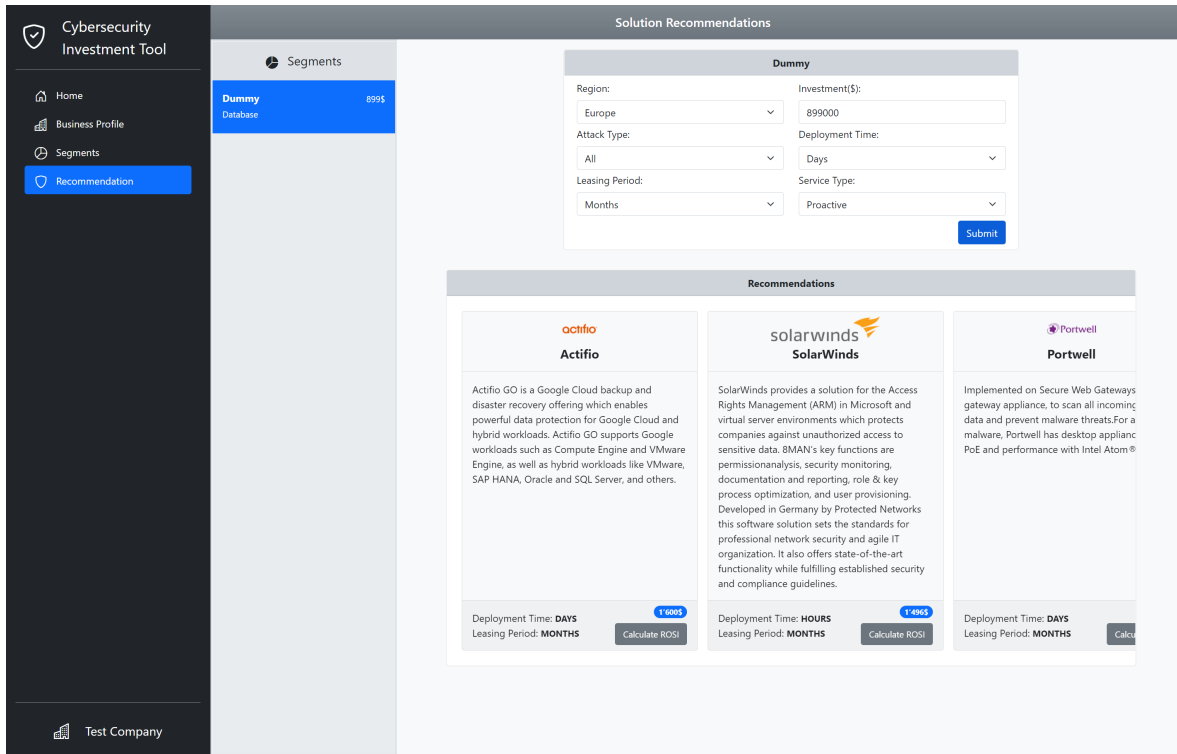


Figure 5.12: Recommendation Page With Recommendations

(a) ROSI Dialog

(b) Recommendation with Calculated ROSI

Figure 5.13: Calculation of ROSI integrated with MENTOR engine

5.4 Server

Figure 5.14 represents the architecture of the server. A distinction is made between two layers. On the one hand, all information relating to the segments is processed in the *Segment Layer* and, on the other hand, the task of the *Recommendation Layer* is to

process the data for the cybersecurity solutions. The *Data Handler* is the interface to the database. This component stores and reads information from the database and prepares it for further processing.

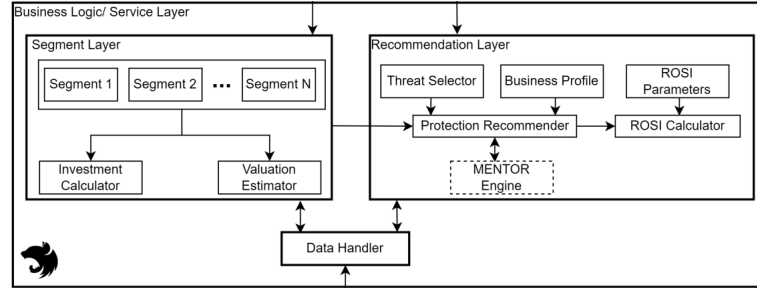


Figure 5.14: Server Architecture

Both the *Segment Layer* and the *Recommendation Layer* use the *Data Handler* to process or store data from the database. The task of the *Segment Layer* is to calculate the optimal investment for each created segment and to provide a suggestion for the value of the segment. The calculation of the optimal investment is discussed in subsection 5.4.1. Subsection 5.4.2 describes the process of estimating the value of the segment. The *Recommendation Layer* consists of two main components. The *Protection Recommender* component is responsible for the preparation of cybersecurity solutions and is discussed in more detail in subsection 5.4.3. The *ROSI Calculator* component is responsible for calculating the ROSI index and is described in subsection 5.4.4.

5.4.1 Investment Calculator

The calculation of the optimal investment level is a core competence of the application. Figure 5.15 shows how the optimal investment is calculated. To perform the calculation the library *nerdamer*² was used, which allows to perform calculation operations that are not provided by JavaScript by default.

The method requires the segment for which the optimal investment is to be calculated, all segments and information about the optimal investment equation as parameters. The equation for calculating the optimal investment is stored on the database and is passed to this method.

On line two of the Figure 5.15 it can be seen that the breach probability function is derived according to z . On the third line, the equation for calculating the optimal investment is composed. The parameter S is replaced by the variable from line 2. Afterwards the remaining parameters are inserted into the equation, which is described on line 7. To meet with the breach probability function of subsection 4.3.2 the parameter z has to be replaced. On line 12, the equation is solved for the variable z , resulting in two extremes. The obtained extremes are compared on line 17 and the larger of the two is returned on line 18.

²<https://github.com/jiggzson/nerdamer>

```

1  getOptimalInvestment(segment: Segment | Partial<Segment>, segments: Segment[], investmentEquation: OptimalInvestmentEquation) {
2    const diff = nerdamer( diff(`${investmentEquation.breachProbabilityFunction}, z`));
3    const optimalInvestmentEquation = nerdamer(
4      investmentEquation.optimalInvestmentEquation,
5      { S: `${diff.toString()}` }
6    ).evaluate();
7    const equationWithParameters = optimalInvestmentEquation.evaluate({
8      L: this.getTotalValue(segments),
9      v: segment.calculatedVulnerability,
10     z: `z/${segment.value / this.getTotalValue(segments)}`
11   });
12   const extremes = equationWithParameters.solveFor('z');
13   const extremesObject = {
14     first: nerdamer(extremes[0].toString()).evaluate(),
15     second: nerdamer(extremes[1].toString()).evaluate()
16   };
17   const result = Number(extremesObject.first) > Number(extremesObject.second) ? extremesObject.first : extremesObject.second;
18   return Math.round(+result.text())
19 }

```

Figure 5.15: Investment Calculator Code Snipped

5.4.2 Valuation Estimator

To estimate the value of the segment the method shown in Figure 5.16 is used. The segment definition which contains the information for calculating the segment value is passed as the first parameter of the method. How the value of the segment should be calculated is provided by the database. As second parameter an array of objects is passed which contain a *key* and *value*. On line three the equation is broken down into an array. From line 5 to line 9, for each key-value pair passed, the value of the *value* property is inserted into the equation. Based on the *key* property, the position in the equation is searched and the *key* is replaced with the *value*. The task of line 12 is to convert the created array into a text. On line 13 the text is evaluated and the value of the segment is calculated and returned.

```

1  calculateValue(segment: SegmentDefinition, keyValuePairs: { key: string; value: number; }[]): number {
2    try {
3      const splittedCalculationString = segment.valueEstimation.calculation.split(' ');
4      if (splittedCalculationString && keyValuePairs && keyValuePairs.every(pair => Number.isFinite(pair.value))) {
5        keyValuePairs.forEach(pair => {
6          const index = splittedCalculationString?.indexOf(pair.key);
7          if (index !== undefined && index !== -1) {
8            splittedCalculationString[index] = String(pair.value);
9          }
10         });
11       }
12       const mergedCalculation = splittedCalculationString.reduce((pre, curr) => pre + ` ${curr}`, '')
13       return eval(mergedCalculation);
14     } else {
15       throw new Error();
16     }
17   } catch (error) {
18     throw new Error();
19   }
20 }

```

Figure 5.16: Value Estimation Code Snipped

5.4.3 Protection Recommender

In order to suggest cybersecurity security systems to the user, the application is connected to the MENTOR[12] system. Figure 5.17 shows the method responsible for the integration of MENTOR. The parameters passed to the method were described in Subsection 4.2.3. On line two the url is stored in a variable on which the MENTOR system can be reached. The request to MENTOR[12] with the information provided by the user is executed on line 3. On the same line the result is put into the correct format and returned.

```
1 recommend(body: RecommendationProfile) {  
2   const url = 'http://192.168.200.130:5000';  
3   return this.httpService.post(`${url}/v1/recommend`, body).pipe(map(response => response.data.recommendedServices));  
4 }
```

Figure 5.17: Protection Recommender Code Snipped

5.4.4 ROSI Calculator

Figure 5.18 illustrates the method which calculates the ROSI index. The parameter of the method includes the information which was described in Subsection 4.2.4. This parameter includes also the price of the cybersecurity solution which is provided by the MENTOR system. On line 5 of Figure 5.18, the method shown in Figure 5.19 is called. The purpose of the *getAnnualInvestmentCost* is to calculate the annual investment cost of the cybersecurity solution. The ROSI index is calculated on line 6 in the *getROSI* method. The calculation is performed based on the formula described in chapter 4.4

```
1 private getROSI(rosiDetail: ROSIDetail): number {  
2   // ROSI = ((SLE * ARO * mitigation rate) - Cost of the investment) / Cost of the investment  
3   // SLE = Estimated cost of a security incident  
4   // ARO = Estimated annual rate of a incidence occurrence  
5   const investmentCost = this.getAnnualInvestmentCost(rosiDetail.price, rosiDetail.leasingPeriod);  
6   return Math.round(  
7     ((rosiDetail.costOfIncident * rosiDetail.incidenceOccurrence * rosiDetail.mitigationRate) - investmentCost)  
8     / investmentCost);  
9 }
```

Figure 5.18: ROSI Calculation Code Snipped

```
1 private getAnnualInvestmentCost(price: number, leasingPeriod: LeadingPeriod): number {  
2   const factor = [  
3     { period: LeadingPeriod.Minutes, annualFactor: 525600 },  
4     { period: LeadingPeriod.Days, annualFactor: 365 },  
5     { period: LeadingPeriod.Months, annualFactor: 12 },  
6   ].find(({ period }) => period === leasingPeriod).annualFactor;  
7   return price * factor;  
8 }
```

Figure 5.19: Annual Investment Cost Code Snipped

5.5 Database

The database is divided into four different components. Each of these database components stores specific information which is of central importance for the prototype. In the following subsections, each component will be discussed.

5.5.1 Business Profiles

To provide the user the best possible user experience (UX), each created business profile is stored in the database. The advantage of this is that the user does not have to recreate the business profile every time he restarts the application. Figure 5.20 represents the schema that is used to store the business profile on the database. The schema has the same properties which were already discussed in Subsection 4.2.1.

```
1 export const BusinessProfileSchema = new mongoose.Schema(  
2   {  
3     companyName: String,  
4     revenue: Number,  
5     numberOfEmployees: Number,  
6     region: String  
7   }  
8 )
```

Figure 5.20: Business Profile Schema

5.5.2 Optimal Investment Equation

In order to implement the prototype as adaptable and generic as possible, the equations for calculating the optimal investment are stored in the database. If the equations need to be adapted for a specific company, this can easily be done in the database and there is no need for a new release of the application. This makes the whole application very

generic and without much effort the equations can be adapted. Figure 5.21 illustrates the scheme which is defined for the calculation of the optimal investment. On the one hand the scheme contains the breach probability function and on the other hand the equation for the calculation of the investment amount. These two properties were described in Subsection 4.3.2. The initial values of the database are shown in Figure 5.22.

```

1 export const OptimalInvestmentEquationSchema = new mongoose.Schema(
2   {
3     breachProbabilityFunction: String,
4     optimalInvestmentEquation: String
5   }
6 )

```

Figure 5.21: Optimal Investment Equation Schema

```

1 {
2   "breachProbabilityFunction": "v/(1+(z/(L*0.001)))",
3   "optimalInvestmentEquation": "S*L+I=0"
4 }

```

Figure 5.22: Optimal Investment Equation Data

5.5.3 Segment Definitions

In Subsection 4.2.2 it was mentioned that the user can choose between different segment types. In order to easily customize and extend the supported segments without touching a line of code in the application, the approach of storing the different segment definitions in the database was chosen. Figure 5.23 illustrates the database schema of a segment definition. On line 14 it can be seen that each segment definition has an *key* which can be used to uniquely identify a segment. In addition, each segment contains a short description. Furthermore, the most frequent cybersecurity threats are specified in each segment definition. Line 7 visualizes the schema definition of the supported threats. Each cybersecurity threat has a label and a list of values. This schema structure allows to create categories of threats that the user can choose. The threats stored in the segment definition are displayed to the user when he selects an attack type while looking for suitable cybersecurity solutions, which can be seen in Figure 5.11.

In addition, the calculation of the segment value and the corresponding input fields are stored in the segment definition. In Figure 5.23 it is described on line 17. The *valueEstimation* property has several input fields which are defined on line 1. Each input has a *key* and a *type*. The *key* is used to identify the input field, the *description* is the text which is visible to the user. The *type* of the input field describes what kind of input field it is.

Supported types are *text* and *number*. The input fields defined here are displayed in the dialog when the user creates a segment. Figure 5.7 shows the input fields defined in the database for calculating the value of the segment for the database segment. This allows to display generic input fields in the user interface without any modification of the server or frontend. Furthermore, the *valueEstimation* property has the definition how the values of the different input fields should be processed to estimate the value of the segment. Line 19 represents the property in which the definition of the calculation is stored.

```
1 const inputType = new mongoose.Schema({
2   key: String,
3   description: String,
4   type: String
5 });
6
7 const supportedThread = new mongoose.Schema({
8   label: String,
9   values: [String],
10 });
11
12 export const SegmentDefinitionSchema = new mongoose.Schema(
13   {
14     key: String,
15     description: String,
16     supportedThreads: [supportedThread],
17     valueEstimation: {
18       inputs: [inputType],
19       calculation: String
20     }
21   }
22 )
```

Figure 5.23: Segment Definition Schema

The initial data for estimating the value of the segment stored in the database for the database segment are presented on Figure 5.24. As shown in figure, five input fields have been defined. Line 29 defines how the values of the different inputs are evaluated. Figure 5.25 provides the same information for the webserver segment type. No value estimation is supported for the network segment type.


```

1 "valueEstimation": {
2   "inputs": [
3     {
4       "key": "customer",
5       "description": "Number of Customer Test",
6       "type": "number"
7     },
8     {
9       "key": "anonymized_customer",
10      "description": "Number of Anonymized Customer Data",
11      "type": "number"
12     },
13     {
14       "key": "employee",
15       "description": "Number of Employee PII",
16       "type": "number"
17     },
18     {
19       "key": "intellectual_property",
20       "description": "Number of Intellectual Property",
21       "type": "number"
22     },
23     {
24       "key": "other_data",
25       "description": "Number of Other corporate data",
26       "type": "number"
27     }
28   ],
29   "calculation": "customer * 157 + anonymized_customer * 153 + employee * 163 + intellectual_property * 151 + other_data * 150"
30 }

```

Figure 5.24: Database Value Estimation Data

```

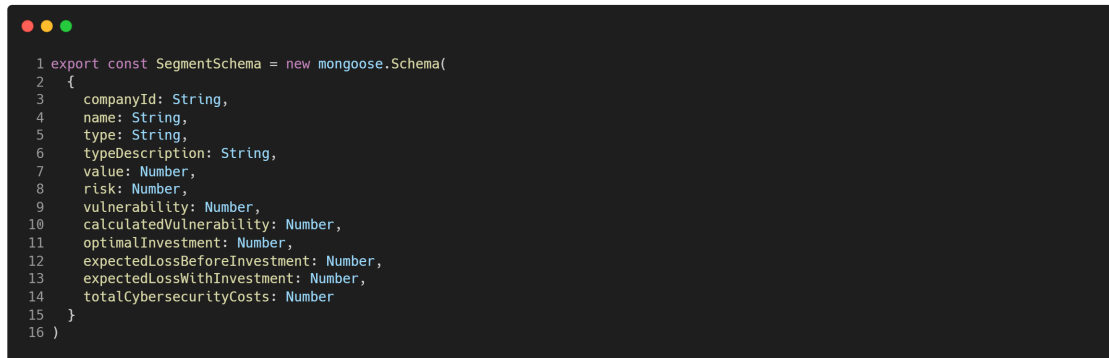
1 "valueEstimation": {
2   "inputs": [
3     {
4       "key": "revenue",
5       "description": "Monthly revenue from website",
6       "type": "number"
7     }
8   ],
9   "calculation": "revenue * 30"
10 }

```

Figure 5.25: Webserver Value Estimation Data

5.5.4 Segments

All created segments are stored in the database in order that the created segments are not got lost when the application is restarted. The database schema of a segment is shown on the Figure 5.26. On line three it can be seen that each segment has a reference to a company, therefore the segments can be assigned to the correct company. The other properties of the scheme are composed of the parameters mentioned in Subsection 4.2.2 and the calculation of the optimal investment described in Subsection 4.3.2.



```
1 export const SegmentSchema = new mongoose.Schema(  
2   {  
3     companyId: String,  
4     name: String,  
5     type: String,  
6     typeDescription: String,  
7     value: Number,  
8     risk: Number,  
9     vulnerability: Number,  
10    calculatedVulnerability: Number,  
11    optimalInvestment: Number,  
12    expectedLossBeforeInvestment: Number,  
13    expectedLossWithInvestment: Number,  
14    totalCybersecurityCosts: Number  
15  }  
16 )
```

Figure 5.26: Segment Schema

Chapter 6

Evaluation

In order to evaluate the correctness and usability of the tool, three case studies are conducted. Each case study focuses on a different core functionality of the application. In addition, the case studies show how helpful the tool is for decision makers who want to invest in cybersecurity. The first case study focuses on calculating the optimal investment of segments. The second case study is dedicated to cybersecurity solution recommendations. The last case study demonstrates the calculation of the ROSI index for supporting the decision between different proposals.

The basis for the case studies is the company Montana AG. The main business of Montana AG is on the one hand to sell electronic devices, such as hardware, computers, and cameras. On the other hand, they distribute household and garden products. The headquarters of the company is located in Switzerland. Montana AG owns ten big retail stores which are spread all over the world. In addition, they also sell their products with the help of two online stores. One store offers the electronic assortment, the other one sells household and garden products. Currently, 2000 employees work for the Montana company. The company generates an annual revenue of 600 million dollars.

The CEO of Montana AG is very concerned about the ever-increasing threat of cybersecurity attacks, so she asks an IT project manager to analyze the current business segments and propose suitable cybersecurity solutions. The CEO emphasizes that the budget for cybersecurity investments is very limited and that the IT project manager should choose the most efficient solution. He has also heard of a tool that calculates how much money should be invested in cybersecurity and also presents suggestions for cybersecurity solutions, so he should use this one. After the CEO's prompting, the project manager gets to work. First, he creates a business profile that depicts Montana AG. Figure 6.1 shows the business profile created by the IT project manager. Since the headquarters is located in Switzerland, the project manager has decided to use *Europe* as the region.

Company Information

Company Name: <input type="text" value="Montana AG"/>	Number of Employees: <input type="text" value="1200"/>
Revenue(\$): <input type="text" value="600000000"/>	Region: <input type="text" value="Europe"/>

[Save](#)

Figure 6.1: Montana AG Business Profile

6.1 Case Study No. 1 - Optimal Investment

At first, the IT project manager focuses on the databases of Montana AG. The company owns three databases which are physically separated from each other and located in Switzerland. The project manager's goal is to determine the optimal level of investment for each database.

The first database manages customer data such as credit card information and personal data of customers. Currently, 764,331 entries are stored in the customer database. The project manager estimates that the probability of an attack is 80% and 50% that a cybersecurity attack will be successful. The second database contains information about internal operations. This database stores information about employees. The database has 368,098 entries. It is estimated that the probability of an attack is 50% and 40% that an attack will be successful. The last database manages records about external operations. This database contains information about business partners. This database contains 133,333 records and the risk of a cybersecurity attack is 20%. The probability of a successful attack was estimated at 50%.

After analyzing the databases, the project manager now creates an information segment for each database. To determine the value of the databases, he uses the calculation help provided by the application. The creation of the segment for the customer data is shown in Figure 6.2 (a). Figure 6.2 (b) presents the dialog for creating the segment for internal operations. Adding the segment for external operations is illustrated in the Figure 6.2 (c).

After creating the segments, the IT project manager is presented with the table shown in Figure 6.3. In the table it is visible that the created segments are displayed as columns. The first row represents the values of the segments and in the *Total* column the sum of the values is displayed. The calculated vulnerabilities of the segments which result from the multiplication of the risk and the vulnerability are shown in the second row. The third row makes statements about how high the expected loss would be if no investments were

Add segment

Segment Name:Customers

Segment Type:Database

Enable value estimation:

No

Yes

Value

Estimation:

Number of Customer Test764331

Number of Anonymized Customer Data0

Number of Employee PII0

Number of Intellectual Property0

Number of Other corporate data0

Calculate Value

Value(\$):120000000

Risk(%):80

Vulnerability(%):50

Save

(a) Customer Segment Creation

Add segment

Segment Name:Internal Operations

Segment Type:Database

Enable value estimation:

No

Yes

Value

Estimation:

Number of Customer Test0

Number of Anonymized Customer Data0

Number of Employee PII368098

Number of Intellectual Property0

Number of Other corporate data0

Calculate Value

Value(\$):60000000

Risk(%):50

Vulnerability(%):40

Save

Add segment

Segment Name:External Operations

Segment Type:Database

Enable value estimation:

No

Yes

Value

Estimation:

Number of Customer Test0

Number of Anonymized Customer Data0

Number of Employee PII0

Number of Intellectual Property0

Number of Other corporate data133333

Calculate Value

Value(\$):20000000

Risk(%):20

Vulnerability(%):50

Save

(b) Internal Operations Segment Creation (c) External Operations Segment Creation

Figure 6.2: Segments Creation

made in cybersecurity. From the row *Optimal Investment* the IT project manager gets information how much money he should invest in cybersecurity. It can be seen that the optimal investment level for the *Customer* database is \$2'400'000. The optimal investment for the *Internal Operations* database is \$788'528 and for the *External Operations* database the optimal investment is \$180'000.

Moreover, it can be seen from the table that the sum of all optimal investments is \$62'000'000. The last column of the table shows that the information segmentation saves almost \$73'000 of investment costs. The second last row shows the expected loss when the optimal investment amount is invested. The last line gives the project manager an overview of the total cybersecurity cost, which is the sum of the optimal investment and the expected loss with optimal investment. In the last column, the project manager gets an overview of the total costs that can be saved thanks to the information segmentation.

He is surprised to see that the information segmentation results in an benefit of \$145'671. Thanks to this table, the IT project manager has obtained important information about how much to invest in each segment and what advantages information segmentation offers. By comparing the information received from the table and table 1 from [15] he makes sure that the calculations of the application are correct.

	Customers	Internal Operations	External Operations	Total	Without Segmentation	Economic Benefits of Information Segmentation
Value of Information	120'000'000	60'000'000	20'000'000	200'000'000	200'000'000	
Calculated Vulnerability	40%	20%	10%		31%	
Expected Loss Before Additional Investments	48'000'000	12'000'000	2'000'000	62'000'000	62'000'000	
Optimal Investment	2'280'000	788'528	180'000	3'248'528	3'321'363	72'835
Expected Loss with Optimal Investment	2'400'000	848'528	200'000	3'448'528	3'521'364	72'836
Total Cybersecurity Costs	4'680'000	1'637'056	380'000	6'697'056	6'842'727	145'671

Figure 6.3: Database Segments Overview

6.2 Case Study No. 2 - Cybersecurity Recommendations

Since the IT project manager now is aware of the optimal investment for the databases, he focuses on the two web servers which are responsible for the online store. The goal of the project manager is to find suitable cybersecurity solutions for both web servers. Both web servers are located in Switzerland. The webshop responsible for the electronic assortment generates a monthly revenue of 17 million dollars for Montana AG. The risk of a cybersecurity attack is estimated to be 60%. The probability that a cyber attack will be successful is estimated at 40%. To determine the value of the segment, the project manager uses feature available in the application. Figure 6.4 (a) illustrates the creation of the segment.

The creation of the segment for the web server responsible for the online store for household and garden items is shown in Figure 6.4 (b). It can be observed that the monthly profit from the online store is 15 million dollars. Again, the project manager uses the application to determine the value of the segment. The risk of a cybersecurity attack is 50% and the probability of an attack being successful is about 40%.

After creating the segments, the project manager begins to determine appropriate cybersecurity solutions for the databases. The *Electronic* web server should be protected against all DDoS attacks, whereas the *Household* web server should be secured against specific SSL DDoS attacks. Figures 6.5 and 6.6 show the configuration of how cybersecurity solutions are searched for the two segments. The project manager did not make any adjustments to the investment level and used the optimal investment calculated by the system. For the *Electronic* web server the generic term *DDoS* is selected for the *Attack Type*. For the *Household* web server, on the other hand, the specific attack *SSL* is selected. The *Deployment Time* selected for both segments is *Hours*. Further, the same *Leasing Period* and *Service Type* were chosen for both segments.

Add segment

Segment Name:
Web Server Electronic

Segment Type:
Web Server

Enable value estimation:

No

Yes

Value

Monthly revenue from website

Estimation:
17000000

Calculate Value

Value(\$):

510000000

Risk(%):

60

Vulnerability(%):

40

Save

(a) Electronic Web Server Segment Creation

Add segment

Segment Name:
Web Server Household

Segment Type:
Web Server

Enable value estimation:

No

Yes

Value

Monthly revenue from website

Estimation:
15000000

Calculate Value

Value(\$):

450000000

Risk(%):

50

Vulnerability(%):

40

Save

(b) Household Web Server Segment Creation

Figure 6.4: Segment Creations

Web Server Electronic

Region:
Europe

Investment(\$):
7390886

Attack Type:
DDOS

Deployment Time:
Hours

Leasing Period:
Months

Service Type:
Proactive

Submit

Figure 6.5: Electronic Web Server Recommendation Configuration

Web Server Household

Region:
Europe

Investment(\$):
5913961

Attack Type:
SSL

Deployment Time:
Hours

Leasing Period:
Months

Service Type:
Proactive

Submit

Figure 6.6: Household Web Server Recommendation Configuration

Figure 6.7 shows the recommended cybersecurity solutions for the *Electronic* web server. The suggestions for the *Household* web server can be seen in Figure 6.8. The IT project manager now receives an overview of the appropriate cybersecurity solutions with a brief description. When he has decided on a solution, he receives more information on the provider’s website and can subscribe to it.

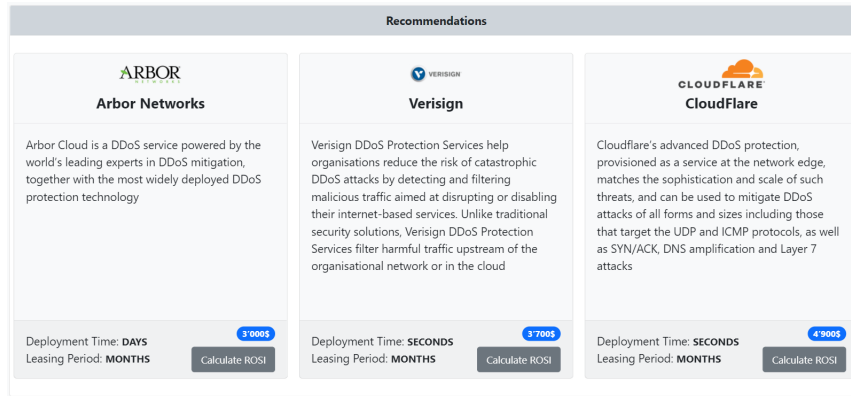


Figure 6.7: Electronic Web Server Recommendations

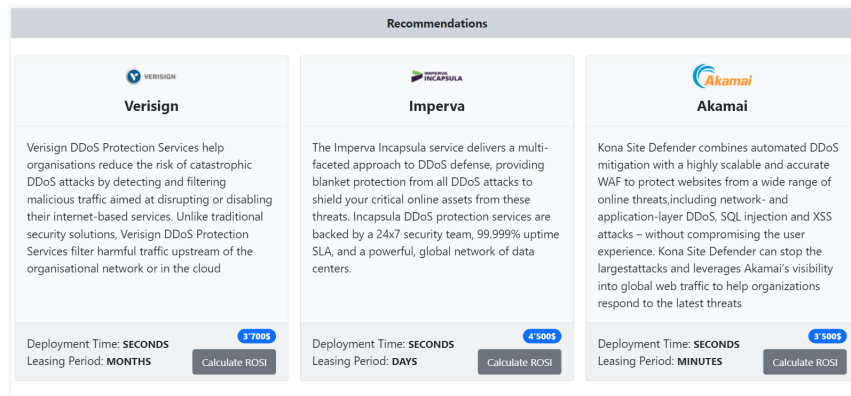


Figure 6.8: Household Web Server Recommendations

6.3 Case Study No. 3 - ROSI Index

After the IT project manager has found suitable cybersecurity solutions for the two web servers, he focus on the the local company network in Switzerland. To prevent malware from spreading through the internal network, he is looking for cybersecurity solutions that will prevent this. To do this, he creates a new segment for the internal network and looks for suitable solutions. Figure 6.9 shows the result of the search. The project manager now wants to know which of the three solutions is the most cost-effective. Therefore he calculates the ROSI index for each recommendation.

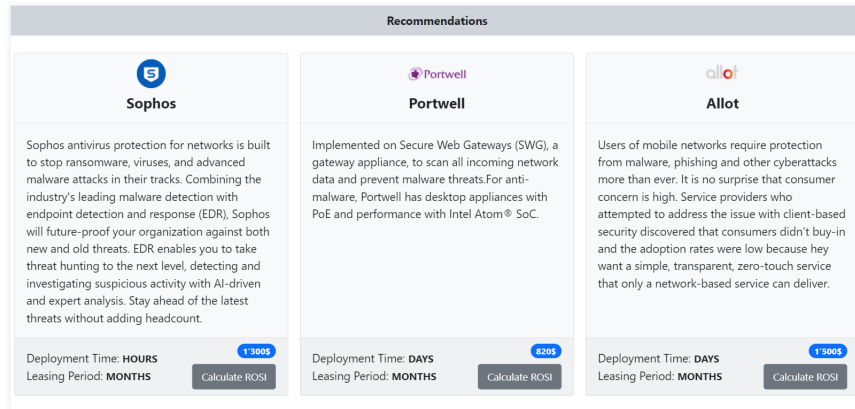


Figure 6.9: Network Recommendations

Figure 6.10 shows the dialog which the project manager needs to fill in to calculate the ROSI index. He does not change the *Mitigation Rate* and takes the value that the system provides. The project manager estimates that a failure of the internal network due to a successful attack would cause a damage of 4 million dollar. He further expects that such an incident can occur twice a year. He enters the obtained information in the dialog and calculates the ROSI index for each recommendation.

Calculate ROSI

Mitigation Rate(%): 60

Cost of Incident(\$): 4000000

Annual Rate of Incidence: 2

Cancel Calculate ROSI

Figure 6.10: ROSI Calculation Dialog

After calculating the ROSI index, the IT project manager can check the value, as shown in the Figure 6.11. The value in the gray box provides information about how cost-effective the cybersecurity solution is. It can be seen that the solution from *Portwell* provides the highest return on cybersecurity investment, which means that this solution is the most attractive for the project manager. The second most attractive is the solution from *Allot* and *Sophos* performs the worst. Thanks to the calculation of the ROSI index, the IT project manager has chosen the solution of *Portwell* and can show the obtained information to the CEO. This information is useful to argue about one solution instead of other, thus providing metrics to support the decision regarding cost-efficient solutions.

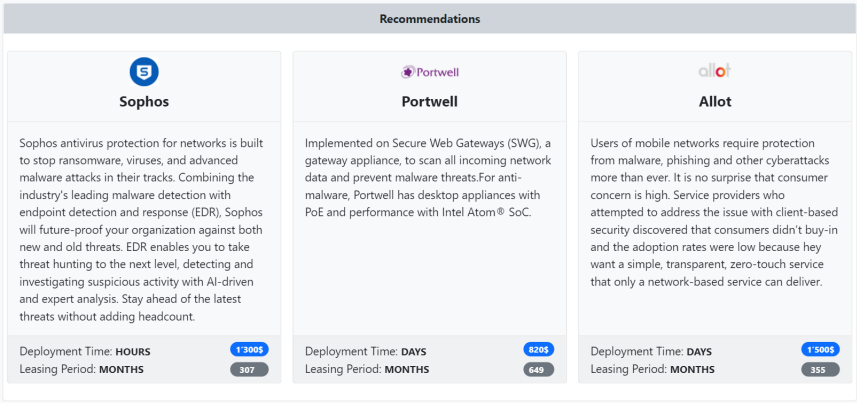


Figure 6.11: Recommendations With Calculated ROSI Index

Chapter 7

Summary, Conclusions & Future Work

Increasing digitization is associated with significant advantages, but companies also face risks. Cybersecurity attacks are increasing year by year and companies are forced to protect themselves against them. However, it is often challenging for a company to determine how much to invest in cybersecurity solutions and which ones to invest in. This bachelor's thesis addresses exactly those challenges. The main objective of this work was to develop a visual tool that supports the decision maker to determine the level of cybersecurity investment and to propose appropriate cybersecurity solutions. For that, this thesis explores concepts of Gordon-Loeb, Return On Security Investment (ROSI), and recommender systems of protections to provide an integrated solution that covers important steps of the cybersecurity planning and investment. Another core competence of the tool is information segmentation. The user is allowed to segment the digital assets of the company, which leads to a financial benefit. Due to the calculation of the ROSI index, the user can distinguish between less and more effective cybersecurity solutions.

The tool developed in this thesis is of central importance for companies which want to protect themselves against cybersecurity attacks but do not have sufficient budget for professional consulting. The tool guides the user from creating a business profile which represents the company, to creating information segments and recommending appropriate cybersecurity solutions. The user is guided step by step through the process and the tool provides the best possible user experience. It is highlighted by the three case studies conducted within a scenario based on a web store that wants to invest in cybersecurity, thus using the proposed tool to (a) calculate the optimal investment, (b) receive recommendations of protections, and (c) calculate the cost-efficiency of each recommended protection.

Currently, the tool does provide, as proof-of-concept, value estimation support for specific segments, such as databases and web stores. This is possible due to the amount of information and reports publicly available. Additional segments (*e.g.*, Network and specific web pages as a segment) can be mapped and added according to the demands of a company. This extension could be implemented as a future work. At the same time, it would be beneficial if the information collected during the creation of the business profile could be included in the value estimation of the segments. At the moment, this is not the case. For example, with the information about the number of employees, the value of the

segments could be estimated more accurately. Another feature, that could be addressed as future work, is the extension of the existing supported segments. Currently, the user has three segment types to choose from, but these three types do not cover all areas that can fall victim to a cyber attack. Therefore, In order to cover all information systems of an enterprise the supported segment types have to be extended. Also, the equations used for the investments calculation can evolve according to the needs of a company or according to new findings from the research field. As of today, the example of calculations being used are based in the most recent work in the literature, but it can be extended as needed.

Bibliography

- [1] Cloudflare. Application layer DDoS attack. <https://www.cloudflare.com/learning/ddos/application-layer-ddos-attack/>, last visit September, 2021.
- [2] Cloudflare. How does a Smurf attack work? <https://www.cloudflare.com/learning/ddos/smurf-ddos-attack/>, last visit September, 2021.
- [3] Cloudflare. What is a DDoS attack? <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>, last visit September, 2021.
- [4] Cognyte. Ransomware Attack Statistics 2021. https://www.cognyte.com/blog/ransomware_2021/, last visit October, 2021.
- [5] Michel Cukier. Study: Hackers attack every 39 seconds. September 2021, [Online] <https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds>, last visit September 2021.
- [6] Adrian Davis. Return on security investment – proving it’s worth it. *Network Security*, 2005(11):8–10, 2005.
- [7] C. Douligieris and A. Mitrokotsa. Ddos attacks and defense mechanisms: a classification. In *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No.03EX795)*, pages 190–193, 2003.
- [8] ENISA European Union Agency for Cybersecurity. Introduction to Return on Security Investment. 2012.
- [9] ENISA European Union Agency for Cybersecurity. Cybersecurity for SMES. 2021.
- [10] F5. DDoS Attack Trends for 2020. <https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020>, last visit October, 2021.
- [11] Summer Fowler and Peter P. Chen. Cspi: A new way to evaluate cybersecurity investments: A position paper. In *2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pages 283–284, 2017.
- [12] M. Franco, B. Rodrigues, and B. Stiller. MENTOR: The Design and Evaluation of a Protection Services Recommender System. In *15th International Conference on Network and Service Management (CNSM 2019)*, pages 1–7, Halifax, Canada, October 2019. IEEE.

- [13] Muriel Franco, Erion Sula, Bruno Rodrigues, Eder Scheid, and Burkhard Stiller. ProtectDDoS: A Platform for Trustworthy Offering and Recommendation of Protections. In *Economics of Grids, Clouds, Systems, and Services*, Izola, Slovenia, 2020. Springer International.
- [14] Lawrence Gordon, Martin Loeb, and Lei Zhou. Investing in cybersecurity: Insights from the gordon-loeb model. *Journal of Information Security*, 07:49–59, 01 2016.
- [15] Lawrence Gordon, Martin Loeb, and Lei Zhou. Information segmentation and investing in cybersecurity. *Journal of Information Security*, 12:115–136, 01 2021.
- [16] Lawrence A Gordon, Martin P Loeb, and Lei Zhou. Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, 6(1), 03 2020. tyaa005.
- [17] IBM. Cost of a data breach report 2020. September 2021, <https://www.ibm.com/security/data-breach>.
- [18] Kaspersky. DDoS Breach Costs Rise to over \$2M for Enterprises finds Kaspersky Lab Report. https://usa.kaspersky.com/about/press-releases/2018_ddos-breach-costs-rise-to-over-2m-for-enterprises-finds-kaspersky-lab-report, last visit October, 2021.
- [19] Kaspersky. What is WannaCry ransomware? <https://www.kaspersky.com/resource-center/threats/ransomware-wannacry>, last visit October, 2021.
- [20] Kerry Krutilla, Alexander Alexeev, Eric Jardine, and David Good. The benefits and costs of cybersecurity risk reduction: A dynamic extension of the gordon and loeb model. *Risk Analysis*, n/a(n/a).
- [21] M. Franco, B. Rodrigues, E. Scheid, A. Jacobs, C. Killer, L. Granville, B. Stiller. SecBot: a Business-Driven Conversational Agent for Cybersecurity Planning and Management. In *16th International Conference on Network and Service Management (CNSM 2020)*, pages 1–7, Izmir, Turkey, November 2020. IFIP.
- [22] Security Magazine. Cyberattacks increased 17% in q1 of 2020, with 77% being targeted attacks. September 2021, [Online] <https://www.securitymagazine.com/articles/95668-cyberattacks-increased-17-in-q1-of-2020-with-77-being-targeted-attacks>, last visit September 2021.
- [23] MYRA. DDoS Angriff. <https://www.myrasecurity.com/de/was-ist-ein-ddos-angriff/>, last visit September, 2021.
- [24] Penta Security. DDoS Angriff. <https://www.pentasecurity.com/blog/ddos-attacks-types-explanation/>, last visit September, 2021.
- [25] Proof Point. Was ist Phishing? <https://www.proofpoint.com/de/threat-reference/phishing>, last visit October, 2021.
- [26] Rapid 7. Phishing-Angriffe. <https://www.rapid7.com/de/cybersecurity-grundlagen/phishing-attacks/>, last visit October, 2021.

- [27] Semrush. How Much Is My Website Worth? A Guide To Uncovering A Website's Value. <https://www.semrush.com/blog/how-much-is-website-worth/#header2>, last visit December, 2021.
- [28] W. Smart. Lessons learned review of the wannacry ransomware cyber attack. [Online] <https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf>, last visit October 2021.
- [29] Software Lab. Was ist Phishing? Definition, Erklärung und 5 Beispiele. <https://softwarelab.org/de/was-ist-phishing/>, last visit October, 2021.
- [30] TechRepublic. Cybersecurity spending to hit \$150 billion this year. September 2021, <https://www.techrepublic.com/article/cybersecurity-spending-to-hit-150-billion-this-year/>.
- [31] TechTarget. ransomware. <https://searchsecurity.techtarget.com/definition/ransomware>, last visit October, 2021.
- [32] TitanFile. 7 Types of Computer Malware and How to Prevent Them. <https://www.titanfile.com/blog/types-of-computer-malware>, last visit October, 2021.
- [33] Trend Micro. What Are the Different Types of Phishing? https://www.trendmicro.com/en_us/what-is/phishing/types-of-phishing.html#whaling-tm-anchor, last visit October, 2021.
- [34] Vade Secure. Cybercrime Statistics: Top Threats and Costliest Scams of 2020. <https://www.vadesecure.com/en/blog/cybercrime-statistics-top-threats-and-costliest-scams-of-2020>, last visit October, 2021.
- [35] Varonis. What is ransomware. <https://www.varonis.com/blog/what-is-ransomware/>, last visit October, 2021.
- [36] ZD Net. 16 DDoS attacks take place every 60 seconds, rates reach 622 Gbps. <https://www.zdnet.com/article/16-ddos-attacks-take-place-every-60-seconds-rates-reach-622-gbps/>, last visit October, 2021.

Abbreviations

ALE	Annualised Loss Expectance
ARO	Annualised Rate of Occurrence
CsPI	Cybersecurity Performance Index
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
EBIS	Distributed Denial-of-Service
EV	Earned Value
GL	Gordon-Loeb
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ICT	Information and Communications Technology
IT	Information Technology
IoT	Internet of Things
IP	Internet Protocol
NIST	National Institute for Standards and Technology
ODM	Object Data Modeling
ROI	Return on Investment
ROSI	Return-On-Cybersecurity-Investment
SME	Small and medium-sized enterprises
SSL	Secure Sockets Layer
SQL	Structured Query Language
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UX	User Experience

List of Figures

2.1	Benefits and costs of an investment in cybersecurity [14]	11
4.1	Methodology Diagram	16
5.1	Technology Stack	24
5.2	Architecture Overview	25
5.3	Home Page	26
5.4	Business Profile	27
5.5	Segments Empty Page	28
5.6	Add Segment Dialog	28
5.7	Add Segment Dialog With Selected Segment Type	29
5.8	Segments Overview	30
5.9	Segment Details	30
5.10	Edit Segment Dialog	30
5.11	Recommendation Page	31
5.12	Recommendation Page With Recommendations	32
5.13	Calculation of ROSI integrated with MENTOR engine	32
5.14	Server Architecture	33
5.15	Investment Calculator Code Snipped	34
5.16	Value Estimation Code Snipped	34
5.17	Protection Recommender Code Snipped	35
5.18	ROSI Calculation Code Snipped	35

5.19	Annual Investment Cost Code Snipped	36
5.20	Business Profile Schema	36
5.21	Optimal Investment Equation Schema	37
5.22	Optimal Investment Equation Data	37
5.23	Segment Definition Schema	38
5.24	Database Value Estimation Data	39
5.25	Webserver Value Estimation Data	39
5.26	Segment Schema	40
6.1	Montana AG Business Profile	42
6.2	Segments Creation	43
6.3	Database Segments Overview	44
6.4	Segment Creations	45
6.5	Electronic Web Server Recommendation Configuration	45
6.6	Household Web Server Recommendation Configuration	45
6.7	Electronic Web Server Recommendations	46
6.8	Household Web Server Recommendations	46
6.9	Network Recommendations	47
6.10	ROSI Calculation Dialog	47
6.11	Recommendations With Calculated ROSI Index	48

List of Tables

3.1	Related Work Comparison	14
4.1	Database Valuation Parameter	19

Appendix A

Installation Guidelines

This chapter provides necessary information to run the prototype.

1. Run Frontend & Backend

- (a) Clone the Git Repository from: <https://github.com/Chreggii/cybersecurity-investment-tool>
- (b) Follow the instructions in the *Usage* part (<https://github.com/Chreggii/cybersecurity-investment-tool#usage>).

2. Run MENTOR

- (a) Clone the Git Repository from: <https://github.com/Chreggii/GordonMENTOR>
- (b) Open your console and run *cd Server*
- (c) To start the server run *python3 server.py*