H. Roßnagel, C.H. Schunck, S. Mödersheim (Hrsg.): Open Identity Summit 2022,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2022 131

Online tool for matching company demands with IT-security offerings

Nicolas Fähnrich[1], Heiko Roßnagel[1]

Abstract: Small and medium sized companies (SMEs) are often insufficiently protected against cyberattacks although there is a wide range of cybersecurity guidelines, products and services available. In this paper, we present an online tool to support SMEs in improving their IT-security level by enabling them to identify critical business processes and to identify the most pressing protection needs by using a lightweight value chain-based approach. For using the online tool, no expert knowledge of the company's IT-infrastructure or implemented IT-security measures is required, since no assessment of cybersecurity threats but of the impact of potential damage scenarios on business processes is carried out. Based on a generated set of recommendations, companies are provided with suitable IT-security measures and corresponding offerings in a prioritized order. These offerings include services and products to implement the given recommendations.

Keywords: IT-security; expert system; value chain; bayesian network; SME; damage scenarios

1 Introduction

The ongoing trend towards digitalization enables companies to slim down processes, shorten response times and save costs. In contrast, there is an increasing threat from cyberattacks, which can cause significant damages to companies [BS20], [G 21]. Although there are numerous guidelines available to improve the IT-security level in companies like the German BSI IT-Grundschutz [BS21] or ISO/IEC 27001 [IS13], in practice the IT-security level is often insufficient, especially among SMEs [BS20], [Bs11], [Hi17]. This circumstance cannot be explained with a lack of IT-security offerings. We assume that the high complexity of existing guidelines and the heterogenous and wide range of IT-security products/services on the market combined with a low willingness to pay lead to a high entry barrier for companies that have so far invested little in IT-security. It's a challenge for companies to identify their protection needs and appropriate security measures, especially if they have not experienced any major damage from IT-security incidents so far. This paper, thus, presents the expert system "Smart Matching" to support SMEs in improving their IT-security level by giving prioritized recommendations and suitable technical/organizational measures for implementation including adequate offerings from a curated database. The expert system doesn't contain a security analysis based on implemented IT-security measures, but was rather designed in a way to be used by various company representatives without expert knowledge in IT-security and to offer a low-threshold entry to suitable IT-security solutions.

[1] Fraunhofer IAO, Nobelstraße 12, 70569 Stuttgart, firstname.lastname@iao.fraunhofer.de

doi:18.18420/OID2022-12

Companies gain insights into which areas of their business are particularly threatened and should be protected. The expert system was developed as part of the German national project TISiM [TI22b] which is financed by the Federal Ministry for Economic Affairs and Energy (BMWi) and is available free of charge as part of the webapp Sec-O-Mat [TI22a].

2 Related Work

There are numerous IT-security standards, guidelines and products/services available, which results in the challenge to identify suitable solutions that meet the respective company's requirements. Conventional approaches in IT-security consulting projects that follow standards like ISO/IEC 27001 [IS13] or BSI IT-Grundschutz [BS21] to support companies in this decision process start off with a documentation of the IT-infrastructure. Furthermore, all business processes with the involved IT-systems and data types are documented. In a following step, possible IT-security threats are identified and potential threats are rated and documented, whereupon a risk is derived. The current state of already implemented IT-security measures is documented and then compared to a target-state that is determined by the risk analysis and corresponding catalogues. These approaches are well established in practice and result in a detailed analysis of the specific IT-security demand including suitable recommendations for implementation. However, this procedure is resource-intensive and requires IT-security experts and the cooperation of company representatives who are familiar with the company's business processes and IT-infrastructure. Furthermore, a key element in various standards is the consideration of possible IT-security threats that lead to suitable mitigation measures, however this can potentially lead to misperceptions if this is not carried out by experts. For these reasons, the existing conventional approaches are not suitable for the given problem of an easy, low-threshold entry into IT-security and a consideration of possible damage scenarios of cyberattacks and their impact on business processes may be helpful to derive suitable measures. However, conventional approaches are indirectly used in the context of creating the knowledge base of our solution.

3 An expert system to assess the impact of damage scenarios and identify suitable IT-security measures

We have developed an expert system that enables SMEs to identify appropriate IT-security measures with little expense and without expert knowledge on part of the companies following a different approach by considering possible damage scenarios which can occur as a result of IT-security incidents. As part of our work in TISiM, it was our task to provide SMEs a low-threshold entry into IT-security for different company representatives without IT-security background, that can only assess the relevance of certain cybersecurity threats to a limited extent. They are, however, able to assess the impact of certain damage scenarios on their company. We therefore modelled the interrelationships between damage scenarios that affect the company's business processes and suitable recommendations for IT-security

to avoid them. We refrain from ascertaining the actual state of implemented IT-security measures as this cannot be determined reliably without expert knowledge. When developing a process model for supporting SMEs to comply with the EU-GDPR in earlier works, we already found many similarities regarding the business processes of companies in different industry sectors and with different sizes [FK19]. We therefore assume that most SMEs can be described based on their value chain activities with sufficient accuracy following Porter's value chain approach [Po85] and that other parameters such as the company size or the industry sector play a subordinate role. To achieve this, we identified major business processes, processed data categories and typical IT-systems and applications for every value chain activity. Based on the information regarding business processes and processed data, we have derived possible damage scenarios that directly affect the business processes, the processed data and the underlying IT-systems. In this procedure, the protection goals "Confidentiality", "Integrity" and "Availability" of the CIA-triad [Pe08] were used to derive damage scenarios for every business process within every value chain activity. The damage scenarios focus on the business impact and not on IT-security incidents that may cause them. This way, we ensure that various company representatives can adequately assess the damage scenarios without technical or IT-security expert knowledge. The procedure outlined above enables us to assess companies based on their value chain activities and the corresponding damage scenarios. To identify recommendations to increase the company's IT-security level, we chose an attack-based approach by using MITRE's "ATT&CK Matrix for Enterprise" [MI22]. With this approach, we made assumptions for each value chain activity based on the identified business processes and IT-systems (e.g. "no portable media in production environment"). Considering these assumptions, we evaluated all attack techniques contained in the matrix according to whether the attack is relevant in the context of the considered value chain activity. Based on this, we identified associated mitigation measures which are given in the matrix. These mitigation measures are described in detail and address specific systems and are therefore not suitable in their given form. Therefore, we derived recommendations on a higher level based on them and aggregated similar recommendations. These recommendations are not new and can be found in various IT-security guidelines. However, in our approach we don't just want to identify recommendations relevant to a specific company but want to identify the most urgent ones where there is the greatest need for action. The recommendations are designed to be easy to understand and to be implemented through various suitable technical and/or organizational measures including adequate offerings (products/services) that are provided by the system. The expert system is based on a Bayesian network [En97], [Je01] that links the company's value chain activities to the recommendations. Every value chain activity forms a node in the Bayesian network that is connected to the nodes of the corresponding damage scenarios, which in turn are connected to the recommendations layer (Figure 1). In total 9 value chain activities with a total of 48 damage scenarios are mapped. The information which recommendations are suitable to address the respective damage scenarios is stored in conditional probability tables within a knowledge base that is built by using specially developed software tools for knowledge extraction and representation, which are described in more detail below. The knowledge base contains the recommendations that are individually rated by IT-security experts based

on their suitability/relevance to address specific damage scenarios for every value chain activity. The expert system is used as follows: Company representatives rate possible damage

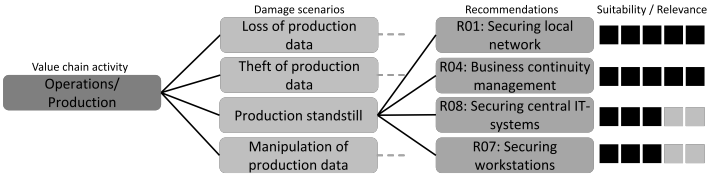

Fig. 1: Simplified, exemplary illustration of the bayesian network used in the expert system

scenarios based on the business impact for every value chain activity. The expert system matches these ratings with the recommendations stored in the knowledge base and outputs suitable ones in a prioritized order. The given recommendations and their priority are based on the information provided by the company representative on the impact of possible damage scenarios and the corresponding expert knowledge to address them. Companies can choose appropriate technical and/or organizational measures for implementing the recommendations that are output by the system. In addition, suitable services and products for each measure are output via a database query. These results can be filtered further, e.g. to find regional providers. By using the expert system, companies receive prioritized recommendations that match their individual requirements. In addition, appropriate technical and/or organizational measures including potential products, services and providers are suggested to implement the recommendations. We developed the expert system as a working prototype with the backend program including additional tools for building the knowledge base implemented in Python. The frontend of the underlying server/client-architecture was implemented in HTML and Javascript as functional mockup in order to be able to perform user tests at an early development stage. The production version of the frontend was implemented according to our specifications by Hochschule Mannheim and is available online [TI22a]. After the company representative has provided all the necessary information, these are transferred to the expert system running in the backend that returns a set of suitable recommendations in a prioritized order. In the backend application the company data is matched with the knowledge base. As a result, a set of recommendations sorted by priority is generated. This ensures a certain degree of transparency and the companies are made aware of the critical value chain activities. To provide additional guidance for the priority of individual recommendations, an indicator for the relative relevance is calculated for every recommendation. The knowledge base containing the values of the conditional probability tables of the Bayesian network is generated using the knowledge representation tool by calculating mean values of individual datasets generated by IT-security experts.

4 First insights from the company data

We evaluated the anonymously collected data that it transmitted to gain insights on the companies' value chain activities and particularly threatening damage scenarios. As shown in

Figure 2, the activities “infrastructure”, “marketing & sales”, “human resource management” and “customer service” were selected most frequently. The frequency distribution shows

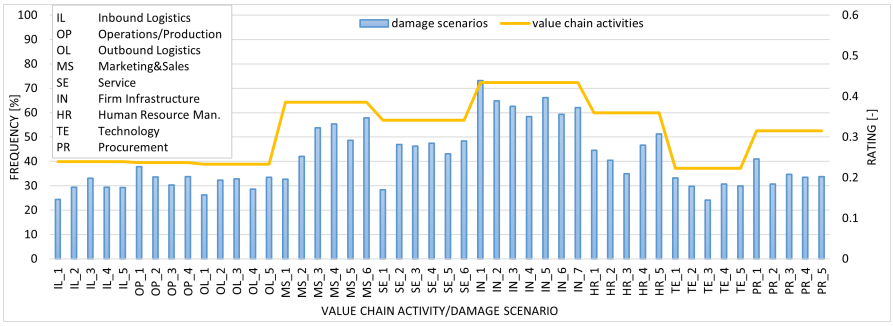

Fig. 2: Rating of damage scenarios and value chain activities (n=3511)

that most of the companies either don’t have production related value chain activities like “inbound logistics” or only use IT-systems within these activities to a limited extent. When considering the data regarding the rating of the damage scenarios within the respective value chain activities, the scenario “IN_1: no/limited availability of IT-systems” is rated the highest (0.61 in a range from 0 to 1), followed by the damage scenario “OP_1: production shutdown” (0.57), “IN_5: loss of company data” (0.55) and “MS_6: theft of customer/contract data” (0.54). The scenarios “SE_1: web presence not available” (0.30), “MS_1: online shop not available” (0.31) are rated the lowest. It’s an interesting result, that the highest rated damage scenarios reflect the results of recent studies, that identify ransomware attacks and the associated downtime and a standstill in production as the greatest threats to companies [Bi21]. These results are an indicator, that the developed solution is being used correctly.

5 Conclusion

The threat of cyberattacks is particularly challenging for SMEs, which are often not adequately protected from them and overwhelmed by complex guidelines and a wide range of IT-security products and services. We have therefore developed an online tool for matching company demands with IT-security offerings described in this paper, that supports SMEs in improving their IT-security level by providing a low-threshold entry into IT-security. The underlying model is based on Porter’s value chain to describe the companies regarding their business processes and possible damage scenarios from cyberattacks. Furthermore, we identified possible recommendations that the expert system can output by using an attack-based approach. For every recommendation a set of suitable technical/organizational measures is provided including suitable IT-security offerings. Companies can use the expert system by rating damage scenarios based on the business impact and receive suitable recommendations in a prioritized form with appropriate technical/organizational measures including adequate products/services. The developed expert system is a lightweight approach that can’t replace resource intensive IT-security consulting projects, especially

because there's no assessment of the company's current state of the IT-infrastructure and implemented IT-security measures. However, we performed several user tests with company representatives of different industry sectors and further optimized the expert system based on the results. Based on our experience from these user tests and an additional focus group discussion, we think that our tool fulfills its purpose to support companies to get started with improving their IT-security. However, only time can tell how the expert system performs in practice. Furthermore, the analyses shown in this paper are not a representative study, but rather the first results from the operation of the expert system that provide an initial insight into the company data. We will constantly optimize the expert system based on our lessons learned and extend the knowledge base with additional datasets created by IT-security experts to further improve the quality of the results.

References

[Bi21] Bitkom: Wirtschaftsschutz 2021, 2021.

[Bs11] BSI; secunet: Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen, Bonn, 2011.

[BS20] BSI: Die Lage der IT-Sicherheit in Deutschland 2020, Bonn, 2020.

[BS21] BSI: IT-Grundschutz: Informationssicherheit mit System, Mar. 2021.

[En97] Enrique Castillo Jose Manuel Gutierrez, A. S. H.: Expert Systems and Probabilistic Network Models. Springer-Verlag, New York, 1997.

[FK19] Fähnrich, N.; Kubach, M.: Enabling SMEs to comply with the complex new EU data protection regulation. In: Open Identity Summit 2019. Gesellschaft für Informatik, 2019.

[G 21] G DATA CyberDefense AG: Cybersicherheit in Zahlen, Hamburg, 2021.

[Hi17] Hillebrand, A.; Niederprüm, A.; Schäfer, S.; Thiele, S.: Aktuelle Lage der IT-Sicherheit in KMU, tech. rep., Bad Honnef: WIK GmbH, 2017.

[IS13] ISO/IEC: Standard ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements, Geneva, 2013.

[Je01] Jensen, F. V.: Bayesian Networks and Decision Graphs. New York, 2001.

[MI22] MITRE: ATT&CK Matrix for Enterprise, `https://attack.mitre.org/matrices/enterprise/`, 2022, visited on: 02/15/2022.

[Pe08] Perrin, C.: The CIA Triad, 2008.

[Po85] Porter, M. E.: Competitive advantage: creating and sustaining superior performance. New York, 1985.

[TI22a] TISiM: Sec-O-Mat, `https://sec-o-mat.de`, 2022.

[TI22b] TISiM: Transferstelle IT-Sicherheit im Mittelstand, `https://tisim.de`, 2022.