Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 93 (2020) 587–592

www.elsevier.com/locate/procedia

53rd CIRP Conference on Manufacturing Systems

Helping companies to evaluate their status quo in information security with a serious gaming-based economical quantification approach

Günther Schuh[a)], Jan Hicking[a)], Jacques Engländer [a)]*, Violett Zeller[a)], Martin Perau[a)]

a) Institute for Industrial Management, FIR at RWTH Aachen University, Campus-Boulveard 55, Aachen 52074, Germany
**Corresponding author. Tel.: +49-241-47705-517; E-mail address: jacques.englaender@fir.rwth-aachen.de*

Abstract

The number of cyber-attacks on small and medium enterprises (SMEs) is constantly increasing. SMEs do not recognize the attacks until the damage has occurred. Only then, they fight with measures to increase IT-security and IT-safety. Many studies come to the point that this refers to a lack of budget, expertise and awareness of the need for IT-security. There are many compendia with recommendations for action, but they are too comprehensive and unspecific to the individual needs of SMEs. In this paper, we present the results of a research activity on the gaps that address the challenges faced by SMEs. In addition, we develop a concept for a serious gaming approach that includes an economic perspective on IT-security measures and shows how SMEs can derive their own IT-security target state.

Keywords: IT-security; serious gaming, economic quantification; manufacturing companies; digital transformation; SMEs

1. Introduction

The continuously widening gap between expert knowledge and laypersons, especially with regard to growing IT-security requirements, induced by the far-reaching trends of digitalization, is creating new challenges. These challenges range from the handling of personal data in the private environment to so-called cyber-physical systems in the industrial context, which are vulnerable to an equally increasing number of attackers. Due to the networking within the framework of Industry 4.0 and the convergence of Information Technology (IT) and Operational Technology (OT), which is also known as shopfloor IT, a company offers attackers a growing attack surface. [1]

According to public figures, 53% of SMEs worldwide were or are affected by cyber-attacks [2]. Numerous sources assume that the dark figure is significantly higher. The Federal Office for Security and Information Technology of Germany (BSI) classifies the risk situation as high in 2018 based on external factors and the state of the art in SMEs [3].

However, an economic evaluation of security measures against these attacks or potential attacks is not available yet, so that the information required for strategic developments is neither valid nor meaningful. In order to be able to carry out the evaluation, knowledge about the situational behavior of companies in the face of various IT-security scenarios must be collected and selected measures must be evaluated in terms of their effectiveness and economic efficiency. This enables an sustainable implementation of IT-security for SMEs.

To achieve this goal, a research project will develop a serious gaming environment as well as a simulation platform embedded in a workshop concept and use it to obtain valid data from the behavior of the participants for the quantitative economic evaluation of IT-security measures.

2. Background

The majority of SMEs do not have an IT-security officer and often the related tasks are performed on a part-time basis and together with other tasks [4]. At the same time, however, ‘hacker attacks’ in 2019, at 43%, are the greatest subjective risk for companies [5]. SMEs are often either unaware that information respectively IT-security can be decisive for the existence of the company, or they simply lack the expertise and

10.1016/j.procir.2020.05.196

budget to select and implement the relevant technical, organizational and cultural measures, or even to know their interrelationships [6]. According to the German Insurance Association, successfully attacked SMEs had to shut down their operations completely in 43% of cases. Thus shows that the IT-security is a critical corporate function.

In companies, the necessity of the profitability of projects is measured by the ROI (Return on Invest). This shows whether an investment is worthwhile or not. The return on investment of IT-security measures is hard to determine, since the costs of a cyber-security incident is difficult to quantify [7]. The topic of return on security investment (ROSI) or the economic consideration of IT-security measures is therefore currently a subject of intense discussion in research and industry.

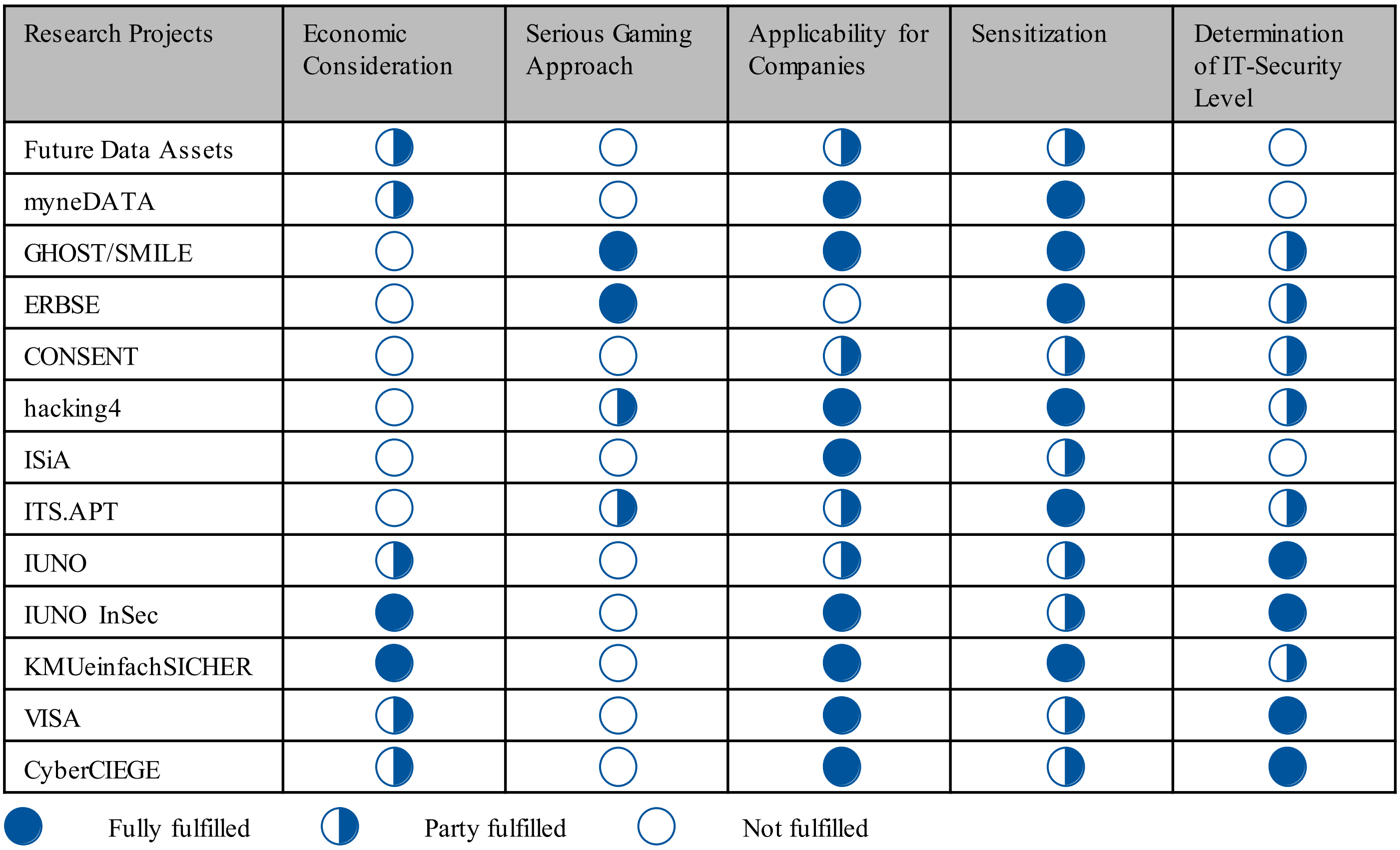
$$\text{ROSI} = \frac{(\text{Risk Exposure} * \text{Risk Mitigated}) - \text{Solution Cost}}{\text{Solution Cost}} \quad [8] \qquad (1)$$

In the research area of IT-security, several projects were carried out with the aim of improving IT-security considering the economical perspective of IT-security measures (Fig. 1.). An explicit example is the project SIDATE. Within the project tools and concepts were developed, which allow a better assessment of the existing security level and thus help to improve the security of the infrastructures of small and medium-sized manufacturing companies. The focus is on the applicability and practicability, which can also be used by operators with special economic, organizational and personnel requirements. Within this project, the economic consideration of IT-security measures was partly considered. In other projects with a focus on raising awareness of possible cyber-attacks, elements of serious gaming were frequently used. In these projects, however, no economic consideration of IT-security measures were included.

Serious games are defined as games that use computer technologies as well as advanced graphic elements and have as their goal the learning or training of employees. In many contexts, serious games are also referred to as digital learning games, game-based learning, business games, applied games, educational games and edutainment games [9].

An example of a serious game is developed by the Center for Cybersecurity and Cyber Operations of the Naval Postgraduate School of the US Armed Forces: CyberCIEGE represents the broad mass of serious games on the topic of IT-security. It was developed to convey network security concepts and to increase awareness. It is used by US government agencies, universities and community colleges as a training tool. The serious games available on the market pursue partly different goals. From 'secure on the internet' [10] to increase user sensitivity, to 'back-doors and breaches' [11] to teach specific IT-security measures, to company-specific cyber ranks in which employees are to be trained on IT-security topics.

It turns out that the topic of the economic consideration of IT-security measures has not been examined with an approach from the field of serious gaming (see Fig.1.). Thus, there is a research gap in the combination of a serious game with an economic evaluation of IT-security measures. The novelty of this approach is to combine the economic evaluation of IT-security with a serious game approach. Both elements are not new in themselves, even though they are currently the subject



Research Projects	Economic Consideration	Serious Gaming Approach	Applicability for Companies	Sensitization	Determination of IT-Security Level
Future Data Assets	◑	○	◑	◑	○
myneDATA	◑	○	●	●	○
GHOST/SMILE	○	●	●	●	◑
ERBSE	○	●	○	●	◑
CONSENT	○	○	◑	◑	◑
hacking4	○	◑	●	●	◑
ISiA	○	○	●	◑	○
ITS.APT	○	◑	◑	●	◑
IUNO	◑	○	◑	◑	●
IUNO InSec	●	○	●	◑	●
KMUeinfachSICHER	●	○	●	●	◑
VISA	◑	○	●	◑	●
CyberCIEGE	◑	○	●	◑	●

● Fully fulfilled ◑ Party fulfilled ○ Not fulfilled

Fig. 1. Classification of previous research projects in the field of IT-security

of research. Business games or serious games are becoming more and more widespread as a professional method, while at the same time the number of efforts to determine the economic impact of IT-security is increasing. By combining these two research elements, the goal of economic evaluation of IT-security can be achieved.

3. Research Methodology

To achieve this goal, a two-year research project is planned in which the tasks listed below must be completed. This will be done in cooperation between RWTH Aachen University and the University of Applied Sciences of Aachen in close collaboration with associations and its member companies from industry. The tasks are:

1. Development of a rough concept [12] of the serious game environment (including storybook, interaction with the players, who will be involved, etc.) based on different requirements, which are determined by the consortium within the project, considering different target groups. This ensures that the serious game environment can be developed in a goal-oriented manner,
2. Description and structuring of relevant IT-security measures based on a hierarchical approach and supplementation with typical attack vectors,
3. Evaluation of the identified IT-security measures with regard to their economic characteristics in order to enable a realistic modelling,
4. Provision of a serious game environment as minimum viable product, into which all results from earlier septs in the project can be integrated. At the same time, an iterative 'further development by design' is ensured.

The overall aim of the research project is to develop a serious game environment and a simulation platform in form of a software application to enable companies to deal independently with IT-security in relation to their specific situation and to evaluate IT-security measures economically. To achieve that, we pursue the following three sub-goals:

- Determination of the actual and target state of the IT-security level under economic aspects of IT-security,
- Integration of an IT-security assessment into business processes,
- Sensitization for dealing with IT-security.

In addition to that, the serious game environment is developed iteratively. It can be ensured that the requirements set is met at an early stage. The associated companies and groups of interests play a special role. Due to the possibility of repeatedly relying on a large number of companies, the external validity and applicability of the serious game environment is ensured. The internal validity is guaranteed by the serious game concept to be considered as the most suitable.

4. Concept and logic

The concept consists of four elements: modelling of the company, derivation of the attack vectors, defense and evaluation of the attacks, debriefing of the actions. The content of the elements is described below (Fig. 2.)

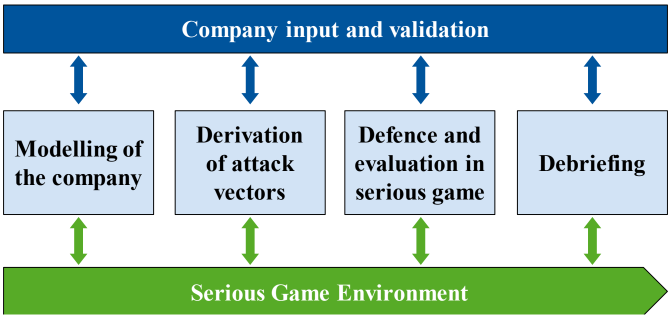

Company input and validation
Modelling of the company
Derivation of attack vectors
Defence and evaluation in serious game
Debriefing
Serious Game Environment

Fig. 2: Project methodology

4.1 Modelling the company

4.1.1 Structural elements

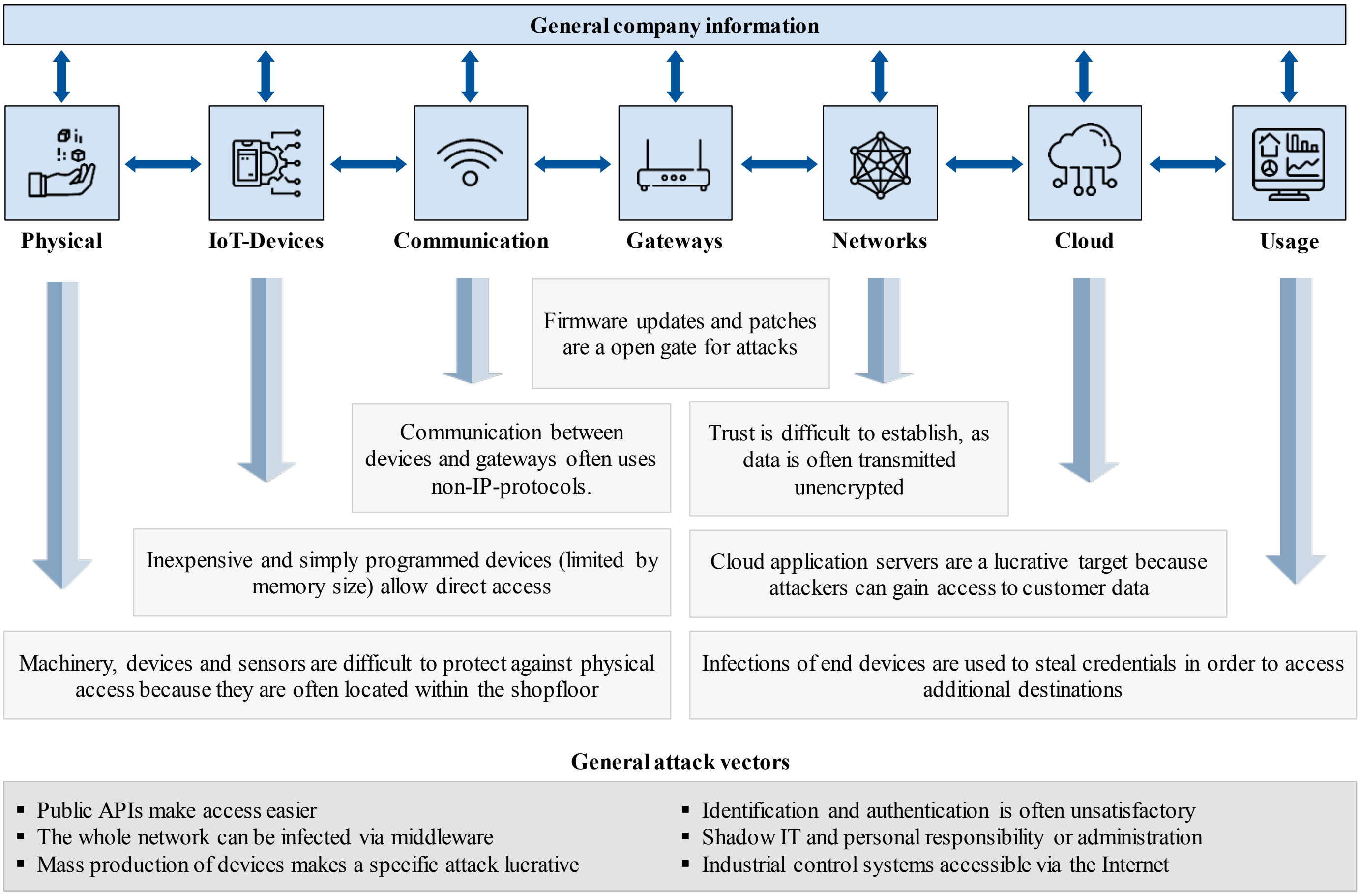
Within the modelling of the company, all relevant structure elements of an enterprise must be represented in an abstract form, which have an influence on potential attack vectors. Currently, eight categories or layers are provided within the modelling (see Fig. 3.):

- General company information
- Physical elements (e.g. machines)
- IoT devices
- Communication
- Gateways
- Networks
- Cloud
- Usage (People)

To ensure an environment in which a wide range of companies are comparable, it is important to address general information about the company that takes part in the serious game. This information includes size of the company, its number of employees and so on.

The physical layer represents the first category that needs to be addressed within the serious game. This category contains mainly components, devices and sensors that are difficult to protect against physical access on the shopfloor. Furthermore, it describes components such as facilities and office areas. On this level, information can be gathered by a physical access to information systems. As a high number of cyber-attacks have their origin within the attacked company itself, it is an important aspect.

IoT-devices represent the second category. The increasing number of IoT-devices within manufacturing companies as well as in our daily life leads to different challenges. The small and cheap devices are produced without any security by design methodology and have a lack of implementation opportunities due to their restricted hardware capacity. They often allow direct access from the internet. Before applying IoT-devices to



Firmware updates and patches are a open gate for attacks

Communication between devices and gateways often uses non-IP-protocols.

Trust is difficult to establish, as data is often transmitted unencrypted

Inexpensive and simply programmed devices (limited by memory size) allow direct access

Cloud application servers are a lucrative target because attackers can gain access to customer data

Machinery, devices and sensors are difficult to protect against physical access because they are often located within the shopfloor

Infections of end devices are used to steal credentials in order to access additional destinations

- Public APIs make access easier
- The whole network can be infected via middleware
- Mass production of devices makes a specific attack lucrative
- Identification and authentication is often unsatisfactory
- Shadow IT and personal responsibility or administration
- Industrial control systems accessible via the Internet

Fig. 3: Modelling the company based on Nokia [13]

a specific use case, several attack vectors and risks need to be evaluated.

Mapping the communication between devices and gateways within an organization is essential for determining the attack vectors, since increased communication significantly increases the impact of a successful attack. As a result, some attack vectors are more likely and potentially more critical to the affected company. To model the communication, the first step is to consolidate the physical devices and gateways into main groups. Afterwards the type of communication between these main groups can be determined.

Typical attack vectors regarding gateways are old software versions and missing updates. Once installed, a continuous update and patch management is missing in many companies. Besides that, the problems occur in earlier stages of the process, too. As companies often do not have the specific expertise and third party consultancy mandates are expensive in long-term, gateways are configured in a wrong and not sufficient way at the same time.

The category networks describes two different types of networks. The first type is a typical network within an company. Movements within this network can due several month before the exploit is triggered. Therefore, network segmentation is a possible IT-security measure. The second type represents networks which include more than one company. Aspects such as a vertical integration in a digital supply chain leads to interesting questions, e.g. how to ensure the trustworthiness of data being shared in these network.

Many companies follow the paradigm ‘cloud first’. Even if a lot of companies see risks and stick to their on-premise solutions, the cloud market increases steadily. By using cloud services, companies transfer a lot of effort to the service and cloud provider. But there are negative side effects, too. By not validating the service provider, the company increases its probability of being hacked via the cloud. For hackers it is much more lucrative to attack a cloud platform than a single company, because accessing the cloud platform ebables accessing data from all connected companies with a lower effort. Cloud providers therefore offer big scale effects for hacker groups.

The usage of IT-systems such as Office-Suite products, ERP-systems or Software-as-a-Service applications in the daily operation builds the last but highly important category. People build the core element of this category. Especially emails became the aim of attackers in the last years, e.g. with spear phishing or outlook harvesting attacks. Therefore, it is more important than ever to implement a continuously awareness and usage training for the employees.

4.1.2 Focus on SMES

In order to focus on SMEs, especially in the area of manufacturing companies, it is important to focus on technologies and the influence of Industry 4.0. To implement this focus in the modelling of the company two possible approaches, both a top-down and a bottom-up approach, are considered. The modelling of the influences of Industrie 4.0

Respectively the implementation of Industrie 4.0 is possible from a top-down approach with the levels of the Maturity Index. The Industrie 4.0 Maturity Index is a guideline that enables the derivation of an individual implementation strategy for Industrie 4.0. As a result of an acatech study carried out in 2017 by an interdisciplinary consortium of research institutions and industrial partners, it helps companies to manage their digital transformation [14]. The Maturity Index considers four different dimensions: resources (workforce, machinery and equipment), information systems, culture and organizational structure (see Fig. 4.). As it is shown in the figure, the Maturity Index is based on six discrete, consecutive and benefit-oriented maturity levels. Each of these maturity levels possesses different potential attack vectors and therefore related IT-security measures. However, in detailing the concept, it must be ensured that there are intersections between the described levels and the eight categories described above.

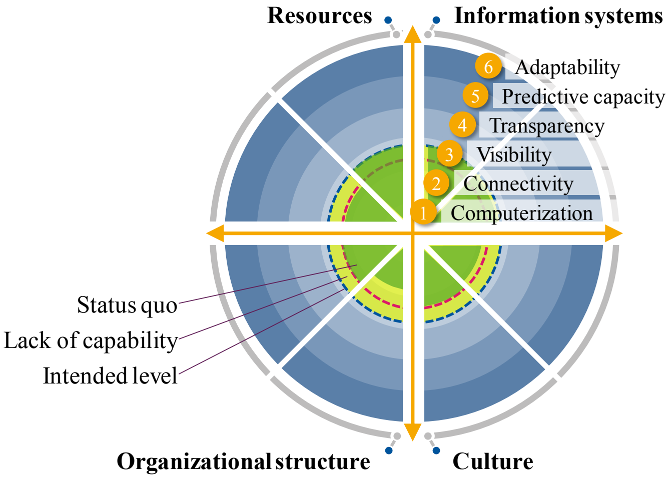


Fig. 4: Industrie 4.0 Maturity Index

Bottom-up it is possible to implement explicit Industrie 4.0 use cases inside the serious gaming environment. This enables companies to determine which use cases have an impact on the risk level and which IT-security measures are necessary for each use case. E.g., a company wants to implement predictive maintenance to a tooling machine along with the support of a service provider via cloud. In this case, other IT-security measures should take place than with an on-premise solution. Several of these specified use cases will found the basis for further implementation and work.

The top-down approach addresses aspects of the overall strategy for a digital transformation, from where implications on IT-security can be derived. The bottom-up approach helps to identify specific IT-security measures for validated use cases. Therefore, both the serious game environment and simulation platform will be developed with high reliability.

4.2 Derivation of the attack vectors

The modelling of the company is the basis for an individualized determination of the attack vectors. The overall aim is to identify an optimal trade-off between the level of detail of the modelling and the time required for the modelling. Within the project, it must therefore be considered if different detail levels of the modeling are possible.

These attack vectors, partially mentioned above (see Fig. 3.), will be a collection of possible scenarios derived from both case study analysis or literature review and expert interviews. As the attack vectors are part of continuous change and development, it is important to implement an iterative process to keep them up to date.

The result will be a longlist of attack vectors, which then needs to be clustered in a second step. The eight mentioned categories, its specification as well as the complexity and possible damage of the attack vectors are dimensions of these clustering process. E.g., to build the attacking scenarios, it is important to know whether a specific attack vector causes a lot of damage or not. By modelling the company and attack vectors, the risk exposure can be determined, which determines how likely an attack is under given conditions.

4.3 Defence and evaluation of the attacks

Based on the modeling of the company and the attack vectors, a quantitative economic evaluation of the IT-security measures can be carried out in the serious gaming environment. The company now decides whether a specific IT-security measure should be implemented to prevent various attacking scenarios or not. If a company decides to do so, the benefit and therefore the ROSI of the IT-security measures rises. At the stage where the company does not want to invest in other measures, the optimal IT-security level is reached. By applying these procedure to a wide range of companies, a economic quantification will be enabled due to the high number of participants and their behavior in the serious game.

For this purpose, the participant is provided with possible attack scenarios in the serious gaming environment. In essence, the participant should determine the monetary effects that a 'successful failure' would have on his enterprise. In order to reduce complexity, a specification of monetary effects should be provided at this point if required. This determination of the risk mitigated is carried out for all possible attack vectors.

Because of this step, a qualitative evaluation of the risk mitigated is carried out depending on the attack vector and the company characteristics. With the help of well-known IT-security solution costs, it is possible to deduce whether the appropriate IT-security measure is economically reasonable or not. Based on the generated data from the studies, a determination of target values for IT-security solution costs is possible.

In addition, the participant could select the correct IT-security measure to defend the given attack vector or to prevent its risk mitigation. This step serves primarily to sensitize the participant in the subsequent debriefing session to show which IT-security measure would be the most appropriate for his modelled enterprise.

4.4 Debriefing of the actions

The focus of the debriefing session is to present the results of the economic evaluation of the IT-security measures applied by the participating companies. It is demonstrated whether the chosen IT-security measures are economically reasonable for the given risk mitigated or not. Besides, if sufficient data is available, companies can access to comparisons on how similar companies have estimated the reduced risk mitigated for similar attack vectors.

During the debriefing, participants are sensitized to the correct selection of IT-security measures. It will be discussed whether the selection of the IT-security measure is best suited for the given attack vector or which IT-security measure would be more suitable. Based on the information provided during the participation it can be determined whether the most suitable IT-security measure is economically reasonable for the participant.

Furthermore, it can be discussed which altered aspects of the modelling would have caused other attack scenarios. This is particularly relevant for companies in order to gain insights into how the potential attack vectors are related to the effects of e.g. digital transformation.

A detailed and personal feedback of the participants guarantees a continuous development of the serious game environment. This enables an increase in the number of participants through a permanent development and optimization of the serious game environment. Due to this procedure, a high number of participants is necessary to evaluate the economic aspects of IT-security measures.

5. Discussion

In order to be able to make valid statements about the economic profitability of IT-security measures, a sufficiently high number of participants is required. The openness of companies towards the topic of IT-security is decisive to reach this number of participants. Querying the economic dimensions of a possible attack represents sensitive company information, a high level of data protection has to be guaranteed. In order to realize the high number of participants, existing company contacts and close cooperation with many associations are relied upon.

Furthermore, the modelling of the companies and the derivation of attack vectors is a complex task, in which multiple challenges can occur. Due to the detailing of these two aspects, a modification of the presented concept may be necessary.

References

[1] BMWi, “Industrie 4.0 und Digitale Wirtschaft - Impulse für Wachstum, Beschäftigung und Innovation“, 2015.
[2] Cisco, “Small and Mighty. How Small and Midmarket Businesses Can Fortify Their Defenses Against Today’s Threats.”, 2018.
[3] BSI Germany, “Die Lage der IT-Sicherheit in Deutschland 2018”, 2018
[4] A. Hillebrand, A. Niederprüm, S. Schäfer, S. Thiele, “Aktuelle Lage der IT-Sicherheit in KMU. Kurzfassung der Ergebnisse der Repräsentativbefragung”, 2017.
[5] Gothaer Versicherungen, “Gothaer KMU Studie 2019”, 2019.
[6] K. Müller, “IT-Sicherheit mit System”, Springer Fachmedien Wiesbaden, 2018.
[7] C. Onwubiko, A. Onwubiko, “Cyber KPI for Return on Security Investment”, International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2019.
[8] W. Sonnenreich, “Return On Security Investment (ROSI): A Practical Quantitative Model”, Journal of Research and Practice in Information Technology 38, pp. 239-252, 2005.
[9] D. Crookall, “Serious Games, Debriefing, and Simulation/Gaming as a Discipline”, Simulation & Gaming 41(6), pp. 898 –920, 2010.
[10] BSI Germany, “Kritische Infrastrukturen (2017)”, 2017.
[11] Black Hills Information Security, “Backdoors and Breaches (2018)”, 2018.
[12] A. M. Darwesh, “Concepts Of Serious Game in Education”, International Journal Of Engineering And Computer Science. Vol. 4 Issue 12, pp. 15229-15233, 2015.
[13] Nokia Threat Intelligence Center, “The Coming of Age of IoT Botnets”, 2017.
[14] G. Schuh, R. Anderl, J. Gausemeier, M. ten Hompel, W. Wahlster, Eds. 2017: Industrie 4.0 Maturity Index. Die digitale Transformation von Unternehmen gestalten (acatech STUDY). Herbert Utz Verlag, Munich.