Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Wirtschaft

CARF Luzern 2020

Controlling.Accounting.Risiko.Finanzen.

Konferenzband

Konferenz Homepage: www.hslu.ch/carf

Cyber-Risks in German SMEs – the Human Dimension

Beitragsart (Extended Abstract)

Prof. Dr. habil. Patrick Ulrich
Aalen University of Applied Sciences, Aalen Management Institute (AAUF), Beethovenstraße 1, 73430 Aalen, Germany, patrick.ulrich@hs-aalen.de

Vanessa Frank, M.Sc.
Aalen University of Applied Sciences, Aalen Management Institute (AAUF), Beethovenstraße 1, 73430 Aalen, Germany, vanessa.frank@hs-aalen.de

Alice Timmermann, LL.M., M.Sc.
Aalen University of Applied Sciences, Aalen Management Institute (AAUF), Beethovenstraße 1, 73430 Aalen, Germany, alice.timmermann@hs-aalen.de

Abstract
Cybercrime represents a growing risk for companies, and human error in particular opens up the possibility for criminals to access sensitive internal company data, which can lead to economic and reputational damage for companies. Based on a comprehensive online survey conducted by the Aalen Institute for Corporate Governance (AAUF) in 2019, German SMEs were asked about the human dimension in Cyber-Security. The lack of security awareness and knowledge of employees as well as a lack of Cyber-Security training in companies could be identified as difficulties in the fight against Cybercrime.

1 Introduction

Cyber-Attacks spy on, manipulate or destroy data, which can have significant economic consequences for companies and ultimately damage their reputation (Marsh/Microsoft, 2018, p. 6). According to a study conducted by the US security company KnowBe4, companies particullary conserned about Cyber-Attacks which exploit the human factor and thus companies consider Phishing Scam (96 percent) and Social Engineering (70 percent) as the main threats for their internal company security (KnowBe4, 2019, p. 3). By feigning a false identity such attacks aim to influence human behaviour and try to exploit human characteristics such fear, trust or curiosity in order to gain access to sensitive internal information of a company (Bundesamt für Sicherheit in der Informationstechnik, n.s.). Consequently, the human factor is considered the most significant weakness in terms of Cyber-Security (Wiederhold, 2014, p. 1).

Therefore, the Aalen Management Institute (AAUF) has conducted a study on Cyber-Security in german SMEs in 2019, which deals with the area of conflict between Cyber-Security and the human factor in companies. This article is intended to illustrate a section of the study's basic findings, to show the need for action for companies and to highlight the human factor in the context of the changing technical framework and Cyber-Security.

2 Survey and Hypotheses

In order to generate a significant database, 14,495 companies were contacted in the period from 23.10.2019 to 31.12.2019. 372 companies participated in answering the questions asked while 184 companies processed the complete questionnaire.

The majority of the evaluated companies has an annual turnover of less than 100 million euros and between 100 and 1000 employees. Most companies indicated to operate as GmbH or GmbH & Co. KG. The sample of companies reflect a wide range of industries. Most of respondents are employed in the respective IT departments or operate as managing directors of the companies.

In order to identify the human factor as a safety problem to be solved, the following hypotheses will be tested:

1. Employees have low security awareness
2. Employees have knowledge deficits
3. Employees are not sufficiently trained

3 Empirical Results

At first the respondents were asked about the greatest challenges in the defense against current Cyber-Risks in their company. Figure 1[1] shows that in addition to the early detection of relevant attacks (61 percent) and the enforcement of security standards (52 percent), the lack of security awareness among employees (61 percent) is seen as one of the greatest challenges in countering Cyber-Risks.

[1] Multiple answers were possible.

■ Bereich (Controlling, Accounting & Audit, Risk & Compliance, Finanzen oder Lehre)

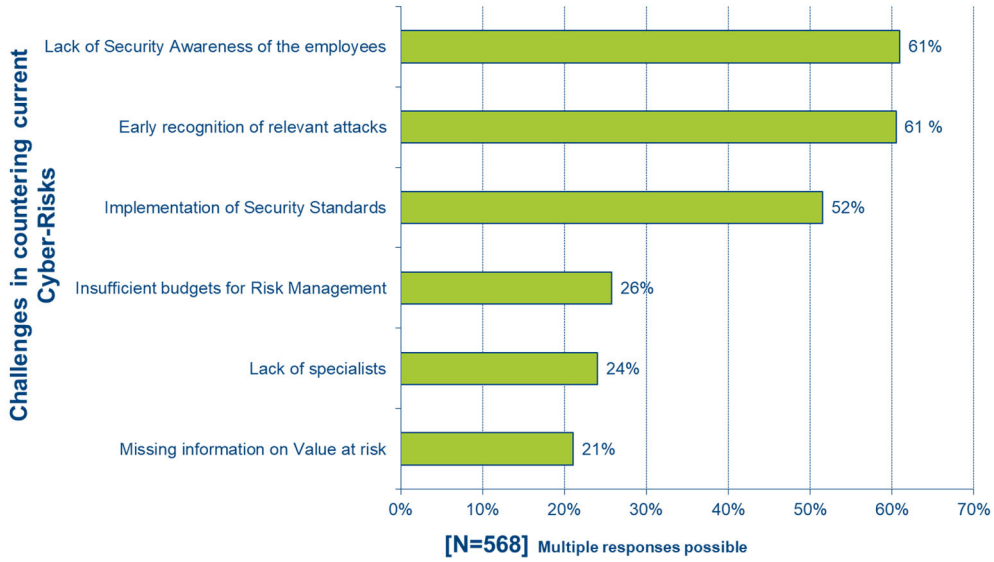

Figure 1: Challenges in countering current Cyber-Risks

In this context, the research also showed that employees are the least aware of information classification, mobile device security, mobile media security, cloud security and phishing/social engineering. Here, the research points out that only between 28 percent and 16 percent of employees have a high or very high level of sensibilisation.

The perception by companies, that the human factor represents a huge challenge, is also reflected in the nature of the vulnerabilities that companies see in the context of Cyber-Security for their businesses. Shown in Figure 2, for example, 51 percent of the companies see untrained personnel as the biggest security gap in this context.

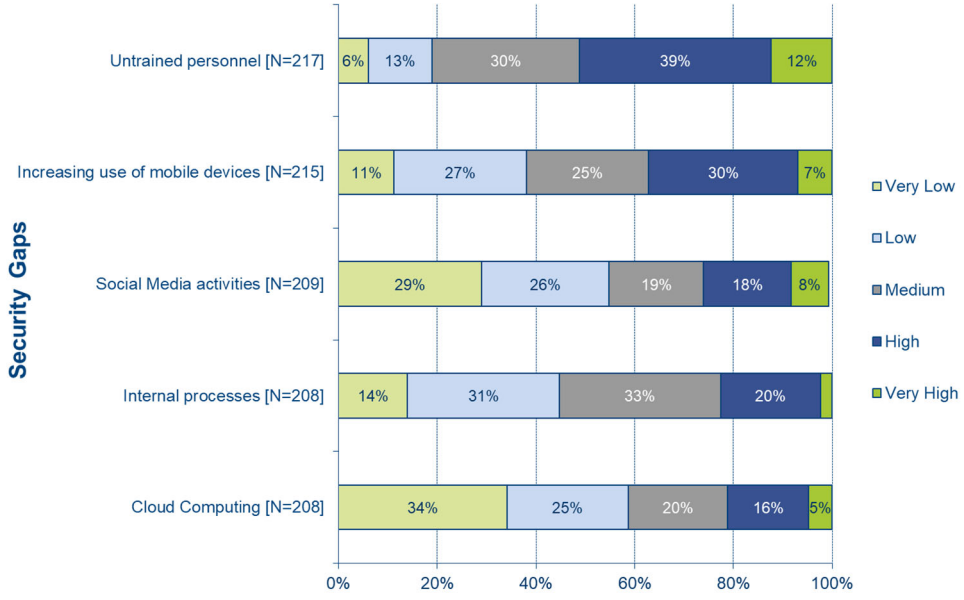

Figure 3: Security gaps

The results clearly illustrate the areas in which there is a need for action in companies. However, the research showed that not sufficient internal and external training is offered in companies. As many as 18 percent of the companies surveyed did not provide internal and 14 percent did not provide external training for their employees.

Furthermore, the test persons were asked for their assessment of the damage potential of the Cyber-Attack. The results show that the test persons are well aware of the potential dangers and nevertheless offer not enough training. In the evaluation, the use of malware was rated as particularly high by 67 percent, computer infection by 48 percent, digital blackmailing by 46 percent and identity theft by 43 percent.

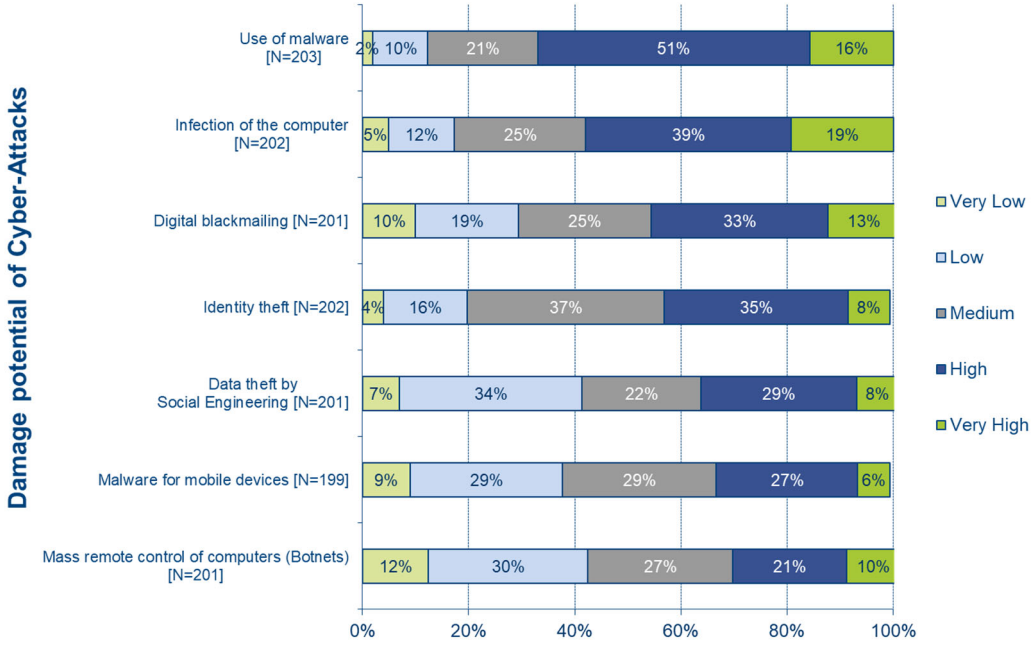

Figure 3: Damage potential of Cyber-Attacks

4 Conclusion

The analyses of this study confirm the assumption that a lack of knowledge and security awareness on the part of employees often represents a weakness and security gap in the company. Often, the human factor is even the biggest problem in combating Cyber-Risks, according to the respondents. A necessary approach for companies in the future will be to sensitize employees to Cybercrime and to greatly expand the training offered by companies. The hypotheses put forward can therefore be confirmed. Furthermore, the research exhibits a list of specific gaps in the knowledge of employees that can be filled by training. Furthermore, the test persons' assessments of the damage potential of Cyber-Attacks in their companies could be shown.

- Bereich (Controlling, Accounting & Audit, Risk & Compliance, Finanzen oder Lehre)

Literature

Bundesamt für Sicherheit in der Informationstechnik (o.J.): Digitale Gesellschaft. Social Engineering – der Mensch als Schwachstelle. https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IT_Sicherheit_am_Arbeitsplatz/SoEng/Social_Engineering_node.html. Abgerufen am 29.05.2020.

Gerdenitsch C./ Korunka C. (2018): Digitale Transformation der Arbeitswelt – Psychologische Erkenntnisse zur Gestaltung von aktuellen und zukünftigen Arbeitswelte. Springer, Berlin.

Klipper S. (2015): Cyber Security – Ein Einblick für Wirtschaftswissenschaftler. Springer Vieweg, Wiesbaden.

KnowBe4 (2019): Security Threats and Trends Report. October 2019.

KPMG (2017): Neues Denken, Neues Handeln - Versicherungen im Zeitalter von Digitalisierung und Cyber Studienteil B: Cyber.

Marsh/Microsoft (2018): By the Numbers: Global Cyber Risk Perception Survey. February 2018.

PWC (2019): Im Visier der Cyber-Gangster - So gefährlich ist die Informationssicherheit im deutschen Mittelstand.

Stirnimann S. (2018): Der Mensch als Risikofaktor bei Wirtschaftskriminalität – Handlungsfähig bei Non-Compliance und Cyberkriminalität. Springer Gabler, Wiesbaden.

Welpe I.M./ Brosi P./ Schwarzmüller T. (2018): Digital Work Design – Die Big Five für Arbeit, Führung und Organisation im digitalen Zeitalter. Campus Verlag, Frankfurt.

Wiederhold, B.K. (2014): The role of Psychology in Enhancing Cybersecurity. Cyberpsychology, Behavior and Social Networking, 17(3): 131-132.