How to Implement AI for Cyber Security in a Corporate Environment – A Process Model

Masterarbeit

zur Erlangung des akademischen Grades „Master of Science (M.Sc.)“ im Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Müller Vorname: Pascal

Geb. am: [redacted] in: [redacted]

Prüfer: Prof. Dr. Breitner

Hannover, den 05.06.2023

Table of Contents

1. Introduction

Cybersecurity Ventures is expecting the costs resulting from global cybercrime to grow by 15 percent annually up to a total of 10.5 trillion USD in 2025 (Morgan 2020).
With the widespread adoption of the home office as a result of the pandemic, companies find themselves at the mercy of additional threats (Struck 2022).
Due to the growing volume and complexity of cyber threats that cyber security analysts have to face, they may feel overwhelmed by the number of threat alerts which are popping up (Aloqaily et al. 2022, p. 4). Based on the current threats, it is essential that companies position themselves for the future in terms of their cyber security.
One way to do this is through the use of artificial intelligence (AI). This term attracted a lot of media attention through the success of ChatGPT, as the AI-based chatbot offers a wide range of possible uses, e.g. the processing of homework for school (Kretschmer 2023).
A study of IBM, which investigated the costs of a data breaches, surveyed 550 companies among other things with statements about their implementation status of AI technology in their cyber security IBM 2022, p. 55). They distinguish between partially and fully implemented. One can see that the share of companies fully implemented AI increased by ten percentage points.

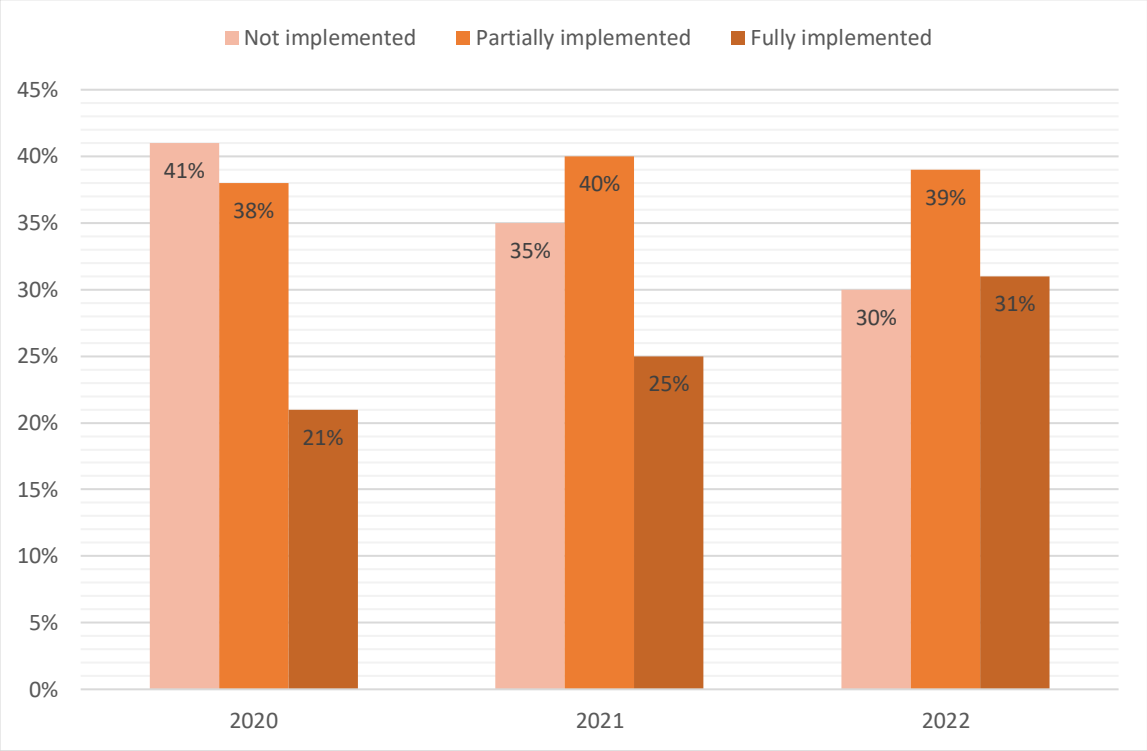

Figure 1: AI technology in cyber security implemented in surveyed companies of IBM study

The last article by Gerlach et al. (2022) created a taxonomy for artificial intelligence (AI) in cyber security. The therein proposed decision tree helps decision makers to find an adequate AI-driven cyber security business model and service. When the right service is found, it has to be implemented in the enterprise. Therefore, this thesis goes further and tries to display the whole implementation process. It should also be looked at, if the implementation of an AI-based solution differs from non-AI-based solutions in cyber security.

Therefore, this thesis addresses a total of three research questions:

RQ1: How can the process of implementing AI be represented in a model?

RQ2: What are critical steps in the implementation process?

RQ3: What are the advantages and disadvantages of AI in Cyber Security?

First, a theoretical insight into the topic is given. For this purpose, the term cyber security is defined and the most common attacks are presented. In the following, an overview of AI is given, in which the sub-areas supervised, unsupervised and deep learning are presented. This is followed by an overview of AI applications in cyber security. Then a look is taken at the literature, how process models are generally presented there. The third chapter deals with the methodologies used for the literature review on the one hand and for the expert interviews on the other hand. To answer the research questions, the literature and the expert interviews are systematically analyzed in chapter four. The interviews are summarized and then analyzed using qualitative content analysis according to Mayring (2014). After that an implementation process model is proposed, also presenting a framework of guiding questions. This is followed by the discussion, which also includes some recommended actions, outlook and some limitations of the methodology. This thesis is then finished with the conclusion.

6. Conclusion

This thesis dealt with the implementation process of AI applications in cyber security in detail, as well as the advantages and disadvantages, which are linked to the technology. Therefore, a literature research and nine expert interviews were conducted.

For the implementation process, an extensive model with eight phases containing separate steps could be proposed combined with a framework of twenty-six guiding questions. The eight phases of implementation are: 1. Problem statement, 2. Requirement Analysis, 3. Searching for a solution, 4. Decision phase / product selection, 5. Learning Phase, 6. Testing phase, 7. Evaluation phase and 8. Go Live. Due to the experts, it became clear, that companies will not develop AI applications on their own and instead rely on already existing products on the market.

Special attention is needed for the fourth phase, as a lot of regulatory questions with regard to data privacy matters are discussed there, and the sixth phase, whereby these can be classified as the most critical steps in the implementation. Surprisingly, these are not technical issues.

The learning phase is an important distinction compared to non-AI based solutions in the cyber security area. The other phases might be commonplace for companies.

All in all, AI offers significant advantages for companies in their cyber security landscape. These include that it facilitates the work of SOC, is able to analyze high-volume data, provides quicker detections and responses and is able to identify anomalies.

The biggest disadvantages were identified in both research sources. One is the possible manipulation of the AI, also called adversarial attacks. The other disadvantage is that the AI may still have misclassification leading to false positives. More questionable for the experts were the explainability of the AI, questioning the trustworthiness of the solutions.

To sum up, one can say that AI will become implemented by more and more companies in the future as a result of the numerous advantages the technology offers. This will be accelerated due to fast changing threat landscape and also due to suffering a lack of skilled workers.

Explainable AI is also explored more and more by researchers. If this moves into more AI applications on the market, it will help the overcome the concerns of the practitioners. Moreover, due to the growing relevance some regulations for data privacy issues regarding the AI models might be expected in the future.