Game-Based Identification of Potential Malicious Insider Threats

Manfred Hofmeier
Universität der Bundeswehr München
manfred.hofmeier@unibw.de

Ulrike Lechner
Universität der Bundeswehr München
ulrike.lechner@unibw.de

Abstract

Malicious insider threats pose a challenge: A large dark field must be assumed, insider attacks are difficult to detect, investigate, or defend against, and the potential for damage is high. At the same time, there is only limited empirical knowledge about malicious insider threats. This study examines insider threats in inter-organizational contexts using a game-based approach to address this gap and a narrow view restricted to single organizations. Using the design science paradigm, a serious game was developed in a tabletop format that explicitly includes relevant external actors: "Operation Digital Butterfly." However, the serious game is not only a result, for example, as an instrument to increase awareness or highlight vulnerabilities, but primarily serves as a tool to identify roles and attack scenarios as well as countermeasures. In this way, knowledge about malicious insider threats can be extended. This paper describes the development and validation of the game and underlines the potential of creative game-based approaches for security research.

Introduction

The European Union Agency for Cybersecurity (ENISA) defines an insider threat as "an action that may result in an incident, performed by someone or a group of people affiliated with or working for the potential victim" (ENISA, 2020). Insider threats can also be distinguished as accidental or malicious (intentional). In this work, we take a close look at malicious insider threats. These represent a particular challenge not only for actual protection but also for research, as it is estimated there is a high number of unreported cases. Organizations tend not to disclose information on malicious insider threats (e.g., not to lose the trust of customers or partners), and typically, only cases with news value become public. Thus, the cases examined in the research do not necessarily represent the current insider threat landscape. Information systems literature such as the UMISPC (Moody et al., 2018) generally addresses insider threats, primarily accidental insider threats, while the malicious type is usually not considered.

Malicious insider threats pose a challenge: A large dark field must be assumed, insider attacks are difficult to detect, investigate, or defend against, and the potential for damage is high. At the same time, there is only limited empirical knowledge about malicious insider threats. Most knowledge about malicious insider threats is based on the 2005 “Insider Threat Study” (Keeney et al., 2005).

To address this gap and a limited view restricted to single organizations, creative approaches that generate fictional yet plausible and realistic attack scenarios can be helpful. This study examines insider threats in inter-organizational contexts using a game-based approach. In contrast to other creative methods, game-based approaches have the advantage that the participants' motivation to create good scenarios is particularly encouraged. Using the design science paradigm, a serious game was developed in a tabletop

format that explicitly includes relevant external actors: "Operation Digital Butterfly." However, the serious game is not only a result, for example, as an instrument to increase awareness or highlight vulnerabilities, but primarily serves as a tool to identify roles and attack scenarios and countermeasures. In this way, knowledge about malicious insider threats can be extended.

This article describes the development and validation of the game as an instrument to expand knowledge of malicious insider threats. It also underlines the potential of creative game-based approaches for security research.

The Game: Operation Digital Butterfly

Figure 1: Game material with gameboard and card deck

"Operation Digital Butterfly" is a tabletop game (playable face-to-face and virtual) with an exchangeable game board, game cards, and guidelines (Figure 1). In the game, three to four teams with two to four players per team compete against each other by developing insider threat actor roles, attacks, and countermeasures. The game has two main rounds: After a briefing on the game and the rules and forming of the teams, each team develops motivation, attack, and a security measure in a creative process. Each team presents its results to the others. The second main round is about the rating: each team rates the roles and attacks of the other teams and gives the rating. This determines the winning team.

The game board describes the environment wherein the insider threats take place. To date, the game has been played with three different game boards: slaughterhouse and cutting plant, logistics hub with warehouse, and travel management in a public authority.

Each team develops an insider role, an attack, and a security measure using a card deck. The cards structure the discussion in the teams and the presentation of results. The teams are instructed to answer four questions on the role card to guide the creative design of attack measures:

- Who is the insider (position in the organization)?
- What does the insider want to achieve (intention)?
- Why does the insider want that (motivation)?
- How does the insider justify this to themself (neutralization)?

The attack is developed using the scene cards. The filmmaking metaphor is used to make development and descriptions of attacks easy – also for players not used to formal notations. A threat is a sequence of scenes. This way, each team can tell their fictional insider attack by using a sequence of scenes.

These role characteristics help to create a plausible insider role that has the potential to give hints about factors that might drive or hamper insider threat actors. In this way, they allow a detailed analysis of the game results regarding potential countermeasures. In particular, justifications of attacks – in the sense of the neutralization theory (Sykes & Matza, 1957) – have shown to be useful.

The attack is developed using the scene cards. The filmmaking metaphor simplifies descriptions of attacks – also for players not used to formal notations. A threat is a sequence of scenes. This way, each team can tell their fictional insider attack utilizing a sequence of scenes.

Each team fills out a security measure card to make the game more fun and gain knowledge about countermeasures to insider attacks. Teams are instructed to anticipate possible attacks from the other teams (the roles are known) and develop an adequate countermeasure. This measure is valid for the attack plans of all teams and is then taken into account when rating the attacks.

Table 1: Serious game iterations

Date	Game board	Players	Attack Scenarios
May 2020	Meat Production	6	2
Jul 2020	Meat Production	15	4
Oct 2020	Logistics Hub	7	3
Nov 2020	Logistics Hub	15	4
Mar 2021	Logistics Hub	12	3
Sep 2021	Travel Management	12	3
Feb 2022	Travel Management	10	6
Feb 2022	Travel Management	9	6
Feb 2022	Travel Management	9	6
Jul 2022	Logistics Hub	13	3

The winning team is determined through a rating system, in which the teams rate each other by three given categories: (1) Plausibility of role, (2) plausibility of the attack story, and (3) damage potential. Each team can give up to ten points for each category to the other teams. Note that the most essential categories for later analyses are the "plausibility" categories. They ensure that the developed attacks and roles are – to some extent – realistic and fit the profile of the role. The "damage potential" category makes the teams more likely to develop attacks that cause significant damage and, therefore, are of particular interest in security research.

The game is also accompanied by a closing discussion, which focuses on possible countermeasures to the attack scenarios developed in the game. The main output of the game is a collection of plausible insider roles and attacks.

Game Development Methodology – Design Science Research

The development of "Operation Digital Butterfly" follows the design science paradigm according to Alan Hevner (Hevner et al., 2004; Hevner, 2007). In ten game performances from May 2020 to July 2022 with participants from research institutions, companies, and public authorities, 40 roles with corresponding attack scenarios were developed and tested for plausibility (Table 1). The teams developing this data were composed in such a way that the expertise was as mixed as possible, while in each game iteration emphasis was placed on a mix of affiliations and professional roles (and thus real-world insights and competences). The game participants were acquired through partners from the project network, while these partners selected personnel for the game with regard to broad competence coverage.

The "Framework for Evaluation in Design Science" (FEDS) (Venable, Pries-Heje & Baskerville, 2016) describes various evaluation strategies for the validation of artifacts. It distinguishes between the dimensions of the evaluation's functional objective and the evaluation study's paradigm. The spectrum of the first dimension ranges from formative, i.e., continuous feedback and improvement during the development process, to summative, i.e., the final assessment of the overall performance or the end product. The second dimension ranges from an artificial to a naturalistic evaluation, whereby an artificial assessment takes place under laboratory conditions and a naturalistic evaluation in the field. The various evaluation strategies differ in the path they take with each evaluation in the course of the research within these

dimensions. The "Human Risk & Effectiveness" strategy, which was chosen for this study, is beneficial when:

- the predominant design risk is social or user-related,
- and/or it is relatively easy to evaluate with real users in a real-world context,
- and/or it is a critical goal of the evaluation to rigorously ensure that the benefits of the artifact persist in the long term under real-world conditions.

This evaluation strategy emphasizes formative evaluations at the beginning of the development process, possibly with artificial, formative evaluations that quickly transition into more naturalistic formative evaluations. Towards the end of this strategy, summative evaluation is increasingly used, with a focus on rigorous evaluation of the effectiveness of the artifact, i.e., that the artifact is still useful when used in real-world situations in the long term, despite the complications arising from the human and social difficulties of adaptation and use. (Venable et al., 2016)

The following sections describe the requirements for the artifact (serious game), the implementation of the Design Science Research Cycles according to Hevner (2007), and the implementation of the associated guidelines defined by Hevner et al. (2004).

Requirements

The requirements for the artifact are defined by the research interest and the underlying conditions of the research, for example, by the stakeholders in the respective research projects. One of the objectives of development is to ensure that the game ultimately meets at least the following requirements:

- The game should motivate and support the players in developing plausible roles and attacks by insiders through a creative process.
- The game should be playable by employees in organizations from all departments (with and without a technical background or knowledge of information security).
- The game should be able to improve game participants' awareness of insider threats.
- The game should fulfill general quality criteria for serious games, such as fun, enabling players to apply what they have learned in real life, and adaptability to different learning situations (Michael & Chen, 2006).

Application of the Design Science Research Cycles

This section explains the game's development according to the Design Science Research Cycles (Hevner, 2007).

The *Relevance Cycle* focuses on the requirements for the game. As part of the NutriSafe project, the requirements were defined in particular by the Bavarian Health and Food Safety Authority (LGL) and industry representatives from the food and logistics sectors. As part of the LIONS project, the requirements were defined in particular by the Federal Office of Bundeswehr Infrastructure, Environmental Protection and Services (BAIUDBw). The requirements to be met by the game were determined in dialog with these partners. Meeting the requirements is achieved through an iterative game testing and validation approach.

In the *Rigor Cycle*, the game is compared with well-known serious games (an overview of several games in this area can be found in Zhang-Kennedy & Chiasson (2020)). In particular, the comparison with games that deal with the topic of insider threats – such as "The Wolf of SUTD" (Harilal et al., 2018), "XL- CITR" (Andre et al., 2011), "Guess Who?" (Gupta et al., 2020), or "Agent Surefire" (Alhadeff, 2012) – is relevant. Also, literature on insider threats is considered, as the game design aims to generate knowledge about insider threats. The plausibility of the results and the innovation potential are analyzed by comparing them with literature on insider threats – including scientific literature and known case studies. The scientific literature on insider threats also forms the basis for the initial game development. On the other hand, the game results, the analyses they made possible, and the results generated from them also contribute to the state of knowledge.

The *Design Cycle* is characterized by an iterative approach: The game is evaluated after each run using various methods (see section "Artifact validation"). Based on the evaluation results, adjustments are made

after each game run. The design process used for the game material and, in particular, for the game board is as follows:

1. desk research on the scenario
2. development of a rough draft based on desk research
3. refinement of the design with an expert from the field
4. development of a first version
5. validation with an expert
6. refinement
7. test run with validation
8. fine-tuning

We carried out a total of eleven iterations (see Table 1).

Application of the Design Science Research Guidelines

Hevner formulates research guidelines for successfully applying the design science paradigm and achieving good results (Hevner et al., 2004). Compliance with these guidelines is described below.

Design as an artifact: Design-oriented research should produce a usable artifact in the form of a construct, a model, a method, or a realization. In this research project, a serious game was developed as a functional artifact in the form of game materials and a game manual.

Problem Relevance: Design-oriented research aims to develop solutions for meaningful and relevant problems in practice. "Operation Digital Butterfly pursues several objectives that address pertinent problems of insider threat research and defense. On the one hand, it aims to raise awareness of malicious insider threats and the vulnerabilities of supply chains and improve attitudes towards information security guidelines. In addition, the game is intended to expand knowledge about insider threats by serving as a tool for generating plausible threat scenarios.

Design Evaluation: The usefulness, quality, and effectiveness of a design artifact must be rigorously demonstrated through well-conducted evaluation methods. The serious game developed in this research was evaluated using various methods: entry and exit surveys, structured participatory observations, and group discussions. Further details on game validation can be found in the game validation section.

Research Contributions: Effective design-oriented research must provide clear and verifiable contributions in the areas of design artifacts, design principles, or design methods. The contributions of the research activities are the artifact (game) itself, the understanding of how the game can be used, the data collected in the game (collection of roles and attacks), and the results of the data analysis (such as causes, risk factors, countermeasures, typology). In addition, knowledge was gained about the game's design.

Research Rigor: Design-oriented research relies on applying rigorous methods in both the development and evaluation of the design artifact. The serious game was developed iteratively. In each iteration, the game concept and the game's effects on the game participants were evaluated using scientific methods. In addition, the results were compared with existing knowledge and literature.

Design as a Search Process: The search for an effective artifact requires using available means to achieve the desired goals while satisfying the constraints of the problem domain. The development process of "Operation Digital Butterfly" is iterative and includes validation to improve the game with each implementation and evaluation.

Communication of research: Design-oriented research must be presented effectively for technology- and management-oriented target groups. The game "Operation Digital Butterfly" has been published as game materials and guidelines under an open-source license (Hofmeier, 2021). Various aspects of research related to the game have also been published, including, for example, interim results from the validation (Hofmeier & Lechner, 2021) and the content analyses of the game results (Hofmeier et al., 2023a; Hofmeier et al., 2023b). This paper also contributes to this criterium.

Artifact validation

The development of "Operation Digital Butterfly" is characterized by continuous validation in accordance with design science principles. The validation methods accompanying the game are quantitative entry and exit surveys, participatory observations, and group discussions. These are supplemented by a parallel interview study and subsequent content analyses, which primarily serve to validate the game results.

Overall, the validation methods serve to address the following questions:

1. Is the game design functional, and does it meet the requirements?
2. Does the game achieve the desired learning effects?
3. Is the game able to identify plausible and realistic threat scenarios?
4. Are the identified threat scenarios usable and, therefore, helpful for research and practice?

The individual validation methods used are presented in the following sections.

Table 2: Game-accompanying methods by iteration

Iteration	Participatory observation (game instructor)	Participatory observation (team instructors)	Group discussion with the players	Group discussion with the team instructors	Entry- and exit surveys
1: April 2019	x		x		
2: May 2020	x		x		
3: Jul 2020		x		x	x
4: Oct 2020	x		x		
5: Nov 2020		x		x	x
6: Mar 2021	x			x	
7: Sep 2021		x		x	x
8: Feb 2022		x		x	x
9: Feb 2022		x		x	x
10: Feb 2022		x		x	x
11: Jul 2022		x		x	x

When game sessions were accompanied by *entry and exit surveys*, the participants received the link to the entry questionnaire by e-mail with the information on participation in the game, usually a few days (maximum seven days) before the game was played. The link to the exit survey was sent to the participants a few days (one to three days) after the game was played as part of a thank-you e-mail. Participation in the surveys was voluntary, and it was also possible to participate in the game without taking part in the survey. The primary goal of the surveys is the validation of the game itself as well as possible learning effects through participation in the game, which represents the secondary goal of the game. The questionnaires changed throughout the game iterations.

Awareness was measured using, among other things, assessment questions on the probability and damage potential of insider threats and the subjective perception of an increase in knowledge. Two subscales from the Security Behavior Intentions Scale (SeBIS) (Egelman & Peer, 2015) were also used: Device Securement and Proactive Awareness. The Device Securement scale relates to securing devices and the workplace and was selected because these items are particularly relevant to attacks from within the organization. Proactive Awareness is used as a proxy for general information security awareness. It is intended to show whether there is also an effect on public security awareness beyond the scope of insider threats.

To measure a change in attitude towards information security policies, two scales were selected that relate to information security policy compliance: Information Security Polity Intentions (ISP Intentions) according to Siponen, Pahnila, and Mahmood (2010) and Information Security Policy Attitude (ISP Attitude) according to Bulgurcu, Cavusoglu and Benbasat (2010). The ISP Intentions scale primarily

examines the intention to comply with policies, recommend compliance to others, and support others in complying. The ISP Attitude Scale, on the other hand, measures the attitude towards the guidelines.

To supplement the results from the surveys, the game sessions were accompanied by *participatory observations*. The smaller-scale sessions, primarily used to test a new playing field (mostly internally), were accompanied by unstructured observation by the game instructor. The other sessions were accompanied by structured participatory observations by the team advisers (see Table 2). A structured observation protocol was used for this purpose. The structured observations by the team supervisors primarily took place in the phases in which the teams were separated from each other: the work phase, i.e. during the development of the role, attack path, and security measure (game phase), and once during the decision on the ratings of the other teams (evaluation phase). The topics of the observations included Comprehensibility of the game material and the scoring system, comprehensibility of the evaluation categories, suitability of the time limits, fun, motivation of the game participants, and fairness of the game.

The *group discussions* complement the participant observations. They usually occur directly after the games to ensure better recall due to the temporal proximity. The game instructor led the discussion. In small-scale sessions, all players participated in the discussion; in the other sessions, the team advisors took part. Just like the participant observations, the group discussions are also structured and follow a discussion guide. The group discussions cover the same topics as the participant observations. The group discussions aim to supplement the observations and to ensure an objective interpretation of the observation results.

Expert *interviews* were conducted as a basis for the development and to support the analysis of the game results. The interviews were guided, and the experts were information security practitioners. The topics of the interviews were the experiences of those responsible for information security with insider threats and the measures implemented to prevent and mitigate insider threats. The comparison of the game results with the interview results is intended to ensure the external validity of the threat scenarios obtained in the game.

Qualitative content analyses are conducted as representatives of possible analyses that can gain further insights from the results obtained through the game. This validates the usability and value of the game results – i.e., the ability of the game to expand knowledge about malicious insider threats.

Validation results

The results of the game validation are presented below. As the entire results would take up too much space, only the most relevant ones are described.

As mentioned, the game should fulfill the general quality criteria of a serious game. The game concept and materials were assessed and refined with each design iteration based on the evaluation results. According to the observations and group discussions, the game concept worked well from the start. The results of the exit surveys confirm this. They show that the average ratings regarding the comprehensibility of the game, rules, and scoring system are almost consistently high and that the game is also fun.

Learning effects validation results

For the game to serve as a research tool and benefit the game participants, it should have a positive effect on their knowledge and security awareness.

In the case of device securement (SeBIS), i.e., the protection of IT devices by the user, there are no apparent changes after participation in the game. Although there is a positive shift in three of the four items, the shift is harmful to the configuration of the automatic screen lock, which is also particularly relevant to insider threats. For proactive awareness (SeBIS), on the other hand, there is a shift in favor of awareness in all items after the game, even though the items are not directly related to insider threats.

The intentions regarding information security policies (ISP Intentions) are higher in all three items after the game than before. The most obvious difference is in those items that affect other individuals: the intention to recommend others to comply with the policies and help others to comply with the policies. The changes are ambiguous for attitudes toward information security policies (ISP Attitudes). While compliance with the policies is perceived to be more important and useful to the individual after the game, it is also less beneficial. When it comes to the perception of necessity, the result needs to be clarified. Overall, game

participation still has an effect on the attitude toward information security policies. It can be assumed that by participating in the game, people become more aware of the importance of policies and their relationship to individuals, raising awareness of the control these policies exert over their person.

Game output validation results

The validation of the game results is primarily concerned with the following questions: (1) are the game results coherent and plausible (internal validity), (2) do they have equivalents in practice (external validity), and (3) are they useful for insider threat research? Internal validity is primarily investigated using the methods accompanying the game, while external validity and usefulness are investigated using content analysis methods.

The main results of the game are a collection of threat scenarios with roles and attacks. First, the teams' ratings assess the plausibility of the attack scenarios (Table 3). Each team is evaluated by the other teams when determining the winner, including in the "plausibility" category. In the executions from the eighth iteration onwards, this category was broken down into the categories "plausibility of the role" and "plausibility of the story" (of the attack).

Table 3: Average plausibility ratings given by the teams

Iteration	∅ Plausibility ratings (role & attack)											
2: May 2020	4,0		2,0									
3: Jul 2020	6,0		2,66		4,33		7,33					
4: Oct 2020	4,5		3,5		7,5							
5: Nov 2020	4,66		6,0		4,33		5,33					
6: Mar 2021	3,5		7,5		4,5							
7: Sep 2021	8,0		4,5		3,5							
	∅ Role plausibility ratings						∅ Attack plausibility ratings					
8: Feb 2022	8,0	9,5	9,0	8,5	8,0	10,0	7,5	4,5	4,5	4,5	3,0	2,0
9: Feb 2022	7,5	7,5	8,0	6,0	6,05	7,5	5,0	4,5	4,5	6,5	7,0	4,5
10: Feb 2022	9,5	8,5	10,0	7,0	9,5	8,0	5,5	6,5	4,0	4,0	6,5	5,0
11: Jul 2022	6,0	8,5	9,0				6,0	6,5	8,5			

It can be seen that most scenarios have at least medium plausibility values on average. It is also evident that the range of plausibility ratings is broad and ranges from low to high plausibility. Not every attack developed is plausible in the opinion of the competing teams, but most of them have at least medium plausibility values on average. After breaking down the plausibility of the role and the plausibility of the attack, the roles are generally considered to be very plausible and that it tends to be the attacks for which the plausibility values show a wide range. It should be noted that it was expressed in the discussions that plausibility ratings were often lowered due to the perception of low probabilities. Thus, attacks that were perceived as unlikely received lower plausibility ratings, which does not mean that they are inconsistent or unrealistic. Also, plausibility ratings were often downgraded based on a single aspect of the attack path or because of a security measure defined by another team. The plausibility of the attack scenarios was also part of the exit surveys. These confirm the above results.

Some of the attack scenarios developed in the game have parallels to known incidents (from the interviews and in the literature). However, no direct equivalent is known for some scenarios. Concluding external validity from this needs to be revised. As mentioned before, the search for incidents is subject to a dark field and distortion, so there may be correspondences that are not visible. On the other hand, one of the game's objectives is to identify threats that are not yet known. The evaluation of the external validity of the game results in this way, therefore, turns out to be limited.

The qualitative content analyses demonstrate the potential of "Operation Digital Butterfly" as a research instrument to generate usable results in the form of usable threat scenarios that can expand knowledge about malicious insider threats. Analysis of the game results allowed the development of a new typology

that goes beyond the existing typologies. It features eleven multidimensional types that include motivational, psychosocial, and attack-related properties: disgruntled employee/leaver, data transfer to competition, industry espionage, state espionage, taking advantage of privileges for personal gain, unauthorized inspection of personal data, intellectual property sale, whistleblowers, politically motivated sabotage, extortion, and illegal use of IT infrastructure. The typology was published at the Bled eConference (Hofmeier et al., 2023a). Also, another content analysis identified risk factors at the technology, organizational, human, and infrastructure levels. These were published at the AMCIS 2023 conference (Hofmeier et al., 2023b) and presented in a lecture at the 10th International Symposium on New Technologies "Digital Tools - Analog Crimes: And the Police?" in Germany (Hofmeier, 2023).

Discussion

This work examines malicious insider threats in inter-organizational contexts with the help of a game-based approach. For this purpose, a serious game was developed in eleven game iterations with validation, by the design science paradigm: "Operation Digital Butterfly". The serious game is not only a result, for example, as an instrument for increasing awareness or highlighting vulnerabilities, but it also serves as a tool for identifying attack scenarios and countermeasures. The game has been validated in terms of game design with quality criteria, learning effect and suitability as a survey instrument and is made available to the public on GitHub (Hofmeier, 2021). The game is playable and fun, the process and rules are understandable. In terms of the educational impact of the game, it has been shown that participants' knowledge has increased, and changes in attitudes toward information security policies are measurable. The game's primary objective, to generate plausible but realistic threat scenarios as a creative method, was also achieved. A total of 40 usable scenarios with roles and attacks were developed in eleven sessions. The content analyses showed that the scenarios are functional and can expand knowledge about malicious insider threats.

Limitations exist with regard to the effect of social acceptance as well as self-selection bias. The risk of social acceptance bias is based on participant acquisition from the project's and institute's networks, which can lead to social proximity. On the other hand, there were indeed games conducted in external organizations, although there was no discernible difference in fun and motivation. A possible self-selection effect is based on the fact that most participants volunteered to take part themselves. This type of self-selection could have a positive effect on both enjoyment and motivation, which could indirectly affect learning success. This can be countered by the fact that in some cases the participants were asked to take part by their supervisors and no difference in enjoyment and motivation was observed. The extent to which personal initiative to participate and interest in the topic influence the enjoyment and motivation of the game and the extent to which this in turn can indirectly influence learning success could be the subject of further research.

Overall, the artifact "Operation Digital Butterfly" and the results of the research provide a basis not only for science but also for practice. Scientific research is provided with a basis that facilitates the further investigation of threat scenarios and opens up the possibility of other (e.g. interdisciplinary) analyses. The results are also relevant for practice. They enable a better awareness and understanding of malicious insider threats and their diversity and a better adaptation of security measures to the diversity of threats. The typology and risk factors, in particular, are a basis for the evaluation and development of security concepts and risk analyses.

Acknowledgements

This work originates in the LIONS research project. LIONS is funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr which we gratefully acknowledge. dtec.bw is funded by the European Union – NextGenerationEU.

References

Alhadeff, E. (2012). Converting Cybersecurity Practice into Engaging Serious Games. *Serious Game Market*. https://www.seriousgamemarket.com/2012/ 02/converting-cybersecurity-practice-into.html

Andre, T. S., Fidopiastis, C. M., Ripley, T. R., Oskorus, A. L., Meyer, R. E. & Snyder, R. A. (2011). Augmented cognition methods for evaluating serious game based insider cyber threat detection training. *International Conference on Foundations of Augmented Cognition, 395-403*.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34 (3), 523–548*.

Egelman, S. & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (SeBIS). *Conference on Human Factors in Computing Systems - Proceedings, 2873–2882*. doi: 10.1145/2702123.2702249

ENISA. (2020). ENISA Threat Landscape 2020 - Insider Threat. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-insider-threat

Gupta, S., Gupta, M. P., Chaturvedi, M., Vilkhu, M. S., Kulshrestha, S., Gaurav, D. & Mittal, A. (2020). Guess Who? - A Serious Game for Cybersecurity Professionals. *Games and Learning Alliance 9th International Conference, 421-427*.

Harilal, A., Toffalini, F., Homoliak, I., Castellanos, J., Guarnizo, J., Mondal, S. & Ochoa, M. (2018). The Wolf of SUTD (TWOS): A Dataset of Malicious Insider Threat Behavior Based on a Gamified Competition. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 9, 54-85*.

Hevner, A. R., March, S. T., Park, J. & Ram, S. (2004). Design Science in Information Systems Research. MIS Quarterly, 28, 75-105.

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. Scandinavian Journal of Information Systems, 19, 87-92.

Hofmeier, M. (2021). Operation Digital Butterfly. https://github.com/LIONS-DLT/operation-digital-butterfly

Hofmeier, M. & Lechner, U. (2021). Operation Digital Ant - A Serious Game Approach to Collect Insider Threat Scenarios and Raise Awareness. *European Interdisciplinary Cybersecurity Conference (EICC). New York: ACM*. doi: 10.1145/3487405.3487655

Hofmeier, M. (2023). Operation Digital Butterfly – Ein spielbasierter Ansatz zur Identifikation und Analyse von Bedrohungen durch „Malicious Insiders“. *10. Internationalen Symposium Neue Technologien “Digitale Tools - Analoge Verbrechen: Und die Polizei?”. Stuttgart*.

Hofmeier, M., Haunschild, I. & Lechner, U. (2023a). Malicious Insider Threat Types – An Empirical Analysis. *36th Bled eConference Economy and Society: The Balancing Act for Digital Innovation in Times of Instability*.

Hofmeier, M., Seidenfad, K., Rieb, A. & Lechner, U. (2023b). Risk Factors for Malicious Insider Threats – An Analysis of Attack. *In Twenty-ninth Americas Conference on Information Systems (AMCIS)*.

Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T. & Rogers, S. (2005). Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. Carnegie Mellon University.

Michael, D. & Chen, S. (2006). Serious Games: Games that Educate, Train, and Inform. Thomson Course Technology PTR.

Moody, G. D., Siponen, M. & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly, 42, 285-311*.

Siponen, M., Pahnila, S. & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *IEEE Computer Society, 43 (2), 64–71*.

Sykes, G. M. & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. American *Sociological Review, 22 (6), 664–670*.

Venable, J., Pries-Heje, J. & Baskerville, R. (2016). FEDS: A Framework for Evaluation in Design Science Research. *European Journal of Information Systems, 25 (1), 77– 89*.

Zhang-Kennedy, L. & Chiasson, S. (2020). A Systematic Review of Multimedia Tools for Cybersecurity. *ACM Computing Surveys, 54, 1-39*.