Operation Digital Ant

A Serious Game Approach to Collect Insider Threat Scenarios and Raise Awareness

Manfred Hofmeier
Institute for Protection and Dependability, Universität der Bundeswehr München, Neubiberg, Germany
manfred.hofmeier@unibw.de

Ulrike Lechner
Institute for Protection and Dependability, Universität der Bundeswehr München, Neubiberg, Germany
ulrike.lechner@unibw

ABSTRACT

Insiders pose severe threats to the supply chain, the security of infrastructures, and the safety of products and services. "Operation Digital Ant" is a tabletop game that explores insider threats in the food supply chain. Three to four teams compete against each other in developing malicious insider roles and attacks. The game can produce plausible and consistent insider threat roles and attacks as a basis for further analyses. “Operation Digital Ant” also raises awareness for insider threats. This article describes the serious game “Operation Digital Ant” with game material, the game development process – following the Design Science paradigm – and the validation methods and results. We released the game Operation Digital Ant with game boards, game cards, and guidelines under a Creative Commons license.

CCS CONCEPTS

• **Security and privacy**; • **Human and societal aspects of security and privacy**; • **Social aspects of security and privacy**; • **General and reference**; • **Document types**; • **General conference proceedings**;

KEYWORDS

Serious Game, Insider Threat, Attacks

ACM Reference Format:
Manfred Hofmeier and Ulrike Lechner. 2021. Operation Digital Ant: A Serious Game Approach to Collect Insider Threat Scenarios and Raise Awareness. In *European Interdisciplinary Cybersecurity Conference (EICC), November 10, 11, 2021, Virtual Event, Romania.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3487405.3487655

1 INTRODUCTION

"Insider threat to food security and safety" is the topic of the serious game "Operation Digital Ant". The context of this game design is the research project NutriSafe which develops Blockchain technology to increase the resilience of food supply chains [1]. Knowledge about insider threats aids technology design to make the supply chain with its information flows more resilient. Food safety and IT security specialists seem to be disjoint communities. The game makes the abstract, clandestine world of insider threats tangible for both food safety and IT security specialists.

"An insider threat is an action that may result in an incident, performed by someone or a group of people affiliated with or working for the potential victim" [2]. In the ENISA Threat Landscape Report 2020, the insider threat is on 9th place among the Top 15 cyber threats [2]. The report distinguishes five types of insider threats by rationales and objectives [2]: *careless workers* mishandling data, violating policies or installing unauthorized applications; *inside agents* who steal information on behalf of outsiders; *disgruntled employees* who seek to harm their organization; *malicious insiders* who use existing privileges to steal information for personal gain; *third-parties* who compromise security through intelligence, misuse or malicious access to or use of an asset. Capelli et al. distinguish three types of insider threats by objectives in the “CERT Guide to Insider Threats”: theft (e.g. of intellectual property or other data), sabotage (malicious manipulation of data or processes or causing reputational damage) and fraud (e.g. stealing financial goods) [3].

Our focus is on malicious insider threats, meaning actions done by insiders on purpose, i.e., being self-motivated, bribed, or blackmailed. From former research such as the Insider Threat Study is known, that most malicious insider actions are triggered by negative work-related events and the most reported motive is revenge [4].

Investigating the motives behind these kind of actions, the German Insurance Association (GDV) defines four perpetrator types [5]: The *crisis perpetrator* who is triggered by crisis events in private or professional life that threaten status and lifestyle, the *inconspicuous* who takes advantage of an emerging opportunity, the *perpetrator with economic-criminological disorder* who actively seeks or creates opportunities to commit a crime, and the *dependent* who is usually hierarchically subordinate to a main offender or owes the main offender a favor and fears repression in case of refusal to cooperate.

There are several more studies about sociological and psychological aspects of insider threats, such as by Greitzer et al. [6] or Shaw et al. [7]. A brief overview of studies in this field can be found in [8]. However, since insider threats are very diverse and context-specific elements may also have an impact in addition to general sociological and psychological markers, it makes sense to consider insider threats in the domain and industry-specific contexts. However, such incidents are difficult to investigate in larger numbers because they are typically not labeled "insider threats" and are therefore hard to find. Also, organizations tend to be reluctant to disclose such incidents. Criminal investigation departments also assume that there are many unreported cases here [5]. Therefore, creative approaches such as serious games can help to gain insights into possible insider threats.

EICC, November 10, 11, 2021, Virtual Event, Romania

ACM ISBN 978-1-4503-9049-1/21/11.
https://doi.org/10.1145/3487405.3487655

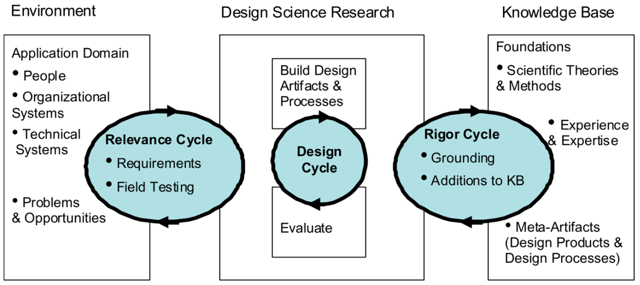

Figure 1: Design Science Research Cycles [10]

This paper presents a serious game that generates fictitious insider threat actor roles and attacks as a game-based data collection instrument. In addition to technical factors, also organizational, psychological, and social factors are taken into account. The game is designed to increase awareness of insider threats. The increase in awareness is the immediate benefit for participants and organizations. The food sector with its critical supply chains and varying level of digitalization was perceived as a promising starting point for the development of such a game.

2 SERIOUS GAME DEVELOPMENT

The development of the game follows the Design Science paradigm, according to Hevner [9, 10], as this approach assures that the game fulfills the requirements - validated at a scientific level. Examples of main requirements are:

- The game must motivate and support players to generate descriptions of plausible roles and attacks of insider threat actors in a creative process.
- The game must be playable by all kinds of employees (with and without technical or security background).
- The game must be able to raise awareness about insider threats within the game participants.
- The game should be about a realistic scenario from the food industry to illustrate vulnerabilities and attack vectors concerning IT security
- The game must meet the general quality criteria of a serious game, such as fun, the ability of the game to make the attendees able to apply the learned knowledge in the real world, and adaptability to various learning situations [11].

2.1 Development cycles

The following section explains the game's development according to the Design Science Research Cycles by Hevner [10] (Figure 1).

2.1.1 Relevance cycle. In the Relevance Cycle, the game's requirements from the NutriSafe project consortium play a significant role. This research consortium includes public authorities as, e.g., the Bavarian State Office for Health and Food Safety (LGL), IT and IT security experts, logistics service providers, and representatives from the food industry [1]. In dialogue with these partners was defined, which requirements the game should fulfill. Matching the requirements is achieved by an iterative approach and validation.

2.1.2 Rigor cycle. In the Rigor Cycle, the game is compared with known serious games (an overview of serious games in this field can be found in [12]). In particular the comparison of games tackling the insider threat domain – such as "The Wolf of SUTD" [13], “XL-CITR” [14], “Guess Who?” [15], or “Agent Surefire” [16] – plays a role.

Above all, literature from the domain of insider threats is considered, since the game design intends to generate knowledge about insider threat actors. By comparison with literature on insiders - including scientific literature and known example cases - the plausibility of the results and innovation potential is analyzed. Besides, the scientific literature on insider threats provides the basis for the initial game development.

2.1.3 Design cycle. The Design Cycle is characterized by an iterative approach: the game is evaluated after each run using different methods (cf. section 4). Based on the evaluation results, adjustments are made after each game. For game material and in particular the game board, we used as design process:

1. Desk research about the scenario.
2. Development of a raw sketch based on desk research results.
3. Refinement of the sketch with an expert from the field .
4. Development of the first draft of the game board.
5. Validation of the board with a subject matter expert.
6. Refinement of the board.
7. Test run with validation.
8. Fine-tuning regarding the previous results.

2.2 Compliance with Design Science Research Guidelines

For a successful application of the Design Science paradigm, Hevner formulates research guidelines [9]. Subsequently, compliance with these guidelines is described:

Design as an Artifact: In NutriSafe, a serious game is developed as a viable artifact in the form of game materials and supplementary guidelines (cf. chapter 3).

Problem Relevance: The serious game pursues several goals. It aims to increase awareness of supply chains' vulnerabilities in food production and logistics. Also, the game aims to increase knowledge about insider threats.

Design Evaluation: The serious game is evaluated using a variety of methods: entry and exit surveys, structured participatory observations, and group discussions. For more details on the game validation cf. section 4.

Research Contributions: The contributions of the research activities are the artifact (game) itself, the understanding of how to use the game, the data collected in gaming (collection of roles and attacks), and the results of data analysis (such as causes, mediating factors, countermeasures). In addition, knowledge about game design is gained.

Research Rigor: The serious game is developed iteratively. In each iteration, both the game concept and the game's effects on the game participants are evaluated using scientific methodology (cf. section 4). Additionally, the results are triangulated with the existing knowledge and literature.

Table 1: Design Iterations

Iteration	Focus	Players (Teams)
1 (Apr. 2019)	Early testing of the game mechanics (without supply chain)	5 (5)
2 (May 2020)	Test run (with supply chain)	6 (2)
3 (Jul. 2020)	Run with the NutriSafe consortium	15 (4)
4 (Oct. 2020)	Test run (new board)	7 (3)
5 (Nov. 2020)	Run with the NutriSafe consortium and project-external practice partners	15 (4)
6 (Mar. 2021)	Run with project-external participants	12 (3)

Design as a Search Process: The development process is iterative and includes validation to enable game refinement with each implementation and evaluation.

Communication of Research: The game, in the form of game materials and guidelines, are published under an open-source license. Besides, information about the design process and design elements such as, e.g., the rating system and the findings of insider threats are about to be published. This article contributes to research communication.

2.3 Development iterations

At the beginning of the development, the experiences from the game "Operation Digital Chameleon" [17, 18] and other tabletop or card-based games (such as “Hatch” [19]) were taken into account: Applicability of card-based attack notation, team compositions and applicability of validation methodologies. For the game boards, the NutriSafe scenarios [20] and the exemplary infrastructure models [21] served as a basis. Then six iterations of development and performance have been done.

In the first iteration, the raw game concept – in the form of a ruleset, rating system, and game materials (e.g. cards and board) – was developed. This first iteration used a scenario that many players can possibly relate to. In the first place, this iteration tested the game mechanics. In the second iteration, the concept was further improved and applied to a supply chain context. A game board with a slaughter and cutting plant inside a meat supply chain was developed based on previous security analyses in the NutriSafe project [22]. The game was then played in an internal test run. After the test, the game was adjusted and then played within the NutriSafe consortium. Participants included individuals with varying backgrounds and expertise (e.g. regarding IT and security) from companies, universities, and food safety agencies from both Austria and Germany. The players were distributed among the teams so that each team contained a mix of skills. Then, besides further improvements of the game materials, a new board with a logistics service provider in the center of a food supply chain was developed in cooperation with a logistics consulting company. The game was then tested again in a test run and then played with members of the NutriSafe project and participants from the industry. Later, the game was played with project-external participants using the logistics board.

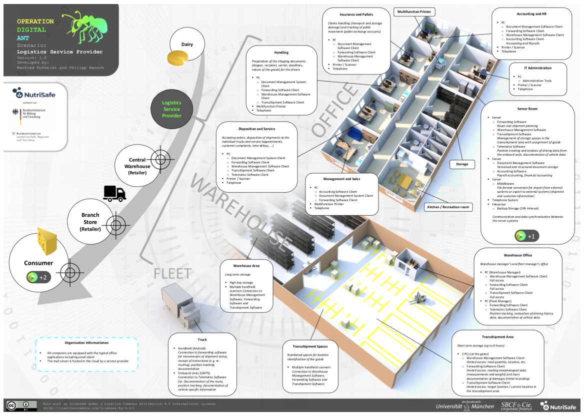

Figure 2: Impression of the logistics game board

3 THE SERIOUS GAME: OPERATION DIGITAL ANT

"Operation Digital Ant" is a tabletop game with game boards, game cards, and guidelines. The game is released on GitHub [23] and in the NutriSafe Toolkit [24].

3.1 Game logic

In the game, three to four teams with two to four players per team compete against each other by developing insider threat actor roles and 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 presents the rating. This determines the winning team.

3.2 Game board

The game board (Figure 2) describes the environment wherein the insider threats take place. It depicts the supply chain with actors (upper left corner) and the focus area with a logistics service provider in the center. The logistics service provider is modeled with visually rendered floor plans and supplementary information on rooms and assets, including IT assets.

The board is designed to be immersive, and that players with various backgrounds can play this game. No knowledge about the industry of IT security is required to participate in such a game.

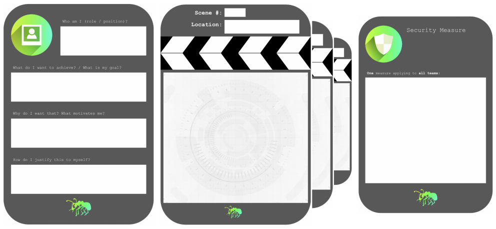
Who am I (role / position)?
What do I want to achieve? / What is my goal?
Why do I want that? What motivates me?
How do I justify this to myself?
Scene #:
Location:
Security Measure
One measure applying to all teams:

Figure 3: Impression of the card deck

3.3 Card deck

Each team develops an insider role, an attack, and a security measure using a card deck (Figure 3). The discussion in the teams and the result presentation are structured by the cards.
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 himself/herself?

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. This way, they later allow a more detailed analysis of the game results in regard to potential countermeasures on different levels (technological, organizational, individual). In particular justifications of attacks (in the sense of the neutralization theory [25]) promise to be useful. The neutralization aspect has been examined in the game "Operation Digital Chameleon" before [26].

The attack is developed using the scene cards. The filmmaking metaphor is used to make descriptions of attacks easy – also for players not used to formal notations. A threat is a sequence of scenes. This way, the teams are able to tell stories about insider attacks.

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

3.4 Rating system

The winning team is determined through a rating system, in which the teams rate each other by three given categories: (1) Plausibility of role and attack, (2) efficiency (relation of the achievement of the goal to the effort), and (3) damage potential. Each team can give up to ten points for each category to the other teams.

This kind of rating system is known from various TV shows and thus familiar to most players. Besides, there are indications that such rating systems are considered fair [27]. Note furthermore that the most important category for later analyses is "plausibility". The "plausibility" category ensures that the developed attacks and roles are – to some extent – realistic and fit the profile of the role. The "efficiency" category drives the teams to develop attacks that balance effort and effect. Again, such attacks are more likely to be realistic. The "damage potential" category makes the teams more likely to develop attacks that cause significant damage and therefore are of particular interest in our research. In addition, teams get bonus points for, e.g., causing an effect an end-consumer would notice for using assets in the server room.

Table 2: Validation methods used in the development iterations

Iteration	Methods
1 (Apr. 2019)	Participatory observation (game master); group discussion with the players
2 (May 2020)	Participatory observation (game master); group discussion with the players
3 (Jul. 2020)	Participatory observations (by team supervisors); entry/exit surveys; group discussion with team supervisors
4 (Oct. 2020)	Participatory observation (game master); group discussion with the players
5 (Nov. 2020)	Participatory observations (by team supervisors); entry/exit surveys; group discussion with team supervisors
6 (Mar. 2021)	Participatory observation (game master); group discussion with team supervisors

4 VALIDATION RESULTS

We consider perceived fun, perceived awareness, and the resulting attack vectors as criteria to validate the game design.
For game validation, a variety of empirical methods is used: participatory observations (structured), group discussions (with players or team supervisors) as well as entry and exit surveys with qualitative and quantitative elements (Table 2).

A protocol structures the participatory observations. The topics include comprehensibility, timing alignment, player motivation, acceptance, and use of the rating system. The entry and exit surveys are conducted via online questionnaires. Topics are individual experiences as well as estimations of supply chain vulnerabilities and insider threats.

It should be mentioned that the following limitations apply to the validation results: Due to participation of players with previous contact to the developers, there may be bias in the surveys due to social desirability. There may also be bias due to self-selection.

4.1 Game design validation

As described before, the game must meet the general quality criteria of a serious game. With every design iteration, the game concept and materials have been validated and refined according to evaluation results. The game concept seemed to be working well from the beginning, according to observations and group discussions. The two iterations with the entry and exit survey confirmed this. The exit surveys asked the game participants to rate fun factor and comprehensibility of rules, game flow, and game board (1 point being the worst and 5 points being the best rating). As summarized in Table 3, the participants gave high ratings regarding these attributes. So, the game concept meets the fun and comprehensibility

Table 3: Ratings from the exit surveys on the game concept

Validation Items (range [1, 5])	Iteration 3 (n = 14)	Iteration 5 (n = 10)
How much fun did you have playing the game?	4,4	4,4
How comprehensible were the rules and the game flow?	4,6	4,6
How comprehensible was the game board?	4,4	4,3

requirements. These results are in line with the results from the participatory observations and group discussions done in all iterations. The small decrease of comprehensibility ratings from iteration 3 to 5 is considered to be experimental variance due to the differing composition of participants.

As the game has been successfully played with different compositions of participants (in regard to profession and previous knowledge) and in physical and virtual formats (due to the Covid-19 pandemic), the game appears to be adaptable to various learning situations. Although no replay with the same players was initially foreseen for the game, it turned out that players have fun and rely on new strategies even if they participate again.

Unfortunately, the validation of the game's ability to make the attendees able to apply the learned knowledge in the real world has turned out to be a challenge, as the player's learnings are implicit and it is rarely possible to follow-up the players a long period of time. So the learnings are measured only directly after game participation.

4.2 Awareness validation

For the game to serve as a research instrument and provide value to the game participants, the game must have a positive effect on the participants' awareness. This impact on awareness was evaluated with entry and exit surveys in game iteration 3 and 5.

Both before and after game participation, the participants were asked to estimate the vulnerability of food supply chains, the likelihood of an insider threat in their organization, and the damage potential of such an insider threat. Table 4 summarizes the changes of these estimations, and the result appears to be ambivalent. In game iteration 3, all three items show an increase, while in iteration 5, only the estimation of the potential damage increases, while the other items decrease. The significance of these changes were tested with the Mann-Whitney U Test. The changes are not significant, except the increase of the estimation of the damage potential of insiders (p = .02872).

Asking about whether the participants notice an increase in knowledge after the game (no = 0, yes = 100), it appears that the participants in iteration 5 still gain knowledge as 80% of the participants answered with values equal or higher than 55 (overall mean = 66).

Estimations of the damage potential are in all games higher after the game than before and also significant. More knowledge about insider threats may lead to better (and this may also be lower) estimations of insider threat probabilities and food supply chain vulnerabilities. Here, further investigation is needed – especially as the results regarding these items are not statistically significant.

Table 4: Estimations before and after game participation

Average estimations [0 = very low; 100 = very high]	Iter. 3entry	Iter. 3exit	Iter. 5entry	Iter. 5exit
vulnerability of food supply chains	63	67 (+4)	68	63 (-5)
probability of an insider threat in the participants' organization	26	39 (+13)	47	38 (-9)
damage potential through insiders in the participants' organization	47	66 (+19)	42	53 (+11)

Table 5: Average plausibility ratings by adversary teams

Attack Scenario	Average Plausibility Rating
Faulty data mapping by a bribed employee	4
Manipulation of disinfectants	2
Poisoning of employees by a cleaner	6
Insertion of botulinum toxin in production	2,66
Salmonella contamination during packaging	4,33
Data manipulation by an IT administrator	7,33
Interruption of the cold chain by an IT administrator	4,5
Label exchange by an accounting employee	3,5
Data leak by a recruited fleet manager	7,5
Blackmail by a warehouse manager	4,66
Placement of a WLAN jammer by an office employee	6
Water damage caused by a dispatch employee	4,33
Data manipulation by an IT administrator	5,33
Data manipulation by an HR employee	3,5
Poisoning and ransom by a driver	7,5
Data manipulation by an employee in handling	4,5

4.3 Game output validation

The main output of the game is a collection of insider roles and attacks. We argue that the game is designed such that insider roles and attacks are plausible. First of all, plausibility is validated through the ratings of the teams (cf. Table 5). Each team rates the other teams. It appears that most of the attack vectors have at least medium plausibility ratings on average. It also appears that the range of plausibility ratings is wide, ranging from low to high plausibility. So not every developed attack is plausible according to the competing teams, but most of them have at least medium plausibility ratings on average.

It should be noted that in the discussions was expressed that often plausibility ratings were lowered due to the perception of low probabilities. So, attacks that were perceived as unlikely got lower plausibility ratings, which does not mean that they are inconsistent or unrealistic. Here, more guidance to the teams might be useful.

The plausibility of the attacks has also been a topic in the exit surveys, the second plausibility validation. In the exit surveys (iterations 3 and 5), the participants were asked about the plausibility of the developed attacks, 1 being the lowest and 5 being the highest value. In both surveys the plausibility evaluation gave medium results: 3,1 (n=14) and 3,2 (n=10). In addition, the collected roles and attacks have been presented and discussed in a workshop with the NutriSafe consortium. The first results of possible countermeasures are included in a poster presentation at the IWSEC 2020 conference [28].

5 SUMMARY AND FUTURE WORK

We could show that the game "Operation Digital Ant" is working out well in terms of concept and design, producing plausible insider roles and attacks. Also, the roles and attacks are interesting and sophisticated – and certainly not naive. Still, there is potential for refinement, e.g., concerning awareness and plausibility ratings.

The game itself is a good instrument for research data collection. In addition, our research contributes knowledge to the domain of serious game design: The rating system used in the game works well for games in professional contexts (however, the rating categories must be distinct), the game is applicable for players with various levels of previous knowledge and expertise, limiting roles or goals helps teams in the finding phase and insider role characteristics (intention, motivation and neutralization) appear to be helpful for later analyses.

Future work will be conducting more games and collect more data. For each iteration, the game will be further finetuned. This data allows detailed text analyses of insider roles, attacks, and potential countermeasures. This may contribute to the knowledge on how to tackle insider threats on technical, organizational, and individual levels. Besides, it would also be interesting to investigate potential negative side effects on game participants through empathizing with a likely criminal insider threat actor, i.e., in the form of discomfort, stress, or malicious learning effects. In the participatory observations, there were no indications for such negative side-effects.

Overall, the artifact has reached a milestone where it is able to produce deeper and broader knowledge about potential insider threats. It can identify technical, organizational, and individual risks, and the collection of roles and attacks can be the basis for further research. Furthermore, it could be applied to other supply chain scenarios beyond the food sector (for the game board development process see chapter 2.1.3). We plan to adapt it to IT supply chain scenarios in the future.

The game is released under Creative Commons license on GitHub [23] and in the NutriSafe Toolkit [24]. It provides researchers an instrument to gather (fictitious) insider threat examples and provides practitioners a tool that combines training with risk analysis while it is easy to use, does not require much resources, and adapts flexibly to different numbers of participants.

ACKNOWLEDGMENTS

We thank the German Federal Ministry of Education and Research (BMBF) for the funding of NutriSafe (FKZ: 13N15070) within the civil security research program as well as the Austrian Federal Ministry for Agriculture, Regions, and Tourism (BMLRT) for funding NutriSafe within the security research funding program KIRAS (project number: 867015).

REFERENCES

[1] NutriSafe - Sicherheit in der Lebensmittelproduktion und -logistik durch die Distributed-Ledger-Technologie, https://nutrisafe.de, last accessed 2021/01/22.
[2] ENISA: ENISA Threat Landscape 2020 - Insider Threat (2020).
[3] Cappelli, D., Moore, A., Trzeciak, R.: he CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Pearson Education (2012).
[4] Keeney, M. *et al.*: Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. Carnegie Mellon University (2005).
[5] Bundeskriminalamt: Monitoringbericht Innentäter in Unternehmen 2 – Aktuelle inländische Forschungsbeiträge, wesentliche Ergebnisse und Handlungsempfehlungen (2020).
[6] Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C. R., Ferryman, T.: Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis. In: e-Service Journal, 9(1), pp. 106 (2013).
[7] Shaw, E. D., Ruby, K., Post, J.: The Insider Threat to Information Systems: The Psychology of the Dangerous Insider. In: Security Awareness Bulletin (1998).
[8] Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., Ochoa, M.: Insight into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. In: ACM Computing Surveys, 52(2) (2019).
[9] Hevner, A. R., March, S. T., Park, J., Ram, S.: Design Science in Information Systems Research. In: IS Research MIS Quarterly, 28(1), 75–105 (2004).
[10] Hevner, A. R.: A Three Cycle View of Design Science Research. In: Scandinavian Journal of Information Systems, 19(2), 87–92 (2007).
[11] Michael, D., Chen, S.: Serious Games – Games That Educate, Train, and Inform. Thomson Course Technology PTR (2006).
[12] Zhang-Kennedy, L., Chiasson, S.: A Systematic Review of Multimedia Tools for Cybersecurity. In: ACM Computing Surveys, 54(1), pp. 1–39 (2020).
[13] Harilal, A. *et al.*: TWOS – A Dataset of Malicious Insider Threat Behavior Based on a Gamified Competition. In: Proceedings of the 2017 International Workshop on Managing Insider Security Threats, pp. 45–56 (2017).
[14] Andre, T. S. *et al.*: Augmented Cognition Methods for Evaluating Serious Game Based Insider Cyber Threat Detection Training. In: International Conference on Foundations of Augmented Cognition, S. 395–403 (2011).
[15] Gupta, S. *et al.*: Guess Who? - A Serious Game for Cybersecurity Professionals. In: Games and Learning Alliance 9th International Conference, S. 421–427 (2020).
[16] Alhadeff, E.: Converting Cybersecurity Practice Into Engaging Serious Games, Serious Game Market, https://www.seriousgamemarket.com/2012/02/ converting-cybersecurity-practice-into.html, last accessed 2021/08/10 (2012).
[17] Rieb, A., Lechner, U.: Operation Digital Chameleon – Towards an Open Cybersecurity Method. In: Proceedings of the 12th International Symposium on Open Collaboration (2016).
[18] Rieb, A.: IT-Security Awareness mit "Operation Digitales Chamäleon". Dissertation, Universität der Bundeswehr München (2017).
[19] Denning, T. *et al.*: Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (2013).
[20] Wilhelmi, T.: Beschreibung und Modellierung der NutriSafe-Szenarien Produktion und Logistik von Bio-Kochschinken und Weichkaṡe. In: NutriSafe Toolkit, https://nutrisafe.de/toolkit (2020).
[21] Hofmeier, M.: Beispiele für IT-Infrastrukturen in den Wertschöpfungsketten der NutriSafe-Szenarien. In: NutriSafe Toolkit, https://nutrisafe.de/toolkit (2020).
[22] Hofmeier, M., Lechner, U.: Schwachstellen und Angriffsketten in der Wertschöpfungskette der Fleischproduktion. In: SICHERHEIT 2020, pp. 67-77. Gesellschaft für Informatik e.V., Bonn.
[23] Operation Digital Ant GitHub Repository, https://github.com/NutriSafe-DLT/operation-digital-ant, last accessed 2021/01/22.
[24] NutriSafe Toolkit, https://nutrisafe.de/toolkit, last accessed 2021/01/22.
[25] Sykes, G. M., Matza, D. Techniques of Neutralization: A Theory of Delinquency. In: American Sociological Review, 22(6), pp. 664–670 (1957).
[26] Rieb, A., Gurschler, T., Lechner, U.: A Gamified Approach to Explore Techniques of Neutralization of Threat Actors in Cybercrime. In: GDPR & ePrivacy - APF 2017 - Proceedings of the 5th ENISA Annual Privacy Forum, pp. 111-127 (2017).
[27] Meyer, D.: Sprechen über das Kochen: eine rezeptionsanalytische Studie der Selbst-technologien im Rahmen der Gouvernementalität am Beispiel der Fernsehsendung "Das perfekte Dinner". LIT Verlag, Münster (2010).
[28] Hofmeier, M., Lechner, U.: Vulnerability in the Food Supply Chain - Approaches and Results from the NutriSafe Project. International Workshop on Security (IWSEC), https://www.iwsec.org/2020/posters.html (2020).