Board Games as Security Awareness Improvement Tools

Eszter Diána Oroszi
National University of Public Service
Budapest, Hungary
e-mail: oroszi.eszter@silentsignal.hu

***Abstract*—Improving security awareness level of users is getting more important in all organizations. Experience shows that traditional training methods and campaign elements are not enough these days. This paper will show new gamified possibilities, and within that, it will introduce a security awareness board game, future works and partial results of a related research performed by author.**

Keywords-security awareness; improvement; gamfication; board game; serious game.

I. INTRODUCTION

Information security is becoming more important in all organizations, and we can say that human factor is one of the most vulnerable elements at the workplace, the so-called weakest link in the chain of security [1]. Employees of companies could be targets of human-based attack types called Social Engineering, which means that attackers try to manipulate, and/or deceive users for example to compromise confidential data, and cause harm or loss to the organization. To reduce this risk, it is very important to improve the security awareness level of users.

Security awareness improvement actions could be trainings (for example, classroom or online presentations, workshops, e-Learning materials, etc.), or campaign elements (for example, posters, puzzles, quizzes, etc.). According to NIST 800-50 [2], the purpose of these actions is to inform and educate employees about the security policies and rules of the organization and the necessity of security aware behavior, improve skills and competences of users to work securely, and increase security awareness level [2]. Besides occasional or periodical trainings and educational events, it is important to maintain users' attention, and constantly remind employees of information security rules and best practices. To do this, organizing a security awareness campaign, or whole year improvement program could be a possible method, which can help employees remember the most important security rules and habits during their daily work, and which can show information security news, share actual knowledge elements for the audience. These events could be even a so-called awareness week, or cybersecurity month, like Cyber October, when the employees take part in trainings, presentations, answer questionnaires, participate in games; or it can be a general annual program with posters in the office, screensavers highlighting threats targeting the human factor, regular newsletters, and games improving security awareness.

According to the author's experiences, traditional security awareness training and campaign elements are quickly forgettable, and usually most of users think that these well-known messages are boring and contain unnecessary information. Finally, a significant problem regarding these is that they do not answer the most important questions: Why do we need information security? What could happen, if a user does not follow the rules? Which are our roles and responsibilities in security?

A useful and effective awareness program should answer the questions mentioned above and present the importance of security-aware behavior of employees. According to Rocha Flores and Ekstedt [3], using personalization in security related trainings and specialized content of educational material can make the security awareness improvement program more relevant and understandable for the participants, and combining the traditional methods with practical exercises will more likely lead to improved security behavior. The author's experience also supports the above-described statements: security awareness trainings are more effective, when the presentation is illustrated with real examples, and contain photos about results of Social Engineering audits. Another effective method is using gamified elements during the training [4]. Based on these, we must improve security awareness programs, and try to use unique and personalized campaign elements that involve employees into the information security. These kinds of actions could be active programs using gamification, games for formal prizes like "The most security aware employee of the month", or a photo competition about information security. The next parts of the paper will show how can we use gamification for security awareness improvement actions.

In Section II, the author presents gamified security awareness campaign elements, and in Section III, the focus is on board games as educational materials. Section IV contains the concept of a security awareness board game designed by the author. Section V shows the conclusions and the future work of the author.

II. GAMIFIED ELEMENTS IN SECURITY AWARENESS

Gamification is getting more popular of a method in companies to motivate employees, improve performance, enhance experiences of trainings. A possible definition of this concept is the following: "Gamification is the use of

Copyright (c) IARIA, 2021. ISBN: 978-1-61208-919-5

game elements and game thinking in non-game environments to increase target behavior and engagement" [5].

According to Burke [6], the most important purpose of gamification is to increase motivation and improve engagement. Besides that, a key element of these methods is that "we most often want everyone to win", but it could have a collaborative-competitive approach, too – in this case, participants competing as teams, rather than individuals.

Typical gamified improvement elements could be badges, leaderboards, points or scores, levels, and challenges [7]. Applying these methods, participants could easily identify their progress and results and could motivate each other, too. Results could be recorded on Intranet sites of the organization, in the e-Learning solution, security awareness mobile application, or other training systems/framework. The essence of them is that users get points for participating in workshops, trainings, solving quizzes and tests, identifying, and participating in other campaign elements, games.

All previous mentioned elements have positive feedback, and it is an important aspect, when using gamification. Besides that, gamified methods provide the users with a sense of autonomy about the training, it is perceived as a fun experience, not as a mandatory task [8]. According to the author's experience, users really prefer positive feedback and "stories" in information security, for example, they are excitedly waiting for the results of phishing tests, and they would like to get better and better results, or they are proud, if someone recognizes a real or test-attack, or solves a security awareness game.

The first gamified method of the author was a security awareness escape room, which was designed in 2014, based on her experience of Social Engineering audits and security awareness trainings, but feedbacks of campaigns were also built into this special exit game. Besides the type of exercise, the most significant difference between a traditional exit room and an information security-based one is the scenario, or story of the game. In a traditional escape game, players are usually locked into the room of a non-realistic character (pirate, scientist, killer, etc.), but in case of the security awareness one, the escape room is mostly the office of a fictional assistant, boss, project manager, system administrator or other employee, who could be the target of any attacker [9]. A normal exit game, usually with two to six players can be solved in 60 minutes, in a security awareness escape room the time could be limited to 15 or 30 minutes, so shorter timeslots do not set back daily work, and managers can support the participation of their subordinates better. In this game the players are not locked in the room like in general cases, and the goal is not finding the key or code to unlock the door. To "escape" the room, and complete the mission, participants need to log into the computer of the targeted person and open a chosen file – if they can open it and read its content, they won, and the game ends. Feedbacks of security awareness escape rooms are very positive; participants really like these programs, and consider them not only exciting, but also useful. Based on these positive experiences, another game-based learning opportunity could be an applicable idea: board games.

III. Board games in information security

Board games as training materials are also new, gamified methods in several areas of education. The baseline of popularity is the same, as in case of escape rooms: tabletop games, puzzles, or card games are also well-liked nowadays, strategical-cooperative ones (for example, Pandemic, King of Tokio, Catan, Activity, etc.) have a serious target audience. Based on that, these games could be used for educational purposes, even in security awareness improvement.

Adam Shostack collected, and shortly introduced a few information security related board games on his website [10]. Some of them are more for fun, and include a little bit of security awareness topics and knowledge, but there are serious games, which are designed for use in corporate environment with less aim for enjoyment. These games show perfectly, what could be the purpose and role of the human factor in information security. To win the game, the players need to prevent attacks and defend against hackers, improve security countermeasures, design and develop securely, or they can even see the impact of a security incident on their assets. Increasing motivation, engagement and providing freedom are advantages that are particularly highlighted by these types of gamification elements. These serious games are not first and foremost designed for children, students or even individuals, rather for employees of organizations, average users, specialists, professionals and managers. For example, Cook et al. [11] introduced a board game called Simulated Critical Infrastructure Protection Scenarios (SCIPS), which is designed for decision makers of critical infrastructure, for showing consequences of cyber-attacks, and highlighting the importance of information security investments and controls.

Another security awareness board game is Riskio, which is a tabletop game for 3-5 players, even without technical knowledge. This game itself is not sold commercially, rather it could be played with the directions of an instructor, who is an information security expert [12]. In contrast, Control-Alt-Hack is a commercially available tabletop card game about white hat hacking, for 3-6 participants. According to the storyline of the game, players are ethical hackers performing audits and working for a security consulting company. Like classical board games, this one also has characters, different decks, and it is played in rounds, which are divided into 7 phases. To win the game, player must become the CEO of his own company [13]. Open source, free downloadable games could also be found on the Internet. For example, [d0x3d!] is a customizable, cooperative board game, focusing mainly on network security, so it is a special kind of security awareness games [14], or OWASP Cornucopia is a unique kind of security awareness card games, because it is designed only for a special user group, development teams, and the topic is secure development [15].

Although the main purpose of most games is to learn by playing, the above-mentioned games (according to the author's opinion, especially Riskio and OWASP

Cornucopia) could be useful in a corporate environment, too. Using these gamified methods, participation in security awareness trainings could be raised, and user satisfaction with information security could become better. Potential limitations of these games include being commercially available only on a limited basis, hard to find, according to the author's opinion, the main focus is not "to be a playful board game", and reaching target audience could be difficult. The author's assumption is that a well-advertised, commercially available security awareness related board game could be popular, and could help to improve security awareness level of both individuals and employees in an effective way. Availability as a classic board game could be more attractive than educational materials, and the audience could buy their own game, or they can try and use them as shared resource at the workplace, educational events (for example, family day, festival), board game cafes, etc.

IV. Concept of a Security Awareness Board Game Designed by the Author

Based on Social Engineering audit and security awareness training experiences, the author of this paper also designed a board game with the purpose of improving security awareness. The board game is designed for an office environment, but development of a home edition, including for children is also in progress. The game focuses on general information security recommendations and awareness knowledge; thus, it is not limited to organizational rules and policies – special organizational editions could be implemented, but the main purpose of the basic game is to improve general security awareness knowledge of users, both at the workplace, and at home. Updates (for example, new threats, attack types, countermeasures) could be released as accessories, packages of additional cards, decks, characters, places, etc.

During the development of this board game, the author's goals were the following:

- Applying strategic-cooperative approach.
- Enables cooperative and competitive playing modes.
- Fit for organizational environment and private life.
- The game should highlight exploitable human traits (Solution: Character cards).
- The game should introduce assets to be protected (Solution: Asset tokens).
- The game should teach security awareness and useful countermeasures (Solution: Security awareness knowledge cards).
- The game should show threats and attacks affected by human factor (Solution: Action cards).
- Could be played with instructor at the workplace.
- Could be played alone at home (without instructor).
- Supports demo mode (applying time limit).
- Be realistic, but still a game (players sometimes need luck).
- Be commercially available, like traditional board games.
- The game should be expandable with accessories.

The game is designed for 6 players and have both cooperative and competitive modes: using the "security awareness meters", players can see the summarized results of the whole team, but in case of a competition, they can measure their own progress in the character cards. The parts of the game are introduced below and could be seen in Figure 1.

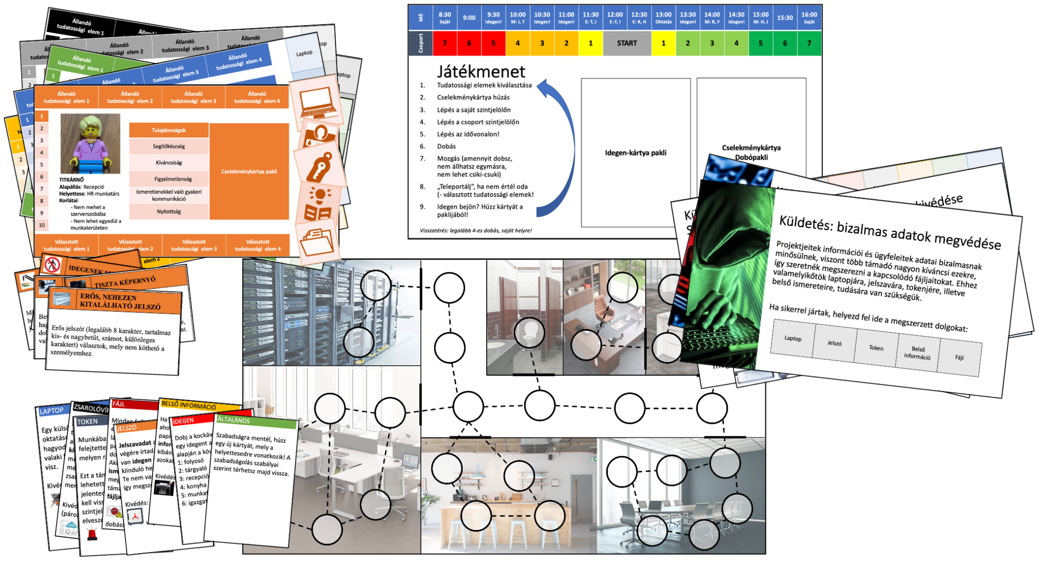
Idő
8:30 Saját
9:00
9:30 Idegen!
10:00 M: I, T
10:30 Idegen!
11:00 Idegen!
11:30 E: T, J
12:00 E: F, I
12:30 E: R, H
13:00 Oktatás
13:30 Idegen!
14:00 M: R, F
14:30 Idegen!
15:00 M: H, J
15:30
16:00 Saját
Csoport
7 6 5 4 3 2 1 START 1 2 3 4 5 6 7
Játékmenet
1. Tudatossági elemek kiválasztása
2. Cselekménykártya húzás
3. Lépés a saját szintjelölőn
4. Lépés a csoport szintjelölőn
5. Lépés az idővonalon!
6. Dobás
7. Mozgás (amennyit dobsz, nem állhatsz egymásra, nem lehet csiki-csuki)
8. „Teleportálj", ha nem értél oda (- választott tudatossági elemek!
9. Idegen bejön? Húzz kártyát a paklijából!
Visszatérés: legalább 4-es dobás, saját helyre!
Idegen-kártya pakli
Cselekménykártya Dobópakli
Küldetés: bizalmas adatok megvédése
Projektjeitek információi és ügyfeleitek adatai bizalmasnak minősülnek, viszont több támadó nagyon kíváncsi ezekre, így szeretnék megszerezni a kapcsolódó fájljaitokat. Ehhez valamelyikőtök laptopjára, jelszavára, tokenjére, illetve belső ismereteire, tudására van szükségük.
Ha sikerrel jártak, helyezd fel ide a megszerzett dolgokat:
Laptop
Jelszó
Token
Belső információ
Fájl
Állandó tudatossági elem 1
Állandó tudatossági elem 2
Állandó tudatossági elem 3
Állandó tudatossági elem 4
TITKÁRNŐ
Tulajdonságok
Segítőkészség
Kíváncsiság
Figyelmetlenség
Ismeretlenekkel való gyakori kommunikáció
Nyitottság
Cselekménykártya pakli
Választott tudatossági elem 1
Választott tudatossági elem 2
Választott tudatossági elem 3
Választott tudatossági elem 4
IDEGENEK
TISZTA KÉPERNYŐ
ERŐS, NEHEZEN KITALÁLHATÓ JELSZÓ
Erős jelszót (legalább 8 karakter, tartalmaz kis- és nagybetűt, számot, különleges karakter) választok, mely nem köthető a személyemhez.
LAPTOP
ZSAROLÓVÍRUS
TOKEN
FÁJL
JELSZÓ
BELSŐ INFORMÁCIÓ
IDEGEN
ÁLTALÁNOS
Szabadságra mentél, húzz egy új kártyát, mely a helyettesedre vonatkozik! A szabadságolás szabályai szerint térhetsz majd vissza.

Figure 1. Elements of board game designed by the author

A. *Game board*

The game board illustrates an office with lobby, open space workplaces, server room, director's office, meeting room, kitchen, corridors, and toilet. Characters can step on fields located within these areas.

B. *Character cards*

The players can choose from 6 characters (director, secretary, lawyer, HR specialist, developer, and system administrator). Each character has different human traits and habits as vulnerabilities, which will become important when attacked, and they all have assets (notebook, token, password, knowledge, documents, files), which must be protected during the game. These elements are shown, or should be placed on the character cards.

C. *Security awareness knowledge cards*

Each character has a deck of security awareness knowledge cards. Players can pick three fixed, and three variable options to protect their assets, and the variable cards can be exchanged after every round of the game, based on predicted actions, or according to the places, where the character is.

D. *Mission cards*

In the current version, there are four missions in the game, which contain different goals and attack types (for example, defending passwords, securing top secret document, etc.), and have different difficulty, too. Players have to focus on the affected assets and protect them from the attacks. After a successful attack, the affected asset must be moved from the Character card to the Mission card. If all the targeted assets are on the Mission card, the players lose the game.

E. *Action cards*

Attacks, or even positive (for example, security awareness training for bonus points) or general (like movement to another location) events happen by drawing Action cards. The action card deck is distributed among the players. These cards must be drawn by everyone in every round, and it will show, what happens. Attacks can be prevented by one of the relevant Security awareness knowledge cards shown in the Action card, which can be found on the Character card of the player (both fixed and variable cards could be used).

F. *Timeline*

The timeline is showing the current round, symbolizing a workday divided into half hour slots. Fields of the timeline show subgoals, for example, some characters have to move to the meeting room, or there are timeslots, when unknown visitors arrive at the office, who could also become potential attackers, activated by Action cards. If players reach the last time slot (16:00), the game ends, and they win the game. (Timelines of demo games are shorter and divided into 8 hours.)

G. *Security awareness meter*

Security awareness meter can be found both for the team, and on the character cards. If a player prevents the attack, he or she, and the team can both step forward on Security awareness meter(s), in case of successful attack, they have to step one field back. At the end of the game, players can see their results, how security-aware they are.

During the game, players have to move their characters every round, and to do this, they have to roll the dice. Direction of movement can be arbitrary, but certain points of the timeline show that certain characters have to be at a place at that time (for example, the developer has to be in the kitchen at 12:00).

The players win, if they are at the end of the timeline and completed the mission (have the needed assets), and the game is ended without success, if the characters fail the mission during the workday (if they cannot protect the assets according to mission).

This game is currently in end-user testing phase, and part of a security awareness research ending in 2022, but some partial results are shared in the next section.

V. Conclusion and future work

Gamification is nowadays a popular weapon to increase user motivation and engagement, and it is also a possible new method in improving security awareness level of employees. Besides traditional gamified actions (for example, gathering points, scores, leaderboards, achievements, levels, badges, etc.), games could be used also as educational materials. The paper introduced results of some conference papers and other related works, which are confirming the effectiveness and usefulness of gamified methods. Based on these statements, it is recommended to use gamified elements in security awareness improvement actions, like information security escape rooms or board games, which were presented in this paper.

Besides the popularity of these new methods, measuring their effectiveness is also important. As future work, the author has ongoing research, which is going to assess the effectiveness of different methods for improving security awareness. The author will compare six possible program elements, which are the following:

- In-person security awareness training,
- online security awareness training,
- using e-Learning materials,
- security awareness escape room,
- security awareness board game,
- security awareness campaign elements (posters, gifts, messages, etc.).

Each program element has the same timeframe (30 minutes) and content (ten chosen areas of knowledge), which makes them comparable with each other. To measure effectiveness, before and immediately after the participation in the improvement action, participants have to fill out an information security awareness survey, and one month later a post course questionnaire (containing same questions) will be performed. All of these surveys ask users to describe important security awareness rules, recommendations. As a result of the research, the author can identify, which are the most important new security awareness knowledge elements coming from the improvement action, which are the deepest knowledge elements (one month later), and how effective the investigated methods work. Participants of the research are 10 organizations, each of them with 30 employees, who are divided into six groups according to the tested methods. (Each user may participate in only one program element.)

The author's hypothesis in this research is that gamified elements will be more effective than traditional ones. Although the research is still in progress, partial results show that 75 percent of participants prefer gamified elements instead of traditional methods and in-person events are more effective than online based solutions. Based on the experiences to date, the highest amount of new knowledge elements was written after the security awareness board game – presumably, the reason could be that both Security awareness knowledge cards and Action cards contain useful information. According to the partial results of a questionnaire about the board game, 93.3 percent of the testers declared that they would like to play the game with their colleagues, 80 percent of the responders would like to use it also at home. 66.7 percent of players stated that they would like to use the game without the help of an instructor. These results suggest that there is a demand for such gamified security awareness improvement tools, like board games. Effectiveness of the gamified methods could be evaluated after performing the last surveys at the end of the research, probably finalizing in Q1, 2022.

Acknowledgment

The author would like to thank Silent Signal LLC. that contributed to the development of the presented board game and supports ongoing research about evaluating effectiveness of security awareness improvement methods. Special thanks for friends and colleagues, who participated in testing the author's security awareness board game and contributed to the development with useful feedbacks and suggestions.

References

[1] K. D. Mitnick, and W. L. Simon, The Art of Deception: Contolling the Human Element of Security. Wiley, 2003, ISBN: 978-0764542800

[2] M. Wilson, and J. Hash, NIST 800-50 Building an Information Technology Security Awareness and Training Program, 2003

[3] W. Rocha Flores, and M. Ekstedt, Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers and Security, 59, pp. 26-44, 2016

[4] E. D. Oroszi, Security awareness escape room - a possible new method in improving security awareness of users. [Conference paper]. Cyber Science Cyber Situational Awareness for Predictive Insight and Deep Learning, C-MRiC.ORG., Oxford, pp. 170-173, 2019

[5] P. Van den Boer, Introduction to Gamification. Whitepaper. 2019. Available from: https://cdu.edu.au/olt/ltresources/downloads/whitepaper-introductiontogamification-130726103056-phpapp02.pdf [retrieved: January, 2019]

[6] B. Burke, Gamify: How Gamification Motivates People to Do Extraordinary Things. Gartner, 2014, ISBN: 978-1937134853

[7] Anadea, How Gamification in the Workplace Impacts Employee Productivity, 2018. Available from: https://medium.com/swlh/how-gamification-in-the-workplace-impacts-employee-productivity-a4e8add048e6 [retrieved: October, 2021]

[8] E. G. B. Gjertsen, E. A. Gjære, M. Bartnes, and W. Rocha Flores, Gamification of Information Security Awareness and Training. [Conference paper] 3rd International Conference on Information Systems Security and Privacy, pp. 59-70, 2017

[9] E. D. Oroszi, Security awareness escape room - a possible new method in improving security awareness of users. [Conference paper]. Cyber Science Cyber Situational Awareness for Predictive Insight and Deep Learning, C-MRiC.ORG., pp. 170-173, Oxford, 2019

[10] Online source, available from https://adam.shostack.org/games.html, 2021.08.08

[11] A. Cook, R. Smith, L. Maglaras H. Janicke, Using Gamification to Raise Awareness of Cyber Threats to Critical National Infrastructure [Conference paper]. 4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR 2016), Belfast, pp. 84-94, 2016

[12] Online source, available from: https://www.riskio.co.uk, [retrieved: October, 2021]

[13] Online source, available from: https://boardgamegeek.com/boardgame/ 128408/control-alt-hack, [retrieved: October, 2021]

[14] Online source, available from: https://d0x3d.com/d0x3d/welcome.html, [retrieved: October, 2021]

[15] Online source, available from: https://owasp.org/www-project-cornucopia/, [retrieved: October, 2021]