Serious Games for IT-Security Education

Roland Schmitz, Dirk Heuzeroth
Institute for Cyber Security
Stuttgart Media University, Stuttgart, Germany
{schmitz,heuzeroth}@hdm-stuttgart.de

***Abstract*—In recent years, the notion of gamification has gained some interest within the scientific community. Gamification denotes the use of typical gaming mechanisms, like collecting points, reaching different levels or gaining a spot on a highscore list, in a non-gaming related context. One of the most important application areas of gamification is education, e. g. learning a foreign language or basic arithmetics. There have been, however, few attempts to use games for IT-Security education.**
The present paper will review the existing approaches in this area, present a serious game that has been produced at Stuttgart Media University on behalf of the swiss bank UBS, and will provide an outlook on planned further activities in this area.

***Index Terms*—Serious Games, IT-Security, Education**

I. Introduction

For a long time, games and game-related mechanisms like scoring points, reaching levels or rising in a highscore list, have been recognised in pedagogics as useful tools for raising students' motivation to learn new skills and for helping them to internalize and apply abstract knowledge. Perhaps one of the earliest examples of this genre is the game *The Number Race* [1], which is designed to help children with dyscalculia.

More recently, serious games have also been adopted in a business context, in the hope to raise the motivation and efficiency of employees. Whereas the idea to use isolated, competitive (e. g. Capture-The-Flag) events in IT-security education is not new, there are few attempts to use gaming based mechanisms in online-based trainings so far. Research in this direction has just started off: [1] provides a first overview of the existing IT-security simulation systems in 2010, but there is no clear distinction between games and simulators. Another, more recent overview is provided by [2]. The authors note that most of the investigated games are no longer available (with *CyberCIEGE*, cf. section II-C, being a notable exception), although the aim of most of those games is to change the long-term behaviour of the players. Finally, in [3], a framework for designing serious games which are aimed at raising an awareness of cyber security to those with little or no knowledge of the subject is presented.

The present paper briefly describes some of the existing serious games in IT-security and gives an overview of current activities at Stuttgart Media University.

II. Existing Games for IT-Security

A. Targeted Attack: The Game (TrendMicro)

Targeted Attack: The Game[2] is a freely available web based game by the renowned security company Trend Micro. In this game the player acts in the role of the CIO of a company which develops a mobile payment app. The player gets introduced to several security relevant situations by video sequences which require security decisions to be made. Each decision has an impact on subsequent options, especially because some decisions encompass costs reducing the available budget. Consequently, some essential options may not be available later on during the game, because the remaining budget is not sufficient. When the player has failed to succeed, all his decisions are shown in a review and hints are given for improvement. The game scenario can be repeated arbitrarily often. One important aspect of this game is to broaden the horizon of the player and show the potential impact of security related decisions in realistic scenarios.

B. Enter — IT Security Game (Swiss IT Leadership Forum)

Enter — IT Security Game[3] is a game developed by the Swiss IT Leadership Forum. It is available as an app in the AppStore and on GooglePlay. The goal of the game is to demonstrate that information from employees of a company can be used for cyber attacks, even if the information does not seem to be security-related. The player acts as the attacker and uses various approaches, techniques and attack targets like WiFi, USB sticks, printers, social media, keys, badges, phone, black mailing, phishing, spear phishing, trojans, data theft, spoofing, code, eavesdropping on conversations, fooling gullible workers, sneaking past unvary employees, stirring up some action and thus collecting data and information to laterally move from one company to another until he reaches the final one.

C. CyberCIEGE

CyberCIEGE[4] [4] is a game developed by the Naval Postgraduate School at Monterey, USA. Users spend virtual money to operate and defend their networks, and can watch the consequences of their choices, while under attack. CyberCIEGE seems to focus on network-security related topics, including configurable firewalls, VPNs, link encryptors and

[1] `http://www.thenumberrace.com/nr/home.php`

[2] `http://targetedattacks.trendmicro.com/`

[3] `https://entergame.ch/en/`

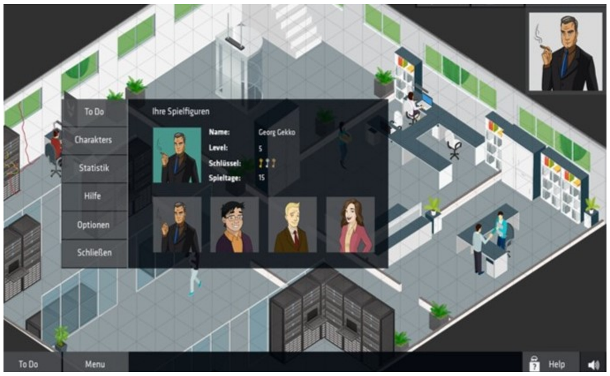
[4] `https://my.nps.edu/web/c3o/cyberciege`

access control mechanisms. It includes identity management components such as biometric scanners and authentication servers. Attack types include corrupt insiders, trap doors, Trojan horses, viruses, denial of service, and exploitation of weakly configured systems. Attacker motives to compromise assets differ by asset and scenario, thereby supporting scenarios ranging from e-mail attachment awareness to cyber warfare.
It is available to agencies of the US government and educational institutions on request.

III. Key to Excellence

Key to Excellence is a game developed at the Institute for Games at Stuttgart Media University on behalf of the swiss bank UBS. The overall goal is to enhance the security awareness of employees in a playful way. While in an earlier study [5] *CyberCIEGE* was used to evaluate the impact of games on the security awareness of players, to best of our knowledge, *Key to Excellence* is one of the first game that was explicity developed for this purpose. More importantly, the game is browser-based and can therefore be played anywhere, in accordance with the assertion given in [1], that in order to have a lasting impact, the game must be easy to use and playable within the students' own environment.

The actual educational scenarios (e. g. detect a Phishing mail) were adopted from tutorials developed by the IT-security department of UBS. The game, however, embeds these scenarios into a less artificial context than is often the case in typical security awareness training. Actually, the goal of the game is not to respond correctly to as many security incidents as possible, but to rise within a fictional organization. Nevertheless, players will feel the consequences of incorrect security decisions within the game, e. g. a lower reputation or decreasing budget. Players live within scenarios and have to complete work-related scenarios. For this, they can choose between characteristical personas (see Figure 1).



Name: Georg Gekko
Level: 5
Schlüssel:
Spieltage: 15

Fig. 1. Typical Scenario with Playable Characters

Currently, the game development process is finalized, but the game is still awaiting active deployment and evaluation within UBS.

IV. Future Plans

At Stuttgart Media University we are currently developing a serious game, that will be multi-player capable, such that players having different roles can play together. It is hoped that this novel feature can further add to the players' motivation and immersion, with the goal of increasing the impact on the players' knowledge and long-term behaviour.

Each player is confronted with situations relevant for his role and has to cooperate with other players or defend against other players. The game scenarios will be realistic, based on state of the art security devices and software, such that a real-life training for job-relevant tasks is conveyed by the game. The attack vectors will be similar to existing games, but the game environment simulates realistic real-life work situations. Moreover, the impact of decisions or actions taken by a player will become evident and visible for other players. This increases the pressure on each player and is therefore comparable to their everyday jobs.

We are plannung to conduct surveys in order to determine the impact of multi-player games versus single-player games.

V. Conclusion

Existing games in the area of IT-security are limited to one acting player. Although several scenarios, attack targets and attack vectors are dealt with, current games do not offer the possibility to act in different roles and learn what is security-relevant for each role. Current games also are not multi-player capable. Thus players can not learn from each other and no unforseen actions can occur, as would be the case in real life scenarios. This also means that current games do not adapt to the player's actions or at least do so only in a very limited way.

We expect that providing serious games which offer these possibilities would be much more beneficial, because they will not get boring so fast, will continuously provide new training situations and offer training that will retain even in real life situations when performing the daily job.

References

[1] V. Pastor, G. Díaz, and M. Castro, "State-of-the-art simulation systems for information security education, training and awareness," in *IEEE EDUCON 2010 Conference*. IEEE, 2010, pp. 1907–1916.

[2] M. Hendrix, A. Al-Sherbaz, and V. Bloom, "Game based cyber security training: are serious games suitable for cyber security training?" *International Journal of Serious Games*, vol. 3, no. 1, 2016.

[3] A. Le Compte, D. Elizondo, and T. Watson, "A renewed approach to serious games for cyber security," in *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*. IEEE, 2015, pp. 203–216.

[4] M. Thompson and C. Irvine, "Active learning with the cyberciege video game," in *4th Workshop on Cyber Security Experimentation and Test (CSET)*. USENIX, 2011.

[5] C. C. Fung, V. Khera, A. Depickere, P. Tantatsanawong, and P. Boonbrahm, "Raising information security awareness in digital ecosystem with games – a pilot study in thailand," in *2nd IEEE International Conference on Digital Ecosystems and Technologies (DEST)*. IEEE, 2008.