Sebastian Pape, Dennis-Kenji Kipker

Case Study: Checking a Serious Security-Awareness Game for its Legal Adequacy

It is generally accepted that the management of a company has a legal obligation to maintain and operate IT security measures as part of the company's own compliance – this includes training employees with regard to social engineering attacks. On the other hand, the question arises whether and how the employee must tolerate associated measures, as for example social engineering penetration testing can be very intrusive.

1 Introduction

Social engineering (SE) attempts to induce and exploit certain behaviour by influencing the victims to obtain sensitive information. A SE attack is often the first step of a larger attack, in which the attacker uses the information gained there for further attacks [1]. However, the latest Data Breach Investigations Report [1] also reports another increase of financially motivated SE, where the attacker directly ask for some money, i. e. by impersonating CEOs or other high-level executives. While a couple of defense methods and counteracting training methods [2, 3] exist, at present, companies have three main strategies to fend off SE attacks: SE penetration testing, security awareness training and campaigns.

For SE penetration testing, penetration testers are, as benign hackers, supposed to attack the employees and find weak points. This is mostly the case to investigate the employees' vulnerability to phishing attacks. Unfortunately, this approach is not without problems. Experiments have shown that this approach can also lead to employees becoming demotivated when confronted with the results of the test [4]. In addition, such a test can interfere with the employees' right of personality, in particular since for an accurate assessment of the situation, employees cannot be told beforehand they are being tested, resulting in ethical issues [5]. As a consequence, there are numerous labour law requirements for SE penetration tests [6, 7].

Security awareness training may prove successful in particular against phishing. However, often employees are not trained at all or the training is conducted insufficiently [1] or in a way that it does not have a long lasting effect [8]. Security awareness campaigns often provide only information about risks and are not engaging, interesting and entertaining enough, evoke negative feelings such as anxiety, fear or stress and therefore are ineffective to change individuals' behavior [9]. Altogether, both strategies have in common that individuals generally dislike following instructions because it is associated with losing control.

A not so common method is the use of serious games, games that have a serious goal besides entertainment. Serious games are more entertaining and engaging than traditional forms of learning and influence individuals' behavior due to their use of pedagogy and game-based learning principles, such as motivation, cognitive apprenticeship and constructivism [10]. Therefore, at a first glance the use of a serious game for awareness raising and training against SE attacks, e. g. HATCH [11, 12], seems to be fine. However, in this paper we investigate the legal challenges to make use of the game HATCH, which offers two different types of scenarios. As a case study, we examine under which circumstances which of HATCH's scenario types is suitable and legal to fulfill its goal. Based on the results, we derive general recommendations what to consider when making use of a serious game for awareness raising.

Dr. Dennis-Kenji Kipker

Wissenschaftlicher Geschäftsführer des Instituts für Informations-, Gesundheits- und Medizinrecht (IGMR) an der Universität Bremen, und Mitglied im Vorstand der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID), Berlin.
E-Mail: kipker@uni-bremen.de

Dr. Sebastian Pape

Wissenschaftlicher Mitarbeiter des Lehrstuhls für Mobile Business & Multilateral Security an der Goethe-Universität Frankfurt und geschäftsführender Gesellschafter der Social Engineering Academy GmbH.[1]
E-Mail: sebastian.pape@m-chair.de

1 Foto: Petra Coddington

2 Background and Related Work

In this section, we first describe HATCH, the game we have investigated. In the second part of the section, we discuss related work.

2.1 HATCH

The serious game considered for our use case is HATCH [11, 12], which aims to improve the employees' understanding of SE. For our analysis, we briefly sketch how HATCH works: Each player is in the role of an attacker.

1. Each player draws a card from the deck of *human behavioral principles*, e. g. the "Need and Greed" principle.
2. Each player draws three cards from the deck of the *social engineering attack techniques*, e. g. phishing.
3. Each player develops an attack targeting one of the personas in the scenario based on the drawn cards.
4. Each player presents his/her attack to the group and the other members of the group discuss if the attack is feasible.
5. The players get points based on how viable their attack is and if the attack was compliant to the drawn cards. The player with the most points wins the game.
6. As debriefing, the perceived threats are discussed and the players reflect their attacks.

The game can be played either with an imaginary (virtual) scenario or a (realistic) scenario that reflects the real working environment. We describe both scenario types in the following.

Virtual Scenarios

Virtual scenarios are used when HATCH is used for training and awareness purposes [11]. These consist of a plan of a department or company (see Fig. 1) and for each of the employees shown in the plan there is a persona card that outlines the basic characteristics of the employee (see Fig. 2). The players' task now is to come up with an attack that is as plausible as possible on the basis of the drawn cards and that exploits the characteristics of the employees present in the game. The attack found is then evaluated for plausibility by the players.

Realistic Scenarios

The basic gameplay of HATCH with a realistic scenario [12] is the same as with a virtual scenario. However, virtual people are not used here, instead a plan of the real working environment is created and the players devise attacks on their colleagues. In doing so, they use their colleagues' existing knowledge of work processes, skills and preferences. Besides training and awareness raising, the result is a list of possible SE threats that can be used to improve work processes and security policies. The advantage over a threat analysis by experts is that the employees of a department or a company know the real work processes very well, so it is easier to train them in social engineering than to have experts study all work processes.

Fig. 1 | Scenario for an Energy Provider

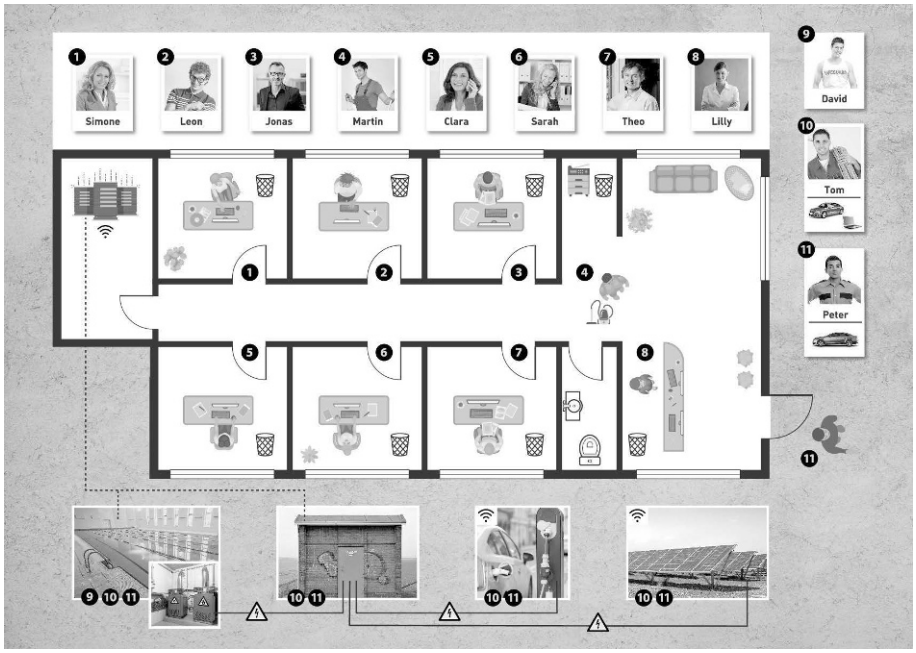
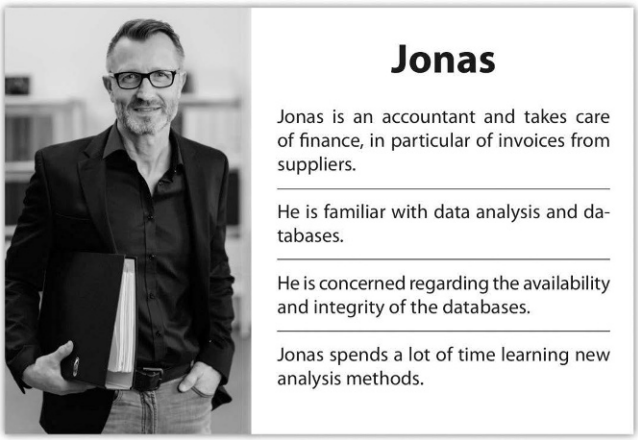


Fig. 2 | Persona Card for Jonas, an Accountant



2.2 Related Work

While there are reports on the use of serious games in the corporate sector [10], the body of literature specific to serious games aiming to raise awareness and allow security training is rather low. Regarding compliance and serious games, there is a lot of work, but only on using serious games to increase the compliance and not on the compliance of serious games. In the area of SE, most of the work is focused on SE penetration testing. [5] discusses the ethics of SE penetration testing, and [6] and [7] discuss SE penetration testing from a legal perspective towards labour law.

3 Legal Adequacy of HATCH

It is generally accepted that management has a legal obligation to maintain and operate IT security measures as part of the company's own compliance – this includes training employees with regard to social engineering attacks. The compliance obligation under IT security law can be derived from the most varied legal provisions and depending on the respective industry, generally from § 43 par. 1 German Limited Liability Companies Act (GmbHG) and § 93 par. 1 German Stock Corporation Act (AktG). Where, on the one hand, there are corporate obligations to implement an appropriate level of IT security, the question arises on the other hand as to whether and how the employee must tolerate associated measures and, if necessary, also participate in them. The conflict between freedom and security is updated here in the form of issues relating to labour law and also data protection law, as well as for corporate compliance and corporate governance. Especially for an SE game like HATCH, which requires the active participation of the individual employee, various legal problem areas therefore open up. A distinction must be made between the realistic and the virtual game scenario.

3.1 Realistic Scenarios

In HATCH's realistic scenario, the actors involved in the company play themselves out. A particular legal relevance for this case arises from the fact that the simulated SE attacks are aimed at real persons and their character traits. With regard to the question of the legal reasonableness for the individual employee, this must be evaluated in compliance with Art. 2 par. 1 in conjunction with Art. 1 par. 1 of the German Constitution ("Grundgesetz", GG), which prescribes the General Right of Personality ("APR"). The APR as a part of the German Constitutional Law has an influence on employment law, among other things, as an ancillary obligation of the employer under the employment contract in accordance with § 241 par. 2 of the German Civil Code ("Bürgerliches Gesetzbuch", BGB).

For the employer, on the other hand, the freedom of occupation resulting from Art. 12 of the GG and the associated protection of entrepreneurial interests, also based on the indirect third-party effect of the fundamental rights in the private-law relationship, is in dispute. In principle, the employer must protect the employee from unlawful interference with his or her personal rights within the scope of his or her obligations arising indirectly from the APR [13, BetrVG, p. 99, Rn. 106]. This also includes protection against potentially embarrassing measures that could have a negative impact on employees [6]. Particularly for an SE game in a realistic scenario, there are risks here in that employees feel exposed or that their company's appreciation is reduced, in that personal limits are exceeded by experiencing the game as a realistic situation and in that unforeseeable courses of the game occur in the group dynamics. It is questionable whether, in contrast to this and in the specific case, the company's interests in the execution of the game outweigh the risks and whether compliance with the obligation under German IT Security Law is therefore to be classified as more important than employee protection. The principle applies here that in sectors and industries that are particularly relevant to security, gaps in corporate security certainly have a high weight in the legal weighing of interests [9]. From this, it can be concluded that, as a rule, the fictitious creation of a potentially employee-damaging environment, in which the real personality of the employee is exposed to weak points relevant to SE, in companies that are not particularly exposed, can hardly be justified by the potentially increased learning success of an awareness raising measure to promote IT security. The situation would be different for Critical Infrastructures with a high risk of attack or for companies that have already been victims of SE incidents and for which a similar threat situation is also apparent for the future: Here, the increased need for awareness-raising measures as a factual connection with the protection of employees and their jobs could justify the feasibility of the measure, above all in the interest of the employee. A different legal assessment may also be required in the case of a threat analysis, as the methodology to be applied here requires that all weak points relevant to IT security in a company be determined, which therefore necessarily also includes the human factor.

3.2 Virtual Scenarios

In the virtual scenario of HATCH, the SE attacks are played out using fictional characters and the imaginary role assignments associated with them. As in the realistic scenario, a legal balancing between the personal interests of the employee and the operational and economic interests of the employer must be carried out. A stigmatization risk for the individual employee exists here to the extent that technical or content-related knowledge gaps with regard to SE threats reveal personal deficits vis-à-vis the employer. However, this can be counteracted by training measures on SE prevention carried out before the game. Clearly formulated communication and game rules also help to ensure that situations of potential hostility, harassment or discrimination during the course of the game can be effectively countered in advance. Last but not least, the choice of fictional characters also significantly reduces the degree of personality impairment, as the employee's inner structures and characteristics are not subject to play [10]. Likewise, in the fictious scenario HATCH offers a possibility to promote and support the personality development of the employees within the scope of the compulsory exercise of § 75 par. 2 German Works Constitution Act ("Betriebsverfassungsgesetz", BetrVG). As in the realistic scenario, the game also enables the employer to protect the company from SE attacks by improving the awareness of its employees. As a result, the employer's interests generally outweigh those of the employee in the virtual game operation, so that the use of HATCH represents a conceivable alternative to the classic training measures in this area.

4 Discussion

In this section, we discuss how the result of our legal analysis could be generalised. First, which parts of the results can be transferred to other games. Second, to which extend it is possible to generalize the results to other (European) countries.

4.1 Generalization to Other Games

All legal considerations are specific to HATCH. Thus, in general one would need to do a legal assessment for each game individually. However, some general conclusion can be drawn in particular from the comparison of the two different scenario types. The

analysis of the virtual scenario suggests that if within the serious game the employee's personal characteristics are not subject to play, the use of the serious game may be admissible if it is operated in a sufficient manner[2]. If the employee's personal characteristics are subject to play, as in the realistic scenario, a legal assessment is needed considering the aim of the game, i. e. threat analysis, the risk situation and exposure of the company to SE attacks to justify the feasibility of the game.

As a consequence, games which merely have a technical focus and do not consider human factors should be playable without the risk that employee's personal characteristics are subject to play. For example, *Elevation of Privileges* [14, 15] based on [16]'s threat modeling method should work out fine if players focus on the system, it's bugs and features as proposed in the game's instructions. Similar considerations hold for security related variants of planing poker [17] such as *Protection Poker* [18, 19], *Security Tactic Planning Poker (SToPPER)* [20].

Ctrl-Alt-Hack [21–23], another tabletop card game about white hat hacking, is based on game mechanics with virtual personas (hackers) and fulfilling the missions in the game does not rely on the players' or employees' characteristics. Therefore, even though it includes attacks based on social engineering, we would consider it comparable to the virtual scenario from HATCH, and thus conclude that there should be no major obstacles to play it within the context of a company.

We went through the descriptions of a couple of educational security games like *Cyber Security Requirements Education Game(SREG)* [24], *Cyber Security-Requirements Awareness Game (CSRAG)* [25], *Harbour Protection Table-Top Exercise (HPT2E)* [26, 27], *Operation Digital Chameleon* [28, 29], and *Operation Digital Snake* [30], but none of them was making use of players' or employees' characteristics. On the other hand, all of them are intended for awareness raising or education and none of them is intended for threat analysis. Thus, they would also be in the same line than the virtual scenario for hatch, which also makes them rather unproblematic game candidates.

4.2 Generalization to Other Countries

All legal considerations made in this context are subject to German law. This is due to the fact that in the EU, labour law is primarily regulated by the Member States themselves. Nevertheless, some general conclusions can also be drawn. For example, some of the legal considerations made in the legal analysis in this article are based on data protection regulations which are governed by EU law, in particular the EU GDPR. In many cases of EU law, as far as the processing of personal data is concerned, the focus is on balancing the interests of the data processor (in this case, the employer) and those whose personal data are processed (in this case, the employee). Thus, to the extent that operational IT security interests are weighed against individual data protection interests, the legal statements in this paper can certainly be generalised to a certain extent. In this respect, the legal weighing of interests carried out here can at least provide an indication of whether the use of HATCH in the operational context would also be legally permissible in other (European) countries.

5 Conclusion

While at a first glance, it seems to be legit to use a serious game for security training and awareness, our legal assessment showed large differences in the assessment of the two different scenarios. If the employee's personal characteristics are part of the game, care needs to be taken to not unnecessarily expose the personality of the employees. This even holds if the employees ask for or volunteer to play the scenario with a realistic environment, where they would suggest social engineering attacks on each other. On the other hand, if the employer can demonstrate a reasonable interest, i .e. if the game is used for threat analysis, the use of the game with a realistic scenario may be admissible.

As future work, the legal assessment should be extended for other countries such as the US or other member states of the EU.

Acknowledgement

This work was supported by European Union's Horizon 2020 research and innovation program from the project CyberSe-

2 e. g. taking care that no personal deficits vis-á-vis the employer are revealed and clearly formulated communication and game rules are applied.

c4Europe (grant agreement number: 830929) and from the project THREAT-ARREST (grant agreement number: 786890). We are thankful to Kristina Femmer for the graphical implementation of the scenario and the persona cards.

References

All urls have been last visited on February 12th, 2021.

[1] G. Bassett, C. D. Hylender, P. Langlois, A. Pinto, and S. Widup, *Data Breach Investigations Report*, (2020).

[2] P. Schaab, K. Beckers, and S. Pape, *A Systematic Gap Analysis of Social Engineering Defence Mechanisms Considering Social Psychology*, in *10th International Symposium on Human Aspects of Information Security & Assurance, HAISA 2016, Frankfurt, Germany, July 19-21, 2016, Proceedings*. (2016).

[3] P. Schaab, K. Beckers, and S. Pape, *Social Engineering Defence Mechanisms and Counteracting Training Strategies*, Information and Computer Security 25, 206 (2017).

[4] T. Dimkov, A. Van Cleeff, W. Pieters, and P. Hartel, *Two Methodologies for Physical Penetration Testing Using Social Engineering*, in *Proceedings of the 26th Annual Computer Security Applications Conference* (2010), pp. 399–408.

[5] J. M. Hatfield, *Virtuous Human Hacking: The Ethics of Social Engineering in Penetration-Testing*, Computers & Security 83, 354 (2019).

[6] J. Kuhn and A. Willemsen, *Arbeitsrechtliche Aspekte von Social Engineering Audits*, DER BETRIEB 02, 111 (2016).

[7] M. Zimmer and A. Helle, *Tests Mit Tücke – Arbeitsrechtliche Anforderungen an Social Engineering Tests*, Betriebs-Berater 21/2016, 1269 (2016).

[8] S. Stahl, *Beyond Information Security Awareness Training: It's Time to Change the Culture*, Information Security Management Handbook, Volume 3 3, 285 (2006).

[9] M. Bada, A. M. Sasse, and J. R. C. Nurse, *Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?*, CoRR abs/1901.02672, (2019).

[10] L. Donovan and P. Lead, *The Use of Serious Games in the Corporate Sector*, A State of the Art Report. Learnovate Centre (December 2012) (2012).

[11] K. Beckers, S. Pape, and V. Fries, *HATCH: Hack and Trick Capricious Humans – a Serious Game on Social Engineering*, in *Proceedings of the 2016 British HCI Conference, Bournemouth, United Kingdom, July 11-15, 2016* (2016).

[12] K. Beckers and S. Pape, *A Serious Game for Eliciting Social Engineering Security Requirements*, in *Proceedings of the 24th IEEE International Conference on Requirements Engineering* (IEEE Computer Society, 2016).

[13] Kreutz, *GK-BetrVG, Bd. 2*, 10th ed. (2014).

[14] A. Shostack, Elevation of Privilege: Drawing Developers into Threat Modeling, Microsoft, 2012.

[15] A. Shostack, *Elevation of Privilege: Drawing Developers into Threat Modeling*, in *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3gse 14)* (USENIX Association, San Diego, CA, 2014).

[16] A. Shostack, *Threat Modeling: Designing for Security*, 1st ed. (John Wiley & Sons Inc., 2014).

[17] K. Moløkken-Østvold, N. C. Haugen, and H. C. Benestad, *Using Planning Poker for Combining Expert Estimates in Software Projects*, Journal of Systems and Software 81, 2106 (2008).

[18] L. Williams, M. Gegick, and A. Meneely, *Protection Poker: Structuring Software Security Risk Assessment and Knowledge Transfer*, in *Proceedings of International Symposium on Engineering Secure Software and Systems* (Springer, 2009), pp. 122–134.

[19] L. Williams, A. Meneely, and G. Shipley, *Protection Poker: The New Software Security "Game"*, Security Privacy, IEEE 8, 14 (2010).

[20] F. Osses, G. Márquez, C. Orellana, and H. Astudillo, *Towards the Selection of Security Tactics Based on Non-Functional Requirements: Security Tactic Planning Poker*, in *2017 36th International Conference of the Chilean Computer Science Society (SCCC)* (IEEE, 2017), pp. 1–8.

[21] T. Denning, T. Kohno, and A. Shostack, *Control-Alt-Hack: A Card Game for Computer Security Outreach and Education (Abstract Only)*, in *The 44th ACM Technical Symposium on Computer Science Education, SIGCSE '13, Denver, CO, USA, March 6-9, 2013* (2013), p. 729.

[22] T. Denning, A. Lerner, A. Shostack, and T. Kohno, *Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education*, in *2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013* (2013), pp. 915–928.

[23] T. Denning, A. Shostack, and T. Kohno, *Practical Lessons from Creating the Control-Alt-Hack Card Game and Research Challenges for Games in Education and Research*, in *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education, 3gse '14, San Diego, CA, USA, August 18, 2014.* (2014).

[24] A. Yasin, L. Liu, T. Li, J. Wang, and D. Zowghi, *Design and Preliminary Evaluation of a Cyber Security Requirements Education Game (SREG)*, Information and Software Technology (2017).

[25] A. Yasin, L. Liu, T. Li, R. Fatima, and W. Jianmin, *Improving Software Security Awareness Using a Serious Game*, IET Software (2018).

[26] R. Kessel and N. Gwatkin, *Harbour Protection Table-Top Exercise Hpt2e: Contextual Read Ahead.*, (2012).

[27] R. Kessel and N. Gwatkin, *Harbour Protection Table – Top Exercise Hpt2e 20 – 23 March 2012, La Spezia: Hpt2e Technologies and Platforms*, (2012).

[28] A. Rieb and U. Lechner, *Towards Operation Digital Chameleon*, in *CRITIS 2016 – the 11th International Conference on Critical Information Infrastructures Security (to Appear)*, edited by G. Havârneanu, R. Setola, H. Nassopoulos, and S. Wolthusen (Paris, 2016), pp. 1–6.

[29] A. Rieb and U. Lechner, *Operation Digital Chameleon – Towards an Open Cybersecurity Method*, in *Proceedings of the 12th International Symposium on Open Collaboration (OpenSym 2016)* (Berlin, 2016), pp. 1–10.

[30] A. Rieb, *KMA Homepage Article about Operation Digital Snake Game*, (2018).