Participatory Research with Schools
to Develop Serious Games for Information Security Awareness

Margit SCHOLL
Department Business, Computing, Law, Technical University of Applied Sciences (TUAS) Wildau
Wildau, 15745, Germany

Regina SCHUKTOMOW
Department Business, Computing, Law, Technical University of Applied Sciences (TUAS) Wildau
Wildau, 15745, Germany

ABSTRACT

Two different research projects developed by the TH Wildau on information security awareness—"Security" and "SecAware4-school"—are focused on sensitizing pupils to the issue of information security in everyday school life by means of experience-oriented scenarios geared to teaching awareness. At the same time, their teachers will be trained, and the parents kept informed about specific measures. The development of such learning scenarios took place in participative dialogue with creative workshops. The learning scenarios are based on the integration of three learning methods: Game-Based Learning, Accelerated Learning, and Authentic Learning. The article introduces the previous game-based learning scenarios for schools.

Keywords: Information security, Data protection, Awareness, Sensitization, Experience-oriented learning scenarios, Digital simulations, Game-Based Learning (GBL), Accelerated Learning (AccL), Authentic Learning (AuL), European Computer Driving Licence (ECDL), Information security officer, Youth security consulting.

1. INTRODUCTION

Digitization and the information technologies it is based on are now permeating our lives. At the same time, the risks associated with the possible misuse of sensitive and confidential data are increasing. The core values inherent to information security (IS) must be clearly laid out [2:13]: *confidentiality*, protection against the unauthorized disclosure and perusal of information; *integrity*, securing the correctness of information and the proper functioning of systems; and *availability*, the ability to access data, information, services, networks, and components at any time. Depending on the purposes for which the security is applied, it may be useful or legally necessary to implement other safeguards, such as *authenticity*—to ensure that a person, IT component, or application is actually who or what it claims to be [2:13]—or *non-repudiation* as a means to verify the dispatch or receipt of information such as e-mails. Vulnerabilities—i.e., gaps in a system's security—can make the system vulnerable to general threats and lead to concrete dangers [2:14]. Vulnerabilities may arise, for example, from product defects, faulty implementation, or incorrect use. People—be they production or software developers or "just" consumers—must become a more central focus in the process of IS sensitization [10] [36] [32] [34] [20] [4]. Since the threats can be technical (e.g., hacking) and/or interpersonal (e.g., social engineering), it is essential to raise people's awareness and improve their knowledge of the dangers associated with digitization and the relevant protection mechanisms needed for their private, school, and working lives. Education about information security cannot take place early enough.

The methodology in the two projects "Security"[1] and "SecAware4school"[2] is focused on a Game-Based Learning (GBL) approach, which is used to develop teaching and learning methods, in both analogue and digital form, on information security topics. This GBL approach is based on psychological findings from corporate-awareness research [13] [25] [12] and has already been successfully implemented in a previous research project (SecAware4job[3]). However, other research projects have had an influence on our procedures and activities: InterKomp 2.0,[4] IT-Sicherheit@KMU, TEDS,[5] and Skill Up.[6] The article introduces the previous game-based learning scenarios, while focusing on the target groups at school.

The structure of the paper is as follows: In the section 2, the six final learning scenarios of the project "Security" will be presented, although these represent only one aspect of the overall goal of this project, which was to attract more girls and young women to embark on a career as a security specialist. It is already in its final phase and will be successfully completed in December 2019. Section 3 presents the procedure in the second school project "SecAware4school," which started with an anonymous survey in schools to find out the major topics of interest. General information on the methodology in both projects as well as the ongoing development of the learning scenarios of "SecAware4school" is outlined in section 4. Broad insights into the development of the learning scenarios and awareness trainings in this project are offered in sections 5 and 6. Section 7 provides a brief summary and section 8 gives an outlook that goes beyond the focus on everyday school life. Acknowledgements and references are given in sections 9 and 10.

---

[1] https://www.security.wildau.biz/en.html. Accessed June 5, 2019
[2] https://secaware4school.wildau.biz/en/pages/page_project_ueber_uns/. Accessed June 5, 2019
[3] https://secaware4job.wildau.biz/index.html. Accessed June 5, 2019
[4] https://kmu-interkomp20.th-wildau.de/?page_id=356. Accessed June 5, 2019
[5] https://teds.wildau.biz. Accessed June 5, 2019
[6] http://skill-up-project.eu. Accessed June 5, 2019

2. INFORMATION SRECURITY AWARENESS IN EVERYDAY SCHOOL LIFE

As users of Internet services and social media, young people should be introduced to the careful handling of sensitive data in a playful, motivational way and develop their digital competence and technical understanding accordingly. Ultimately, the pupils should be self-reliant and capable of operating in the digitized world in a conscious manner. They should, for example, be able to independently recognize potential dangers on the Internet, assess risks, and take preventive protective measures. Experience should not be limited to the individual; instead it should lead to a closed loop in which knowledge is transferred and maintained among pupils.

Table 1 Game-based learning results in the project "Security" at the TH Wildau

The "Security" project developed six analogue game-based learning scenarios—which are described in brief with objectives and tasks in table 1—with a focus on pupils in grade 9:

- Security and safety on the move during school excursions
- Encryption principles
- Image acquisition and image-use rights
- Apps and the risks associated with them
- Phishing mails
- Password hacking.

These six analogue experience-oriented learning scenarios created by the gender-based project "Security" (see table 1) can be borrowed by schools after the project ends in December 2019.

3. SURVEY AND PARTICIPATIVE DIALOGUES TO IDENTIFY TOPICS

An anonymous survey was conducted online using Lama-Poll[7] from September 28 to December 3, 2018. Four pilot schools—the Humboldt Gymnasium in Berlin (HGB), the Rudolf-Virchow-Oberschule in Berlin (RVO), the Friedrich-Wilhelm-Gymnasium (FWG) in Königs Wusterhausen (KW), and the Friedrich-Schiller-Gymnasium (FSG) in KW—participated in the survey from the beginning. The fifth pilot school, the Dr.-Hans-Bredow-Oberschule (HBO) in KW, filled out the online survey late. Altogether the survey was accessed 1,821 times: it was filled out 827 times and completely filled out 768 times. This constitutes 42,2 percent of all participants completely filled out. Not all the questions in the online system were mandatory, so some questions could be skipped. As a result, some questions have a higher number of answers than others.

The survey consisted of a total of nine questions. The first questions were used to collect demographic data from the participating schools. 51,6 percent of all online respondents from the pilot schools took part in the survey at the HGB. The FWG contributed 30,2 percent of the respondents surveyed online. In third place came the RVO with 13,9 percent interviewed online of the total. The FSG is in fourth place with 3,6 percent of the total from all pilot schools. Due to the relatively short period of participation, the HBO came last among the participating pilot schools with 0.7 percent and is not included in comparative evaluations of the pilot schools for data protection reasons owing to the low number of participants. Based on their own audit, 63 percent pupils, 11 percent teachers, and 26 percent parents took part.

Further questions were:
- The warm-up question about secure passwords
- "Do you know how you can protect your own private sphere online?"
- "How often do you use images from the Internet—e.g., for presentations?"
- "Have you ever been the victim of data theft (e.g., was your log-in data stolen)?"
- "To what extent are you interested in the following topics?"
- "What other topics are you interested in?"

The topic of fake news is of similar interest to all respondents from the pilot schools (who find the issue very to moderately interesting). In corporate-awareness research, this online phenomenon has also become an ongoing issue, but its significance for the economy and the company's own working environment is still largely underestimated [24:19]. A current study with qualitative field research shows that disinformation is not a consequence of digital overload, which is why it is not enough simply to check the source of information [24:21] [35]. Rather, it is important to understand the principle of false reporting in the *context* of the institution and situation and to recognize one's own mechanisms for dealing with information. A sensitization measure that takes this into account "goes beyond the mere recognition of right and wrong—it demands self-reflection and digital prudence" [24:21].

4. CONTENT SUMMARY AND REVIEW OF CURRENT ACTIVITIES

The GBL, Accelerated Learning (AccL), and Authentic Learning (AuL) approaches are combined in order to achieve the stated goals. In addition to the varied and stimulating form of learning it offers [21], GBL enables students to look at a set goal and provide direct feedback [11]. The three different levels that are planned for the GBL scenarios are intended to help participants in their development process without demanding too much of them [7]. AccL, on the other hand, challenges students to go beyond passive perception and actively create knowledge [3] [23] [26] [6]. In this approach, the goal is for learners to internalize their competencies independently over the long term. The combination of the two methods is applied in the "SecAware4school" project in the form of experience-oriented learning scenarios in everyday school life through analogue and digital games that are both emotionalizing and motivating. According to Steve Revington,[8] AuL, in turn, focuses on the application of knowledge in real contexts and situations. The central aspect here is learning from experience, from real or simulated problems, and it enables the students to create a meaningful joint outcome. This is also necessary for team-based exchange on information security [30] and thus supports experiential learning in the scenarios.

For the two research projects "Security" and "SecAware4-school," various phases were defined in cyclical rather than classical terms. The survey in the initial phase related the objectives set out in the proposal for the research project to the questions and interests of all the target groups involved. In a further step, the information events were intended to offer details about the project to the classes that would actively participate in the course of the project in the experience-oriented learning scenarios and awareness trainings. This proved to be a very time-intensive activity, as in many cases the school classes could only be informed one by one. In other words, the complexity of organizing separate meetings to suit the individual school curricula often meant that

several dates were scheduled for the information sessions at each pilot school.

The "SecAware4school" project also includes lower-level (ca. grade 6) and higher-level (grade 11) classes, developing ten learning scenarios at three different levels of difficulty—a total of thirty analogue and digital learning scenarios. Examples are shown in table 2 below. While younger pupils benefit in this way from the experience of older pupils, the older ones consolidate their knowledge by subsequently providing independent moderation and support for the learning scenarios in their school. The qualification of the pupils as so-called youth security advisors is thus another important cornerstone of the project "SecAware4school."

Table 2 Game-based learning results in the project "Sec-Aware4school" at the TH Wildau

The background to the development of the learning scenarios shown in table 2 is described in more detail in section 5. GBL is often described as an entertaining and motivating form of learning [21] using game elements (e.g., points,

rankings, scores, levels, rewards, progress indicators) [18] [9] [33]. In our own school example, the process of coming up with a group name together and the team-based exchange that was required to solve the tasks in each learning station strengthened the group dynamic and gave the participants a stronger sense of solidarity and team spirit. The unofficial competition motivated all groups to successfully complete the GBL scenarios. As a result, we do not end up with any loser groups, only winners, because in the final analysis each group learns something new about information security from the experience-oriented learning stations, which is crucial in a play-based awareness-learning scenario.

5. DEVELOPMENT OF THE LEARNING SCENARIOS

In the development of the learning scenarios in the project, there are several factors to be taken into consideration: each of the methodological approaches used GBL, AccL, and AuL, which rely on motivating people to learn through playing in gamification infrastructures. An important role is played by the presentation of the game, which should have the appropriate character and mechanics to enable the didactic material to be conveyed [14]. In addition, consideration must be given to the target audience and age group, the topicality of the facts, new technical advances, and the interests of the target subjects.

The project "SecAware4school" defines three different age groups according to the level of difficulty: Grades 6 and 7; grades 8 and 9; grades 10 and 11. The experience-based learning scenarios must therefore be developed at three different levels of difficulty. The age of the pupils and any prior knowledge they have must be taken into account.

In order to be able to make successful use of game-based approaches to teach sixth- to eleventh-graders about information security, it is important to know the target groups, involve teachers and parents, and regularly evaluate the results. For the research project, information sessions in the participating classes were carried out in advance, and information was provided to the teachers and legal guardians. By means of an online survey, it has been possible to filter out the interests of the participants on the subject of information security and to develop analogue game-based learning scenarios in response to topics of interest and real contexts.

The varied and stimulating form of learning [21] allows participants to exchange knowledge in the form of discussion and feedback [11]. In the project "SecAware4school," ten learning scenarios were designed according to the interests of the respondents. The development of three learning scenarios in more detail is presented here.

Rapid Guessing (see table 2) is a learning scenario that sets out to familiarize learners with IS terminology and present new terms. The original idea was to compete in teams and speed-guess concepts against the clock. There are three attempts per question. As a punitive measure, a camera made of Lego bricks was set up a piece at a time after every failed attempt. After three failed attempts, the camera is complete-

ly set up, and the team is caught on camera. In Germany, this happens if you drive too fast. The construction of the camera symbolizes fast, thoughtless, and misjudged behavior on the part of the participants. The moral here is that you should act quickly but in a considered way. Extensive testing of this learning scenario showed that the pupils were interested in these questions and were especially keen to defeat the opposing team. The Lego camera turned out to be a nice toy but not necessarily applicable to the learning scenario. It has been omitted in the latest version. After using the learning scenario in the USA, the game's original name ("Speed Camera") turned out to be incomprehensible. As a result, the learning scenario was renamed "Information Security: Rapid Guessing." The design of the questionnaires is now in its final version. The learning scenario contains thirty-six question cards, each at three levels of difficulty. The levels of difficulty are indicated by three different symbols and color gradations on the question cards. All of the question cards are laminated in A5 format. Sustainability is taken into consideration inasmuch as all the cards can be wiped clean and reused.

Behavior in Social Networks is a learning scenario that came out of the creative workshops with pupils. Social media was identified as problematic by the participating pupils. The idea of the learning scenario is to sensitize users to safe behavior on social media. The learning scenario is interactive. It includes questions to enable certain terms and activities relating to information security and social media to be guessed, explained, and executed. Pupils have the option of playing against each other in teams. The game leaflet shows images representing different activities. For each field, there is a specific task that the team has to solve to get ahead. The tasks are based, for example, on questions about personal behavior on social media. It is important to reflect on one's own behavior and to draw conclusions. Other tasks include prompts, such as "Choose privacy settings for your account." Tasks of this kind motivate pupils to think about correct behavior on social media and help them make the right decisions. The learning scenario has been designed for about 20 minutes of playing time. At the request of the pupils, the learning scenario was also extended to about 60 minutes of playing time. The process of sensitizing learners to their behavior on social media involves two components: personal reflection and group exchange.

The third analogue learning scenario of table 2 described here is ***Hazards and Protective Measures***. This learning scenario deals with the knowledge of IS threats and safeguards. The game pad shows several islands of different sizes in the ocean. The players must answer questions, recognize the dangers, and find appropriate protective measures to ride from wave to wave and discover the islands. The vast ocean symbolizes the Internet and the dangers it hides. For each of these dangers, a solution and protective measure must be found. Only with the correct protective measure is it possible to discover parts of the islands. The sensitization derives from questions drawn from everyday (school) life and examples for which there is often no clear solution. The awareness of information security is stimulated in this learning scenario by connecting everyday Internet topics with a haptic game.

All ten learning scenarios in the "SecAware4school" project are systematically thought out and coordinated with the three levels of difficulty. The development of the learning scenarios involves an intense process of testing, revision, and evaluation conducted with the schools, coupled with careful consideration of the criteria applied.

6. THE AWARENESS TRAINING

Awareness training (AT) raises learners' awareness of information security and its critical importance. Everyday situations such as *shoulder surfing, bullying at school, disclosure of personal information on social media*, etc. are realistically illustrated by GBL scenarios. The AT is to be understood as a game-based, informal training, which stimulates participants' awareness of information security, encouraging them to think about situations from everyday life and to exchange ideas and experiences, while practicing and sustainably internalizing protective measures.

The importance of the AT is that pupils can expand their knowledge through appropriate measures—haptic analogue and GBL scenarios—and playfully learn to develop an awareness of information security, which can then be implemented. The AT makes it possible to sensitize participants who are interested in the subject of information security and thus reaches a wider group of people (teachers and caregivers). The design of the AT allows each participant to comment and ask questions. The learning scenarios that are played out in the AT form a basis for discussion and exchange. Each learning scenario is adapted to the age group through three levels of difficulty.

Practice shows that students provide many examples of individual analogue and digital learning scenarios. This confirms the intention of the particular method. The AT is a non-standard teaching method involving participating pilot schools and is unlike conventional frontal teaching. Cooperative learning has an effective structure based on three elements: reflection, exchange, and imagination [8] [19]. Pupils are encouraged to reflect on their own experiences and to draw parallels to everyday situations, to exchange ideas within the group and to work together to come up with solutions and present them. For this reason, pupils show more interest in the individual analogue learning stations. This leads to stimulating discussions and an exchange of content, offering a number of advantages: it promotes the ability to communicate and cooperate, creates a link to real everyday problems, and reduces the complexity of the challenges involved to learnable content. At the same time, AT is used as an opportunity to try out and, if necessary, further develop and adapt the experience-based scenarios.

It is important to participate in the AT before the first creative workshop and before certain learning scenarios (including new pilot scenarios). In this way, participants can more easily accept the role of moderators and take this into account in the creative workshop. The AT take different forms in different school contexts.

A classroom AT lasts about 90 minutes because of the standard timetable in German schools. During this time, participants are sensitized one after another through four to six learning scenarios on different topics relating to information security. At the beginning of the AT, the class is divided into groups. The individual groups of three to six participants per class go through the various learning stations set up in advance and change stations after 15 to 20 minutes. The learning scenarios are designed for short-term play and provide room for discussion during the learning station. The discussions and explanations within the group reinforce the content of the learning scenario, allowing participants to gain practice as moderators of the learning station at the same time.

Pupils in the Awareness Training are particularly interested in learning stations that are designed to be more interactive and colorful. In all learning scenarios, the participants want to touch and play with the materials. This observation validates the project and its aim—to teach the subject matter of information security to pupils in a playful way. The learning effect among pupils can be observed in the AT, when participants explain each other's terms or reflect on their own experience based on everyday situations.

Pupils are free to select and organize their groups as they wish. The consequence of this is that possible communication disruptions in the group can be avoided from the outset if pupils are allowed to choose their own work group.

The different grade levels and repeated playing of the learning scenarios allow the three difficulty levels to be assessed more effectively and the learning scenarios adapted. In the interests of quality assurance and evaluation, feedback forms for individual learning stations are filled out by the participants and possible suggestions are noted.

7. SUMMARY

The results of the survey, the information events, and the prototypes in "SecAware4school" as well as the final versions of the learning scenarios in "Security" confirmed the assumption that sensitization and training are needed on the topic of information security in everyday school life. In schools, too, there is a gap between individual pupils' knowledge of particular aspects of information security and their specific behavior.

Following on from this, after creative workshops in both projects, the new game-based learning and teaching scenarios on selected topics gleaned from respondents in the project "SecAware4school" will be developed at three levels of difficulty appropriate to grades 6, 9, and 11. In order to further sensitize participants, further creative workshops will be offered and carried out in the future to evaluate the analogue and digital scenarios that have been developed.

In addition, pupils will be trained as security advisors and will be able to complete the ECDL "IT Security" certification. Teachers will be given the tools to support them, and the necessary knowledge will be imparted. ECDL certification will also be facilitated and one teacher from each pilot

school will have the opportunity to complete further training at no cost to become an information security officer. This will be followed by a certification exam. In addition, instructions and recommendations are provided that are specially tailored to parents. Here too, it is hoped that the knowledge acquired will be passed on through parents' evenings and similar forms of social interaction between parents and between parents, pupils, and teachers. The project "SecAware4school" will end in August 2020.

8. OUTLOOK BEYOND SCHOOLS

The scientific knowledge gained from the project to increase information security awareness is by no means limited to schools. Rather, it is in general necessary for companies and public administrations to continuously sensitize employees to the requirements of information security and data protection in the first step and then to train them according to their specific usage patterns. Adults should also be introduced to the topics in an emotional way if sensibility is to be successful [28]. For this to succeed, the important topics should be worked on in a game-based manner in the context of the specific field and the specific terms.

In addition, it is important for the whole population in a democracy to raise awareness of information security and data protection: to reach people's attention without falling into actionism and xenophobia. And finally, special attention must be paid to public digitization projects: no digitization without information security and no information security without awareness [27] [28] [29].

Digitization is thus having an influence on the work of employees and managers, on collaborative processes, and on the social structure of work as well as on change and learning processes [15]. Digitization offers the individual hitherto undreamt-of new opportunities. The ability to handle data independently is subjectivizing the way people search for information and the way information is used [15]. However, the path to becoming a "smart worker" requires the training and development of new "e-competences" [16] [17] [31], which go beyond mere technical skills.

Studies in Germany show that the specific knowledge required for e-government to function is not adequately incorporated into the educational system, either in university courses or in advanced training programs [22]. The educational landscape in e-government is highly fragmented [5]. Thus, digitization must also be coupled with education and the development of appropriate competencies across the board.

The current study "E-Government Monitor" and the "D21 Digital Index" show that Internet usage in Germany is shifting more and more to mobile devices [1]. However access to digital government services develops, additional hardware is needed, and this remains one of the main barriers to use. In future, governmental applications in Germany must be more responsive to everyday usage habits by the public, and, to that end, people also need to be educated about technical security settings. Moreover, sensitization measures to increase information security awareness and trainings in advanced skills and abilities are needed to develop broader competences that go beyond mere technical skills.

10. REFERENCES

[1] C. Akkaya, and H. Krcmar, "E-Government in Deutschland: Es ist noch viel Potential vorhanden", **AWV**-Informationen. Foreword, p. 4, 2019. https://initiatived21.de/publikationen/egovernment-monitor-2019/. Accessed: October 28, 2019.

[2] BAköV, Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern (Ed.), **Handbuch IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung**, Version 5.0, 2016.

[3] A. Bandura. "Social-learning theory of identificatory processes", **Handbook of socialization theory and research (213)**, 1969, p. 262.

[4] M. Beyer, S. Ahmed, K. Doerlemann, S. Arnell, S. Parkin, A. Sasse, and N. Passingham. "Awareness is only the first step. A framework for progressive engagement of staff in cyber security", Hewlett Packard, Business white paper, 2016.

[5] J. Becker, V. Greger, O. Heger, K. Jahn, H. Krcmar, H. Müller, B. Niehaves, N. Ogonek, M. Räckers, T. Schuppan, and R. Zepic, „E-Government-Kompetenz". Studie im Auftrag des IT-Planungsrats. Berlin/München/Münster/Siegen 2016.

[6] D. Boyd, "Effective teaching in accelerated learning programs", **Adult Learning**, 15 (1-2), 2004, pp. 40-43.

[7] D. Bressler, and A. Bodzin, "A Mixed Methods Assessment of Students' Flow Experiences During a Mobile Augmented Reality Science Game", **Journal of Computer Assisted Learning**, 29(6), pp. 505-517, 2013.

[8] L. Brüning, and T. Saum, "Individuelle Förderung durch Kooperatives Lernen". In (I. Kunze, and C. Solzbacher, Eds.) **Individuelle Förderung in der Sekundarstufe I und II**, Baltmannsweiler, 2008, pp. 83-91.

[9] D. Codish, and G. Ravid, "Gender Moderation in Gamification: Does One Size Fit All?", **Proceedings of the 50th Hawaii International Conference on System Sciences**, 2017, pp. 2006-2015.

[10] M.J. Dark, "Security Education, Training and Awareness from a Human Performance Technology Point of View". In (M.E. Whitman, and H.J. Mattord, Eds.): **Readings and Cases in Management of Information**

Security, Course Technology, Mason, 2006, pp. 86-104.

[11] X. Fang, J. Zhang, and S. Chan, "Development of an Instrument for Studying Flow in Computer Game Play", **International Journal of Human-Computer Interaction**, 29(7), 2013, pp. 456-47.

[12] A. Haucke, and D. Pokoyski, "Mea culpa - Schuld, Scham und Opferrolle bei Social Engineering", **kes**, 1, 2018, pp. 6-8.

[13] M. Helisch, and D. Pokoyski (Eds.), **Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung**. Wiesbaden, Vieweg + Teubner, 2009.

[14] M. Herzog, J. Sieck, & C. Kiefer "Spielbasiertes Lernen mit nutzergenerierten Inhalten". In (K. Rebensburg, and N. Apostolopoulos, Eds.): **Grundlagen Multimedialen Lehrens und Lernens**, 2008, pp. 175-184.

[15] H. Hill, "Führung in digitalisierten Arbeitswelten", **VM Verwaltung & Management,** *22*(5), 2016, pp. 241-249.

[16] H. Hill, „E-Kompetenzen". In: (B. Blanke, et al., Eds.): **Handbuch zur Verwaltungsreform**, Springer VS, 4. Aufl., 2011, pp. 385-392.

[17] S. Hunnius, „Kompetenzentwicklung im Rahmen von eGovernment". In (H. Hill, Ed.): **E-Transformation**, Baden-Baden/Nomos, 2014, pp. 209-219.

[18] K. Huotari, and J. Hamari, "A Definition for Gamification: Anchoring Gamification in the Service Marketing Literature", **Electronic Markets**, 27 (1), 2016, pp. 21-31.

[19] S. Kagan, **Cooperative Learning. San Clemente**, 1992, pp. 2-11.

[20] E.B. Kim, "Recommendations for information security awareness training for college students", **Information Management & Computer Security**, 22 (1), 2014, pp. 115-126.

[21] S. Linek, and D. Albert, "Game-based Learning: Gender-specific Aspects of Parasocial Interaction and Identification", **Proceedings of the International Technology, Education and Development Conference (INTED)**, 2009.

[22] D. Lück-Schneider, and T. Schuppan, "Gestaltungskompetenzen für die Öffentliche Verwaltung im digitalen Zeitalter", **VM Verwaltung & Management**, *23*(5), 2017, pp. 236-244.

[23] M. Mataric, "Reward functions for accelerated learning", **Machine Learning Proceedings**, 1994, pp. 181-189.

[24] I. Matas, and D. Pokoyski, „Von der Ente zur End-Täuschung", **kes** 5, 2018, pp. 19-23.

[25] D. Pokoyski, „Security Awareness: Von der Oldschool in die Next Generation – eine Einführung". In (M. Helisch, and D. Pokoyski, Eds.): **Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung**, Wiesbaden, Vieweg+Teubner, 2009, pp. 1-8.

[26] C. Rose, and M. Nicholl, **Accelerated learning for the 21st century: The six-step plan to unlock your master-mind**. Dell Books, 1998.

[27] M. Scholl, "Awareness in Information Security", **Journal on Systemics, Cybernetics and Informatics (JSCI)**, 16 (4), 2018, pp. 80-89. http://www.iiisci.org/journal/sci/FullText.asp?var=&id=IP059LL18. Accessed: October 28, 2019.

[28] M. Scholl, "Play the Game!" **Journal on Systemics, Cybernetics and Informatics (JSCI)**, 16 (3), 2018, pp. 32-35. http://www.iiisci.org/journal/sci/FullText.asp?var=&id=IP048LL18. Accessed: October 28, 2019.

[29] M. Scholl, "Information Security Awareness in Public Administrations". In (Ubaldo Comite, Ed.): **Public Management and Administration.** InTechOpen. Open Access, 2018, pp. 1-30. https://www.intechopen.com/books/public-management-and-administration/information-security-awareness-in-public-administrations. Accessed: October 28, 2019.

[30] M. Scholl, F. Fuhrmann, and D. Pokoyski, "Information security awareness 3.0 for job beginners". In: (J.E. Varajão, M.M. Cruz-Cunha, R. Martinho, R. Rijo, N. Bjørn-Andersen, R. Turner, and D. Alves, (Eds.): **Proceedings of the Conference on ENTERprise Information Systems (CENTERIS)**, 2016, pp. 433-436, 2016.

[31] T. Schuppan, "Neue Kompetenzanforderungen für (vernetztes) E-Government", **VM Verwaltung & Management**, 15(3), 2009, pp. 126-135.

[32] A.N. Singh, A. Picot, J. Kranz, M.P. Cupta, and A. Ojha, "Information security management (ism) practices: Lessons from select cases from India and Germany", **Global Journal of Flexible Systems Management**, 14 (4), 2013, pp. 225-239.

[33] M. Silic, and A. Back, "Impact of Gamification on User's Knowledge-Sharing Practices: Relationships between Work Motivation, Performance Expectancy and Work Engagement", **Proceedings of the 50th Hawaii International Conference on System Sciences**, 2017, pp. 1308-1317.

[34] M. Styles, "Constructing Positive Influences for User Security Decisions to Counter Corporate or State Sponsored Computer Espionage Threats". In (L. Marinos, and I. Askoxylakis, Eds.): **HAS 2013, Lecture Notes in Computer Science**, Vol. 8030, Berlin/Heidelberg, Springer, 2013, pp. 197-206.

[35] TAKE AWARE EVENTS (Ed.): Von der Ente zur End-Täuschung. Studie, veröffentlicht anlässlich der 2. Social Engineering-Konferenz BLUFF CITY 2018 in Köln, 2018.

[36] M. Workman, "Gaining Access with Social Engineering: An Empirical Study of the Threat", **Information Systems Security**, 16 (6), 2007, pp. 315-331.