Work in Progress – Brick by Brick: Using a Structured Building Blocks Method to Engage Participants and Collect IT Security Insights

Uta Menges[1(✉)], Jonas Hielscher[2], Annette Kluge[1], and M. Angela Sasse[2]

[1] Faculty of Psychology, Ruhr-University Bochum, Bochum, Germany
{uta.menges,annette.kluge}@ruhr-uni-bochum.de
[2] Ruhr-University Bochum, Horst-Görtz-Institute of IT-Security, Bochum, Germany
{jonas.hielscher,mangela.Sasse}@ruhr-uni-bochum.de

Abstract. Qualitative research methods from psychology and social sciences are feasible tools to gain deep understandings of people's IT security behaviour, knowledge, sentiments and routines. One of these methods, individuals' own expression in the form of drawings, sketches, charts and other visual representations, are important to understand deep knowledge and mental models. However, those methods are, to some degree, dependent on the *artistic skills* of the participants – those that are not confident in their handwriting and drawing might engage less. Building Blocks (sets of interlocking bricks) require less artistic ability and it is very easy to engage participants – they can *just start building*. IT security researchers already used such bricks to model participants thoughts, but in heterogeneous ways. We on the other hand used the LEGO© SERIOUS PLAY© (LSP) method – that describes a structured way on how to build models – to conduct four workshops (with $n = 48$ participants in total), in which the participants were asked to build multiple models of everyday IT security in different contexts. We performed a first initial coding of the pictures we took during the workshops. In this paper we report our research method, what we did to improve the workshops and data collection and what we learned so far by using LSP.

Keywords: Building Blocks Workshop · Building Blocks in IT-Security · Qualitative Research Methods · Human-Centred Security · Security Workshops

1 Introduction

To collect and analyse knowledge and to understand the mental models of people in IT security, researchers often use well established methods from social science and psychology like interviews [20], diary studies [8], questionnaires [11], interactive group sessions [1], or even ethnographic observations in the field [14]. Those

M. Mehrnezhad and S. Parkin (Eds.): STAST 2022, LNCS 13855, pp. 134–145, 2025.
https://doi.org/10.1007/978-3-031-83072-3_8

methods have been established for decades but they do not necessarily encourage participants to fully engage in the research process. Here, more interactive and game-based methods come into play. LEGO© SERIOUS PLAY© (LSP) is used in different areas and for diverse purposes, such as individual coaching or in an organisational context to promote team building or to develop the corporate culture [13]. It defines a strict way of using interlocking bricks to collect thoughts and knowledge of participants. The advantage over more traditional methods, like drawing on boards or creating mind maps, is the low hurdle for active participation.

Interlocking bricks were in different forms already used in previous IT security studies, foremost by Coles-Kemp et al. [6,7,9,10]. The used building methods were heterogeneous (e.g. modelling by coloured bricks, modelling based on communication flows) as were the data collection and analysis methods (coding of participants explanations, video and audio transcripts of the workshops). In this paper we outline a new, more structured way of using those bricks for qualitative data collection: by using the LSP method that has a clear pathway and set of rules on how to build models and engage participants. We organised 4 independent in-person workshops with $n = 48$ participants, where we tasked the participants to build and explain models of bricks that describe different forms of everyday security. In a first attempt we coded the pictures we took of the models. In this paper we report our work-in-progress with this method and how far we came to answer our research question: *Q1: Can LSP be used to generate qualitative in-depth knowledge of IT security from workshop participants, to learn more about their everyday and work-related experiences and challenges in the context of IT security measure, and to activate them to approach and deal with the topic of IT security in a creative and cooperative way?*

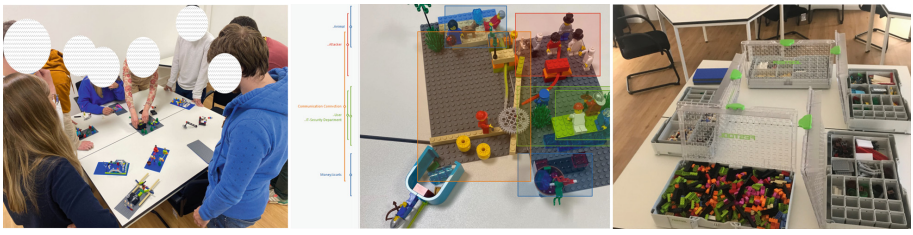

Fig. 1. (I) Participants discussing a group model, (II) the coding process in MaxQDA, (III) the LSP bricks arranged at a central table.

2 Related Work and Background

2.1 IT Security and Interlocking Bricks

Interlocking bricks were used in IT security research but we are the first to use the structured LSP method to collect qualitative data. Among other things, Coles-Kemp [6] developed a study approach based on "creative security", described

as a technique for participatory and playful engagement. A total of 55 security practitioners used kits of interlocking bricks to model technical, security and social impacts of IoT surveillance. Data analysis was based on handwritten annotations and photos of the models. Heath et al. [10] describe that these creative methods include participatory physical modelling for co-creation and representation. By having participants build models with coloured bricks, it is possible to model relevant issues into tangible scenes. In another study aimed at better understanding the conditions under which a smart city brings benefits to citizens, Heath et al. [9] again used a methodology based on creative safety. In addition to a standardised protocol, modelling components in the form of Lego were introduced. The study participants worked with interlocking bricks on scenarios and questions related to smart technologies. To address the difficulties that the human dimension is often glossed over in the context of cybersecurity studies and that different degrees of trust and solidarity lead to different perceptions of security, the authors [7] describe that a four-stage case study was undertaken. During the last two stages of this process, participants were given interlocking bricks selected so as to encode the movement of shared information and data, actors and devices.

2.2 LEGO© SERIOUS PLAY©

Hillmer describes the LSP method in his practice guide as a format that follows a clear process [13]. Participants have the opportunity to present their thoughts, concepts and feelings. At the heart of each process is a specific question or problem that relates to the topic of IT and information security in the workshops described here. Participants are "forced" to radically simplify in the LSP process, as they have to present complex models and concepts with the Bricks. This is especially helpful to prioritize and structure their own thoughts [13]. In this case, the simplification can primarily serve to make the seemingly abstract subject area of IT security more tangible. In addition, this method is suitable for a more reserved group member, since they share their models with the others. The flow state also plays a crucial role in connection with the LSP method. Zenk et al. [23], investigated whether LSP workshops lead to improved flow experience components as well as higher creative output than traditional meetings. Their results show that two components of the individual flow experience were significantly higher in LSP and the group experience component – continuous communication – was significantly lower, as expected. In terms of creative output, their study showed that LSP teams outperformed traditional meeting teams. A crucial role is assigned to the LSP moderator since, in addition to the tasks of preparation, follow-up and implementation, they also take on the role of support and mediator during the process. In the case of the workshops described here, the two authors assume this role. They have familiarised themselves with this method in advance, in particular through literature, and have prior experience in the counselling context with individuals and groups. At the beginning of the LSP process there is skill building, which serves to familiarise oneself with the

method and the material. This is followed by the main part, which consists of two required and a third optional building stage.

A few authors report how they used LSP for scientific purposes, but only to transfer knowledge. Mccusker [17], presents her findings on the LSP method in the educational domain. In order to identify hazardous situations in group models, exchange ideas and discuss alternative proposals, the LSP method of Cerezo-Narváez et al. [5] was used by student engineers as a tool for teaching industrial risk prevention skills. In their exploratory study, Kranawetleitner et al. [15] addressed the problem that the digitisation process in organisations is often dependent on the size of the organisation and the sector. The majority of the 21 participants did not know the LSP method and had never used it before. The playful element of LSP was adopted by the clear majority of participants. The method also helped employees become aware of the practical implications of digitalisation, with some even learning through their participation. Furthermore, Uslar and Hanna [21] discuss how they have applied the LSP method in the context of domain-specific requirements engineering in industrial projects. Similar to the authors of this article, Asprion et al. [2] approached the topic of cybersecurity using LSP and used the method to teach core topics of cybersecurity and resilience in higher education. The initial results of their study indicate that LSP has a positive impact on learning and increases student engagement.

3 Method

We conducted 4 workshops, where the in total $n = 48$ participants were asked to solve IT security tasks with the LSP method. We then did a first initial coding.

3.1 Workshops

All 4 workshops were embedded in other events. Workshop I, II and IV were part of lectures or seminars at our university. Workshop III was part of a security training event we co-organised with a large European industrial corporation with more than 25,000 employees where we are currently performing research about Human Centred IT security. The participants were informed beforehand about the LSP method and our intent to use the results for our research. The workshops differed from each other in the type of participants and in the tasks given to the participants (see also Table 1). The general structure was a short introduction by the researchers (also acting as moderators – or as they are called in LSP: *Facilitators*), followed by the task to build a (I) model of a tower or bridge, (II) an abstract model of an IT security concept (e.g. VPN, phishing, ransomware, firewall), (III) models of workshop specific tasks – which were all created around the topic of **everyday IT security the participants faced themselves or were in a given case study** – that are end-user routines like authentication processes, VPN usage but also the communication with the IT security department or the prevention of tailgating. We did not define what we

understood as IT security and left it open to the interpretation of the participants. With this task we aimed to get insights into the mental models that participants have about the interplay of security (department) and users, e.g. whether they would model *security friction*? The participants created the models individually, in pairs, or in bigger groups. We used 1,5 full sets of LSP bricks[1] that were arranged at a central table all participants had access to.

During each workshop we collected three types of data: (I) We took pictures of every model the participants built. (II) We took notes on the participants' explanations of their models. (III) We asked the participants for feedback in a short online survey directly after three of the workshops. From the second workshop on the participants also had to explain their models on small cards, which we included in the data collection.

3.2 Coding

Our coding process is still in progress. So far we have used MaxQDA to code the pictures we took of the models built during the main tasks, following [19]. We have also used MaxQDA to partially code the participants' notes as well as our own and the pictures of the warm-up tasks. We deductively defined the following categories of codes: (I) persons, (II) everyday security, (III) structures and (IV) technologies. The data was then inductively coded by two researchers (two workshops per researcher). We are planning to rerun our coding process and try to follow Kuckartz's [16] approach, which is more collaboratively on the one hand (including the calculation of the intercoder reliability), and on the other hand we then will create code-sets that span all the workshops. We have not done that so far, as we wanted to focus first on the improvement of the workshops and the respective data collection between the workshops. In order to evaluate the workshops and improve them for the following workshops, we used the evaluations and feedback from the online surveys and took the comments – if possible – into account in the design and implementation.

3.3 Ethics and Data Privacy

Our institution does not yet have an institutional review board (IRB) nor an ethics review board (ERB) that we could consult for our study. We got consent from all participants to take pictures of their models and use them in our research. In the first workshop we took pictures of the participants themselves, for what we got their consent (see Fig. 1). Except these pictures, no personal data of the participants was collected at any time.

3.4 Limitations

Our study has several limitations. Foremost, we report work in progress, especially regarding the coding strategy, therefore all results should be taken with

[1] Each consisting of thousands of interlocking bricks.

care. The tasks were changed slightly between each workshop to match the participants' context, which reduces the comparability between the results. The time we had available per workshop made amendments to the LSP method necessary, therefore we reduced the warm-up phase to two tasks each. Our participant sample is in no way representative and hence, generalisation of our results is not possible. Within the framework of the evaluation, it would have been desirable to also go into conversations as well as discussions of the participants during the individual construction phases. However, since we as facilitators had to respond to the participants' questions during the construction phases, accompany the process and prepare the other phases, it was not possible to include this aspect in the documentation. Furthermore, we did not want to create an impression of control and and evaluation of the discussions among the participants.

4 Results

4.1 Demographics

We did not ask the participants for demographic data. What we can report, based on the context of the workshops, is that all participants were less than 35 years of age, more than 1/3 were female, all were German speaking and all had a connection to IT security (either due to their education or due to their interests). The educational backgrounds of the participants are tied to the respective workshops (see also Table 1).

4.2 Workshops

All 4 workshops conducted have a common basic structure: The bricks were arranged on a central table, warm-up tasks had to be solved by participants individually and in teams and the main tasks were designed around the topic of everyday security (see also Table 1). We selected the main tasks in each workshop according to the background of the event and prior knowledge. In the following we report the results drawn from our coding process of the main-task model. The participants' explanations of their models and/ or individual bricks are summarised by us in a descriptive way based on our notes.

Workshop 1. The first workshop was conducted in April 2022. It was part of a graduate school program. The $n_1 = 8$ participants were PhD students with interdisciplinary research areas related to IT security topics. The workshop lasted 90 min. In total five building tasks had to be completed, with the main task being: *Build a model that shows how IT security should work in your everyday life.* Despite this positive framing, some participants showed how IT security does not work for them: crumbling (fire-)walls, multiple different path for attackers to reach assets, no help by IT security experts (modelled as an user left alone in the rain) and unintended data leaks. IT security was exclusively understood as a technique to protect either communication channels (by tunnelling them or

placing guards at the entrance points) or assets (data or money). Attackers were in all cases modelled as outsiders that try to circumvent the security measures. One participant showed that IT security is a bottomless pit at the moment: just throwing more money on security will not improve the level of security. In two cases the users were shown on lonely islands together with their assets, where attackers will not reach them.

Workshop 2. The second workshop was conducted in May 2022 with $n_2 = 19$ IT security master's students as part of a lecture series. In the lecture series the students worked with a case study in a hospital setting. We used this case study to model the primary task of the workshop: *Build a model that shows how IT security does work/ does not work in the hospital.* Firewalls and gates were the most frequently used concepts appearing on 6 and 7 occasions, respectively. In all models where defenders were represented the defence was exclusively represented as a task for security specialist, never for employees. On the other hand, in 7 models the employees (doctors and nurses) circumvented security in some regard (password sharing, RFID card sharing, single account usage). None of the models described that this might be the case due to task overload, as was described in the case study – a typical form of an exhausted compliance budget [3]. Only once was the blame put on the security staff when technical problems with the hospital IT were displayed. Overall, participants exclusively chose to show problems with IT security routines in the hospital, despite the task description being open to positive examples as well. Attackers were in all cases modelled as outsiders (behind walls or in front of gates) that would use tools to infiltrate the hospital. Only in some cases did the models show the intention of the attackers (e.g., to disturb a surgery or steal assets – in form of money bricks). In one case, the attacker was modelled as a spy, overseeing the hospital routine from a "watchtower". In another case, the hospital's CISO was sitting on a throne and was unreachable for other hospital employees. And in a third case, the IT department was stealing time from employees through useless technological innovations.

Table 1. The 4 workshops differ in their context and in the models the participants had to build.

	Workshop 1	**Workshop 2**	**Workshop 3**	**Workshop 4**
n	8	19	17	4
Setting	Graduate school	Lecture	Inter-Organisation	Seminar
Participants	PhD researchers (different disciplines)	IT security MA students	multidisciplinary apprentices	Psychology BA Students
Duration	1.5h	1.5h	1h	3h
Content	IT security in every day life	IT security in a case study (hospital)	IT security in the participants organisation	IT security at work and/or at university

Workshop 3. The third workshop was also conducted in May 2022. It was organised within a 3-day, in-person workshop hosted by a German corporation that partners with us. At this workshop apprentices were educated on different aspects of corporate information security. $n_3 = 17$ apprentices participated in our workshop. The group was divided into two groups. Both groups participated in our workshop one after another independently. Both sessions lasted 60 min. The task considered for this evaluation was the following: *Build a model of IT and information security as it should work in your everyday working life.* The participants focused their models on generic IT security measures, but also on specific measures including two-factor authentication, passwords, password managers, virus scanners, firewalls and face recognition. In addition, the coding process revealed that they built different types of data worth protecting. IT security staff and attackers were also frequently represented in the models. A participant in the second group tried to show, through his model, that IT security departments that are slow in their responses lead to delayed learning and working in the organisation. Another participant from group one presented as desirable in his model that IT security should be a simple and linear means to achieve the goal of "secure behaviour". In his model, he used several figures to show that this goal could only be achieved as a group. In another model, it was impressively shown how employees stand waiting behind the wall (firewall) and neither know nor understand what is actually happening in the context of IT security.

Workshop 4. The fourth and last workshop was held with $n_4 = 4$ psychology students as part of a seminar in which they dealt with the topic of IT security in organisations in the beginning of July 2022. The LSP workshop took about three hours. The main task of a total of five consisted of: *Build a model that shows how IT security should work in your everyday work/ study life.* These students dealt with the topic of IT security in an organisational context for the first time. Among other things, they were familiarised with the security learning curve [12] as part of a theoretical introduction. None of the participants had previously been involved with LSP or gone through an LSP workshop. The coding process showed that the participants mainly chose IT security staff, employees, users and animals (for attackers or protection) for their models. Generic IT security measures, firewalls and (organisational) data requiring special protection were represented especially often. In the group model, the participants built a model that contained parts from all four individual models. Threats were presented in the form of attackers who were placed in front of the organisation. Security measures were presented in both generic and detailed forms (anti virus, password manager, etc.). They used connecting elements to show that the different security mechanisms must "work together" and not interfere with each other. A gap in the "corporate wall" was built to show that an organisation can never experience 100% security, as technology is always evolving and so are attackers. The students used green bricks to depict a room with two employees, symbolising that it is important and helpful to have a protected place to talk to each other in peace about the topic of IT security, to ask questions and to be able to talk about challenges. A comprehensive IT security/ awareness training was presented on a black board and concrete instructions for the employees were symbolised with

the help of a white board. It was shown that only three out of four employees represented can undergo a security training. One employee is not able to do so because he is busy following a security measure.

4.3 Post-workshop Survey Results

Of the $n = 48$ participants, 38 took part in the post-feedback online survey. Some of the participants reported back that by approaching the topic of IT security through the LSP method, they had become aware that the reason some employees do not participate in awareness and IT security training may be that they cannot, because they are not given the necessary time by their employer. Some have also noticed that the model they have built presents IT security in organisations in a very positive way.

5 Discussion

Here we discuss a) substantive results: the models the participants created, and b) methodological results: what we learnt about conducting model workshops.

What We Learned about IT Security from Participants' Models. Having a background in IT security does not necessarily lead to a deeper understanding of everyday security (routines). For example, did the IT security master's students in the second workshop had a very narrow perspective on how security works for security staff (defender at the walls of the fortress) versus employees (bad guys circumventing security) and those differ not from models from the other groups. In multiple models, communication problems between different security stakeholders were shown – something we want to investigate in more detail in future rounds of coding and further workshops. Interestingly, independent of whether the task was formulated negatively or positively, the majority of models showed problems with security: Flaws in the security itself, blaming of others (e.g. employees) and communication problems between security staff and users/employees. This fits into the image that IT security is rarely seen as an enabler and with a positive connotation [18].

The evaluation also showed that in several models, the topic of interaction and collaboration – on different levels – was taken into account and considered relevant. This relates firstly to the technical side: the individual security mechanisms should function together. Furthermore, this concerns the human-technology interaction, as individual models emphasised the relevance of the fact that the IT security mechanisms and the IT security staff must also "work together". On the other hand, the human level was presented and it was shown that both users and organisations are only protected if the IT security staff and the employees communicate and work together.

Learnings from the Method. Comparing results from the four workshops, it becomes clear that having enough time is an important factor for the success of LSP. As there was more time available at the fourth, the participants were able

to share and reflect on the individual and group models in more detail. It was very helpful to introduce the rules for sharing the models in detail (do not tell a story but explain the model; tap the bricks you are telling about beforehand, etc.) and to repeat them during the process. These insights made the authors aware of the central role of the facilitator – already described in the literature [13] – who is responsible for the process.

The quality of our data collection is limited to the pictures and our notes. It seems promising to also record the complete workshop with a camera as in [10], where individual interactions and discussions among participants could be analysed as well. We decided not to record these sessions because we did not want to put off participants concerned about privacy; the company of the participants in Workshop 3 only agreed on the condition that individual participants remained anonymous.

Without explanations and notes by the participants it is hardly possible to reconstruct the content later. We found that the models are not self-explanatory. Therefore, the focus of the evaluation was not exclusively on the representational value of the models, but rather on observing and recording the participants' explanations about their models and the exchange about them.

The Chances of LSP. LSP has the advantage to be a structured method – compared with so many other (creative or brick-based) methods. This makes (I) the single steps and results reproducible (like we did between the four workshops), (II) the method teachable to other researchers (like we thought ourselves based on the description by Hillmer [13]), (III) it easier to transfer it back to the industry, where it already used for teaching purposes.

In our workshops even participants who did not previously know each other quickly interacted with each other through the LSP method, and a productive working atmosphere characterised by mutual respect was established in a very short time. Even participants who had not previously dealt with the topic of IT security were able to approach this topic under these conditions with the help of this method. This means it works as a communication focus as intended in participatory design [4,22].

6 Conclusion and Further Work

We report work-in-progress from qualitative research with LSP. So far we conducted four workshops with $n = 48$ participants. We coded the collected data, but are still in the process of improving this strategy and will report the final coding strategy. Our preliminary results show that participants model IT security as a hurdle for users/employees – independently of whether they have an IT security background. LSP is a promising research method than engages most people and could serve as an alternative to focus group or as a method in action research. To be able to answer our research question, we still need to compare LSP with other qualitative data collection methods. We are planning to perform workshops with the same tasks but other creative methods (like drawing, creating mind maps, etc.) and then compare the coding results.

Acknowledgments. We want to thank all participants of our Lego workshops. Many thanks also to Mary Cheney, Marco Gutfleisch and Markus Schöps for their proofreading as well as to the anonymous reviewers for their helpful feedback. The work was supported by the PhD School "SecHuman - Security for Humans in Cyberspace" by the federal state of NRW, Germany and also by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

References

1. Ashenden, D., Lawrence, D.: Security dialogues: building better relationships between security and business. IEEE Secur. Priv. **14**(3), 82–87 (2016). https://doi.org/10.1109/MSP.2016.57
2. Asprion, P.M., Schneider, B., Moriggl, P., Grimberg, F.: Exploring cyber security awareness through LEGO serious play Part I: the learning experience. Management **20**, 22 (2020)
3. Beautement, A., Sasse, M.A., Wonham, M.: The compliance budget: managing security behaviour in organisations. In: Keromytis, A., Somayaji, A., Probst, C.W., Bishop, M. (eds.) Proceedings of the 2008 Workshop on New Security Paradigms, p. 47. Association for Computing Machinery, New York (2008). https://doi.org/10.1145/1595676.1595684
4. Bodker, S.: Through the Interface: A Human Activity Approach to User Interface Design. Taylor & Francis Group, Milton (1990)
5. Cerezo-Narváez, A., Córdoba-Roldán, A., Pastor-Fernández, A., Aguayo-González, F., Otero-Mateo, M., Ballesteros-Pérez, P.: Training competences in industrial risk prevention with lego® serious play: a case study. Safety **5**(4), 81 (2019)
6. Coles-Kemp, L., Jensen, R.B., Heath, C.P.R.: Too much information: questioning security in a post-digital society. In: Bernhaupt, R., et al. (eds.) Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, pp. 1–14. ACM, New York, NY, USA (2020). https://doi.org/10.1145/3313831.3376214
7. Hall, P., Heath, C., Coles-Kemp, L.: Critical visualization: a case for rethinking how we visualize risk and security. J. Cybersecur. tyv004 (2015). https://doi.org/10.1093/cybsec/tyv004
8. Hayashi, E., Hong, J.: A diary study of password usage in daily life. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2627–2630 (2011)
9. Heath, C.P.R., Crivellaro, C., Coles-Kemp, L.: Relations are more than bytes: rethinking the benefits of smart services through people and things. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1–12. CHI '19, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3290605.3300538,
10. Heath, C.P., Hall, P.A., Coles-Kemp, L.: Holding on to dissensus: participatory interactions in security design. Strateg. Des. Res. J. **11**(2), 65–78 (2018). https://doi.org/10.4013/sdrj.2018.112.03
11. Herbert, F., Farke, F.M., Kowalewski, M., Dürmuth, M.: Vision: developing a broad usable security & privacy questionnaire. In: European Symposium on Usable Security 2021, pp. 76–82 (2021)
12. Hielscher, J., Kluge, A., Menges, U., Sasse, M.A.: Taking out the trash: why security behavior change requires intentional forgetting. In: New Security Paradigms

Workshop, pp. 108–122. ACM, New York, NY, USA (2021). https://doi.org/10.1145/3498891.3498902
13. Hillmer, D.: PLAY! Der unverzichtbare LEGO SERIOUS PLAY Praxis-Guide für Trainer, Coaches und Moderatoren (German). Hanser, München (2021)
14. Kocksch, L., Korn, M., Poller, A., Wagenknecht, S.: Caring for it security: accountabilities, moralities, and oscillations in it security practices. Proc. ACM Hum.-Comput. Interact. **2**(CSCW), 1–20 (2018)
15. Kranawetleitner, T., Krebs, H., Kuhn, N., Menner, M.: Needs analyses with LEGO serious play. In: Ma, M., Fletcher, B., Göbel, S., Baalsrud Hauge, J., Marsh, T. (eds.) Serious Games, LNCS, vol. 12434, pp. 99–104. Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-61814-8
16. Kuckartz, U.: Qualitative Text Analysis: A Guide to Methods, Practice & Using Software. SAGE, Los Angeles and London and New Delhi and Singapore and Washington, DC (2014)
17. McCusker, S.: Lego, seriously: thinking through building. Int. J. Knowl. Innov. Entrep. **2**(1), 27–37 (2014)
18. Menges, U., Hielscher, J., Buckmann, A., Kluge, A., Sasse, M.A., Verret, I.: Why IT Security Needs Therapy. In: Computer Security. ESORICS 2021 International Workshops. Springer (2022). https://doi.org/10.1007/978-3-030-95484-0
19. Rädiker, S., Kuckartz, U.: Videodaten, Audiodaten und Bilder codieren (German). In: Rädiker, S., Kuckartz, U. (eds.) Analyse qualitativer Daten mit MAXQDA, pp. 85–94. Springer Fachmedien Wiesbaden, Wiesbaden (2019). https://doi.org/10.1007/978-3-658-22095-2
20. Redmiles, E.M., Acar, Y.G., Fahl, S., Mazurek, M.L.: A summary of survey methodology best practices for security and privacy researchers (2017)
21. Uslar, M., Hanna, S.: Teaching domain-specific requirements engineering to industry: applying lego serious play to smart grids. In: 1st Workshop on Innovative Software Engineering Education (2018)
22. Winograd, T.: Bringing design to software. ACM (1996)
23. Zenk, L., Primus, D.J., Sonnenburg, S.: Alone but together: flow experience and its impact on creative output in lego serious play. Eur. J. Innov. Manag. (2021)