

1 **Résumé of the Gamified Increase in Security Awareness**
2 **in German Small and Medium-Sized Businesses**
3 **after Three Years’ Practice of “ALARM Information Security”**
4

5 Margit C. Scholl
6 University of Applied Sciences Wildau (TH Wildau)
7 Hochschulring 1, 15745 Wildau, Germany
8 margit.scholl@th-wildau.de
9

10

11

12

13 **Abstract**
14

15 Latest cybersecurity reports for 2023 again show a critical situation in IT security in Germany—
16 in fact, the threat in cyberspace is higher than ever before. There can be no doubt that small
17 and medium-sized enterprises (SMEs) need to build their cyber resilience with people. Hu-
18 mans are increasingly becoming the center of events to increase information security. Within
19 just three years and under the difficult conditions of the COVID-19 pandemic, the “Awareness
20 Lab SME (ALARM) Information Security” project has developed a practice-oriented mix of
21 methods in analog and digital form (serious games). All the tested materials have now been
22 made available free of charge. The aim of the overall scenario was to promote the urgently
23 needed operational awareness raising of executives and employees in SMEs. This article sum-
24 marizes the key findings.

25

26

27

28 **Keywords**
29

30 Information security, awareness raising, serious games, awareness training, on-site attack
31 simulations, low-threshold security concepts
32

32

33

34 1. Introduction of the Information Security Situation in Germany

35
36 Ignorance of or non-observance of information security and the corresponding operational guidelines
37 poses significant risks for all companies [1][2]. The term information security refers to the protection
38 of information of all types and origins [3] and goes beyond the terms IT security, cyber security, and
39 data protection, which—despite their differences—are often used synonymously. Dangers exist in the
40 form of human error, organizational deficiencies, intentional actions, technical failure, or force
41 majeure. Managers and employees of companies should therefore be attentive to technical and or-
42 ganizational measures (TOM) that can be used to adequately address the risks. This requires active
43 personnel development in companies for information security and extensive risk management with
44 regard to operational processes.

45 Owing to the time lag between, for example, a cyberattack and its operational impact, there can also
46 be prolonged consequences for a company, so a long-term mindset plays a crucial role in reducing
47 security risks. According to Li et al. (2018), this long-term orientation includes three dimensions that
48 must be established in companies in the area of information security: continuity, future viability, and
49 endurance [4]. This approach was also pursued as part of the “Awareness Lab SME (ALARM) Infor-
50 mation Security” project presented here with the focus on “helping small and medium-sized enter-
51 prises (SMEs) to help themselves.” The results of this practice-oriented research project make a sound
52 contribution to active personnel development and sustained awareness raising. The project and its
53 results are of particular importance as a means to increase the level of security in German SMEs, as
54 investigations into the situation repeatedly show that, despite advancing digitization, awareness of IT
55 security in Germany is still inadequate (see, for example, [5]). Even if risk perception has increased,
56 there is a lack of comprehensive implementation of various information security measures, which can-
57 not only be of a technical nature. The current study by the German Chamber of Industry and Commerce
58 [6] highlights that although SMEs are now taking technical precautions to reduce risks, there has been
59 no significant increase in organizational measures for information security—including awareness rais-
60 ing and staff training—and only a third of the companies surveyed have an emergency plan.

61 According to the Federal Office for Information Security (BSI), information security awareness (ISA)
62 should address the following threats and vulnerabilities [7]: insufficient knowledge of regulations, in-
63 sufficient ISA, and carelessness in handling information. Tsohou et al. (2012) concludes from recent
64 global security surveys that ISA trainings (ISATs) are not currently working [8]. One reason might be a
65 “technocratic” view of risk communication, meaning the tendency for technical experts to tell people
66 what they think and ought to know [9]. A second reason might be policies “ending up as long lists of
67 dos and don’ts located on web pages most employees only access when they have to complete their
68 mandatory annual ‘security training’ and which has little to no effect on their security behavior” [10];
69 a third reason is that training aimed at addressing security awareness gaps is not sufficient to ensure
70 compliance with a security culture [11].

71
72 Psychological research shows that in addition to the classical theoretical approach to knowledge trans-
73 fer and the marketing-oriented approach of emotionalization, a systemic approach to team-based
74 communication is needed (see [12-14]). ISAT needs a “methodology 3.0”: social participation in a com-
75 municative team process is a key component in this third stage of emotionally based awareness-raising
76 activities [15]. This is because IS and IT are about more than technology [16]. ICT systems involve hu-
77 man actors, and users do not always behave the way they are supposed to [17]. The adverse charac-
78 terization of people in the field of IS has now been rethought, because there are fundamental strategic
79 IS deficits in institutions themselves (see, for example, [18, 19]). Alotaibi et al. (2023) argues that the
80 significant evidence of unsecure employee behavior, which is a major threat and can undermine cy-
81 bersecurity in companies, should not lead to staff being sanctioned [20]. Rather, there are often a large

82 number of technical-organizational obstacles and stressful situations in the core business of everyday
83 working life, which lead to employees not making safety-related decisions and not being able to be-
84 have in the approved way [20].

85 Within just three years and under the difficult conditions of the COVID-19 pandemic, the “Awareness
86 Lab SME (ALARM) Information Security” project [21] has developed a practice-oriented mix of methods
87 in analog and digital form as a concrete response to this general situation. Our participatory research
88 design involved SMEs as pilots for material testing in specified operational situations. All the materials
89 have now been made available free of charge and serve to raise awareness among managers and em-
90 ployees; they have been developed, tested, improved, and finalized with the pilot SMEs. There is no
91 doubt that SMEs also need to build their cyber resilience at the human level.

92 The complexity of the practice-oriented “ALARM Information Security” project was clear from the
93 start, as it was intended to develop an overall scenario to raise awareness and support SMEs for infor-
94 mation security through to self-help within just three years. The underlying research design mainly
95 contained new developments—within the purview of a central project management control—which
96 were carried out iteratively in three agile and participatory phases, involving an innovative process
97 scenario for information security with analog and digital experience-oriented scenarios as well as “on-
98 site attacks” and other checks, such as awareness measurements, quizzes, and tests. The aim of the
99 overall scenario was to address the urgent need for operational awareness raising among executives
100 and employees and personnel development in SMEs, which has not yet been widely effective. To this
101 end, IT security in connection with increasingly digital work processes should be made concrete; at the
102 same time, people should be emotionally touched, motivated, and given an active role in developing
103 awareness-raising measures. The aim is to strengthen a sustainable, company-wide information secu-
104 rity culture and increase the level of security in German SMEs.

105 The “ALARM Information Security” project is funded by the Federal Ministry for Economic Affairs and
106 Climate Protection (BMWK) until March 31, 2024. The project documentation in German [22] refers to
107 the results achieved in the period from October 1, 2020, to the original project end on September 30,
108 2023. The cost-neutral extension (CNE) of the project until March 31, 2024, is intended to make the
109 high-quality materials that were obtained as a mix of methods more widely known at other SME
110 events. In addition, the CNE enables the publication of the project documentation in book form, along
111 with further articles about the results in English.

112 This article summarizes the key phases and findings and reflects on the results in the light of the inter-
113 national literature on the subject. The central project manager of the “ALARM Information Security”
114 project also presents her own summary of the complex project carried out. The article is structured as
115 follows: chapter 2 outlines the background for the gamified analog and digital developments in the
116 project; chapter 3 sets out the methods of testing and the final results, which are further discussed
117 and reflected on in chapter 4; chapter 5 presents the conclusions drawn from the project.

118 **2. Background of “ALARM Information Security”**

119
120 Over the last decade, the University of Applied Sciences Wildau (TH Wildau) and its corporate partners
121 have developed a variety of modern materials to increase information security awareness in various
122 projects for various target groups. The motivation for this was, on the one hand, the increasing preva-
123 lence of cyberthreats in Germany and worldwide (see, for example, [23] [24]). On the other hand, the
124 realization that traditional learning methods have obviously not yet led to the hoped-for success of
125 increased mindfulness in increasingly digitized work processes (see, for example, [25]). Current studies
126 also point to the ongoing critical situation. Tanriverdiyev (2022) notes that the reliance on information

127 and communications technologies (ICT) has led to an increase in cyberattacks against individuals, com-
128 panies, and governments worldwide and that these attacks are no longer limited to data theft or fi-
129 nancial losses but have broader implications for national security and economic stability [26]. Sharma
130 and Zamfiroiu (2023) emphasizes the increasing complexity and frequency of cyberattacks, which re-
131 quire innovative and proactive cybersecurity measures. The previous reactive approach to cybersecu-
132 rity is no longer sufficient; a proactive, adaptive strategy is required [27] to maintain an adequate level
133 of security in the institutions. But technology alone is not enough. The critical role of human factors in
134 shaping cybersecurity outcomes and practices continues to be explored [28]. Whether malicious or
135 not, employees' actions can have significant and detrimental outcomes for their organizations [29].
136 However, there is a long-standing requirement that traditionally *knowledge-based* training methods
137 must change [30]. Moreover, security training must be implemented as continuous training and as
138 further education in institutions/companies [28].

139
140 Several studies emphasize the critical role of public perception and awareness in cybersecurity for the
141 better protection of organizations and individuals [28]. Abrahams et al. (2024) argues that effective
142 cybersecurity strategies must include educational components that cater to different audiences, from
143 college students to working professionals [28]. The findings of Epstein & Zankich (2022) suggest that a
144 third of Internet users disclose more personal information than they would if they were more effec-
145 tively warned about the risks involved [31]. The results of Posey & Shoss (2023) support the idea that
146 targeted (whether malicious or not) security breaches can be viewed as events that occur in the com-
147 plex interface between organizational behavior and security, and that stressors are related to em-
148 ployee security breaches [29]. Information security policies (ISPs) play a key role in organizational in-
149 formation security [32]. Clear organizational rules, even for emergencies, are necessary in all institu-
150 tions, but they are by no means present everywhere; they are especially hard to find in stressful situ-
151 ations and certainly not written in a comprehensible way [32, 33]. The approach cannot therefore be
152 to denigrate employees as the weakest link in the security chain [20, 25]. Likewise, involving organiza-
153 tional members in ISP development offers a number of benefits, providing detailed knowledge of the
154 context, forming a common language, and promoting an information-security mindset [32]. However,
155 the involvement of organizational members requires special skills on the part of the project manager,
156 because he/she has to clarify the goals of the contributions to a policy and make it clear what is ex-
157 pected from the participants; different methods also need to be used to achieve the goals of the group
158 work [32].

159
160 The serious games we developed, which are presented in chapter 3, can also be useful for such a task.
161 The basis for this was the "3.0 Systemic Approaches" of [15], which were implemented and tested at
162 TH Wildau in different projects, starting with the projects "IT-Sicherheit@KMU" (2013–2014) [34] and
163 "SecAware4job" (2015–2017) [35] [36] (Figs. 1 and 2). The holistic approach of the current "ALARM
164 Information Security" project is aimed at promoting awareness of information security in SMEs, in light
165 of the specific requirements and needs of these companies. The following aspects were of central im-
166 portance:

167 **1. Concept development:** At the beginning of the project, a comprehensive concept was developed
168 for integrative awareness raising in the area of information security. By recording the current situation
169 using in-depth psychological interviews and online surveys, this concept considers the specific require-
170 ments and needs of SMEs.

171 **2. Practical tests:** The individual awareness-raising methods and training measures developed were
172 tested intensively in practice. Real everyday scenarios in the companies were simulated in order to
173 check the effectiveness of the awareness-raising content.

174 **3. Awareness measurements and maturity statements:** Based on the practical tests, awareness meas-
175 urements and maturity statements should be explored for future purposes. Such complex instruments
176 are intended to provide information about the extent to which awareness-raising methods and secu-
177 rity measures are ready for use and effective.



178

179 Figure 1 The “Security Arena” was developed and implemented at the TH Wildau together with the project partner
 180 known_sense, starting with the projects “IT-Sicherheit@KMU” (2013–2014) [34] and “SecAware4job” (2015–2017) [35] [36].
 181 Ten scenarios were developed and tested with students and employees in German and English: Clear Desk, Data Security,
 182 Internet Services, Incident Management, Password Hacking, Phishing, Security on the Go, Social Engineering, Social Media,
 183 and Network Domino. These learning scenarios (analog serious games) are still in use. They can be used individually as an
 184 awareness measure on the current issue or for groups in competition; the latter is often carried out by students. But they can
 185 also be used in classic teaching formats simply as a didactic interruption and motivational boost. So far it has always been
 186 possible to motivate people to actively participate.



Picture taken at WMSCI/IMSCI/CISCI 2018 conference, Orlando, USA.

187

188 Figure 2 The Security Arena’s English-language learning scenarios were also used in workshops at conferences (the picture
189 shows an example from Orlando in 2018), and tested with international partners at DePaul University in Chicago and the
190 University of Illinois at Urbana-Champaign, as well as in a hospital in Chicago, the Illinois Department of Children & Family
191 (DCFS), in 2018/2019. These analog interactive serious games to increase information security awareness enable the inclusion
192 of all participants and an intensive exchange of experiences on the specific topic, thus representing a good basis for awareness
193 raising and training.

194

195 **4. Instructions for action:** Specific, comprehensive instructions for action have been developed that
196 help SMEs to successfully implement the awareness-raising measures and integrate them into their
197 everyday operations.

198 **5. Possible certifications for awareness moderators:** As part of the project, an initial moderator train-
199 ing course for analog serious games was developed and tested. The future certification of individuals
200 as moderators of innovative learning methods could promote awareness-raising measures within
201 SMEs and stabilize their use in the long term. In addition, an “awareness certification” of selected em-
202 ployees could serve the SME as a quality criterion and proof of the implementation of the requirement
203 for awareness-raising measures according to ISO/IEC 27001 and the BSI standard 200-2 (see BSI 2021).

204 **6. Security strategy:** Within the three-year project period, a holistic strategy for information security
205 awareness in SMEs was developed, which can be integrated into the overall corporate strategy. The
206 awareness-raising content was included as an important component of the company’s information
207 security strategy.

208 **7. Sustainability aspects:** Ideas for greater sustainability were included in the development process of
209 the learning scenarios/serious games and all materials to ensure that the awareness-raising measures
210 for appropriate personnel development are effective in the long term and can be continuously im-
211 proved.

212 **8. Building a company-wide information security culture:** All project results, particularly through their
213 integrative interlinking and the extensive, practice-oriented assistance, serve to increase awareness of
214 information security in all areas of the SME and the practical integration of security practices into

215 everyday operational life. This promotes the development of the company's information security cul-
216 ture and increases the SME security level.

217 **3. Methods and Results**

218

219 The starting point for all material developments were the in-depth psychological interviews that were
220 carried out in the project by the subcontractor known_sense [37] and whose results are published in
221 the form of three studies on the project website (called Study 1, Study 2, and Study 3; see [21]). At the
222 same time, online surveys were designed, and international literature research was done by the TH
223 Wildau research team and carried out to ascertain the current status quo in SMEs. Based on the analog
224 serious games that were subsequently developed and their successive practical tests, the feedback
225 from different target groups of pilot SMEs, and the improvements made to the learning scenarios and
226 material developments, the "ALARM Information Security" research project has a considerable wealth
227 of empirical findings about information security and awareness in SMEs. Effective cybersecurity strat-
228 egies require a balanced approach that combines technological advances with understanding human
229 factors and compliance with international standards, incorporating a holistic view [28]. As part of the
230 research project "Awareness Lab SME (ALARM) Information Security," the research team at TH Wildau
231 conducted numerous scientific workshops and other events with great enthusiasm. The primary goal
232 was to promote a strong information security awareness in SMEs by increasing the reach and aware-
233 ness of the developed learning scenarios and using other materials and low-threshold concepts to raise
234 awareness among SME employees.

235

236 **3.1 Didactical background of the developed analog serious games**

237

238 The seven developed analog serious games can be used as a part of a company's holistic awareness
239 concept that is based on the "station learning" methodology (see, for example, [38]). They can be used
240 in combination with other serious games of this format as awareness training with or without an initi-
241 ated competition between target group teams. they can also be used as an introduction or as a teaser
242 for more in-depth training on the topic of information security. The general time frame for an aware-
243 ness-raising measure should be only about 15 minutes; this requires good time management on the
244 part of the moderator. The moderation steps are [21, 37]:

- 245 • Step 1: Introduction (approx. 4–6 min.)
- 246 • Step 2: Game (if necessary two phases: 2 × 2.5–3.5 min. = 5–7 min.)
- 247 • Step 3: Debriefing (approx. 2–5 min.).

248

249 Figure 3 shows the seven developed analog serious games that are available for download in German
250 on the project website [21]. An overview is given in [39]:

- 251 • "Home Office" (Live & Work Securely at Home) provides an overview of the most important op-
252 erational and private information security and data protection risks in your own apartment or
253 house as well as associated preventative measures to minimize the risks.
- 254 • "Multi-Factor Authentication" (MFA) combines aspects of password protection and MFA and
255 demonstrates that the protection of information depends to a large extent on secure authentica-
256 tion. It shows how a "strong"—i.e., secure—password is created and demonstrates that one (1!)
257 factor is not sufficient to protect very sensitive information.
- 258 • "The Five Phases of CEO Fraud" provides an overview of the overall process of CEO fraud attacks
259 and corresponding prevention measures. Of particular interest is the often overlooked "prelude"
260 involving the preparations for an attack.
- 261 • "Mobile Communication, Apps & Co." raises awareness of risks and preventative measures that
262 reduce the potential dangers of mobile communication or app usage.

- 263 • “Cyber Pairs” (Social Engineering) breaks down possible barriers and leads to more security when
264 dealing with the terminology and names of common or new cybercrime attacks by helping to
265 understand them in detail and fostering the ability to distinguish between possible preventive
266 measures. The clarification of terms is always linked to the question of what each of us can do to
267 minimize risks.
- 268 • “Data and information protection” refers to the protection of information and data from custom-
269 ers, employees, and business partners as part of the business process of every company. It helps
270 clarify how data and information protection can be ensured by recapitulating and practicing the
271 use of the most important protection strategies.
- 272 • “Information Class Roulette” illustrates the purpose of information classification in every organi-
273 zation. The “right” classes for protecting valuable information depend on the potential impact on
274 availability, damage, or loss of information. It provides an understanding of information classi-
275 fication and the need for it, even if the organization has not yet adopted classification as a routine.

276 The specific didactic aspects of the seven developed analog serious games are described in brief below.
277 Each analog learning scenario comes with four downloads: a moderation guide, a construction guide,
278 a handout on the serious game, and the print templates. As a result of funding from the BMWK, all
279 materials are available in German free of charge for internal, noncommercial use (see [21]).



280
281 *Figure 3 Seven new analog serious games of the project “ALARM Information Security” developed to raise information secu-*
282 *rity awareness in SMEs. The funding applied only to the development of the German version.*

283
284 **3.1.1 Didactic intention of analog serious game 1: Home Office**

285 For this serious game, one can download for internal, noncommercial use, the German moderation
286 guide [40], the construction guide [41], the handout [42], and the templates for print [43]. In recent
287 years, more and more employees have worked from home. The topic of “home office” has become
288 even more popular, especially as a result of the COVID-19 pandemic. Since you are usually on the same
289 home network for work as you are for private purposes, the same or similar rules must be observed
290 when it comes to information security as are applied at work. There are also risks from the “Smart
291 Home” area. This serious game is intended to provide an overview of the most important operational
292 and private information security and data protection risks in your own apartment or house as well as
293 the associated prevention measures in order to minimize risks. A detailed description of the home
294 office situation is given in [44]. At the end of the debriefing phase, the moderator can explain the given
295 “golden rules.” Examples of games for the home office include [40]:

- 296 • Security risks for the employer arise in the home office primarily through the shared use of the in-
297 house network or devices for work AND private purposes.
- 298 • The same safety requirements apply in the home office as in the workplace.
- 299 • In addition, the employer’s guidelines for working from home must be observed.
- 300 • Work at home only with the tools provided or approved by the company; always separate profes-
301 sional and private matters and transfer data via an encrypted VPN (virtual private network) con-
302 nection.

303

304 **3.1.2 Didactic intention of analog serious game 2: Multi-Factor Authentication**

305 For downloading of the second analog game material in German, see the moderation guide [45], the
306 construction guide [46], the handout [47], and the templates [48]. Protecting sensitive information and
307 specific assets is one of the most important information security tasks in companies/institutions/public
308 administrations. The loss of customer data can lead to the loss of customers, complex legal disputes,
309 reporting obligations, fines, and reputational damage with high collateral costs. When backups of cus-
310 tomer data are stored in the cloud, the topic becomes even more explosive, because with cloud ser-
311 vices the company is no longer solely responsible for the data stored there without outside help. The
312 biggest risks in this regard include negligence in authentication, such as weak passwords and poorly
313 managed access rights or security gaps in the cloud service as well as inadequate preparation for the
314 worst-case scenario of a possible incident. This serious game combines aspects of password protection
315 and multi-factor authentication (MFA) and is intended to demonstrate that the protection of infor-
316 mation depends to a large extent on secure authentication. In this case, some examples of “golden
317 rules” are [45]:

- 318 • Your password should not
 - 319 – be known to anyone but you;
 - 320 – be accessible to anyone but you;
 - 321 – be stored unencrypted on your computer;
 - 322 – contain any character strings that can be associated with you, such as user IDs, vehicle li-
323 cense plates, dates of birth or telephone numbers, or terms that can be found in dictionar-
324 ies.
- 325 • In order to significantly increase your security standard and better protect your company against
326 phishing or brute force attacks, it is recommended that password protection be supplemented
327 with a second barrier (MFA).

328

329 **3.1.3 Didactic intention of analog serious game 3: The Five Phases of CEO Fraud**

330 For downloading of the third analog game material in German, see the moderation guide [49], the
331 construction guide [50], the handout [51], and the templates [52]. CEO Fraud (sometimes also called
332 “boss scam” or “fake president scam” or “BEC” = business email compromise) is the name of a social
333 engineering scam that is “popular” in cybercrime circles and involves identity fraud. Employees can be
334 made to believe that high-ranking superiors have requested that large sums of money be transferred
335 to foreign accounts. However, CEO Fraud does not start with the actual financial fraud but is charac-
336 terized by an intensive preparation phase during which the fraudsters collect information about their
337 targets and combine various attack vectors. This serious game is intended to provide an overview of
338 the overall process of CEO Fraud and point out preventive measures—especially for the often over-
339 looked “prelude.” A detailed description of the CEO situation is given in [53]. Some examples of “golden
340 rules” to protect yourself against CEO Fraud are [49]:

- 341 • Use personal data and information and that of your company sparingly within social networks
342 and on other websites.

- 343 • Pay particular attention to fake emails (phishing) that appear to come from the company man-
344 agement and in which—often accompanied by pressure and a request for absolute confidenti-
345 ality—a request is made to transfer large amounts of money to a foreign bank account.
- 346 • Also pay attention to the content details of the emails: legitimacy checks for payment requests,
347 deviations from standard emails from superiors in terms of sender address, address, greeting,
348 structure, or overall design.
- 349 • Verify suspicious payment requests by calling back or asking the person who placed the order in
350 writing.
- 351 • Remain critical of attempts at intensive, penetrating contact by people you do not know.
352

353 **3.1.4 Didactic intention of analog serious game 4: Mobile Communication, Apps & Co.**

354 For downloading of the fourth analog game material in German, see the moderation guide [54], the
355 construction guide [55], the handout [56], and the templates [57]. In recent years, mobile communi-
356 cation has shifted from notebooks to smartphones and tablets, which boast practical apps. A separa-
357 tion between work and private life no longer seems possible for most users, especially if there is no
358 clear demarcation between work and private hardware—for example, as a result of a regulation. This
359 mix, along with increasingly insecure apps and the lax handling of access rights, poses a high risk for
360 companies. This serious game is intended to raise awareness of risks and preventive measures that
361 reduce the potential dangers of mobile communication or the use of apps. Some examples of “golden
362 rules” for mobile communication are [54]:

- 363 • Smartphones and tablets are practical helpers, but some apps do more with your devices than
364 you think and want.
- 365 • Apps can be gateways for malware and cybercriminals and promote identity theft and manipula-
366 tion.
- 367 • You generally install apps on all your mobile devices under your own responsibility—i.e., you must
368 inform yourself about possible risks.
- 369 • Install apps from trustworthy sources: if in doubt, only use official stores. Otherwise, there is a
370 risk of malware or keyloggers.
- 371 • Remove apps you no longer use, as every additional app is a security vulnerability.
372

373 **3.1.5 Didactic intention of analog serious game 5: Cyber Pairs (Social Engineering)**

374 For downloading of the fifth analog game material in German, see the moderation guide [58], the con-
375 struction guide [59], the handout [60], and the templates [61]. The aspect of white-collar crime is be-
376 coming an increasingly crucial competitive factor for companies. As a result of digitization and the
377 associated cybercrime activities of criminals, numerous attack methods or vectors to which organiza-
378 tions feel exposed have been successfully adapted by actors and become effective as new phenomena.
379 This means that new security gaps and attack methods are emerging in ever shorter cycles, sometimes
380 with terminology that requires explanation—such as English terms or Anglicisms—in which technically
381 based vectors are often combined with human-social factors to form complex structures. This serious
382 game is intended to break down possible barriers and lead to greater security when dealing with terms
383 and names of common or new cybercrime attacks by helping people to understand them in detail and
384 enabling them to differentiate between possible prevention measures—this always goes hand in hand
385 with the question of what each of us can do to minimize risks. Social engineering, a form of manipula-
386 tion in which unauthorized persons attempt to gain unauthorized access to information or IT systems
387 under false pretenses, is the most effective form of deception [58]. Some “golden rules” are [58]:

- 388 • Ensure the identity of the person you are speaking to and do not open any email attachments or
389 links from unknown senders.
- 390 • In the analog and digital world, pay attention not only to your personal data but also to data
391 entrusted to you by your company and its customers: cybercriminals are attacking our information
392 infrastructures more and more frequently and with ever better tools.

- 393 • Networking is one of the basic principles of your business, and trust in the security of the infor-
394 mation entrusted to you by customers is the basis of your company's business.
395 • Cybersecurity aspects such as firewalls, password security, virus and spam protection, and net-
396 work monitoring are highly relevant not only for all employees but also for customers and busi-
397 ness dealings with them.
398 • In the end, defending against potential perpetrators is not just about outstanding technology but
399 above all about your personal awareness and healthy security consciousness.
400

401 **3.1.6 Didactic intention of analog serious game 6: Data and information protection**

402 For downloading of the sixth analog game material in German, see the moderation guide [62], the
403 construction guide [63], the handout [64], and the templates [65]. Protecting information and data
404 from customers, employees, and other parties is part of every company's business. This serious game
405 is intended to help ensure data and information protection by recapitulating and practicing how to use
406 the most important protection strategies. Information is the "crown jewel" of your company and must
407 therefore be particularly protected. Examples of "golden rules" for this topic are [62]:

- 408 • Everyone is personally responsible for the security of all the information in their own work envi-
409 ronment.
410 • Adhere to the "need-to-know" principle—i.e., you only pass on information to the extent abso-
411 lutely necessary and to authorized persons.
412 • You are also clear about what customer data is stored where.
413 • Only store or process necessary customer data.

414 Moreover, if customer data is personal,

- 415 • this data must be collected, processed, and used lawfully;
416 • this data may only be collected, processed, and used for a specific purpose within the scope of
417 legal permissions;
418 • this data must be appropriate and relevant and must not be collected and processed in a way
419 disproportionate to the intended use.
420

421 **3.1.7 Didactic intention of analog serious game 7: Information Class Roulette**

422 For downloading of the seventh analog game material in German, see the moderation guide [66], the
423 construction guide [67], the handout [68] and the templates [69]. The purpose of information classifi-
424 cation is to protect the valuable information of any organization. The "right" classes depend on the
425 potential impact on availability, corruption, and loss of information. This serious game helps you un-
426 derstand information classification and the need for it. Because information classification is not com-
427 mon for all small businesses, in this serious game the "golden rules" provide more insight [66]. In most
428 organizations, on average, four classes of information appear in this context:

- 429 • Secret / Very High / Strictly Confidential: Information that is only accessible to a very limited group
430 of named people and that has a strong impact on the company or its stakeholders if it becomes
431 public—e.g., strategic or organizational information and restructuring documents, business plans,
432 trade secrets, medical data, and documents containing sensitive personal information. Therefore,
433 great care must be taken when managing and transmitting it.
434 • Confidential/High: Information that is only accessible to a limited group of designated persons
435 and that has a medium impact on the company and its stakeholders for business use if made
436 public—e.g., incident and test reports, back-up data carriers, technical documentation and dia-
437 grams, source codes, contracts, customer data, project plans, and project documentation.
438 • Internal/Normal: Information for business use with a low impact on the company and its stake-
439 holders when it becomes public—e.g., internal communications/publications, travel plans, stand-
440 ards, internal guidelines, project documentation, personal data such as customer data, such as
441 names, address books, email addresses, and telephone numbers.

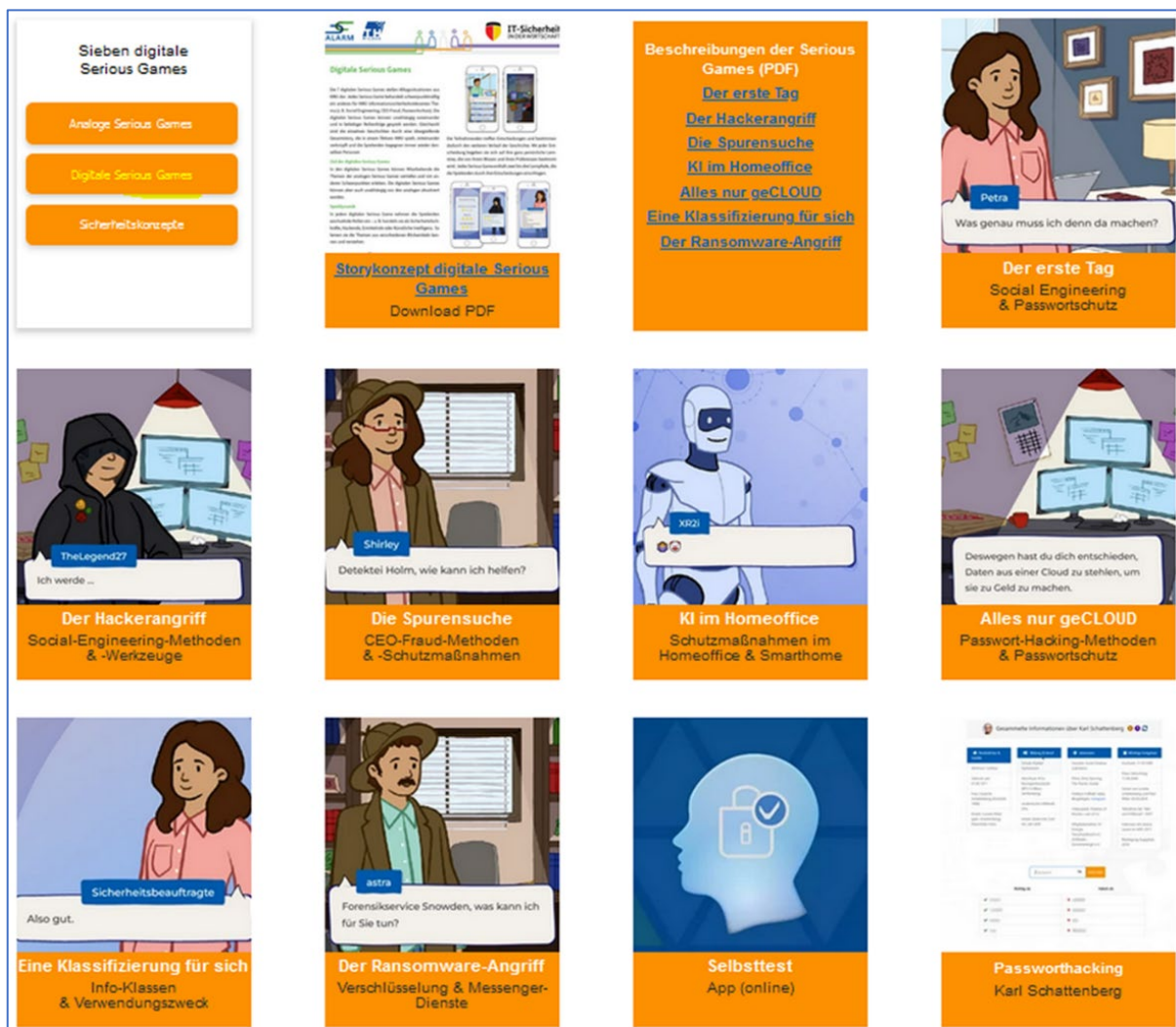
- Public/Open: Information that is neither privileged nor needs to be protected. Disclosure would have no impact on the company and its stakeholders—e.g., PR information for newspapers, websites, and published marketing materials such as brochures or flyers.

3.1.8 Digital addition to the analog serious game 7: A Roulette game

If the institution is unwilling to buy a small roulette wheel for the seventh serious game “Information Class Roulette” of “ALARM Information Security” project, it can be played digitally. The digital roulette was used in the earlier project called “Development of game-based learning scenarios for social engineering and security risk management in the manufacturing industry” [70]; it can also be used in other projects or trainings [71]. In the original project, the two game-based learning scenarios on social engineering and security risk management in the manufacturing industry were developed for the project “SME 4.0 Competence Center Stuttgart” [70].

3.2 Didactical background of the developed digital serious games

The aim of the digital serious games of “ALARM Information Security” is that employees can independently deepen the topics of the analog serious games and experience them with other focuses [72].



460
461 *Figure 4 Seven new digital serious games of the “ALARM information security” project to raise information security aware-*
462 *ness in SMEs and two additions (a self-test and a password-hacking game). The funding applied only to the devel-*
463 *opment of the German version.*

464 However, the digital serious games—as part of a holistic awareness concept—can also be played inde-
465 pendently of the analog games and in any order. We strongly recommend a personal debriefing. The
466 seven digital serious games represent everyday situations from SMEs [72]. Each game focuses on a
467 different topic relevant to information security for SMEs; they correspond to the analog games but do
468 not duplicate them. The individual stories of the digital games are linked together by an overarching
469 overall story that takes place in a fictional SME; the players meet the same people again and again and
470 get to know the company better with each serious game they play. Figure 4 shows the website area
471 for the digital serious games in the “ALARM Information Security” project [21]. At the beginning, there
472 is a general story concept available as a PDF download [72], along with a specific description for each
473 digital game. This is followed by the seven digital games, which can be played directly from the project
474 website. In the end there are two digital add-ons: a personal self-test, which has been recently rede-
475 veloped, and an adapted hacking game, the original idea of which comes from the previous “Security
476 Arena” [36] [37]. The seven new digital serious games are described in brief below (see Figs. 4 and 5).
477

478 **3.2.1 Digital serious game 1: The first day**

479 In the first digital game, it’s your first day in the imaginary company Grüsselig. Because they “know so
480 much about computers”—or so the boss thinks—the players are directly tasked with IT security, a task
481 that they first have to familiarize themselves with. And which is accompanied by some pitfalls and
482 challenges. But first, it’s time to get to know your new colleagues. The target group consists of first-
483 time players and players who have previously had little or no contact with the topic of information
484 security. It is primarily intended as an introduction to the topic of information security and a first step
485 in awareness training, in combination with other serious games in this format. The game can also be
486 used as an introduction or to loosen up an analog training course on the subject of social engineering
487 and password protection. As with all our digital serious games, the players have to select their deci-
488 sions from a list of suggestions, and at the end the actions they have taken are evaluated (Fig. 5, 1.).
489

490 **3.2.2 Digital serious game 2: The hacker’s attack**

491 In this serious game, the players take on the perspective of the attackers. As hackers, the players try to launch a
492 social engineering attack at Grüsselig and break into the company network. There are different approaches to
493 choose from, but only one leads to success. The focus is on players who want to specifically engage with social
494 engineering methods and test various tools. It is intended as an introduction, to loosen up or intensify a training
495 course on the topic of social engineering (Fig. 5, 2.).
496

497 **3.2.3 Digital serious game 3: The search for clues**





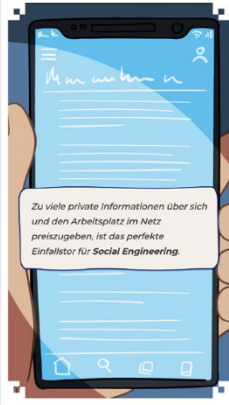


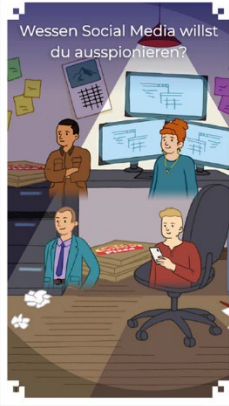

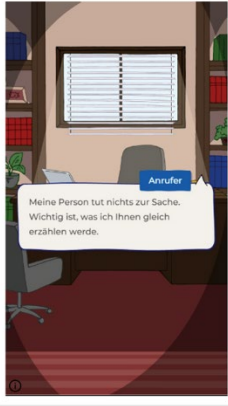

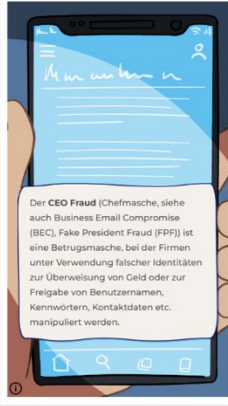
498 As a forensic scientist, the players receive information via an anonymous call that the Grüsselig company has
499 fallen victim to CEO Fraud. If the player finds out quickly enough which scam was used and who skimmed the
500 money, they might be able to get it back. The focus is on players who would like to specifically deal with CEO
501 Fraud methods and test various protective measures (Fig. 5, 3.).
502

503 **3.2.4 Digital serious game 4: AI in the home office**

504 The players take on the role of an artificial intelligence (AI) that monitors the computers of the Grüsselig employ-
505 ees for security issues and helps them. As AI, the players visit the home offices of three company employees from
506 different business areas. From an AI perspective, they experience how the same mistakes are always made in
507 the home office. The target group consists of people who would like to specifically deal with security in the home
508 office and would like to test various protective measures. The idea is to provide intensive training on the topic of
509 security in the home office and smart home (Fig. 5, 4.).
510

511 **3.2.5 Digital serious game 5: Cloud**



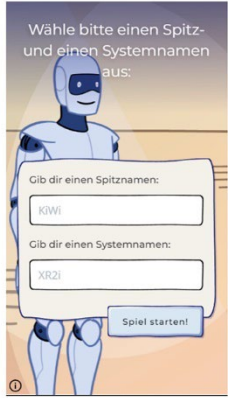










512 As a forensic scientist, the players receive information via an anonymous call that the Grüsselig company has
513 fallen victim to CEO Fraud. If the players find out quickly enough which scam was used and who skimmed the
514 money, they might be able to get it back. The game focuses on players who would like to specifically deal with
515 CEO Fraud methods, test various protective measures, and deepen their experience in the area of CEO Fraud
516 (Fig. 5, 5.).

 		
		
<h2>Seven developed digital learning scenarios (serious games)</h2>		
1.	<p>The First Day Social engineering & password protection</p>	  
2.	<p>The Hacker's Attack Social engineering methods and tools</p>	  
3.	<p>The Search for Clues CEO Fraud methods & protection measures</p>	  

517
518
519
520
521
522
523
524
525

Figure 5 Seven developed digital learning scenarios (serious games) to increase information security awareness in SMEs (final versions). Time frame per serious game: 15–20 min. (one game played through). On the left side you can see the number and the titles of the serious game translated into English. On the right, three key images from the game are shown, which were used in the German game descriptions made available for download from the project website [21]. The digital serious games were developed by the subcontractor Gamebook GmbH in coordination with the TH Wildau research team. In terms of implementation, all the digital games are played individually. Our recommendation is that a joint debriefing and exchange with the other participants in the company should take place online or in person. The funding applied only to the development of the German version.

526

 			
			
<h2>Seven developed digital learning scenarios (serious games)</h2>			
<p>4.</p> <p>AI in the Home Office</p> <p>Protective measures in the home office & smart home</p>			
<p>5.</p> <p>Everything Just CLOUD</p> <p>Password hacking methods & password protection</p>			
<p>6.</p> <p>A Classification in It-self</p> <p>Info classes and intended use</p>			
<p>7.</p> <p>The Ransomware Attack</p> <p>Encryption and messenger services</p>			

528 **3.2.6 Digital serious game 6: Information Classification**

529 The players deal with the topic of information and data classifications separately. What exactly is in-
530 formation classification in a business context? What part does it play in everyday life, and how is it
531 used sensibly in the company? To do this, the players take on the role of the AI. The AI in the gaming
532 context is now ready for the market and has been established as an assistance system at the Grüsselig
533 company. The target group consists of people who want to delve deeper into information classification
534 (Fig. 5, 6.).
535

536 **3.2.7 Digital serious game 7: Ransomware**

537 The Grüsselig company was hacked. Owing to a ransomware attack, all of the company's data has been
538 encrypted, and only one person has the code to unlock everything again. The players take on the role
539 of the forensic scientist to uncover the case and limit the damage. The only clue is that it happened via
540 a messenger service. The target group consists of people who want to delve deeper into encryption
541 and messenger services (Fig. 5, 7.).

542 **3.2.8 Digital additions to the digital serious games: A digital self-test**

543 The self-test is a low-threshold awareness-raising measure that generates data, determines the level
544 of knowledge of the participants, allows comparison with other self-test users and expands or re-
545 freshes the level of knowledge of the participants with an immediate evaluation. This became neces-
546 sary because defining areas of activity and the awareness measurements based on them would only
547 produce results that can be evaluated at a later point in time. A parallel development began with the
548 self-test in order to be able to supply basic questions for automated recommendations. The collected
549 data thus forms the basis for scientific considerations. The main goal was to identify indicators and the
550 learning paths calculated from them or recommendations for targeted awareness-raising measures in
551 response to the knowledge gaps identified by the self-test.

552 **3.2.9 Digital additions to the digital serious games: A password attack scenario**

553 The idea for the second additional digital game, Password Hacking, has been in use for several years in
554 the "Security Arena" of the project partner known_sense [37] and was first used at the TH Wildau in
555 the "IT Security@KMU" project [34] for students and employees. This project was financed from 2013
556 to 2014 as a technical investment in a mobile awareness-raising initiative by the Ministry of Science,
557 Research and Culture (MWFK) of the state of Brandenburg with funds from the European Regional
558 Development Fund (ERDF). Figure 6 shows the poster (A) of the old digital learning station "Password
559 Hacking" of the "Security Arena" (see Fig. 1). In the initial screen for exercise (Fig. 6, B), the login name
560 and passwords must be guessed and entered using an imaginary user profile of a person on a social
561 media platform.

562 The new version, which has now been adapted in the "ALARM information security" project, can be
563 seen under C to E. The information collected about the imaginary person Karl Schattenberg (C) is put
564 together (D), and the game provides information about the scenario and the possible time mode (C).
565 Here too, simple passwords should be derived from the information and entered (E). If the assumed
566 password is correct, it will be displayed with a green tick on the left; if it is wrong, it will be visible on
567 the right with a red cross (E). In the old version, for correctly guessed passwords, we not only listed
568 the password with a green tick but also showed its hash value (F). Depending on the target group, we
569 were able to provide further training on the meaning and purpose of the passwords saved as hash
570 values. However, this required a personal discussion, which is not a problem in the analog setting but
571 requires a digitally initiated debriefing in the digital setting. To reduce complexity, this was omitted
572 from the "ALARM Information Security" project.

573

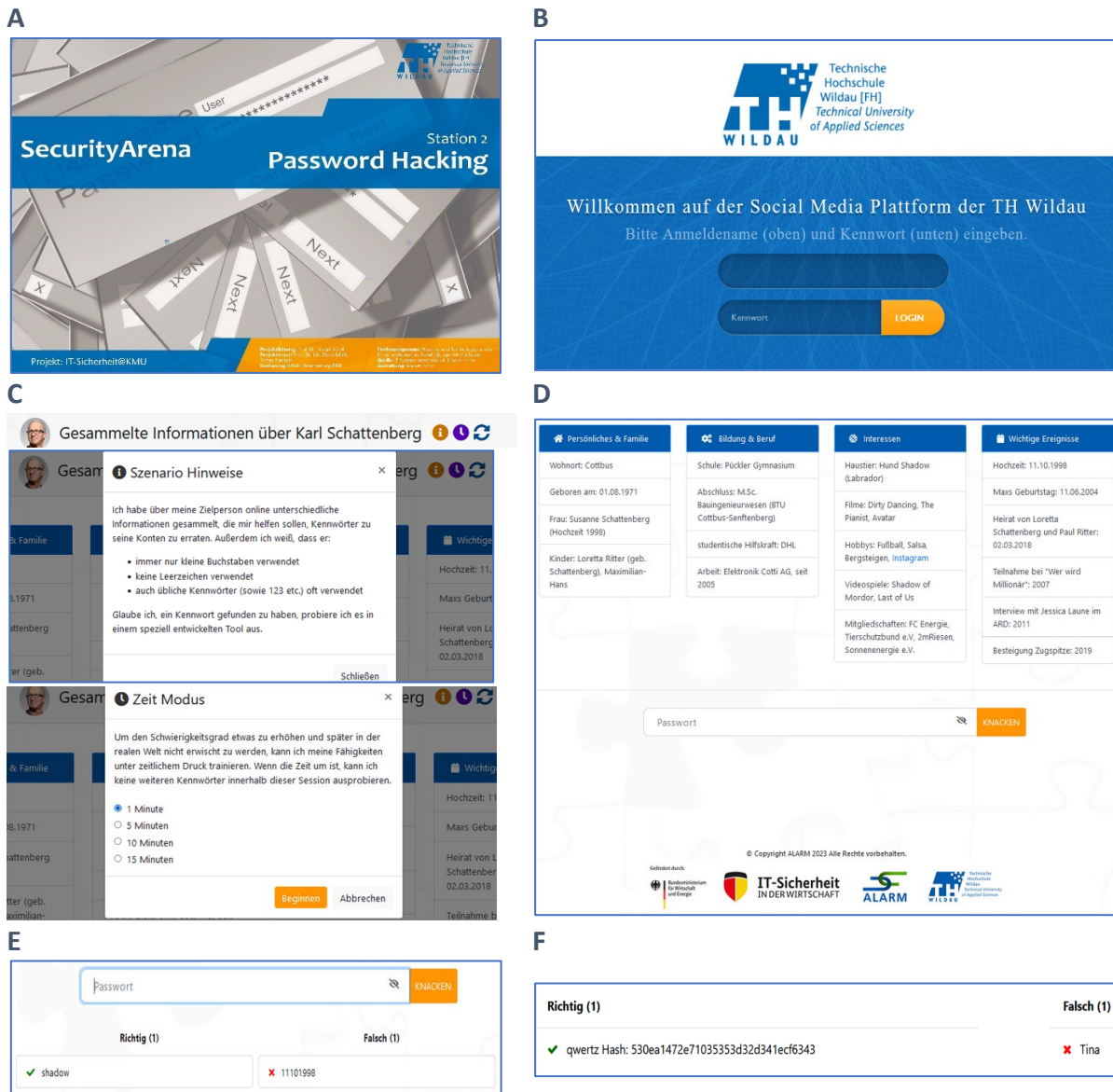


Figure 6 Digital add-ons to the "ALARM Information Security" project

3.3 Didactical background of the developed low-threshold security concepts derived from the seven on-site attack simulations

In addition to the seven analog and digital learning scenarios, the "ALARM information security" project also includes the results of seven on-site attacks for which another subcontractor, Thinking Objects, was primarily responsible. Ethical questions and the agreements with the managing directors of the pilot SMEs also play a key role. Additional practice-oriented instructions and tips for low-threshold security concepts for SMEs emerge from the findings. These are now available. Conducting on-site attacks is tricky and must be done with extreme caution. The aim of our project is to enhance employee awareness: the procedure should thus not be perceived by employees as an "attack" on their personal work processes or lead to personal exposure. Specific didactic aspects of the seven developed on-site attack simulations are briefly described below. Each simulation comes with two downloads: an information sheet and a low-threshold security concept. Again, as a result of funding from the BMWK, all materials are available in German free of charge for internal, noncommercial use (see [21]).



592

593 *Figure 7 Seven new information sheets and low-threshold security concepts derived from seven on-site simulation attacks of*
 594 *the project "ALARM information security" [21] to raise information security awareness in SMEs. The funding applied*
 595 *only to the development of the German version.*
 596

597 **3.3.1 On-site attack simulation 1: CEO Fraud**

598 The information sheet [73] points out that everyone makes an important contribution to ensuring that
 599 the employer, the company, or you personally do not fall victim to a cyberattack. It then briefly explains
 600 what CEO Fraud is and why SMEs should be familiar with this attack method, because it involves a lot
 601 of money. The attacker sends a fake email to someone in the company, usually someone in the finance
 602 or accounting department [73]. The email looks like it comes from a CEO or other executive and asks
 603 the person to complete a financial transaction [73]. The reason for the transaction is often presented
 604 as urgent or secret in order to put the employee under pressure [73]. The fake emails are often very
 605 convincing and can be made to look official by including an imitation of the company logo and being
 606 written in the kind of language and style used by actual executives [73]. The information sheet advises
 607 end users to [73]

- 608
- 609 • check emails;
 - 610 • use authentication methods;
 - 611 • respect confidentiality;
 - 612 • verify the requested transaction internally; and
 - 613 • verify the contact(s).

614 The low-threshold security concept on the topic of CEO Fraud for management and IT managers [74]
 615 deals with technical measures such as email filters and organizational protective measures. It is em-
 616 phasized that with this type of attack, the number of technical protective measures in the area of CEO
 617 Fraud is limited, which is why organizational measures are significantly more effective [74]. Passwords
 618 also play a role here, because if the criminals have gained access to a management mailbox, technical
 619 protection measures will actually not work at all, and the attacker can write even more authentic
 620 emails or copy and use real emails with old payment orders [74]. The most important organizational
 621 measures are regular information and clear regulations. There must be clear procedures for reviewing
 622 requests and approving payments or transactions [74]. Possible exceptional situations should also be
 623 discussed in advance to determine whether special procedures will be established for this, such as
 624 telephone reassurance [74].

625 **3.3.2 On-site attack simulation 2: E-Mail Check**

626 We are responsible for our own information security, which is why we must also handle our own identity
627 data carefully. Email check and password security are therefore also important in the second simulation.
628 The information sheet [75] shows that identity theft is a relevant topic in the area of IT security.
629 Illegally copied collections of identity data leaks circulate in criminal circles via various media and those
630 affected often only find out about the existence of such leaks when their own identity is used illegally
631 and damage occurs [75]. Online tools are presented that allow end users to check whether their email
632 address is part of known large data leaks [75]. The usual protective measures are recommended [75].
633

634 It is also pointed out that no reputable company will ask for your password and that it is important to
635 be regularly informed about the current recommendations on password criteria [75]. The topic of passwords
636 is discussed in more detail in the low-threshold security concept for management and IT managers [76].
637 It should be noted that, in addition to regular changes, a password must always be changed
638 if there is a suspicion or certainty that it has fallen into someone else's hands [76]. In addition, two-
639 factor login and password-less login are briefly discussed [76].
640

641 **3.3.3 On-site attack simulation 3: Hacking**

642 Raising awareness of the security of one's own identity files also plays a major role when it comes to
643 hacking. The corresponding information sheet lists the following protective measures for end users
644 [77]:

- 645 • Use strong passwords and two-factor authentication.
 - 646 • Keep software and operating systems current with patches and updates.
 - 647 • Be careful and attentive when opening emails and attachments.
 - 648 • Use firewall and antivirus software.
 - 649 • Be careful and alert when using public Wi-Fi.
 - 650 • Carry out regular data backups.
 - 651 • Have healthy skepticism about unexpected requests.
 - 652 • Keep personal information private.
- 653

654 The low-threshold security concept on the topic of best practice protective measures for management
655 and IT managers [78] goes into these aspects in detail and also deals with the topics of risk assessment
656 and redundancy in the systems.
657

658 **3.3.4 On-site attack simulation 4: Phishing**

659 The information sheet on the subject of phishing makes it clear that phishing emails are one of the
660 main gateways for cyberattacks and can cause major economic and operational damage [79]. End users
661 are therefore also called upon to make an important contribution by paying greater attention to
662 protecting the company from this form of attack. The attackers target all the access data to the company
663 network and try to trick people in front of their screens into clicking on links or entering personal
664 access data on fake websites [79]. If access to the company network is successful, hackers can surreptitiously
665 paralyze systems or steal important data [79]. The following information is given to end users
666 [79]:

- 667 • Pay attention to discrepancies between the supposed sender and the email address used.
- 668 • Cybercriminals often rely on the urgency factor and try to put pressure on the recipient group
669 to act.
- 670 • Pay attention to the date and time.
- 671 • Often no personal salutation is used. In official emails you will generally be addressed by your
672 name.
- 673 • Incorrect spelling and grammar are often an indication of fake emails.

- 674 • Pay attention to the signature. Often this does not correspond to the company’s signature re-
675 quirements.

676

677 With regard to error culture, it is recommended that, in case of an attack, IT support be informed
678 immediately, and the compromised device disconnected from the (work or private) network and In-
679 ternet. In addition, reference is made to a public checklist with concrete action steps [80]. In the low-
680 threshold security concept [81], the topic is treated more intensively and primarily with regard to tech-
681 nical measures. Information is compiled in a generally comprehensible form for management and IT
682 managers: email filters, antivirus and endpoint protection, web filters, passwords, multi-factor authen-
683 tication, patch management, backups, hard drive Encryption, smartphones, the cloud, and tricks. How-
684 ever, organizational regulations also play an important role, especially with respect to the last point. It
685 is made clear that employees must react appropriately if they are tricked, and there must be a clearly
686 defined and communicated reporting channel in the company [81]. The helpdesk should be a central
687 contact point and have suitable measures available, based on a checklist on how to proceed [81]. In
688 such a case, accusations and blame quickly lead to users no longer asking or not reporting the next
689 time an incident occurs [81]. Here too, a positive error culture in the company is very valuable.

690

691 **3.3.5 On-site attack simulation 5: Smishing**

692 Smishing is a portmanteau combining SMS (short messages) and phishing (theft of access data via fake
693 messages or emails) [82]. A smishing attack is therefore a phishing attack via SMS, which is why the
694 corresponding information sheet has very similar content to the phishing information sheet [4a]. Since
695 2021, the BSI has been continuously providing public information about smishing attacks and their
696 increasing importance for cybercriminals [82]. The following tips are compiled for end users in the
697 “Error Culture” section of the information sheet [83]:

- 698 • If the work cell phone is affected,
699 ○ activate airplane mode to unplug the device; and
700 ○ inform your IT department.
- 701 • If the private cell phone is affected,
702 ○ activate airplane mode to unplug the device;
703 ○ inform your mobile phone provider;
704 ○ file a criminal complaint with the local police station, being sure to take your
705 smartphone with you; and
706 ○ back up all your important data such as photos and documents locally—for example,
707 via a USB connection. After you have filed a report, reset your smartphone to factory
708 settings. With a factory reset, all your saved and installed data will be lost. However,
709 this step is necessary to completely remove the Android malware distributed via the
710 current SMS spam messages.

711

712 The low-threshold security concept also briefly explains alternatives such that a company smartphone
713 does not need to be used directly in the internal company network as an access point for attacks [84].

714

715 **3.3.6 On-site attack simulation 6: Tailgating**

716 Tailgating is a physical security attack in which an unauthorized person attempts to gain access to a
717 building or a specific area within the building. This is often achieved by the person walking through a
718 secured door directly behind an authorized employee [85]. The corresponding information sheet
719 makes it clear that tailgating is one of the classic social engineering attacks [85]. A social engineer is a
720 psychologically well-trained person who often exploits employees’ human traits, such as helpfulness,
721 respect for authority/uniforms, and trust, in order to gain unauthorized access to a site or building. By

722 raising their own awareness, employees can recognize the dangers and help prevent unauthorized
723 persons from gaining access to protected areas by [85]

- 724 • remaining vigilant at all times and ensuring that no unauthorized person follows;
- 725 • using the company's access systems and not sharing access cards or keys with others;
- 726 • politely but firmly asking unauthorized persons to move away from a secured area;
- 727 • remaining calm and controlled and not provoking an attacker;
- 728 • notifying the security services; and
- 729 • reporting incidents to company management.

730

731 The low-threshold security concept for SMEs [86] covers the aspects of access control, visit manage-
732 ment, and clean-desk and clear-screen policy as well as the locking of rooms and of sensitive data and
733 devices. In addition, renewed emphasis is put on the importance of having a clear reporting channel
734 for such a safety-relevant event, which must be known to the employees [86].

735

736 **3.3.7 On-site attack simulation 7: Incident response**

737 An incident is an unexpected event that affects the IT security or operations of a company, such as a
738 cyberattack, data leak, physical damage to IT systems, or the failure of critical applications and services
739 [87]. If employees suspect an incident, they should immediately report it to their manager or the IT
740 department, as a quick report is important to minimize the damage and facilitate the restoration of
741 normal operations [87].

742

743 For management and IT managers, the low-threshold security concept [88] primarily addresses the
744 special importance of emergency management in the area of IT security. It briefly describes how to
745 deal with emergencies that can threaten the existence of the company [88]. Relevant questions are
746 posed so that managers can see whether they are able to answer them on behalf of their company
747 and are therefore prepared for emergencies.

748 **4. Discussions and Reflection**

749

750 **4.1 Story and game dynamics of the seven analog games**

751

752 With 15 minutes per serious analog game, a circuit training with four learning stations can be set up
753 so that participants cover four topics in one hour. However, the time frame can also be intensified and
754 last up to an hour with discussions between interested participants. These analog scenarios are based
755 on one person as a moderator for each serious game (learning station), who has spent from 10 to 60
756 minutes familiarizing themselves with the game descriptions. Moderators can also be chosen from the
757 target group itself. The group size per station should be a minimum of four people and a maximum of
758 twenty people. From our experience, the optimal group size for an intensive exchange is eight to
759 twelve people per station.

760

761 **Story and game dynamics of analog serious game 1: Home Office**

- 762 • As part of this serious game, we see the house on the playing area where the friendly couple
763 Yvonne and Thomas work; they live together with Thomas's father and Anke and Marco, their
764 children.
- 765 • Seventeen scenarios are assigned to your work, each containing an information security or data
766 protection risk. The risks are described on seventeen orange risk cards, with the corresponding
767 protective measures on seventeen green protection cards.
- 768 • The orange risk cards should first be placed on the corresponding scenarios, and in a second
769 round the green protection cards should be placed on the appropriate risks.

- 770
- 771
- 772
- 773
- 774
- 775
- 776
- 777
- Start the clock as soon as the team begins placing the risk cards corresponding to the appropriate scenarios on the playing area.
 - Stop the time after 2½ minutes. Put the risk cards that were misplaced in the correct position and count the points.
 - Start the timer again once the team begins matching the protection cards next to the relevant risk cards. Stop the time after another 2½ minutes (a total of 5 minutes).
 - Scoring: there is one point for each correctly sorted card (with two pre-sorted example cards, there is a possible maximum of 32 points).

778

779 **Story and game dynamics of analog serious game 2: Multi-Factor Authentication**

- 780
- 781
- 782
- 783
- 784
- 785
- 786
- 787
- 788
- 789
- This serious game consists of several parts and follows the logic of escape games.
 - First, the twenty password cards should be ranked according to their strength by distributing them on the twenty boxes in the playing area in the correct order from 1 to 20.
 - The numerical codes of the top three cards, in the correct order of the “Strength” ranking, give the appropriate numerical code for the large box—i.e., the combination lock can be opened with this three-digit code.
 - In the large box, there is a small box with a lock, to which the corresponding key should be found (document bag!) and used.
 - Once the small box is opened, the serious game is over.
 - Scoring: A maximum of 30 points can be scored, 20 for the correct order of the passwords (one point for each correctly positioned password), and 5 points each for opening the two boxes.

790

791

792 **Story and game dynamics of analog serious game 3: The Five Phases of CEO Fraud**

- 793
- 794
- 795
- 796
- 797
- 798
- 799
- 800
- 801
- 802
- 803
- 804
- 805
- 806
- 807
- 808
- 809
- 810
- As part of this serious game, we see a kind of infographic on the playing area that depicts the five main phases typically found in CEO Fraud (research, testing, maintaining contacts, attack, damage) as a process.
 - Each of the five main phases is divided into further detailed process steps (twenty-one in total), each represented on the playing cards with a suitable icon and the associated plain text label.
 - These twenty-one playing cards should be sorted on the playing field in the correct processing order. The three “wrong” cards that do not fit into this process are sorted out by the participants.
 - It can be helpful to instruct the participants to first sort all the cards into categories according to the five main phases and then start with the detailed assignment.
 - Optionally, in a second part of the exercise, the four cards that use phishing to initiate CEO Fraud or support scam should be selected from the six email cards and placed in the center of the playing area. The two non-critical cards are placed next to the playing area.
 - Start the clock as soon as the team begins placing the playing cards on the appropriate spaces on the playing area.
 - After 6 minutes, stop the time, rearrange the playing cards that were incorrectly placed, and count the points.
 - Scoring: there is one point for each correctly sorted card (maximum: 24 points; optionally including e-mail cards: 30 points).

811

812 **Story and game dynamics of analog serious game 4: Mobile Communication, Apps & Co.**

- 813
- 814
- 815
- 816
- 817
- 818
- On the playing area of this serious game, we see a section through three floors of a subway station and a house in the background as the central key visual. This learning card with a hidden object picture shows twelve scenarios for smartphone or app use as well as focused smartphones with screenshots belonging to the scenarios on the edges.
 - Twelve information security and data protection risks are assigned to the twelve numbered scenarios and twelve numbered smartphones that match the scenarios in the subway station or

819 house. The risks are described on twelve orange risk cards, and the corresponding protective
820 measures, on twelve green protection cards.

- 821 • First, the orange risk cards should be placed on the corresponding scenarios; in a second round,
822 the green protection cards should be placed on the appropriate risks.
- 823 • Start the clock as soon as the team begins placing the risk cards corresponding to the appropriate
824 scenarios on the field.
- 825 • Stop the time after 2½ minutes. Put the risk cards that were misplaced in the correct position and
826 count the points.
- 827 • Start the stopwatch again once the team begins matching the protection cards to the relevant risk
828 cards. Stop the time after another 2½ minutes (for a total of 5 minutes).
- 829 • Scoring: there is one point for each correctly sorted card (maximum: 24 points).

830

831 **Story and game dynamics of analog serious game 5: Cyber Pairs (Social Engineering)**

- 832 • First, the thirty-two blue cyber memo cards should be arranged so that sixteen correct cyberse-
833 curity terms are created—next to each other in two columns, each with space for two more cards
834 to the right of the two blue ones.
- 835 • In the second round, the sixteen orange cyber risk cards with the definitions should be assigned
836 to the sixteen terms and placed next to the blue cyber memo card on the right.
- 837 • In the third round, the sixteen green cyber protection cards with prevention measures should be
838 placed next to the orange cyber risk cards.
- 839 • Scoring: One point is awarded for each correctly sorted term from two blue cyber memo cards
840 (maximum 16 points in the first round). For each additional cyber risk card (orange, second round)
841 and each additional matching cyber protection card (green, third round), there is one additional
842 point for each correct assignment (a maximum of 16 additional points per round). A total of up to
843 48 points can be achieved in three rounds.

844

845 **Story and game dynamics of analog serious game 6: Data and Information Protection**

- 846 • As part of this serious game, we see five typical scenarios from the administration building of a
847 model company in which customer rights play a role (first row from top) and eleven scenarios,
848 each of which is on the playing area in the style of a hidden object picture, containing information
849 security or data protection risks (in the second and third rows).
- 850 • First, all sixteen blue and green playing cards on the playing area should be arranged in one go so
851 that they match the scenarios shown.
- 852 • Optionally, in a second part of the game, the “picture frame” cards can be brought into play to
853 simulate the distinction between personal and non-personal data.
- 854 • For this purpose, those cards that do NOT contain any personal information are placed on the
855 walls of the offices on the playing field wherever there is space. The personal cards are not placed
856 and are therefore sorted out.
- 857 • Scoring: For each correctly sorted card there is one point (16 for part one, and 6 for part two—
858 i.e., only for those placed on the playing area: a maximum of 22 points).

859

860 **Story and game dynamics of analog serious game 7: Information Class Roulette**

- 861 • The moderator or a participant spins the roulette wheel and inserts a ball.
- 862 • The number received decides which category a card should be drawn from—for example, the
863 “Five,” the top card from the classification category “General Classification” is drawn and dis-
864 cussed.
- 865 • If the roulette wheel puts the ball on the “zero,” a category can be selected.
- 866 • The participants take turns reading the contents of the card they have drawn out loud.

- 867 • The statement given there must be judged as “true” or “false” by assigning the allocated chips in
868 the playing area to “TRUE” or “FALSE.”
- 869 • The teams are free to decide on the number of chips or their amount; however, you must bet a
870 minimum of 5 chip points per card drawn.
- 871 • After the chips have been placed, the moderator resolves the correct answer and explains the
872 background, although discussions will need to be reduced as the game progresses
- 873 • Teams with a correct answer receive their amount plus half of their “stake” back, and an addi-
874 tional amount of at least 5 chip points. The chips of the teams with the wrong answer go to the
875 “bank”—i.e., they are confiscated by the moderator.
- 876 • The ball is then thrown into the roulette wheel again, as allowed by the playing time, after which
877 a new playing card is drawn.
- 878 • Scoring: At the end of the game, the team with the most points wins.
- 879 • Note: This moderation guide refers to teams. The game can also be played by individual people
880 against each other.

881

882 **4.2 The goals of the seven digital games**

883

884 The game dynamics of the digital games is that in every digital serious game, the players take on chang-
885 ing roles [72]—e.g., they act as security specialists, hackers, investigators, or artificial intelligence. In
886 this way, they get to know and understand the topics from different perspectives. The participants
887 make decisions and thereby determine the further course of the story. With every decision, they em-
888 bark on their own personal learning journey, which is determined by their knowledge and preferences.
889 Every serious game contains two to three learning paths that the players take through their decisions.
890 At the end of a game, participants receive feedback on the points they achieved. This includes sugges-
891 tions and requests to the players as well as a short summary of the lessons learned in the specific
892 game. Over the course of the game, messages are displayed that draw attention to advantageous or
893 disadvantageous decisions and behaviors. In addition, a lexicon module offers participants the oppor-
894 tunity to read important information security terms before and after the game.

895

896 The goals of the digital serious games are as follows:

- 897 • The aim of serious game 1 (The First Day) is to introduce players to the topic of information
898 security using classic situations involving social engineering and password protection, which of-
899 fer a high level of identification for all players. Participants’ understanding of safety and social
900 skills are assessed.
- 901 • The aim of serious game 2 (The Hacker’s Attack) is to familiarize players with the common strat-
902 egies used by hackers in a real situation, looked at from the hacker’s perspective, and to experi-
903 ence in a playful way how even the smallest security gaps are enough to allow hackers access.
904 Efficiency and the variability of attack routes that the players try out are evaluated.
- 905 • The aim of serious game 3 (The Search for Clues) is for players to uncover common CEO Fraud
906 practices and take effective protective measures. Time plays a special role in this topic: only if
907 the players resolve the attack in time can they prevent greater damage. Efficiency, discovered
908 learning content and social skills are assessed.
- 909 • The aim of serious game 4 (AI in the Home Office) is for players to identify the most common
910 mistakes that people make in the home office carrying out smaller tasks. Practical and funny
911 examples are used to draw attention to the pitfalls of working from home. Security awareness
912 and machine learning are assessed.
- 913 • The aim of serious game 5 (Everything Just CLOUD) is for players to uncover common CEO Fraud
914 practices and take effective protective measures. Time plays a special role in this topic: only if

915 the players resolve the attack in time can they prevent greater damage. Efficiency, discovered
916 learning content, and social skills are assessed.

917 • The aim of serious game 6 (Information Classification) is for players to uncover common CEO
918 Fraud practices and take effective protective measures. Time plays a special role in this topic:
919 only if the players resolve the attack in time can they prevent greater damage. Efficiency, dis-
920 covered learning content and social skills are assessed.

921 • The aim of serious game 7 (Ransomware) is for players to uncover common CEO Fraud practices
922 and take effective protective measures. Time plays a special role in this topic: only if the players
923 resolve the attack in time can they prevent greater damage. Efficiency, discovered learning con-
924 tent, and social skills are assessed.

925

926 **4.3 Results of the seven on-site attack simulations**

927

928 Every on-site attack simulation must be designed in such a way that it does not have a negative impact
929 on the working atmosphere and the culture of trust in the company. It is important to ensure that
930 employees feel safe/secure in their work environment and see the on-site attacks as a supporting tool
931 to raise awareness. The attacks were always discussed with the responsible persons in the company,
932 and all employees receive all the relevant information and results before and/or after the attacks, so
933 that these attacks do not damage the company's trust and error culture.

934

935 By educating yourself, for example, about the fraud method, you can minimize risks, identify fraud
936 attempts, and take appropriate measures to protect yourself. The information sheet advises end users
937 for protection [73]. The low-threshold security concept on the topic of CEO Fraud for management and
938 IT managers [74] deals with technical measures such as email filters and organizational protective
939 measures. The last point in the information sheet is the error culture in the company, as mistakes can
940 happen to all of us. If a person falls for the fake email, he/she will complete the requested transaction
941 without realizing it is a scam [73]. The money is then usually transferred to an account controlled by
942 the fraudsters; in some cases, confidential information such as company secrets or employee data is
943 stolen, too [73]. In such a case, action must be taken very quickly, which is why the company must be
944 open about errors. Possible exceptional situations should also be discussed in advance and whether
945 special procedures will be established for this, for example telephone reassurance [74].

946

947 With regard to error culture, the recommendation in the phishing example is that IT support should
948 be immediately informed, and the compromised device disconnected from the (work or private) net-
949 work and Internet. In addition, reference is made to a public checklist with concrete action steps [80].
950 However, organizational regulations also play an important role, especially with regard to the last as-
951 pect. It is made clear that employees must react appropriately if they are tricked, for which there must
952 also be a clearly defined and communicated reporting channel in the company [81]. The helpdesk
953 should be a central contact point and have suitable measures available based on a checklist on how to
954 proceed [4b]. In such a case, accusations and blame quickly lead to users no longer asking or not re-
955 porting the next time an incident occurs [81]. Here too, a positive error culture in the company is in-
956 valuable.

957

958 When it comes to tailgating, the company must have a clear reporting channel for such a security-
959 relevant event, which must be known to the employees [86]. At the end of the security concept train-
960 ing, management and IT managers are reminded of the need for employee awareness to be raised.
961 How sensitive the employees should be, or how low-threshold the reports of incidents should be must
962 be based on the protection needs of the particular company area and communicated accordingly [86].
963 For management and IT managers, the low-threshold security concept [88] primarily addresses the
964 special importance of emergency management in the area of IT security. The incident management

965 story includes a brief description of how to deal with emergencies that can threaten the existence of
966 the company [88]. With the help of relevant questions, managers discover whether they can answer
967 such questions on behalf of their company and are thus prepared for emergencies. In the event of an
968 IT security emergency, targeted communication with customers, partners, and employees is important
969 [88]. In addition, depending on the extent of the emergency, the police, the BSI and, if necessary, the
970 public must also be informed from a certain point in time. Emergency management is important for all
971 institutions and always has two sides: a proactive aspect with preventive measures that must be im-
972 plemented, and a reactive aspect with coping measures that will hopefully be effective in an emer-
973 gency. In addition to setting up an appropriate information security management system (ISMS), an
974 SME also needs to take care of an effective business continuity management system. Larger and me-
975 dium-sized companies can use BSI Standard 200-4 [89] as a guide; smaller and microenterprises should
976 establish minimum measures.

977 **5. Conclusions**

978

979 In the future, hardly anything will work without information technology—but it will only work with it
980 if the basic values and protection goals of information security as well as the guarantee goals of data
981 protection are integrated, observed, and actively implemented. Using secure digital processes, digital
982 technologies, and digital business models, and thus securing and increasing the competitiveness and
983 innovative ability of German medium-sized businesses is a MUST for Germany, for the prosperity of its
984 citizens, for the further development of SMEs, and for the authorities funding new programs.

985 We are dealing with an increasingly dynamic environment of digitization, which is characterized by a
986 constantly changing threat situation and a variety of new and old attack vectors. Individuals, the econ-
987 omy, and society as a whole are all affected. A sustainable level of security can only be effectively
988 guaranteed in all institutions through an ongoing systematic approach to adequately protect business
989 processes with a continuous improvement process. A correspondingly well-thought-out, appropriate
990 ISMS with adapted, effective security process and qualified personnel must be established in the insti-
991 tutions [3]. The use of technology is essential, but, without people, a security process will not work or
992 be viable. When developing analog and digital learning scenarios (serious games / realistic simulations)
993 for information security awareness, we discovered that the term “gamification” is largely unknown in
994 German SMEs and needs to be explained first. Afterwards, the principle was understood and made
995 sense to most respondents [90].

996 The increasingly comprehensive digitization of business processes requires analog sensitization. Our
997 modern game-based analog awareness-raising program, which has long-term positive effects on infor-
998 mation security and data protection includes the following features:

- 999 • Active involvement of the participants
- 1000 • Use of haptics to enhance comprehension
- 1001 • Interactivity
- 1002 • Discursive settings
- 1003 • Stories/narratives as an aide-memoire
- 1004 • Ability to contribute personal experience
- 1005 • Flexible scheduling (from 15 minutes during a break to an hour for intensification).

1006 However, it is becoming clear on the basis of repeated instances that the game-based training of se-
1007 curity awareness in German SMEs should not be focused on the idea of play, which causes awareness-
1008 raising measures to be met with significant resistance [90]. The managers of SMEs putatively take a
1009 customer-oriented perspective. The in-depth psychological background is that information security in

1010 SMEs is primarily aimed at customers, and therefore the devaluation of the gamified aspects of training
1011 among managers can be interpreted as a projection [90]. The supposedly pejorative perspective of the
1012 customers is taken here, so that, in the opinion of many managers, any efforts made in the context of
1013 information security would be in vain [90]. This is a consequence of the fact that information security
1014 in German SMEs has so far been determined by extrinsic factors. However, managers should also rec-
1015 ognize intrinsic factors that make information security critical to their organization.

1016 Based on our experiences in the “ALARM Information Security” project and in previous security pro-
1017 jects with a focus on “the human factor” and with a wide variety of target groups and actors, this is
1018 achieved through visualization, narration, and reducing complexity, while at the same time building an
1019 understanding of complex conditions. This would probably also bring people closer to the technologies
1020 of the future: they should be informed in a participatory manner, be involved in discussions that pro-
1021 mote understanding, be able to engage proactively, and take part on an equal footing [91].

1022 Peter Danil (2023) from the BSI recently reiterated the following point:

1023 “Everyone is under attack.
1024 There are no exceptions!” [92]

1025 As Tim Berghoff (2023) puts it,

1026 “Neither criminals nor industrial spies
1027 are interested in the size of a company.” [93]

1028

1029 What is of interest are the products, the content, the business processes, the structure, the partners,
1030 and the business relationships (as well as the private relationships that make people vulnerable to
1031 blackmail). The EU’s NIS 2 directive is intended, among other things, to strengthen security along the
1032 value and supply chains [93]). According to Berghoff (2023), it is already clear here that more compa-
1033 nies will be directly affected by NIS-2 than many IT managers would assume [93].

1034 Our evaluation results from the developed learning scenarios can be summarized as follows [94]:

- 1035
- 1036 • Gamified security awareness in the form of the serious games developed is taken seriously by
1037 the participants. They are viewed as an important component of information security and also
1038 have a revitalizing effect. This means that when playing the learning scenarios, all participants
1039 were motivated, in a good mood, and concentrated, and everyone was also on task when it
1040 came to feedback during the review.
 - 1041 • In our experience, we have succeeded with the help of gamification in bringing awareness-
1042 raising measures to a level that ensures the involvement of those involved. The awareness-
1043 raising performance of the learning scenarios significantly exceeds the usual learning theory
1044 approaches and works well with all participating groups.
 - 1045 • The didactic concept on which the learning scenarios are based in the “ALARM Information
1046 Security” project—“Talking Security”—also works smoothly in SMEs. Above all, the discursive
1047 setting and the team-oriented interactions in the analog learning scenarios promote conver-
1048 sations about “real-life situations” and confirm the project’s suitability as a simulation of real
1049 work and everyday scenarios.

1050 Our discursive, team-oriented storytelling approach is also borne out internationally. Leitner (2023)
1051 uses dynamic surveys in the digital awareness exercises, which go beyond our customizable digital
1052 learning scenarios, in order to visualize individual decisions for all participants during the digital exer-
1053 cise [95]. We can summarize our essential aspects according to Leitner (2023) as follows [95]: The story
1054 must be

- 1055 • captivating, inspiring participants, while getting them to concentrate;
- 1056 • interactive, actively involving participants by having them make decisions;

- 1057
- 1058
- 1059
- 1060
- 1061
- 1062
- informative so that participants receive immediate feedback on their decisions;
 - security conscious, including one or more security incidents;
 - comprehensible and close to the reality of participants; and
 - involving, ensuring that participants submit their [digital] decisions, with answers typically anonymized

1063

1064

1065

1066

1067

1068

1069

1070

1071

1072

It should also be noted that a training approach that only emphasizes the technical aspects not only does not work [96] but the resulting overtaxing of most employees with too much technical information can even have a negative effect through the training [97]. In addition, it has been scientifically recognized for decades that a mix of different methods is necessary for different target groups, different learning types, and abstract topics (see, for example, [98], [99]). Alshaikh et al. (2018) confirms that linking information security with the private life of employees on the topic of information security has a motivating effect [100]. In addition, international study results suggest that informal methods for increasing employees' security awareness are effective and cost-effective and measures to promote the exchange of advice can lead to an improved security situation [101].

1073

1074

1075

1076

1077

1078

1079

1080

1081

1082

1083

1084

1085

As an outlook, we assumed that an interdisciplinary team will definitely have to integrate psychological aspects and tests for ISA in future awareness projects. According to Sykosch (2022), the established quality criteria for psychological tests are: Objectivity, reliability, validity, scalability, normalization, economics, usefulness, reasonableness, non-falsifiability, and fairness [102]. The first [90] and second study [94] of the "ALARM Information Security" project showed that no two German SMEs are the same. This has an impact on the fit and use of the learning scenarios developed in the project, even if no fine-grained differentiation was diagnosed in the project owing to the necessity for basic sensitization. SMEs must therefore think about which learning scenario—provided free of charge—can be used sensibly for which target group, at what time and in what way. To achieve this, employees should be trained as moderators. Moderators for awareness-raising measures within an SME would have the task of using practical, pictorial, narrative methods and formats in order to illustrate relevant but abstract topics and thus eliminate significant barriers to information security within the SME.

1086

1087

1088

1089

1090

1091

1092

1093

1094

1095

1096

1097

We also recognized that the level of maturity of the German SME is obviously crucial for the sustainable use of such modern simulations. The project also made it clear that the awareness maturity level correlates with the digital autonomy of employees. If the digital autonomy of employees in SMEs is not promoted by not allowing anything, then measures to increase security awareness will remain ineffective because employees will feel disempowered, and they will not accept the security measures. This can, in turn, lead to (unconscious) resistance and, as a result, to new security incidents. Sensitization and security awareness are therefore "internal social work" [90, 94] and require role modeling from managers, a discourse about concrete experiences with security measures and their necessity within business processes, and active involvement of employees in the improvement processes. Combined with "giving SMEs more of a hand," consulting companies could also have their employees trained in experience-oriented moderation for better support.

1098

1099

1100

1101

1102

So, as a first step, it is to be hoped that many German SMEs will seize this opportunity to increase the necessary information security awareness (ISA) in their company and proactively implement our tools from the "Awareness Lab SME (ALARM) Information Security." Memorable stories (narratives, storytelling) should be developed about the security situation that use imagination and metaphors to help reduce topic complexity and simplify security communication. Above all, we advocate systemic

1103 communication with, in particular, “discursive didactics” and an increase in the principle of “talking
1104 security” in SME business processes.

1105 Acknowledgements

1106
1107 I am grateful to our long-standing security awareness partner, the firm known_sense, and the other
1108 subcontractors, Gamebook Studio GmbH, Thinking Objects GmbH, and sudile GbR, whose individual
1109 input on the project is documented on the project website. A special word of thanks to my university
1110 research team (in various constellations) for their great commitment to all of our projects. Finally, I
1111 would like to acknowledge the anonymous reviewers for their helpful critical comments. Many thanks,
1112 too, to Simon Cowper for his detailed and professional proofreading of the text.

1113 Funding

1114
1115 As project manager and initiator of all Wildau University’s awareness projects, I would like to thank
1116 the German Federal Ministry for Economic Affairs and Climate Action for funding the current project,
1117 “Awareness Lab SME (ALARM) Information Security,” which runs from October 2020 to March 2024.

1118 References

- 1119 [1] BSI—Bundesamt für die Sicherheit in der Informationstechnik/Federal Office for Information Security (Ed.), Die Lage der
1120 IT-Sicherheit in Deutschland/The situation of IT security in Germany (in German).
1121 <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410>,
1122 2023 (accessed 7 November 2023).
- 1123 [2] F. Quader, V.P. Janeja, Insights into organizational security readiness: Lessons learned from cyber-attack case studies.
1124 *Journal of Cybersecurity and Privacy*. 1/4 (2021) 638-659.
- 1125 [3] M. Scholl, E.P. Ehrlich, E.-P. Information Security Officer: Job profile, necessary qualifications, and awareness raising ex-
1126 plained in a practical way, Buchwelten-Verlag, Frankfurt am Main, 2020.
- 1127 [4] Y. Li, N. Zhang, M. Siponen, Keeping secure to the end: a long-term perspective to understand employees’ consequence-
1128 delayed information security violation, *Behaviour & Information Technology*, 2018. doi: 10.1080/0144929X.2018.1539519.
- 1129 [5] I. Henseler-Unger, A. Hillebrand, Aktuelle Lage der IT-Sicherheit in KMU/ Current situation of IT security in SMEs (in Ger-
1130 man), *Datenschutz und Datensicherheit (DuD)* 42, 686–690 (2018). <https://doi.org/10.1007/s11623-018-1025-y>.
- 1131 [6] DIHK—Deutscher Industrie- und Handelskammertag e. V. (Ed.). Zeit für den digitalen Aufbruch: Die IHK-Umfrage zur Di-
1132 gitalisierung/Time for the digital awakening: The IHK survey on digitization (in German). <https://www.ihk.de/blueprint/servelet/resource/blob/5488158/8d01cc3ef58c3a251d6520f2ac4653b2/ergebnisse-der-ihk-digitalisierungsumfrage-data.pdf>,
1133 2022 (accessed 2 November 2023).
- 1135 [7] BSI—Bundesamt für die Sicherheit in der Informationstechnik/Federal Office for Information Security (Ed.), ORP.3: Sensi-
1136 bilisierung und Schulung/Sensitization and training (in German). https://www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-GrundschutzKompodium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html, 2016 (accessed 17 January 2018).
- 1138 [8] A. Tsohou, M. Karyda, S. Kokalakis, E. Kiountouzi, Analyzing trajectories of information security awareness, *Information
1139 Technology & People*. 25 (2012) 327-335.
- 1140 [9] G. Stewart, D. Lacey, Death by a thousand facts: Criticising the technocratic approach to information security awareness.
1141 *Information Management & Computer Security*. 20 (2012) 29-38.
- 1142 [10] I. Kirlappos, A. Beautement, M.A. Sasse, ‘Comply or die’ is dead: Long live security-aware principal agents, in: A.A. Adams,
1143 M. Brenner, M. Smith (Eds.), *Financial Cryptography and Data Security*, Lecture Notes in Computer Science, Springer, Heidel-
1144 berg, 2013, 7862, pp. 70-82.
- 1145 [11] T. Fagade, T. Tryfonas, Security by compliance? A study of insider threat implications for Nigerian banks, in: T. Tryfonas,
1146 (Ed.), *Human Aspects of Information Security, Privacy, Trust*, HAS 2016, Lecture Notes in Computer Science, Springer,
1147 Cham., 2016, 9750, pp. 128-139.
- 1148 [12] D. Pokoyski, Security Awareness: Von der Oldschool in die Next Generation – eine Einführung, in: M. Helisch, D.
1149 Pokoyski, (Eds.), *Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung*, Vieweg+Teubner.
1150 Wiesbaden, 2009, pp. 1–8.
- 1151 [13] B. Khan, K.S. Alghathbar, S.I. Nabi, M.K. Khan, Effectiveness of information security awareness methods based on
1152 psychological theories, *African Journal of Business Management*. 5/26 (2011) 10862–10868.
- 1153 [14] M. Beyer, S. Ahmed, K. Doerlemann, S. Arnell, S. Parkin, A. Sasse, N. Passingham, Awareness is only the first step: A
1154 framework for progressive engagement of staff in cyber security. Hewlett Packard, Business White Paper, 2016.

- 1155 [15] M. Scholl, F. Fuhrmann, D. Pokoyski, Information security awareness 3.0 for job beginners, in: J.E. Varajão, M.M. Cruz-
1156 Cunha, R. Martinho, R. Rijo, N. Bjørn-Andersen, R. Turner, D. Alves (Eds.), Proceedings of the Conference on ENTERprise
1157 Information Systems (CENTERIS), 2016, pp. 433-436.
- 1158 [16] H. Kruger, L. Drevin, T. Steyn, Email security awareness: A practical assessment of employee behavior, in: L. Futcher, R.
1159 Dodge (Eds.), Fifth World Conference on Information Security Education, IFIP – International Federation for Information
1160 Processing, Springer, Boston/MA, 2007, 237, pp. 33-40.
- 1161 [17] K. Aytes, C. Terry, Computer security and risky computing practices: A rational choice perspective, Journal of Organiza-
1162 tional and End User Computing. 16, 2004, 22-40.
- 1163 [18] M. Scholl, Information Security Awareness in Public Administrations, in: U. Comite, Public Management and Admin-
1164 istration, Open Access: INTECH d.d.o. Rijeka (InTechOpen). <https://www.intechopen.com/chapters/59667>, 2018 (accessed 6
1165 January 2024).
- 1166 [19] M. Scholl, F. Fuhrmann, L.R. Scholl, Scientific Knowledge of the Human Side of Information Security as a Basis for Sus-
1167 tainable Trainings in Organizational Practices, in: Proceedings of the 51th Hawaii International Conference on System Sci-
1168 ences (HICSS), Big Island, Hawaii, 2018, 2235-2244. <http://hdl.handle.net/10125/50168> (accessed 20 January 2018).
- 1169 [20] S. Alotaibi, S. Furnell, Y. He, Towards a Framework for the Personalization of Cybersecurity Awareness, in: International
1170 Symposium on Human Aspects of Information Security and Assurance, Springer Nature Switzerland, Cham, 2023, pp. 143-
1171 153.
- 1172 [21] Homepage of the project “Awareness Lab SME (ALARM) Information Security”. <https://alarm.wildau.biz/> (German),
1173 <https://alarm.wildau.biz/en> (English), 2023 (accessed 2 February 2024).
- 1174 [22] M. Scholl, R. Schuktomow, H. von Tippelskirch, F. Prott, P. Koppatz, D. Pokoyski, U. Küchler, M. Vogt, Neue Wege für
1175 mehr Informationssicherheit in KMU: Projektdokumentation Awareness Labor KMU (ALARM) Informationssicherheit, M.
1176 Scholl (Ed.), Buchwelten Verlag, Frankfurt/M, 2024, pp. 232.
- 1177 [23] AGCS—Allianz Global Corporate & Specialty SE (Ed.) (2022a). Allianz risk barometer 2022 (English version: worldwide
1178 results). https://www.allianz.com/en/press/news/studies/220118_Allianz-Risk-Barometer-2022.html (accessed 12 Septem-
1179 ber 2022).
- 1180 [24] AGCS—Allianz Global Corporate & Specialty SE (Ed.) (2022b). Allianz Risk Barometer 2022 (German version: results of
1181 Germany). <https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2022-press-de.html> (accessed
1182 10 February 2024).
- 1183 [25] M. Bada, A.M. Sasse, J.R. Nurse, Cyber Security Awareness Campaigns: Why do they fail to change behaviour? ArXiv,
1184 abs/1901.02672; 2019.
- 1185 [26] E. Tanriverdiyev, The state of the cyber environment and national cybersecurity strategy in developed countries. Studia
1186 Bezpieczeństwa Narodowego. 23/1 (2022) 19-26. <https://doi.org/10.37055/sbn/149510>.
- 1187 [27] R.C. Sharma, A. Zamfiroiu, Cybersecurity Threats and Vulnerabilities in the Metaverse, in: 2023 International Confer-
1188 ence on Intelligent Metaverse Technologies & Applications (iMETA), IEEE, 2023, pp. 1-7.
1189 doi: 10.1109/iMETA59369.2023.10294950.
- 1190 [28] T.O. Abrahams, S.K. Ewuga, S.O. Dawodu, A.O. Adegbite, A.O. Hassan, A REVIEW OF CYBERSECURITY STRATEGIES IN
1191 MODERN ORGANIZATIONS: EXAMINING THE EVOLUTION AND EFFECTIVENESS OF CYBERSECURITY MEASURES FOR DATA
1192 PROTECTION, Computer Science & IT Research Journal. 5/1 (2024) 1-25.
- 1193 [29] C. Posey, M. Shoss, Employees as a Source of Security Issues in Times of Change and Stress: A Longitudinal Examination
1194 of Employees’ Security Violations during the COVID-19 Pandemic. Journal of Business and Psychology. (2023) 1-22.
- 1195 [30] M. Helisch, D. Pokoyski (Eds.), Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung, Vieweg+
1196 Teubner, Wiesbaden, 2009.
- 1197 [31] R. Epstein, V.R. Zankich, The surprising power of a click requirement: How click requirements and warnings affect users’
1198 willingness to disclose personal information. PLoS ONE 17/2 (2022): e0263097. [https://doi.org/10.1371/jour-
1200 nal.pone.0263097](https://doi.org/10.1371/jour-
1199 nal.pone.0263097).
- 1200 [32] H. Paananen, M. Siponen, Organization Members Developing Information Security Policies: a Case Study. Rising like a
1201 Phoenix: Emerging from the Pandemic and Reshaping Human Endeavors with Digital Technologies. ICIS, 2023.
1202 https://aisel.aisnet.org/icis2023/cyber_security/cyber_security/14.
- 1203 [33] I. Kirlappos, M.A. Sasse, What usable security really means: Trusting and engaging users, in: Human Aspects of Infor-
1204 mation Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, He-
1205 raklion, Crete, Greece, June 22-27, 2014. Proceedings 2, Springer International Publishing (2014) pp. 69-78.
- 1206 [34] Landing page. Summary of projects. The project “IT-Sicherheit@KMU”/IT Security@SMEs (in German) was funded by
1207 the Land Brandenburg with ESF. <https://wildau.biz/>, 2014 (accessed 10 February 2024).
- 1208 [35] F. Fuhrmann, M.C. Scholl, D. Edich, P. Koppatz, L.R. Scholl, K.B. Leiner, E.P. Ehrlich, Informationssicherheitsbewusstsein
1209 für den Berufseinstieg. Final report of the Project “SecAware4job” (in German), Shaker, Aachen, 2017.
1210 doi: 10.2370/9783844054668.
- 1211 [36] Project website “SecAware4job”. The project was financed by the Horst Görtz Foundation (HGS).
1212 <https://secaware4job.wildau.biz/>, 2017 (accessed 10 February 2024).
- 1213 [37] known_sense (homepage). Compliance parcourses. <https://www.known-sense.de/compliance-parcours> (accessed 4
1214 January 2024).
- 1215 [38] Methodpedia website. <https://methopedia.eu/de/posts/learning-stations/learning-stations/> (accessed 4 January
1216 2024).
- 1217 [39] Project website “ALARM Information Security”. [https://alarm.wil-
dau.biz/static/21fb54f246157ed6a1668ee840dfec0f/handout-aLS-A4-final.pdf](https://alarm.wil-
1218 dau.biz/static/21fb54f246157ed6a1668ee840dfec0f/handout-aLS-A4-final.pdf), 2023 (accessed 4 January 2024).

- 1219 [40] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/64c89b39ca8fd082ca46962fd7dcfd8/moderation.pdf>, 2023 (accessed 4 January 2024).
- 1220 [41] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/fdb35a8e957e2b77ead449be5610b035/konstruktion.pdf>, 2023 (accessed 4 January 2024).
- 1221 [42] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/1a931bd03a1cc07d7aa195d8ca515ee3/handout.pdf>, 2023 (accessed 4 January 2024).
- 1222 [43] Project website "ALARM Information Security". <https://alarm.wildau.biz/als1/>, 2023 (accessed 4 January 2024).
- 1223 [44] M. Scholl, German SMEs & Home Office: Narrative-Driven Game-Based Awareness Raising with Long-Term Efficacy, in: S. Mistretta, Reimagining Education - The Role of E-learning, Creativity, Technology in the Post-pandemic Era, IntechOpen, London, 2023. <https://www.intechopen.com/online-first/1171513> (accessed 6 January 2024).
- 1224 [45] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/4e3dd32ac8b65dffdc6248d5a2899c1/moderation.pdf>, 2023 (accessed 4 January 2024).
- 1225 [46] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/4069f8d7ea17cad084dc0f8b49e452c1/konstruktion.pdf>, 2023 (accessed 4 January 2024).
- 1226 [47] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/7ef7165382627cd57d9a2b60f20caa27/handout.pdf>, 2023 (accessed 4 January 2024).
- 1227 [48] Project website "ALARM Information Security". <https://alarm.wildau.biz/als2/>, 2023 (accessed 4 January 2024).
- 1228 [49] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/03a867dc24427973dfe941f4f90694de/moderation.pdf>, 2023 (accessed 4 January 2024).
- 1229 [50] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/0e2cda8206ac30f3381b61431da1f295/konstruktion.pdf>, 2023 (accessed 4 January 2024).
- 1230 [51] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/5fdc750bb6399eaf7c42c06aee294d9a/handout.pdf>, 2023 (accessed 4 January 2024).
- 1231 [52] Project website "ALARM Information Security". <https://alarm.wildau.biz/als3/>, 2023 (accessed 4 January 2024).
- 1232 [53] M. Scholl, Raising Awareness of CEO Fraud in Germany: Emotionally Engaging Narratives Are a MUST for Long-Term Efficacy, in: Á. Rocha, C. Ferrás, W. Ibarra, Information Technology and Systems, Springer International Publishing, Cham, 2023. doi: 10.1007/978-3-031-33258-6_40.
- 1233 [54] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/1f91fc14e336446b8d14b649c47c4bcd/moderation.pdf>, 2023 (accessed 4 January 2024).
- 1234 [55] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/ee318d5d31472905f9beb598529ba621/konstruktion.pdf>, 2023 (accessed 4 January 2024).
- 1235 [56] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/dff-cfb290b5264185532b7ce21e43580/handout.pdf>, 2023 (accessed 4 January 2024).
- 1236 [57] Project website "ALARM Information Security". <https://alarm.wildau.biz/als4/>, 2023 (accessed 4 January 2024).
- 1237 [58] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/a09006b5358532fffd1ef9dc8232cd9/moderation.pdf>, 2023 (accessed 4 January 2024).
- 1238 [59] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/49f710e6d0dc14e82c2634533fb0601f/konstruktion.pdf>, 2023 (accessed 4 January 2024).
- 1239 [60] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/0abbc531a6825528d233fa0eee85d7fe/handout.pdf>, 2023 (accessed 4 January 2024).
- 1240 [61] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/d3a36f8873ae241bf327242ae37baf6f/druckvorlagen.pdf>, 2023 (accessed 4 January 2024).
- 1241 [62] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/16cf17b914c4dcd92e8ccd8b8d193a31/moderation.pdf>, 2023 (accessed 4 January 2024).
- 1242 [63] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/402265cad09aa5d2722b4ac0cf3d1f27/konstruktion.pdf>, 2023 (accessed 4 January 2024).
- 1243 [64] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/c821510cf4c34138161e22057cbf0dd2/handout.pdf>, 2023 (accessed 4 January 2024).
- 1244 [65] Project website "ALARM Information Security". <https://alarm.wildau.biz/als6/> (accessed 4 January 2024).
- 1245 [66] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/a732b3d5f31a1732b0a05b0d68451943/moderation.pdf>, 2023 (accessed 4 January 2024).
- 1246 [67] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/e77b171bec8e36204d9e4f604fcc508d/konstruktion.pdf>, 2023 (accessed 4 January 2024).
- 1247 [68] Project website "ALARM Information Security". <https://alarm.wildau.biz/static/a1111e0d37e4d6a93d365ace3a77b9ed/handout.pdf>, 2023 (accessed 4 January 2024).
- 1248 [69] Project website "ALARM Information Security". <https://alarm.wildau.biz/als7/>, 2023 (accessed 4 January 2024).
- 1249 [70] Project website "DIZ". <https://diz.wildau.biz/index-en.html>, 2021 (accessed 4 January 2024).
- 1250 [71] Project website "DIZ". Digital roulette. <https://diz.wildau.biz/roulette/index.html#0>, 2021 (accessed 4 January 2024).
- 1251 [72] Project website "ALARM Information Security". Storykonzept der digitalen Serious Games (PDF)/Story concept of digital serious games (in German). <https://alarm.wildau.biz/static/68a7aaceafb85c9e2b8e6ee7a3f3d557/handout-dLS-A4-final.pdf>, 2023 (accessed 4 January 2024).
- 1252 [73] Project website "ALARM Information Security". TO (Hrsg.), INFOBLATT – Security kompakt zum Thema CEO Fraud für Endanwender:innen (Mai 2023)/TO (Ed.), INFO SHEET – Security compact on the topic of CEO fraud for end users (in German) (May 2023). <https://alarm.wildau.biz/static/51370b1daaac6d3627f907f6dd44320d/infoblatt-ceo-fraud.pdf>, 2023 (accessed 20 December 2023).
- 1253

- 1284 [74] Project website "ALARM Information Security". TO (Hrsg.), Niederschwelliges Sicherheitskonzept zum Thema CEO
1285 Fraud für Geschäftsführung und IT-Verantwortliche (in German) (Mai 2023)/TO (Ed.), Low-threshold security concept on the
1286 topic of CEO fraud for management and IT managers (May 2023). [https://alarm.wil-](https://alarm.wildau.biz/static/4113fae4179e3edfd988f780eac72377/sicherheitskonzept-ceo-fraud.pdf)
1287 [dau.biz/static/4113fae4179e3edfd988f780eac72377/sicherheitskonzept-ceo-fraud.pdf](https://alarm.wildau.biz/static/4113fae4179e3edfd988f780eac72377/sicherheitskonzept-ceo-fraud.pdf), 2023 (accessed 20 December
1288 2023).
- 1289 [75] Project website "ALARM Information Security". TO (Hrsg.), INFOBLATT – Security kompakt zum Thema E-MAIL-CHECK
1290 für Endanwender:innen (in German) (Mai 2023)/TO (Ed.), INFO SHEET – Security compact on the topic of E-MAIL CHECK for
1291 end users (May 2023). <https://alarm.wildau.biz/static/1339d766094b7540eb3917dfd16efd47/infoblatt-e-mail-check.pdf>,
1292 2023 (accessed 20 December 2023).
- 1293 [76] Project website "ALARM Information Security". TO (Hrsg.), Niederschwelliges Sicherheitskonzept zum Thema Pass-
1294 wörter für Geschäftsführung und IT-Verantwortliche (Mai 2023)/TO (Ed.), Low-threshold security concept on the subject of
1295 passwords for management and IT managers (in German) (May 2023). [https://alarm.wil-](https://alarm.wildau.biz/static/2490c04004c3fed16c4e42f8c023b6aa/sicherheitskonzept-passwoerter.pdf)
1296 [dau.biz/static/2490c04004c3fed16c4e42f8c023b6aa/sicherheitskonzept-passwoerter.pdf](https://alarm.wildau.biz/static/2490c04004c3fed16c4e42f8c023b6aa/sicherheitskonzept-passwoerter.pdf), 2023 (accessed 20 December
1297 2023).
- 1298 [77] Project website "ALARM Information Security". TO (Hrsg.), INFOBLATT – Security kompakt zum Thema Hacking für
1299 Endanwender:innen (Mai 2023)/TO (Ed.), INFORMATION SHEET – Security compact on the subject of hacking for end users
1300 (in German) (May 2023). <https://alarm.wildau.biz/static/3b7be8d4e19aeb0acbdf2725aff83025/infoblatt-hacking.pdf>, 2023
1301 (accessed 20 December 2023).
- 1302 [78] Project website "ALARM Information Security". TO (Hrsg.), Niederschwelliges Sicherheitskonzept zum Thema Schutz-
1303 maßnahmen BestPractice für Geschäftsführung und IT-Verantwortliche (August 2023)/TO (Ed.), Low-threshold security con-
1304 cept on the topic of best practice protective measures for management and IT managers (in German) (August 2023).
1305 <https://alarm.wildau.biz/static/c01309141eb514821ae4f062018ea316/sicherheitskonzept-hacking.pdf>, 2023 (accessed 20
1306 December 2023).
- 1307 [79] Project website "ALARM Information Security". TO (Hrsg.), INFOBLATT – Security kompakt zum Thema Phishing für
1308 Endanwender:innen (Mai 2023)/TO (Ed.), INFORMATION SHEET – Security compact on the subject of phishing for end users
1309 (in German) (May 2023). <https://alarm.wildau.biz/static/2930c5b73cae1bf26d4cad18918d160b/infoblatt-phishing.pdf>,
1310 2023 (accessed 20 December 2023).
- 1311 [80] BSI—Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.)/Federal Office for Information Security (Ed.)
1312 (2019). Checkliste von BSI und Polizei (ProPK): Phishing vom 30.10.2019 / Checklist from BSI and police (ProPK): Phishing
1313 from October 30, 2019 (in German). [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/BSI-ProPK-](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/BSI-ProPK-Checkliste-Phishing.pdf?__blob=publicationFile&v=1)
1314 [Checkliste-Phishing.pdf?__blob=publicationFile&v=1](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/BSI-ProPK-Checkliste-Phishing.pdf?__blob=publicationFile&v=1) (accessed 11 January 2024).
- 1315 [81] Project website "ALARM Information Security". TO (Hrsg.), Niederschwelliges Sicherheitskonzept zum Thema Phishing
1316 für Geschäftsführung und IT-Verantwortliche (August 2023)/TO (Ed.), Low-threshold security concept on the subject of
1317 phishing for management and IT managers (in German) (May 2023). [https://alarm.wil-](https://alarm.wildau.biz/static/18bef186ff53794592b6e72b5c372472/sicherheitskonzept-phishing.pdf)
1318 [dau.biz/static/18bef186ff53794592b6e72b5c372472/sicherheitskonzept-phishing.pdf](https://alarm.wildau.biz/static/18bef186ff53794592b6e72b5c372472/sicherheitskonzept-phishing.pdf), 2023 (accessed 20 December 2023).
- 1319 [82] BSI—Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.)/Federal Office for Information Security (Ed.)
1320 (2021) (in German). [https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Smishing_SMS-](https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Smishing_SMS-Phishing_141021.html)
1321 [Phishing_141021.html](https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Smishing_SMS-Phishing_141021.html) (accessed 11 January 2024).
- 1322 [83] Project website "ALARM Information Security". TO (Hrsg.), INFOBLATT – Security kompakt zum Thema Smishing für
1323 Endanwender:innen (Mai 2023)/TO (Ed.), INFO SHEET – Security compact on the topic of smishing for end users (in German)
1324 (May 2023). <https://alarm.wildau.biz/static/807b021566fa7de971256a7804a06d0c/infoblatt-smishing.pdf>, 2023 (accessed
1325 20 December 2023).
- 1326 [84] Project website "ALARM Information Security". TO (Hrsg.), Niederschwelliges Sicherheitskonzept zum Thema Smishing
1327 für Geschäftsführung und IT-Verantwortliche (Mai 2023)/TO (Ed.), Low-threshold security concept on the topic of smishing
1328 for management and IT managers (in German) (May 2023). [https://alarm.wil-](https://alarm.wildau.biz/static/b092a1f2e1f8f26e3d2653b642e137e3/sicherheitskonzept-smishing.pdf)
1329 [dau.biz/static/b092a1f2e1f8f26e3d2653b642e137e3/sicherheitskonzept-smishing.pdf](https://alarm.wildau.biz/static/b092a1f2e1f8f26e3d2653b642e137e3/sicherheitskonzept-smishing.pdf), 2023 (accessed 20 December 2023).
- 1330 [85] Project website "ALARM Information Security". TO (Hrsg.), INFOBLATT – Security kompakt zum Thema Tailgating für
1331 Endanwender:innen (Mai 2023)/TO (Ed.), INFORMATION SHEET – Security compact on the topic of tailgating for end users
1332 (in German) (May 2023). <https://alarm.wildau.biz/static/c69f87fc21c42f7682e96d34355b164/infoblatt-tailgating.pdf>, 2023
1333 (accessed 20 December 2023).
- 1334 [86] Project website "ALARM Information Security". TO (Hrsg.), Niederschwelliges Sicherheitskonzept zum Thema Tailgating
1335 für Geschäftsführung und IT-Verantwortliche (in German) (Mai 2023)/TO (Ed.), Low-threshold security concept on the topic
1336 of tailgating for management and IT managers (May 2023). [https://alarm.wil-](https://alarm.wildau.biz/static/9b0746bca2b4de7e3cb093bbf7aa7db0/sicherheitskonzept-tailgating.pdf)
1337 [dau.biz/static/9b0746bca2b4de7e3cb093bbf7aa7db0/sicherheitskonzept-tailgating.pdf](https://alarm.wildau.biz/static/9b0746bca2b4de7e3cb093bbf7aa7db0/sicherheitskonzept-tailgating.pdf), 2023 (accessed 20 December
1338 2023).
- 1339 [87] Project website "ALARM Information Security". TO (Hrsg.), INFOBLATT – Security kompakt zum Thema Vorfallsmeldung
1340 für Endanwender:innen (Mai 2023)/TO (Ed.), INFORMATION SHEET – Security compact on the topic of incident response for
1341 end users (in German) (May 2023). <https://alarm.wildau.biz/static/e1ddf24fcf73b4f705d3203995171dd/infoblatt-vorfallsmeldung.pdf>, 2023 (accessed 20 December 2023).
- 1342 [88] Project website "ALARM Information Security". TO (Hrsg.), Niederschwelliges Sicherheitskonzept zum Thema Incident
1343 Response für Geschäftsführung und IT-Verantwortliche (Mai 2023)/TO (Ed.), Low-threshold security concept on the subject
1344 of incident reporting for management and IT managers (in German) (May 2023). [https://alarm.wil-](https://alarm.wildau.biz/static/c833bc1d2a42cc26040b0f2648d719bf/sicherheitskonzept-incident-response.pdf)
1345 [dau.biz/static/c833bc1d2a42cc26040b0f2648d719bf/sicherheitskonzept-incident-response.pdf](https://alarm.wildau.biz/static/c833bc1d2a42cc26040b0f2648d719bf/sicherheitskonzept-incident-response.pdf), 2023 (accessed 20 Decem-
1346 ber 2023).
- 1347

- 1348 [89] BSI—Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.)/Federal Office for Information Security (Ed.)
1349 (2023) Business Continuity Management. BSI-Standard 200-4. (pp 310, in German), Reguvis Fachmedien GmbH, Bonn, 2023.
1350 [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf?__blob=publi-](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf?__blob=publicationFile&v=8)
1351 [cationFile&v=8](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf?__blob=publicationFile&v=8) (accessed 11 January 2024).
- 1352 [90] D. Pokoyski, I. Matas, A. Haucke, Qualitative Wirkungsanalyse Security Awareness in KMU: Tiefenpsychologische
1353 Grundlagenstudie im Projekt Awareness Labor KMU (ALARM) Informationssicherheit. M. Scholl (Ed.), Technische
1354 Hochschule Wildau, Wildau, 2021. [https://alarm.wildau.biz/static/d6490e49f8d31adfa35259134b8d1b9d/220316-alarm-](https://alarm.wildau.biz/static/d6490e49f8d31adfa35259134b8d1b9d/220316-alarm-studie-final.pdf)
1355 [studie-final.pdf](https://alarm.wildau.biz/static/d6490e49f8d31adfa35259134b8d1b9d/220316-alarm-studie-final.pdf) (accessed 5 September 2023).
- 1356 [91] M. Scholl, Sustainable Information Security Sensitization in SMEs: Designing Measures with Long-Term Effect, in: Uni-
1357 versity of Hawai'i at Manoa (Ed.), Proceedings of the 56th Hawaii International Conference on System Sciences, Honolulu,
1358 HI: University of Hawai'i at Manoa, Hamilton Library, 2023. <https://hdl.handle.net/10125/103369>, (CC BY-NC-ND 4.0), pp.
1359 6058-6067.
- 1360 [92] P. Danil (BSI – Bundesamt für die Sicherheit in der Informationstechnik/Federal Office for Information Security). IT-Si-
1361 cherheit für KMU/ IT security for SMEs (in German). Webinar der IHK Koblenz am 14.11.2023, 13:30-14:30 Uhr.
1362 <https://www.ihk.de/koblenz/unternehmensservice/digitalisierung/aktuelle-trends-5879040>, 2023 (accessed 17 November
1363 2023).
- 1364 [93] T. Berghoff, Mit NIS-2 wird IT-Sicherheit zur Chefsache. Security Insider vom 22.11.2023, online. [https://www.security-](https://www.security-insider.de/mit-nis-2-wird-it-sicherheit-zur-chefsache-a-cc064ecceaa1e4fdcf500c3b22f847b4/)
1365 [insider.de/mit-nis-2-wird-it-sicherheit-zur-chefsache-a-cc064ecceaa1e4fdcf500c3b22f847b4/](https://www.security-insider.de/mit-nis-2-wird-it-sicherheit-zur-chefsache-a-cc064ecceaa1e4fdcf500c3b22f847b4/) (accessed 23 November
1366 2023).
- 1367 [94] D. Pokoyski, A. Haucke, A., Enabling vs. Entmündigung: Qualitativer Konzepttest analoger Security Awareness-
1368 Lernszenarien für KMU im Projekt Awareness Labor KMU (ALARM) Informationssicherheit/Enabling vs. incapacitation: Qual-
1369 itative concept test of analog security awareness learning scenarios for SMEs in the Awareness Labor SME (ALARM) infor-
1370 mation security project. Scholl, M. (Hrsg.), Technische Hochschule Wildau, Wildau, 2022. [https://alarm.wildau.biz/sta-](https://alarm.wildau.biz/static/c0e4d00beefe1dc5fac9b50b6087265f/studie-2-master-final.pdf)
1371 [tic/c0e4d00beefe1dc5fac9b50b6087265f/studie-2-master-final.pdf](https://alarm.wildau.biz/static/c0e4d00beefe1dc5fac9b50b6087265f/studie-2-master-final.pdf). Letzter Zugriff: 05.09.2023.
- 1372 [95] M. Leitner, A Scenario-Driven Cyber Security Awareness Exercise Utilizing Dynamic Polling: Methodology and Lessons
1373 Learned, in: Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023),
1374 634-642. Copyright 2023 by SCITEPRESS – Science and Technology Publications, Lda, under CC license (CC BY-NC-ND 4.0).
1375 doi: 10.5220/0011780400003405.
- 1376 [96] S.H. von Solms, J. du Toit, E. Kritzinger, Another Look at Cybersecurity Awareness Programs, in: International Sympo-
1377 sium on Human Aspects of Information Security and Assurance, Springer Nature Switzerland, Cham, 2023, pp. 13-23.
1378 https://doi.org/10.1007/978-3-031-38530-8_2.
- 1379 [97] B. Alkhazi, M. Alshaikh, S. Alkhezi, H. Labbaci, Assessment of the Impact of Information Security Awareness Training
1380 Methods on Knowledge, Attitude, and Behavior. IEEE Access, 10, 2022, pp. 132132-132143.
- 1381 [98] P. Eyerer, D. Krause, Methoden-Mix erhöht die Lehr-Lern-Effektivität und deren Effizienz/Method mix increases the
1382 teaching-learning effectiveness and its efficiency (in German), Neues Handbuch Hochschullehre/New handbook for univer-
1383 sity teaching 36, 2009.
- 1384 [99] B. Hoffmann, U. Langefeld, Methoden-Mix. Unterrichtsliche Methoden zur Vermittlung beruflicher Handlungskompe-
1385 tenz in kaufmännischen Fächern/Teaching methods for teaching professional skills in commercial subjects, 3, 1998.
- 1386 [100] M. Alshaikh, S.B. Maynard, A. Ahmad, An exploratory study of current information security training and awareness
1387 practices in organizations, in: Proceedings of the 51st Hawaii International Conference on System Sciences 2018, pp. 5085-
1388 5094. <http://hdl.handle.net/10125/50524> ISBN: 978-0-9981331-1-9 (CC BY-NC-ND4.0),
- 1389 [101] S. Farshadkhah, M. Maasberg, T.S. Ellis, C. van Slyke, An Empirical Examination of Employee Information Security Ad-
1390 vice Sharing, Journal of Computer Information Systems, (2023) 1-16. <https://doi.org/10.1080/08874417.2023.2176947> (ac-
1391 cessed 1 August 2023).
- 1392 [102] A. Sykosch, Zur Messbarkeit von IT-Sicherheitsbewusstsein. Dissertation, Universitäts- und Landesbibliothek Bonn,
1393 2022. <https://bonndoc.ulb.uni-bonn.de/xmlui/bitstream/handle/20.500.11811/9568/6526.pdf?sequence=1&isAllowed=y>
1394 (accessed 19 November 2023).