Conceptualization of a CyberSecurity Awareness Quiz

Sebastian Pape[1,2]✉[0000−0002−0893−7856], Ludger Goeke[1], Alejandro Quintanar[1], and Kristian Beckers[1]

[1] Social Engineering Academy (SEA) GmbH
Eschersheimer Landstrasse 42, 60322 Frankfurt am Main, Germany
[2] Goethe University Frankfurt, Faculty of Economics and Business Administration
Theodor-W.-Adorno-Platz 4, 60323 Frankfurt am Main, Germany

Abstract. Recent approaches to raise security awareness have improved a lot in terms of user-friendliness and user engagement. However, since social engineering attacks on employees are evolving fast, new variants arise very rapidly. To deal with recent changes, our serious game *CyberSecurity Awareness Quiz* provides a quiz on recent variants to make employees aware of new attacks or attack variants in an entertaining way. While the gameplay of a quiz is more or less generic, the core of our contribution is a concept to create questions and answers based on current affairs and attacks observed in the wild.

Keywords: Serious game · CyberSecurity Awareness · Human factor

1 Introduction

Social engineering attacks represent a continuing threat to employees of organizations. With a wide availability of different tools and information sources [5], it is a challenging task to keep up to date of recent attacks on employees since new attacks are being developed and modifications of known attack scenarios are emerging. The latest Data Breach Investigations Report [2] reports another increase of financially motivated social engineering, where the attacker directly ask for some money, i. e. by impersonating CEOs or other high-level executives. However, during the writing of the report, scammers have already varied their approach and also ask for purchase and transfer of online gift cards[1] in order to scam employees. Additionally, scammers also base attacks on the current news situation, such as COVID-19 Ransomware [15]. While a couple of defense methods and counteracting training methods [16, 17] exist, at present, most of them can not be adapted fast enough to cope with this amount and speed of new variations.

The *CyberSecurity Awareness Quiz* is a serious game in form of an online quiz to raise the security awareness of employees, in particular against social engineering attacks. The game follows the approach that quiz questions are based

[1] `https://twitter.com/sjmurdoch/status/1217449265112535040`

on real-world social engineering attacks. Additionally, the pool of questions will constantly be extended by new questions in relation to current social engineering attacks. For this purpose, a specific process for the procurement of appropriate information is developed, which is described in detail in Section 3.2. Our contribution within this paper is the conceptualization of the *CyberSecurity Awareness Quiz* with a focus on the concept how to generate questions for the quiz game based on current affairs and attacks observed in the wild.

The remainder of the paper is structured as follows: Sect. 2 lists some related games, explains the relationship of the *CyberSecurity Awareness Quiz* with previously developed games and how it integrates into a more general training platform. Its concept is explained in Sect. 3 along with the planned components in Sect. 4. We conclude in Sect. 5.

2 Background and Related Work

There is a large number of tabletop games for security training or awareness raising [6, 8, 4, 3, 14] targeting different domains, asset and areas in the academia.

However, the ones which are closer to *CyberSecurity Awareness Quiz* are mostly commercial without a detailed description. Nevertheless, we give a brief overview of them in the following. The "Emergynt Risk Deck" highlights IT-security risks to business leadership [7]. "OWASP Snakes and Ladders" is an educational game to raise security awareness about application security controls and risks [13]. Within the game "Quer durch die Sicherheit" players move towards the target by answering questions correctly [10]. "Stadt Land HACK!" is a quiz about data privacy and security [11].

Since the above mentioned games are all tabletop or card games, they can not be adapted to recent security incidents easily. While there is only a limited variation of different variants of a quiz-style game, our main contribution of this conceptual paper is the process for the creation of questions along with the idea to mostly use the *CyberSecurity Awareness Quiz* to keep users informed about recent attacks in an entertaining way.

2.1 Relation to Existing Games

Naturally, the aim and scope of a game can not be too broad. Similar to security awareness campaigns [1], serious games also benefit from an adaption to the user and his/her specific needs. Therefore, *CyberSecurity Awareness Quiz* is part of a series of games dovetailed to a chain aiming at raising security awareness (cf. Fig. 1). For security requirements engineering, employees are playing HATCH [3], in order to identify relevant attacks and develop countermeasures. All identified threats which can not be technically addressed, need to be integrated into the organisation's security policy. Once the security policy is developed or updated, employees can train to apply it and get an understanding how it addresses certain attacks by playing PROTECT [9]. However, naturally different attacks or variations of attacks will sprout faster than the security policies can be adapted.

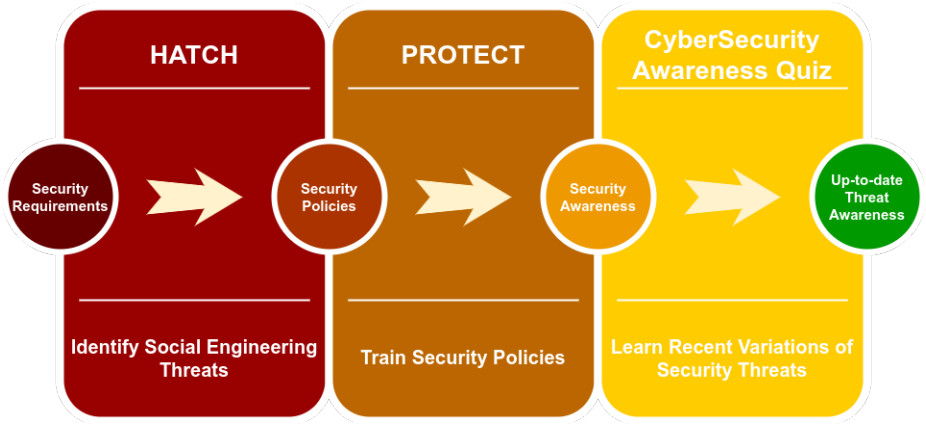

Fig. 1. The Relation of HATCH [3], PROTECT [9] and *CyberSecurity Awareness Quiz*

Thus, *CyberSecurity Awareness Quiz* is used to raise awareness about the latest attacks and their variations, based on the player's general understanding developed in the game sessions of HATCH and PROTECT.

2.2 Embedding into a CyberSecurity Training Platform

Besides the use and interplay of *CyberSecurity Awareness Quiz* with other serious games, it is also important to integrate them into a more general training platform, such as the THREAT-ARREST [12] advanced training platform (cf. Fig. 2).

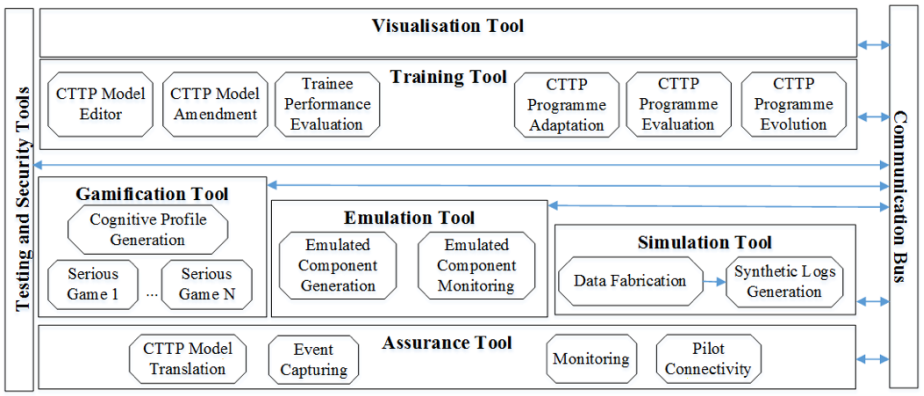

Fig. 2. The THREAT-ARREST Advanced Training Platform [12]

This way it is not only possible to train employees during their use of the serious games, but also to embed and manage their efforts in a broader way.

The result of *CyberSecurity Awareness Quiz* sessions contribute to THREAT-ARREST's continuous evaluation of the individual trainees' performance and the effectiveness of the training programs. Within the platform for each trainee results of the serious games, the emulation, the simulation and the training tool are brought together to spot possible gaps in the employee's knowledge or awareness. If knowledge gaps are identified, it can be checked if there already exists a training on the specific topic as serious game, simulation or emulation of the cyber range system. If no appropriate training can be identified, this might indicate the need of producing a new training, tailored to the organizational needs and the trainee types.

3 Concept

The fast change and adaption of attacks as sketched in the introduction show the necessity for employees to keep their knowledge about social engineering up-to-date.

Since we expect only a reasonable amount of new attacks or attack variations, we decided to aim for a lightweight game with the idea that it could be played occasionally (e. g. when traveling in trams or subways). In general, the game should be playable alone since this avoids any necessity to find or wait for other players, but in particular for long term motivation, comparisons with or games against other players should be possible. In summary, we identified the following requirements:

- Questions refer to recent real-world threats
- Lightweight
- Playable on mobile devices
- Single and multi-player modes

3.1 Game Concept

One game type which fulfills the requirements is a quiz game, where players have to answer a set of questions. In *CyberSecurity Awareness Quiz,* a question describes a certain social engineering attack scenario which is based on a recent attack observed in the real world in an abstract and general way. For every question, the possible answers contain one or more correct answers and one or more incorrect answers. Correct answers will represent consequences which result from the attack that is described in the question. Accordingly, incorrect answers will represent effects which can not result from the attack. A mockup of the planned GUI which also shows a sample question is illustrated in Fig. 3.

CyberSecurity Awareness Quiz will provide different modes in which a quiz can be played. Either by a single player or in competition between two players. These modes are described in the following:

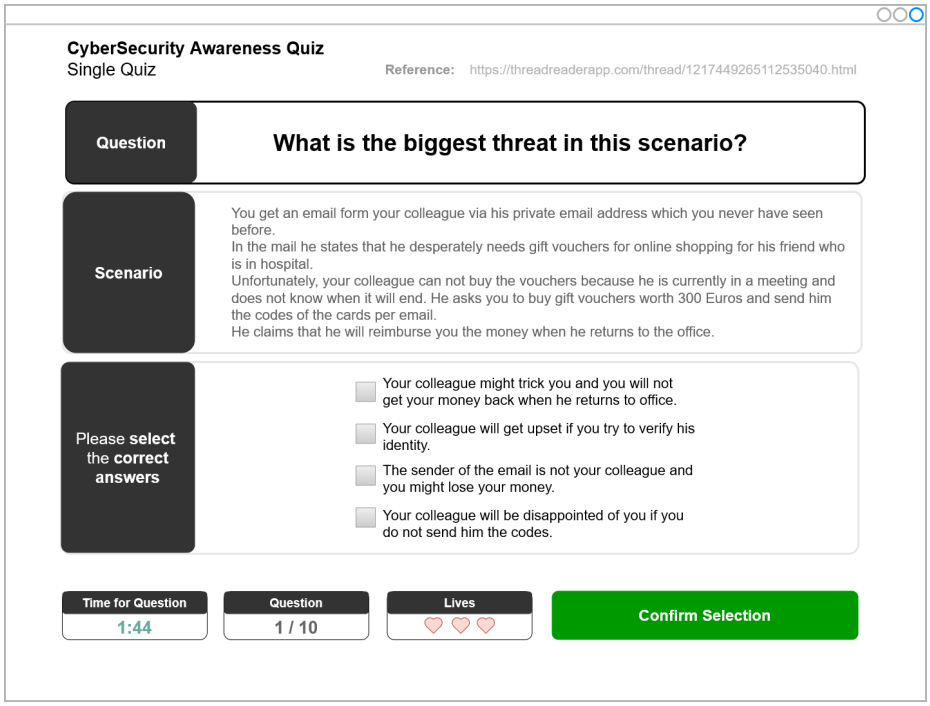

Fig. 3. Mockup of the User Interface along with a Sample Question

Single Quiz: A player will answer the questions of a quiz alone.

Context Quiz: Single-player quiz with specific questions depending on the preferences of a player. Examples for specific questions are scenarios concerning a certain location, industry sector or role/position in the company. Furthermore, it is possible to play only recent added questions, e. g. questions added in the last 3 months.

Versus Quiz: Two players will compete in a quiz against each other. A question will be asked simultaneously to both players. The player who will answer a question correctly gets a point. If both players are correct, the faster player wins. The player who will answer more questions correctly, wins the quiz round.

Pick Quiz: In this mode, two players will answer questions one after the other. Here, the player who has answered his/her last question correctly chooses the next question for the opponent out of different options until the opponent answers a question correctly. If this is the case, the right for choosing questions changes and so on. Only the first question will be asked to both players simultaneously. The player who answers this question correctly first will have the right to choose the next question for the opponent.

Draw Quiz: This mode will have the same rules as the *Pick Quiz* mode with the following modification: Instead of choosing the next question out of dif-

ferent options, the player who has answered his/her last question correctly will choose the industry/sector to which the next question for the opponent relates.

For the the modes context quiz, pick quiz and draw quiz, certain metadata on the scenarios is needed. Therefore, question will be tagged by predefined types of metadata. This metadata will enable a categorization of questions which allows it to combine questions to different quizzes for certain training objectives or specific groups of players. For example, a specific set of questions will be able to reference a certain type of attacks (e. g. different forms of phishing), industry sector (e. g. energy suppliers), department (e. g. human resources), a geographic area (e .g. Europe) or all new attacks added after a given date. The possibility of adapting a quiz to the players needs aims to enable players to map the mediated learning content directly to their work routine.

Additionally, the metadata will enable an on the fly compilation of the questions for a quiz round played in the Context Quiz mode. Here, the player provides information which refers to certain aspects of social engineering he/she wants to be considered in the next quiz round. This quiz round will include all the predefined questions which are tagged with metadata that matches the provided information.

We describe the different types of metadata used in Sect. 3.2.

3.2 Process for Information Procurement and Question Generation

A key feature of *CyberSecurity Awareness Quiz* will be the fact that its questions are based on real-life attacks whereby the amount of questions will be permanently expended to cover new social engineering attacks. To fulfill this requirement, an appropriate process for gathering content regarding attacks and the creation of corresponding questions and answers is needed. This process is sketched in Fig. 4.

The first step of the process includes the procurement of information with respect to current social engineering attacks. While the number of relevant attacks might be feasible, there is a huge amount of reports of attacks, privacy breaches, data losses, etc. Due to the high frequency in which they occur as well as the multitude of information sources, the information procurement presents an enormous challenge. To meet this challenge, the information procurement will include automated tasks which are discussed later in this section.

The second step of the process for the creation of questions and answers includes the formulation of questions for a quiz. Usually, questions will be created based on content about social engineering attacks which has been collected in Step 1. If this is the case, the game content designer will check for a new relevant web feed first if a corresponding question already exists. For this check he/she will filter the existing questions by the types of metadata which are relevant for the new web feed.

In the third step, a created question will be tagged with metadata. This metadata will represent characteristics of an attack like the category of an attack

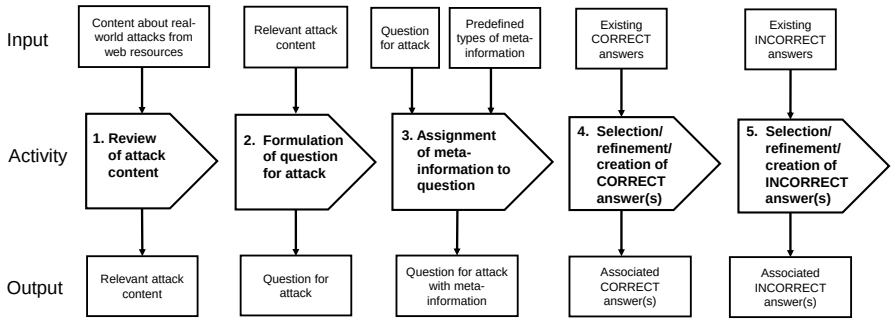

Fig. 4. Process for the Creation of Questions and Answers for Social Engineering Attacks

(e. g. phishing). *CyberSecurity Awareness Quiz* will provide predefined types of metadata, which are specified in Tab. 1. This table includes the name of a metadata type and its description. The metadata of questions is important for the reuse of questions during the creation of certain predefined quizzes and the compilation of on the fly quizzes within the Context Quiz mode (see Section 3.1). As discussed in the previous section, metadata allows to filter questions by special categories when creating a quiz with a certain topic. For example, if a quiz shall refer to attacks which are targeting employees of the human resources department, questions whose metadata parameter of the type *Department* has the value "human resources" should be assessed for consideration. The same concept is applied when a quiz round is played in the Context Quiz mode. Here, the player provides information regarding his/her preferences and the started quiz comprises only such questions whose metadata corresponds to the provided information. For example, if a player is interested in all types of new phishing attacks from a certain point in time, he/she can selects the value "phishing" for the metadata type *Attack category* and the value "from 01.06.2020" for the metadata type *Time of attack*.

In the fourth step of the process **correct** answers are assigned to a question. In this context, new correct answers can be created or already existing correct answers can be reused.

The last step of the process includes the assignment of **incorrect** answers to a question. As for correct answers, incorrect answers can be newly created or already existing incorrect answers can be reused.

Information Procurement One objective of the information procurement is to gather content related to social engineering attacks which is published on appropriate web resources like news websites, websites about information security, websites of institutions, blogs or even twitter. In this context, in particular websites which provide information about their new content in a structured manner

(e. g. web feeds) will be considered. Figure 5 shows an overview of the steps for the information procurement.

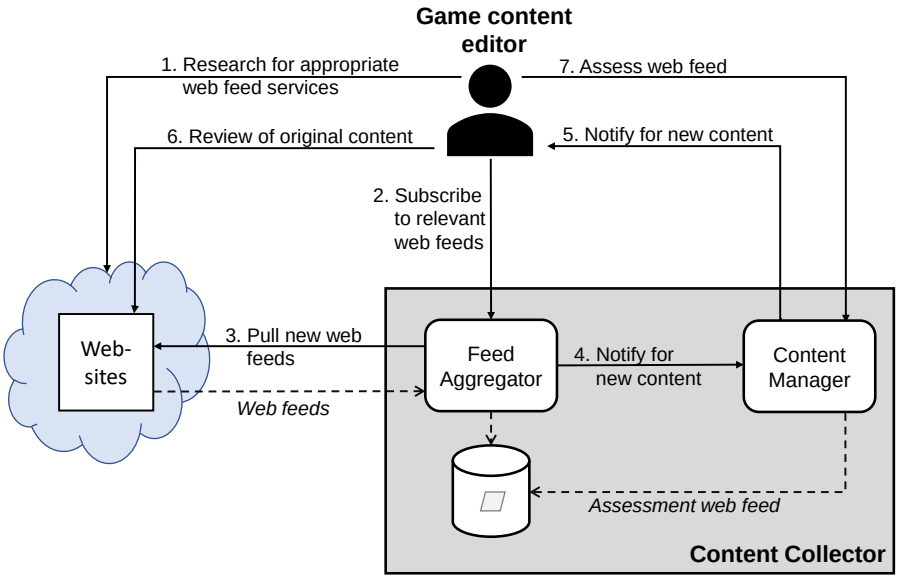

Fig. 5. Tasks for Gathering and Analysing Content about Attacks

Web feeds present a form of pull data. This means, that users can request frequently information in relation to new content on subscribed websites by using appropriate tools (e. g. feedreaders). Web feeds are machine-readable files which are provided in standardized formats like RSS[2] or Atom[3]. They include data which addresses among others the title and a short description of the new content, the URL of the original resource, the publishing date and the name of the author.

As Fig. 5 illustrates, some tasks for the information procurement need to be performed manually by the *game content editor*. Other steps will be performed automatically by a component of *CyberSecurity Awareness Quiz* which is named *Content Collector*. The different steps of the process for information procurement are explained in the following.

In the initial step of the process, the game content editor will search for websites which publish content about social engineering attacks and implement a web feed service. This step will be repeated periodically to check if new appropriate web resources are available. In the second step, the game content editor

[2] depending on the version RSS means: RDF Site Summary or Really Simple Syndication

[3] Atom Syndication Format is an XML language used for web feeds

will subscribe to the found web feed services by using the *Feed Aggregator* which is a subcomponent of the Content Collector. The Feed Aggregator will query automatically and periodically the subscribed websites for new web feeds (step 3). If new web feeds have been found, it will notify the *Content Manager* (step 4) which is another subcomponent of the Content Collector. The Content Manager, which is responsible for the management of gathered web feeds, will inform the game content editor that new content is available (step 5). Then, the game content editor will review the original content of the corresponding web feed (step 6). Afterwards he/she will assess in the Content Manager if the content to the web feed is relevant or not (step 7).

Web feeds which will be marked as relevant can be used for the formulation of new quiz questions (see Figure 4, step 2).

Types of Metadata As already discussed, questions need to be tagged by metadata in order to allow the categorization of questions during the creation of predefined quizzes and within on the fly compilation of quizzes with respect to the Context Quiz mode (see Section 3.1). The different types of metadata are specified in Tab. 1. Additionally, (correct and incorrect) answers will be also tagged with metadata (cf. Tab. 2). The *Multiplicity* will specify the number of data items which have to be assigned at least and can be assigned at most.

Table 1: Types of Metadata for Tagging of Questions

Type of metadata	**Description**	**Multiplicity**
Title	Title of an attack	1
Type of attack execution	Specification if an attack is executed (i) directly on site by an attacker (e.g. an attacker tries to get access to a secured server room by pretending to be a service technician), (ii) indirectly by using a technical medium (e.g. phishing via email) or (iii) different combinations of direct and/or indirect executions.	1
Attack category	Categories which typify an attack (e.g. vishing). In this connection, an attack can be assigned to exactly one category or to several categories. For example, an attack which uses dumpster diving can only be associated to the category *dumpster diving*. An attack in which emails with malicious links are sent to CEOs can be assigned to the categories *email fraud*, *phishing*, *email phishing* and *whaling*.	1..*
Type of attacker	Typing of the attacker who executes an attack (e.g. cyber criminal, fraudster, intelligence service, hacker).	1..*

Type of metadata	**Description**	**Multiplicity**
Feigned identity	Defines the identity of the entity/person which/who is feigned by the attacker during an attack. Regarding enterprises or institutions, a feigned identity could refer to internal persons like colleagues, C-level personnel and employees from other branches or external persons like customers, technicians and cleaning stuff. In the private context, an attacker could pretend to be a relative, friend or a person who seeks for help. When feigning an entity, an attacker could pretend to be an employee of a state authority (e.g. tax authority) or a private institute (e.g. banks).	1..*
Context of victims	Specifies the context(s) of the victims who are targeted by an attack. For this parameter the values *individual* and *organisation* are predefined.	1..2
Characteristics of private victim[4]	Specifies the characteristic(s) for a group of victims in person of *individual* who are threatened by an attack. For individuals this could be demographic characteristics (e.g. age, gender, interests, internet usage).	0..*
Sector[5]	Specifies the sector/industry of organisations which are threatened by an attack (e.g. energy suppliers, financial institutes, state institutions).	0..*
Department[5]	Defines certain departments of an organisation (e.g. human resources, finance, IT) which are affected by an attack.	0..*
Role[5]	Indicates certain roles of employees of an organisation (e.g. CEO, administrator, financial accountant) which are threatened by an attack.	0..*
Motivation for attack	Specifies the motivation for the execution of an attack (e.g. espionage, criminal intend, interest in hacking).	1..*
Objective description	Defines the objective of an attack (e.g illegal financial transactions, gaining of sensitive information/data, identity theft).	1..*
Exploited psychological pattern	Psychological pattern which is tried to be exploited by an attack (e.g. authority, good faith, laziness).	1..*
Used technology	Technology which has been used during the attack (e.g. email for phishing or telephone for vishing).	0..*

[4] CONDITION: This parameter is only used when the parameter *Context of victims* has the value *individual*

[5] CONDITION: This parameter is only used when the parameter *Context of victims* has the value *organisation*

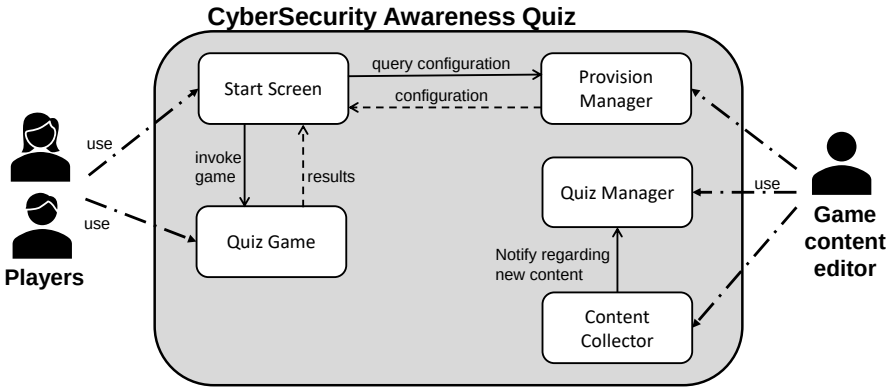

Fig. 6. Components of *CyberSecurity Awareness Quiz*

Type of metadata	**Description**	**Multiplicity**
Geographical spreading	The geographical area where the attack has been conducted (e.g. worldwide, Europe, United States, California, Milan).	1..*
Time of attack	Period(s) of time in which the attack has been conducted.	1..*
Sources	Sources of the content on which the attack bases.	1..*

Table 2: Types of Metadata for Tagging of Answers

Type of metadata	**Description**	**Multiplicity**
Attack category	Specifies the attack category or rather different attack categories of questions to which an answer could be assigned.	1..*
Answer type	Indicates if an answer is correct or incorrect in the context of its attack categories.	1

4 Architecture and Components

This section discusses the different components of *CyberSecurity Awareness Quiz* which will implement the concepts described in Sect. 3. Figure 6 provides an overview of these components and the rudimentary communication between them. Additional, it shows the different roles which will use certain components. For the sake of clarity, a representation of the database and the corresponding communication between the database and components has been omitted.

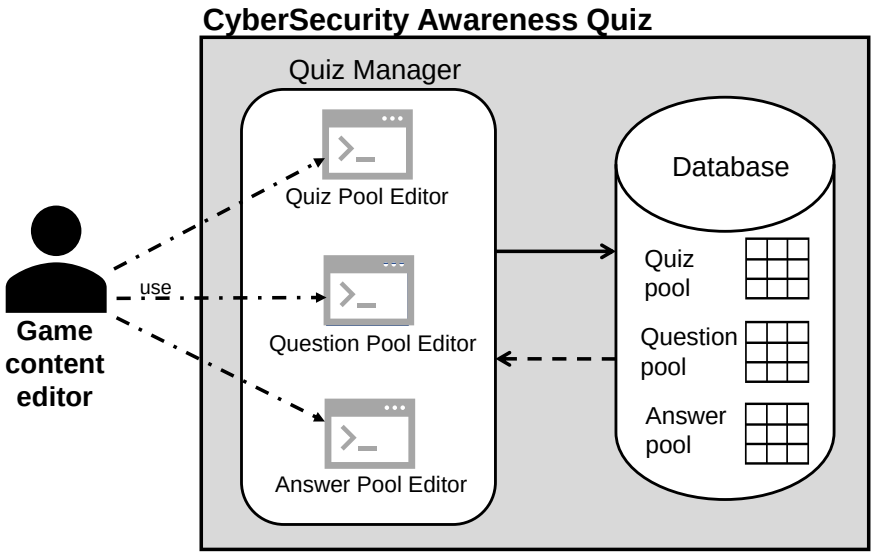

Fig. 7. Editors provided by the Quiz Manager

4.1 Content Collector

We have already introduced the *Content Collector* in Section 3.2, thus the following description is limited to the essentials.

The Content Collector will provide functionality for the collection of new content about social engineering attacks in the form web feeds. To this, it will check the subscribed web feed services frequently for new content.

A further functionality of the Content Collector will enable the management of collected web feeds. It will inform the game content designer when new content has been collected and will allow to assign his/her assessments regarding its relevance to the related web feeds. If a web feed will be considered as relevant by the game content editor, the Content Collector will notify another component in form of the *Quiz Manager* (see Section 4.2) that new relevant content is available.

The content collector will be exclusively used by the game content editor.

4.2 Quiz Manager

The *Quiz Manager* will enable the game content editor to manage (i) the pool of available quizzes and the separate (ii) pool of questions and (iii) pool of answers. For that purpose, the Quiz Manager will implement corresponding editors named *Quiz Pool Editor*, *Question Pool Editor* and *Answer Pool Editor*. These different editors, which are represented in Figure 7, are discussed in the following.

The *Question Pool Editor* will enable the creation of questions which are added to the question pool (cf. Fig. 7) and the specification of the corresponding metadata. In general, the questions are based on content that has been collected

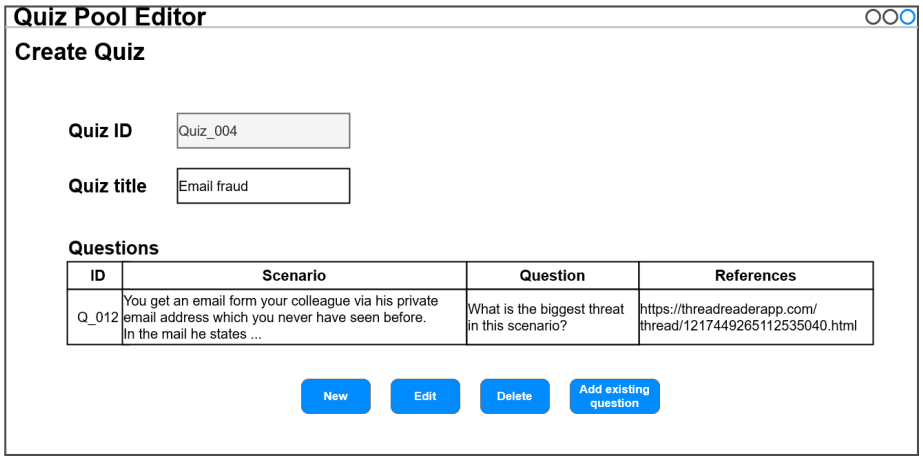

Fig. 8. Mockup of the User Interface of the Quiz Pool Editor

by the *Content Collector* (see Section 4.1). Additionally, the Question Pool Editor will allow the editing of questions in the pool and their deletion.

In the context of creating or editing a question, the Question Pool Editor will also implement the assignment of correct and incorrect answers to a question. For that purpose, it will supply a dialogue for the creation of new answers and the related metadata. When the input is finalized, a created answer will be added to the answer pool (cf. Fig. 7).

The Question Pool Editor will also display a list of existing answers from the answer pool which could be relevant for the current question because of their assigned attack categories. Besides adding new answers, it will be possible to assign any existing answer to the edited question.

With respect to the management of the answer pool (cf. Fig. 7), the *Answer Pool Editor* will implement the creation of new answers and the related metadata as well as the editing and deletion of answers.

The functionality of creating new quizzes and adding them to the pool of available quizzes (cf. Fig. 7) will be implemented by the *Quiz Pool Editor* (cf. Fig. 8). In the mockup of the user interface of the Quiz Pool Editor it is shown that every quiz has a title and is identified by an unique identifier.

It will be possible to reuse predefined questions from the question pool for a new quiz. For that purpose, the Quiz Pool Editor will display a list of predefined questions from the question pool which can be filtered by the metadata of the questions. This way, the game content designer will be able to restrict the number of displayed questions.

During the creation of a quiz, the Quiz Pool Editor will also allow the creation of new questions and the related answers. A newly created question will be added additionally to the question pool, when it is finalized. If newly created answers will be assigned to a created question, these answers will be also added to the

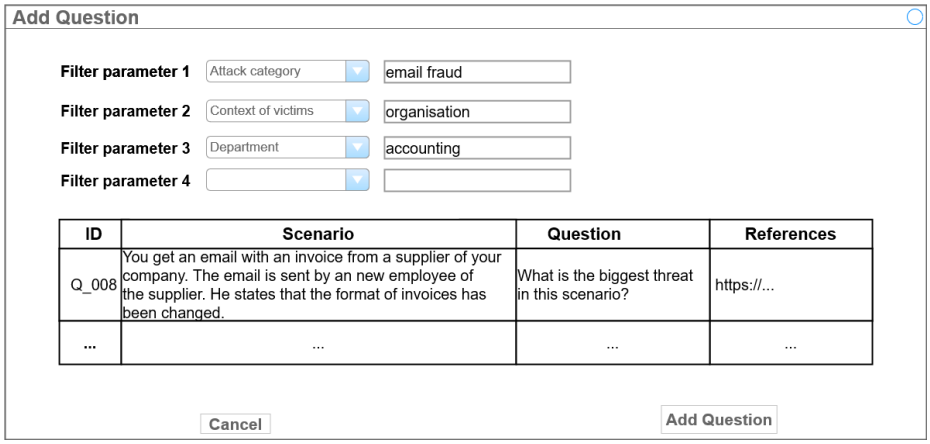

Fig. 9. Mockup of the User Interface of the Add Question Dialogue of the Quiz Pool Manager

answer pool. Figure 9 shows the dialogue for adding existing questions to a quiz. Here, the set of displayed questions corresponds to the selected filter parameters.

Functionalities for the editing and deletion of quizzes will also be supplied by the Quiz Pool Editor.

4.3 Provision Manager

The *Provision Manager* facilitates configurations with respect to provisions of *CyberSecurity Awareness Quiz*. These configurations will be managed by the game content editor. The different configuration parameters are represented in Tab. 3.

Table 3. Configuration Parameters for the Provisioning of *CyberSecurity Awareness Quiz*

Configuration parameter	**Description**
Available quizzes	Specifies the quizzes which shall be available for the player to be played.
Activated modes	Indicates which single-player modes and/or multi-player modes shall be activated within a provision.

4.4 Start Screen

When a player will start the *CyberSecurity Awareness Quiz* client, the *Start Screen* will appear. Depending on the configuration provided by the *Provison*

Manager, the Start Screen will show which gaming modes are activated and which quizzes can be played.

The Start Screen acts as a frontend of *CyberSecurity Awareness Quiz* to start games in the component *Quiz Game* (see Section 4.5) with one of the activated quizzes. If the player plays a game in the *Context Quiz* mode (see Section 3), he/she will be able to provide the information which determines how the content of the quiz to be played will be compiled.

If any multi-player mode is activated, the Start Screen will display other players which are currently online. Accordingly, a player will be able to arrange a game in one of the multi-player modes with an available competitor.

4.5 Quiz Game

The component *Quiz Game* will implement the actual quiz game. A certain quiz game can be invoked by the *Start Screen* (see Section 4.4). For that purpose, the Start Screen will pass the required parameters for a quiz to the Quiz Game. These parameters will include among other information, the set of questions and the mode in which the quiz will be played.

The graphical user interface (GUI) of the Quiz Game will differ depending on the gaming mode in which the quiz is played. A mockup was already presented in Fig. 3 in Sect. 3.1.

5 Conclusion

We presented a conceptualization of *CyberSecurity Awareness Quiz* based on the requirements defined in Sect. 3. From a conceptual perspective, all requirements are fulfilled. In particular, one of our contributions is a detailed description of the process for information procurement and deduction of questions based on recent social engineering attacks. The game offers different quiz modes to maintain the players' long-term motivation and interest to gather knowledge on new attacks. Besides the obvious implementation of *CyberSecurity Awareness Quiz,* in future work we intend to investigate by user studies if the implementation is also perceived as lightweight by the players and if players perceive the game suitable for occasional playing.

Acknowledgements

This work was supported by European Union's Horizon 2020 research and innovation program from the project THREAT-ARREST (grant agreement number: 786890) and CyberSec4Europe (grant agreement number: 830929).

References

1. Bada, M., Sasse, A.M., Nurse, J.R.C.: Cyber security awareness campaigns: Why do they fail to change behaviour? CoRR **abs/1901.02672** (2019), `http://arxiv.org/abs/1901.02672`

2. Bassett, G., Hylender, C.D., Langlois, P., Pinto, A., Widup, S.: Data breach investigations report (2020), https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
3. Beckers, K., Pape, S.: A serious game for eliciting social engineering security requirements. In: Proceedings of the 24th IEEE International Conference on Requirements Engineering. RE '16, IEEE Computer Society (2016). https://doi.org/10.1109/RE.2016.39
4. Beckers, K., Pape, S., Fries, V.: HATCH: Hack and trick capricious humans – a serious game on social engineering. In: Proceedings of the 2016 British HCI Conference, Bournemouth, United Kingdom, July 11-15, 2016 (2016), https://ewic.bcs.org/content/ConWebDoc/56973
5. Beckers, K., Schosser, D., Pape, S., Schaab, P.: A structured comparison of social engineering intelligence gathering tools. In: Trust, Privacy and Security in Digital Business - 14th International Conference, TrustBus 2017, Lyon, France, August 30-31, 2017, Proceedings. pp. 232–246 (2017). https://doi.org/10.1007/978-3-319-64483-7_15
6. Denning, T., Lerner, A., Shostack, A., Kohno, T.: Control-alt-hack: the design and evaluation of a card game for computer security awareness and education. In: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. pp. 915–928 (2013)
7. Emergent Network Defense: Emergynt risk homepage. https://emergynt.com/risk-deck/
8. Frey, S., Rashid, A., Anthonysamy, P., Pinto-Albuquerque, M., Naqvi, S.A.: The good, the bad and the ugly: a study of security decisions in a cyber-physical systems game. IEEE Transactions on Software Engineering **45**(5), 521–536 (2017)
9. Goeke, L., Quintanar, A., Beckers, K., Pape, S.: PROTECT - an easy configurable serious game to train employees against social engineering attacks. In: Fournaris, A.P., Athanatos, M., Lampropoulos, K., Ioannidis, S., Hatzivasilis, G., Damiani, E., Abie, H., Ranise, S., Verderame, L., Siena, A., Garcia-Alfaro, J. (eds.) Computer Security - ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC, Luxembourg City, Luxembourg, September 26-27, 2019, Revised Selected Papers. Lecture Notes in Computer Science, vol. 11981, pp. 156–171. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-42051-2_11
10. Known Sense: Quer durch die Sicherheit game reference. http://www.known-sense.de/quer_durch_die_sicherheit_folder.pdf
11. Known Sense: Stadt Land HACK! homepage. http://www.known-sense.de/stadt_land_hack.pdf
12. Koshutanski, H., Tsantekidis, M., Damiani, E., Frati, F., Cimato, S., Riccobene, E., Hatzivasilis, G., Fysarakis, K., Spanoudakis, G., Blinder, O., Vinov, M., Hildebrandt, T., Wortmann, D., Rompoti, V., Bravos, G., Chatzigiannakis, V., Beckers, K., Pape, S., Kunc, M., Bašta, P.: Threat-arrest platform's initial reference architecture. Tech. rep., Threat-Arrest (2019), Deliverable 1.3
13. OWASP: Owasp snakes and ladders homepage. https://owasp.org/www-project-snakes-and-ladders/ (2013)
14. Rieb, A., Lechner, U.: Operation digital chameleon: towards an open cybersecurity method. In: Proceedings of the 12th International Symposium on Open Collaboration. pp. 1–10 (2016)
15. Saleh, T.: Covidlock update: Deeper analysis of coronavirus android ransomware. https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware (2020)

16. Schaab, P., Beckers, K., Pape, S.: A systematic gap analysis of social engineering defence mechanisms considering social psychology. In: 10th International Symposium on Human Aspects of Information Security & Assurance, HAISA 2016, Frankfurt, Germany, July 19-21, 2016, Proceedings. (2016), https://www.cscan.org/openaccess/?paperid=301
17. Schaab, P., Beckers, K., Pape, S.: Social engineering defence mechanisms and counteracting training strategies. Information and Computer Security **25**(2), 206–222 (2017). https://doi.org/10.1108/ICS-04-2017-0022, https://doi.org/10.1108/ICS-04-2017-0022

All URLs haven been last accessed on July 22nd, 2020.