Escape room pour la sécurité : sensibilisation à la sécurité informatique

Erwan Beguin, Eric Alata et Vincent Nicomette
beguin@etud.insa-toulouse.fr,eric.alata@laas.fr
vincent.nicomette@laas.fr

LAAS-CNRS,
Univ. de Toulouse, CNRS, INSA, Toulouse, France

Résumé. Dans cet article, nous proposons l'utilisation de jeux d'évasion pour la sensibilisation à la sécurité informatique. Nous expliquons tout d'abord la justification de ce choix et nos motivations. Ensuite nous décrivons les ingrédients qu'il nous semble intéressant d'inclure dans un jeu d'évasion pour la sécurité pour qu'il soit efficace et ludique. Enfin, nous décrivons deux scénarios réalisés avec les étudiants de l'INSA.

1 Contexte et motivation

Les jeux d'évasion grandeur nature, plus connus sous le nom d'*escape room*, se multiplient actuellement. Un jeu d'évasion grandeur nature se joue en général en équipe et se déroule dans une pièce dont il faut tenter de sortir dans un temps limité en résolvant un certain nombre d'énigmes. Les membres de l'équipe doivent collaborer, trouver des indices, s'organiser pour être le plus efficace dans la résolution d'énigmes et ainsi remporter le jeu (i.e. sortir avant le temps imparti). Quelques articles témoignent aujourd'hui de l'engouement pour ces jeux [3, 4].

En même temps, la sécurité informatique est aujourd'hui un vrai sujet de société. Il y a un consensus général aujourd'hui pour reconnaître qu'elle ne concerne plus uniquement les experts informatiques et réseaux, chargés de protéger les entreprises contre des attaques perpétrées par des *hackers*, eux-mêmes spécialistes de la discipline. Elle concerne maintenant également les employés des entreprises, qui sont utilisateurs des outils informatiques ainsi que toute personne du grand public. Cette évolution est justifiée par l'importance que les objets connectés prennent dans la sphère privée et publique.

Un exemple flagrant et récent montre que la technique n'est pas suffisante. En 2015, le ver Mirai [2] se propage en compromettant tout un ensemble d'objets connectés, dont des caméras IP. La principale faille qu'il

utilise correspond à une faiblesse dans la configuration des objets connectés : identifiant et mot de passe faciles à trouver. La même vulnérabilité (mots de passe faciles à découvrir) était déjà utilisée dans le premier ver de l'Internet, écrit par Robert Morris J. en 1988 [5]. De plus, les deux dictionnaires de logins et mots de passe utilisés sont du même ordre de grandeur. En 1988, ces problèmes étaient nouveaux. Aujourd'hui, ils sont parfaitement connus ainsi que les moyens pour les résoudre. La persitance de ces problèmes indique la nécessité de sensibiliser tout un chacun aux enjeux de la sécurité informatique.

De nombreuses formations à la sécurité existent pour les personnels des entreprises ou pour les étudiants, mais dans une forme relativement traditionnelle et pour un public bien spécifique. Ces formations « classiques », où un intervenant partage son expérience du domaine, sont bien sûr très utiles. Mais très souvent, les participants ne sont pas acteurs et restent passifs. Il ne leur est pas facile de réaliser l'importance des propos de l'intervenant, ni même de réaliser la facilité avec laquelle un attaquant peut progresser si les victimes ne sont pas vigilantes. Il nous semble pertinent de proposer une sensibilisation à la sécurité où les participants sont acteurs, ce que les jeux d'évasion permettent. Notons qu'une autre approche, basée sur les jeux de rôles a été proposée récemment [1].

2 Les avantages d'une sensibilisation par les jeux d'évasion

Une sensibilisation par un jeu d'évasion doit confronter autant que possible le candidat aux problèmes d'actualité et doit éviter de se focaliser sur des problèmes trop spécifiques et/ou rares. Il est important selon nous que plusieurs ingrédients soient réunis :

- Il faut évidemment aborder un minimum de techniques et ne pas se cantonner à des généralités. Un discours trop général ne permet pas d'ancrer un message ou une idée dans l'esprit des gens par manque d'illustrations et d'applications.
- Il faut aborder des aspects liés à l'ingénierie sociale, qui forment un facteur fondamental aujourd'hui dans la réussite d'une attaque informatique : l'humain est aujourd'hui très souvent le maillon faible, tout autant que la faute logicielle.
- Il faut confronter le participant à des scénarios réels, dans lesquels il est acteur et rencontre des cas concrets qu'il doit résoudre. Cette confrontation lui permettra de mieux se souvenir de telle ou telle

énigme car il aura eu du mal à l'élucider, et ainsi il associera de façon plus précise et plus durable un risque de sécurité à une bonne pratique.

Les jeux d'évasion nous semblent parfaitement contenir ces ingrédients. En effet, les énigmes proposées peuvent contenir de multiples défis techniques, de tout ordre, relatifs à la sécurité informatique. Il est tout à fait possible d'envisager la création de différents scénarios, avec des niveaux de difficultés techniques croissants. Les différentes énigmes peuvent également faire intervenir de l'ingénierie sociale. Nous pouvons imaginer différentes formes même si les jeux d'évasion actuels ne prévoient pas forcément des communications avec des personnages extérieurs. Enfin, les jeux d'évasion ont le grand intérêt de mettre en situation le participant dans une situation quasi réelle, faisant intervenir plusieurs personnes et différents objets. Ces objets peuvent être des objets techniques informatiques ou informatisés, mais aussi des objets de notre quotidien, a priori indépendants de tout système informatique, mais qui peuvent être l'origine d'une faille de sécurité s'ils sont utilisés sans précaution. Les différents challenges de sécurité qui existent aujourd'hui sont en général uniquement composés de défis techniques et ne comprennent pas, à notre connaissance, de déplacement dans un lieu, à la recherche d'un indice ou d'une faille ; il s'agit alors simplement d'un document déchiré dans une poubelle, qui contient des informations confidentielles. Les jeux d'évasion présentent cette caractéristique intéressante.

3 Proposition de scénarios d'escape room

Le jeu d'évasion que nous proposons vise à sensibiliser tout type d'utilisateur à la sécurité informatique, et non pas seulement les informaticiens. Il doit donc prendre en compte cette dimension dans la conception des énigmes. Une salle dédiée à sa réalisation a été préparée dans les locaux du Département Génie Electrique et Informatique (DGEI) de l'INSA de Toulouse. Cette salle est aménagée par des étudiants de 4^{e} année qui réalisent un projet pédagogique sur ce thème, avec l'aide des enseignants et du personnel technique du département.

Les scénarios sont bâtis sur les grands principes suivants :

- Ils nécessitent l'utilisation d'une pièce ou deux (en fonction du scénario). À cet effet, une cloison amovible a été conçue.
- Ils contiennent des énigmes relevant de l'informatique technique. Elles doivent être adaptées aux compétences des participants. Par exemple, pour des participants familiers de l'informatique mais n'ayant pas

de compétences particulières en sécurité, il est important qu'ils comprennent les éléments suivants :

  - en quoi consiste la sécurité d'un mot de passe ;
  - le risque de naviguer sur des sites Internet sans aucune précaution ;
  - l'importance d'utiliser des mécanismes cryptographiques pour consulter sa messagerie électronique, quel que soit le protocole utilisé ;
  - l'importance de se méfier des messages électroniques reçus, en remettant en cause systématiquement l'identité de l'émetteur et sans jamais se fier aux documents attachés ;
  - le fait que les périphériques et objets physiques peuvent être malvaillants ou corrompus (et non uniquement les logiciels et les fichiers téléchargés).

– Ils incluent des situations mettant en jeu différentes formes d'ingénierie sociale, dans lesquelles les participants doivent soit communiquer avec une personne extérieure (par téléphone ou connexion Internet type Skype), soit écouter ou lire des documents/consignes laissés par une personne extérieure.
– Il mettent en situation les mauvaises habitudes fréquentes des utilisateurs de systèmes informatiques (informations importantes sur post-it, dans la poubelle, sous le clavier, sur un tableau, etc.).

Nous proposons deux types de scénario pour notre jeu d'évasion, un premier orienté défense et un second orienté attaque. Pour le scénario orienté défense, les participants sont dans une pièce (qui peut représenter le bureau d'une société ou un domicile) et disposent d'un certain temps pour débarasser cette pièce de toute « vulnérabilité » permettant à un attaquant, une fois présent dans la pièce ou connecté à distance, de compromettre le système informatique. Pour le scénario orienté attaque, les participants sont dans une première pièce d'une société et jouent le rôle de personnes désirant frauder au sein de cette société. Leur but n'est pas de sortir de cette pièce dans le temps imparti, mais de pénétrer dans une seconde pièce et d'y perpétrer ces activités frauduleuses en temps contraint.

Les grands principes sont présentés dans les deux sous-sections suivantes. Étant donné qu'il est important que les participants puissent venir continuer à tester cet escape room après la parution de cet article, nous ne donnons volontairement pas tous les détails précis du jeu.

Les deux scénarios ont été conçus en utilisant la même démarche, basée sur l'élaboration de fiche d'énigme (voir figure 1). Chaque fiche présente l'énigme, sa solution, ses liens avec les autres énigmes, mais

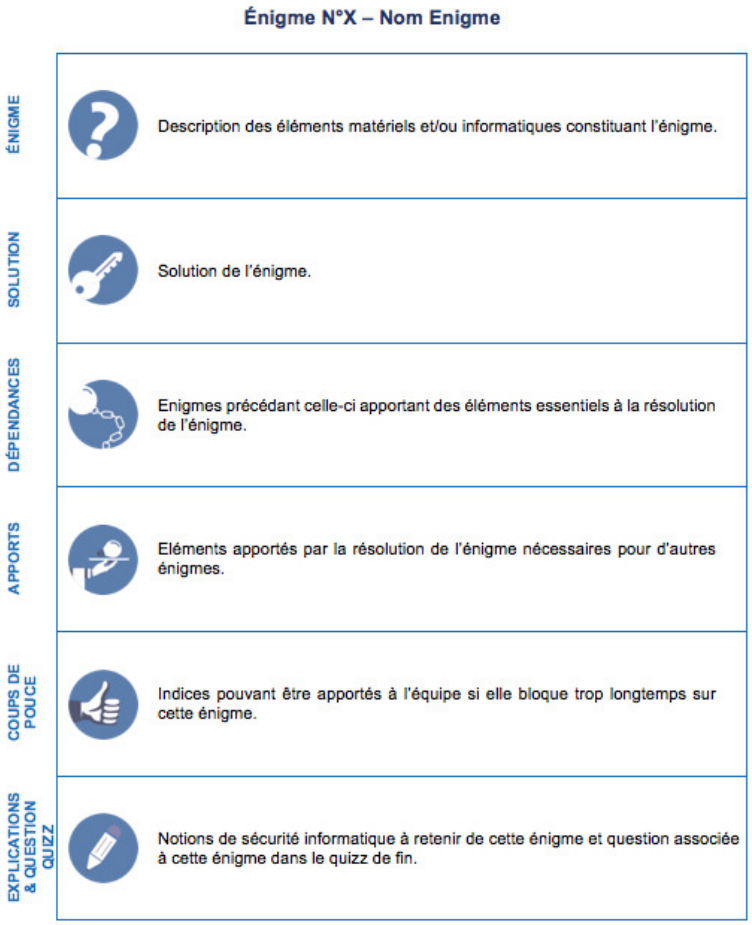

Fig. 1. Exemple de fiche énigme

aussi ses apports quant à la sensibilisation des participants à la sécurité informatique. Pour chaque scénario, les fiches sont regroupés sous la forme de graphes, permettant de vérifier la cohérence du scénario.

À la fin de l'épreuve, un quizz est proposé aux participants afin de cerner les différentes notions qu'ils viennent d'assimiler. Cela constitue également, en plus de leur score lors de l'escape room, une bonne évaluation de leurs compétences en sécurité informatique et nous permet également d'ajuster les détails de notre scénario.

3.1 Scénario défense

Le scénario d'escape room orientée défense se base sur la recherche et la correction de vulnérabilités informatiques mais aussi la correction de mauvaises habitudes qui peuvent mettre indirectement en danger un système informatique. Le cadre choisi est celui d'une startup et se déroule dans une unique salle où se trouvent les bureaux de quatre salariés qui

sont joués par quatre participants. Cette salle est composée de postes informatiques, d'armoires sécurisées, de documents et d'autres équipements électroniques comme des téléphones, une imprimante et un vidéoprojecteur. Chaque participant reçoit une « fiche personnage » avec des informations sur un des quatre salariés de la société. Ces informations leur permettent de rentrer dans la peau des personnages afin d'aborder plus sereinement la partie.

Le scénario s'articule autour de la menace d'une attaque informatique sur la startup par un hacker inconnu. Le rôle des participants est 1) de sécuriser leur espace de travail et 2) d'identifier si possible l'attaquant dans un temps imparti d'une heure. Afin de les guider vers ces deux objectifs, nous avons mis en place une suite de quinze énigmes. De la gestion de mots de passe faibles à la configuration de routeur Wifi, en passant par des mails de phishing, les participants doivent faire preuve de méthodologie et de vigilance pour mener à bien leur mission. Chaque énigme résolue leur octroie des points qui servent à évaluer leur réussite à la fin du jeu. Ainsi, ces énigmes permettent d'aborder plusieurs facettes de la sécurité informatique tout en étant ludique pour les joueurs.

Le défi pour les participants est donc de regarder d'un œil nouveau cet environnement familier afin d'identifier d'éventuelles menaces. Le temps imparti et les pièges disséminés tout au long des énigmes est un facteur de stress pour les participants, les forçant à remettre en question des pratiques faisant possiblement partie de leurs habitudes. C'est aussi l'occasion d'inculquer des consignes de sécurité préconisées notamment par l'ANSSI. Les thèmes considérés dans ce scénario sont les attaques matérielles, les attaques via Internet et les attaques d'ingénierie sociale. Chaque énigme s'appuie donc sur un de ces thèmes et implique pour sa résolution un moyen de défense réaliste. Toutefois, il n'est pas nécessaire d'avoir une connaissance poussée de l'informatique ou du domaine de la sécurité pour résoudre ces énigmes. Notre objectif est de sensibiliser les participants aux bonnes pratiques à adopter dans leur environnement de travail afin que toute personne travaillant quotidiennement avec un ordinateur puisse être capable de les appliquer.

L'enchaînement des énigmes est non linéaire. Pour résoudre une énigme, il est souvent nécessaire d'avoir un élément donné par une autre énigme ou trouvé dans un endroit différent de la pièce. Cette approche évite l'écueil d'une simple liste de failles à corriger et permet une découverte graduelle de l'identité du hacker. Les participants peuvent être aidés par des indices s'ils bloquent sur une énigme. Des informations supplémentaires peuvent également être distribuées en début de partie. Plusieurs niveaux

de difficulté peuvent donc être distingués en fonction du nombre d'indices distribués avant le début de l'épreuve.

3.2 Scénario attaque

Ce scénario débute par un *briefing* par un Maître du Jeu (MJ) qui donne aux participants leur mission. L'entreprise $\mathcal{A}$ nous a engagé pour voler les plans du dernier projet secret de l'entreprise $\mathcal{B}$. Votre mission, si vous l'acceptez, est de trouver et récupérer les fichiers du projet. Attention, il y a fort à parier que tous les employés n'ont pas accès à ces fichiers hautement confidentiels ! Une fois que vous aurez ces fichiers, sortez vite pour me rejoindre, je vous attends en bas de l'immeuble, dans la camionnette. Si vous avez des questions lors de votre mission, vous pourrez me joindre grâce à ce Talkie-Walkie. De plus, prenez ce kit, il vous sera utile. Attention, les employés sont partis manger, mais ils reviennent dans une heure, le temps vous est donc compté.

Ensuite, les participants entrent dans la salle avec du matériel basique donné par le MJ : talkie-walkie, clé USB, kit de crochetage. La salle est divisé en deux pièces : la salle de l'administrateur, qui est fermée à clé, et la salle principale où se trouve deux postes appartenant à des employés. L'environnement général est celui d'une entreprise du tertiaire avec des postes de travail, de nombreux documents papier, des posts-it et divers affichages muraux. On notera également la présence d'une pendule (pour décompter le temps restant), d'une caméra de surveillance et d'un ou plusieurs contenant(s) verrouillé(s).

Les fichiers que les participants doivent trouver se situent dans le poste de l'administrateur. Pour y accéder, ils doivent donc procéder à une élévation de privilège, non pas sur une machine, mais dans l'espace : ils doivent obtenir l'accès à deux postes employés puis enfin au poste administrateur. Chaque ordinateur étant utilisé comme « pivot » vers le suivant.

Pour atteindre l'objectif du scénario, il est nécessaire de résoudre un certains nombre d'énigmes dont certaines peuvent être traitées en parallèle. La trame générale est donc linéaire de façon à guider les participants un minimum. La résolution d'une énigme implique une étape de récolte d'informations et une étape d'exploitation de celles-ci. Par exemple trouver une liste des employés et leurs logins permet de s'introduire de façon illégitime sur un poste de travail. Bien entendu les exploitations ne sont pas toujours aussi simples. Les participants peuvent anticiper les étapes de récolte d'informations de plusieurs énigmes sans pour autant avoir identifié ces énigmes. Ce qui est important pour eux est de conserver

les informations ou objets collectés et les utiliser au bon moment. Cette capacité à bien se représenter la situation et à recouper les informations utiles est nécessaire tout au long de cette épreuve.

Chaque énigme importante met en exergue un ou plusieurs points de sécurité des systèmes d'informations, du point de vue d'un utilisateur. Les participants sont sensibilisés à l'exploitation de ces failles ou aux manquements aux bonnes pratiques d'hygiène informatique. Les points principaux abordés sont le social engineering, la gestion des mots de passe et des informations personnelles, la sécurité physique, la cryptographie, la sécurité des mails et des périphériques informatiques. Réaliser la facilité avec laquelle ils peuvent avancer dans leur intrusion les sensibilise à l'importance d'appliquer des bonnes pratiques.

4 Conclusion

Cet escape room est mis en place à l'INSA de Toulouse pour un public varié (étudiants de l'INSA, doctorants, employés de sociétés, grand public, etc.). Nous envisageons de le faire évoluer vers des milieux plus ciblés tels que le milieu bancaire, le milieu hospitalier ou l'IoT, sans perdre de vue l'aspects sensibilisation pour tout le monde.

Remerciements

Nous tenons à remercier tous les étudiants de l'INSA qui se sont investis dans la production de cet escape room : Solal Besnard, Adrien Cros, Barbara Joannes, Ombeline Leclerc-Istria, Alexa Noel, Nicolas Roels, Faïçal Taleb et Jean Thongphan.

Références

1. Dungeon, Dragons and Security. Black Hat 2016, 2016.
2. Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. Understanding the Mirai Botnet. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 1093–1110, Vancouver, BC, 2017. USENIX Association.
3. Blandine Le Cain. L'escape game : un phénomène mondial qui séduit un public varié. *Le figaro.fr*, September.
4. Valentin Davodeau. Nantes. La plus grande salle de jeux d'évasion de France ouverte. *Ouest France*, October.
5. Eugene H. Spafford. The Internet Worm Program : An Analysis. *SIGCOMM Comput. Commun. Rev.*, 19(1) :17–57, January 1989.