Article

Sensibilisation à la cybersécurité : une approche innovante par le jeu

Barbara Joannes et Solal Besnard, experts en cybersécurité et co-fondateurs de Kaïno.

Ces dernières années, le nombre de cyberattaques a explosé partout dans le monde. Ce constat alarmant est également vrai en France, où près d'une entreprise sur deux aurait été victime d'une attaque informatique en 2018[1].

Bien que les entreprises soient conscientes de l'importance de ces enjeux et investissent de plus en plus dans des moyens, aussi bien techniques que de gouvernance, autour de la lutte contre la cybercriminalité, le facteur humain reste la problématique centrale. En effet, dans près de 46% des attaques, un.e employé.e, négligent.e ou mal informé.e, a contribué à l'attaque informatique[2], de sorte que le danger vient également de l'intérieur des organisations.

La sensibilisation du personnel doit donc devenir une priorité pour la sécurité informatique.

Une nouvelle approche nécessaire

Les responsables sécurité mettent régulièrement en place un ensemble de règles qui doivent permettre de garantir un bon niveau de sécurité pour l'entreprise. Cependant, ces règles sont souvent perçues et ressenties comme des contraintes, créant un écart significatif entre le niveau de sécurité théorique et les comportements réels des utilisateur.trice.s.

Le but de la sensibilisation est donc double : apprendre les bonnes pratiques et faire comprendre le fondement ainsi que le but de

1 | https://www.pwc.fr/fr/espace-presse/communiques-de-presse/2018/fevrier/la-cybercriminalite-devient-la-fraude-la-plus-frequemment-signal.html
2 | https://www.kaspersky.com/blog/the-human-factor-in-it-security/

celles-ci. Face à un défi aussi ambitieux s'inscrivant dans un long processus de changement des habitudes au travail, les méthodes de sensibilisation habituelles semblent inefficaces.

Cours magistraux, présentations de diapositives, webinars, formations en ligne sont autant de vecteurs d'apprentissage qui peinent à trouver leur public sur le sujet de la cybersécurité. Nous nous sommes demandés pourquoi ces vecteurs étaient si peu efficaces, et surtout s'il était possible de trouver une meilleure approche ?

Le constat est en réalité assez simple, c'est le manque d'implication de chaque personne, couplé à une incompréhension de la rigueur des consignes données par l'entreprise, qui conduit à un désintérêt du sujet et à l'émergence de risques. Il nous a donc semblé pertinent d'identifier le moyen d'impliquer la personne et lui faire comprendre qu'elle était une composante essentielle de la politique de cybersécurité.

Partant de là, il nous a semblé que le jeu était un choix naturel pour atteindre cet objectif car cela permet de sensibiliser la personne, on parlera d'ailleurs directement du.de la joueur.euse, et lui faire prendre conscience qu'elle est partie prenante du sujet. En plus, le jeu introduit une vraie motivation, un challenge qui permet de mieux retenir car il crée « *des conditions favorables à l'apprentissage et, en ayant un impact positif sur les apprentissages cognitif, affectif et psychomoteur […], le jeu motive l'apprenant, structure et consolide les connaissances* »[3].

Il existe de très nombreuses études montrant un lien de causalité entre le jeu éducatif et le renforcement de l'apprentissage. C'est donc après cette anlayse de l'état de l'art que nous avons choisi un type de jeu particulier : l'*escape game* (un concept qui vise à convoquer 4-5 joueurs dans une pièce avec pour but de sortir de la pièce en résolvant une série d'énigmes, le tout en maximum 1 heure). Il nous a semblé que l'*escape game* avait l'avantage de pouvoir s'inscrire dans le cadre et les règles de l'univers de l'entreprise. Autrement dit, il permettait de faire directement un lien entre le jeu, tel que vécu par les joueur.euse.s, et l'espace de travail, cotoyé quotidiennement par ces mêmes personnes.

Nous avons donc suivi ce projet de créer des mises en situations physiques où chaque participant.e serait acteur.trice de son devenir et pourrait appréhender la cybersécurité sous un angle nouveau. Toute la difficulté de la création d'un *escape game* éducatif était donc de créer un scénario qui serait naturel pour les joueur.euse.s tout en trouvant un équilibre entre les aspects ludiques et pédagogiques.

La création d'un *escape game* éducatif

Suite à ces constats, nous avons décidé de créer notre société, Kaïno, afin de proposer une nouvelle expérience associant jeu et sensibilisation à la sécurité informatique en entreprise.

Pour designer cette nouvelle expérience, il a fallu associer, tout en conservant les codes de l'*escape game*, des concepts de *game design* et de cybersécurité, afin de créer un jeu accessible à une population large et dont l'expérience de jeu serait la meilleure possible. Nous avons donc créé des scénarii jouables par des personnes n'ayant que les notions simples d'utilisation de l'informatique.

Le game design

Créer une bonne expérience de jeu éducatif nécessite un certain nombre de critères issus une fois de plus des sciences sociales :

- Les applications doivent inclure un objectif pédagogique clair ;
- Les projets doivent intégrer un large éventail d'objectifs d'apprentissage ;
- Le rôle de l'enseignant.e *in situ* doit être pris en compte.

En plus de ces éléments, qui permettent de créer l'aspect pédagogique de l'expérience, il faut que le jeu soit adapté aux joueur.euse.s, qu'il ne soit pas trop difficile pour ne pas être frustrant mais pas non plus trop simple et donc inintéressant.

3 | Sauvé Louise, Renaud Lise & Gauvin Mathieu (2007). « Une analyse des écrits sur les impacts du jeu sur l'apprentissage ». Revue des sciences de l'éducation, vol. 33, n° 1, p. 89–107.

Le but est d'atteindre un état d'équilibre appelé le *flow*. Il est probable que vous ayez déjà ressenti cet état lorsque vous étiez totalement plongé.e dans une activité, perdant toute notion du temps qui passe.

L'escape game

Fort.e.s de tous ces constats, nous avons commencé à créer un scénario se déroulant dans un *open space* analogue à n'importe quel espace de travail de façon à ancrer l'aspect sensibilisation.

À partir du cadre établi, nous avons réfléchi aux différents points à aborder, c'est-à-dire les dangers les plus souvent rencontrés en entreprise et leurs les bonnes pratiques associées (ex : les mots de passe, l'intégrité physique des objets, le *social engineering*[4], la gestion des mails, le *phishing*[5] etc...). Une fois les points à aborder définis, nous avons créé un ensemble de petites mises en situation qui pourraient être intégrées à un scénario plus large.

La création du scénario est certainement l'étape qui a été la plus difficile car il a fallu trouver un enchaînement naturel des points de sensibilisation qui permette au.à la joueur.euse de vraiment s'inscrire dans le jeu. Pour nous aider dans la conception de chaque scénario, nous avons utilisé plusieurs outils. Dans un premier temps, nous avons créé une fiche descriptive pour chaque point à intégrer au scénario incluant l'énigme à résoudre, l'aspect de sécurité informatique à retenir et sa place dans le scénario. Une fois tous ces éléments définis, nous avons représenté sous forme d'organigramme (voir la figure ci-dessous) une vision d'ensemble du scénario afin d'être en capacité de suivre aisément l'avancé des joueur.euse.s.

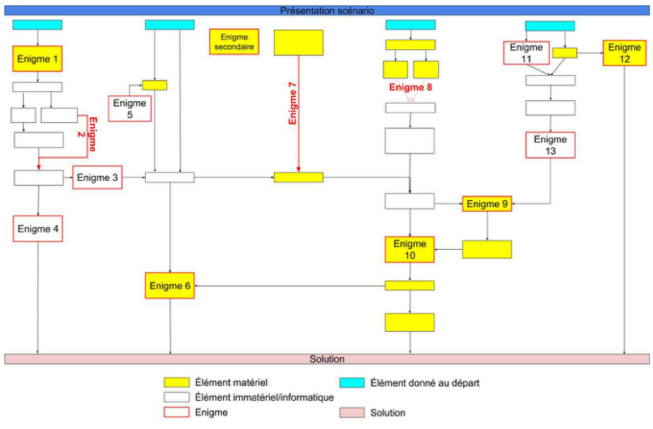

Figure - Enchaînement des énigmes pour un scénario

Cet organigramme illustre le lien entre les différents personnages du scénario, le matériel de la salle et les énigmes. On peut y voir en bleu les 4 postes de travail, représentant le point de départ de la plupart des énigmes liés aux 4 personnages du scénario. On peut noter ainsi de nombreux échanges d'informations (représentés par les flèches) entre les différents postes permettant de résoudre les énigmes (en rouge). Ce schéma illustre la nécessité pour les joueur.euse.s de communiquer leurs découvertes respectives afin de pouvoir avancer dans le scénario.

Pour travailler plusieurs dimensions de la sécurité informatique, il a été décidé de créer deux scénarii différents mais complémentaires : l'un où la.le joueur.euse joue l'attaquant.e d'une entreprise, la.le joueur.euse doit voler les données les plus confidentielles de celle-ci et l'autre où la.le joueur.euse est responsable de la sécurité informatique qui doit sécuriser son entreprise avant l'arrivée de potentiel.le.s attaquant.e.s.

Les deux scénarii permettent donc d'explorer à la fois les bonnes pratiques sous l'angle du quotidien (ce qui renvoie à la vie professionnelle) mais également sous l'angle de la menace (ce qui ouvre des perspectives sur l'approche du.de la pirate informatique), donnant ainsi un réel fondement et une légitimité aux bonnes pratiques de sécurité, qui deviennent une nécessité plus qu'une contrainte.

Chaque séance commence par un *briefing* afin de donner aux participant.e.s tous les éléments nécessaires au bon déroulement du jeu : définition du scénario (attaquer ou défendre l'entreprise) et leurs objectifs (résoudre les énigmes en 1 heure maximum). Un *debriefing* est fait systématiquement à l'issue du jeu afin de faire le point sur ce que les joueur.euse.s ont retenu et pensé de l'*escape game*. Ce *debriefing* est extrêmement important car il permet de recentrer toute l'expérience sur l'aspect pédagogique et de consolider les connaissances latentes développées pendant le jeu, notamment en mettant des mots sur l'expérience sensible ressentie.

Une fois les différents scénarii établis, nous avons entrepris de les faire tester par un large panel de personnes, le but étant de voir les retours des personnes diverses : certain.e.s ayant peu ou aucune connaissance en informatique et d'autres ayant quelques notions de cybersécurité. Ainsi nous avons pu recueillir des avis venant de sources très différentes pour être sûr.e.s que notre *escape game* soit adapté.

Cette étape capitale a permis d'ajuster la jouabilité des scénarii de façon à se rapprocher aux mieux des divers prérequis évoqués précédemment. Heureusement nous n'avons pas eu à faire de grandes modifications, la plupart des joueur.euse.s étant satisfait.e.s aussi bien de la difficulté du jeu que de la balance entre les aspects ludiques et didactiques. Les retours ont été globalement

4 | Une pratique de manipulation à des fins d'escroquerie.
5 | Technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.

très positifs, ce qui nous a conforté dans notre idée que cette nouvelle méthode d'apprentissage avait un réel intérêt et fonctionnait sur le terrain. À ce jour, plus de 200 personnes ont participé à cette sensibilisation. Le taux de réussite, équivalent sur les deux scénarii, approche les 90%.

Aujourd'hui nous proposons ce service à divers organismes aussi bien privés que publics, fort.e.s de nos réussites passées avec des entreprises telles que Thalès, Airbus Defense & Space, Spie ICS ou bien iSphère. Les *escape games* prennent donc le pari d'une nouvelle approche de la sensibilisation dans un domaine où le besoin est aujourd'hui énorme et devrait le rester pendant encore des années. Les retours des clients montrent que c'est une réussite et que cela soude les équipes tout en atteignant le but de la sensibilisation.

Nous continuons sans cesse d'améliorer nos formations, avec notamment dans le contexte difficile d'aujourd'hui, un scénario en ligne qui est en préparation.

L'œil de la revue Third

Vous avez l'impression de beaucoup entendre parler de cybersécurité mais de ne pas comprendre les risques que vous cotoyez au quotidien ou de ne pas savoir les bons réflexes à adopter ? Rassurez-vous, c'est le cas de beaucoup de monde et la sensibilisation à ces sujets en entreprise reste faible, comme en témoignent les nombreuses attaques. C'est également le constat de Barbara Joannes et Solal Besnard qui ont créé Kaïno, une société qui créé des *escape game* autour de la sécurité informatique dans une perspective pédagogique. Nous espérons pouvoir y jouer prochainement !

www.third.digital