cigref
Réseau
de Grandes Entreprises

INHESJ
INSTITUT NATIONAL
DES HAUTES ÉTUDES
DE LA SÉCURITÉ ET DE LA JUSTICE

Sûreté et Risques Numériques

Scénario d'un serious game

cigref
Réseau
de Grandes Entreprises

PROMOUVOIR LA CULTURE NUMERIQUE
COMME SOURCE D'INNOVATION ET DE PERFORMANCE

Sûreté et Risques Numériques

Scénario d'un Serious Game

Octobre 2013

SYNTHESE

La sécurité numérique est un sujet particulièrement sensible pour les entreprises aujourd'hui, à l'heure où les attaques se font de plus en plus fréquentes et de plus en plus violentes.

Face à cela, dans une grande majorité des cas, l'utilisateur est une des lignes de défense les plus importantes, au-delà de l'ensemble des solutions techniques et juridiques que l'entreprise peut déployer. Pourtant, ce sujet reste difficile à aborder, considéré souvent comme technique, contraignant et inintéressant par les collaborateurs.

Il est donc primordial de trouver une manière de faire passer les messages clés en matière de sécurité auprès de l'ensemble des employés, par un moyen remportant l'adhésion de tous.

Dans ce contexte, la solution du *Serious Game* convient parfaitement à la situation. Ce nouveau vecteur de formation permet de faire aisément passer les messages clés, tout en faisant adhérer les utilisateurs à un outil ludique innovant, qui adopte une démarque pédagogique attractive et stimulante et qui s'adapte à la disponibilité des utilisateurs.

Le groupe de travail CIGREF et les auditeurs de la promotion 2012/2013 du cycle CIGREF-INHESJ « Sécurité Numérique » ont donc cherché à faire un premier pas en ce sens en élaborant un scénario de *Serious Game*.

Il comprend un ensemble de situations de la vie courante des collaborateurs de l'entreprise, qui peuvent amener à des risques de sécurité importants pour le patrimoine informationnel de l'entreprise. Ces situations ont été catégorisées selon quatre environnements :

- en voyage,
- dans son entreprise,
- à son bureau, devant son ordinateur,
- à son domicile.

Ces situations sont accompagnées de fiches pratiques qui regroupent les bonnes pratiques à suivre dans ces cas et les risques qu'elles couvrent.

Le CIGREF, réseau de Grandes Entreprises, a été créé en 1970. Il regroupe plus de cent très grandes entreprises et organismes français et européens de tous les secteurs d'activité (banque, assurance, énergie, distribution, industrie, services...). Le CIGREF a pour mission de promouvoir la culture numérique comme source d'innovation et de performance.

TITRE DU RAPPORT : SURETE ET RISQUES NUMERIQUE : SCENARIO D'UN *SERIOUS GAME*

EQUIPE DU CIGREF

Jean-François PÉPIN – Délégué général
Sophie BOUTEILLER – Directrice de mission
Anne-Sophie BOISARD – Directrice de mission
Josette WATRINEL – Secrétaire de direction
Frédéric LAU – Directeur de mission
Matthieu BOUTIN – Chargé de mission
Marie-Pierre LACROIX – Chef de projet
Josette LEMAN – Assistante de direction

REMERCIEMENTS :

Nos remerciements vont à Jean-Marc de FELICE, Directeur des Ressources Techniques de Radio France, qui a piloté cette réflexion.

Nous remercions les personnes qui ont participé au groupe de travail CIGREF :

Nicolas BURTIN – Caisse des Dépôts
Pierre CACCAVELLI – RSI
Brigitte DECLERCK – Agirc Arrco
Martine FREREBEAU – La Poste
David GARCIA – France Télévisions
Emmanuel GARNIER – Systalians
Philippe GEERAERT – Thalès
Mathias LARGILLIERE – Saur
Frédéric LENOIR – RTE
Marc MENCEL – Nexter Group
Fabrice NERACOULIS – SNCF
Guy NICOLAS – Nexans
Joël NOIROT – SNCF
Jean-Michel PERRIN – La Poste
Gérard PESCH – Thalès
Yann PIEDERRIERE – Air Liquide
Gilles SAINT JEVIN – SNCF
Charles SUTTER – Société Générale
Pierre TARIF – GDF Suez
Matthieu WILLM – Dassault Aviation
Isabelle ZAWADZKI BERTHET - Areva

et les auditeurs de la promotion 2012-2013 du cycle Sécurité Numérique CIGREF-INHESJ :

Emmanuel ADELINE – Société Générale
Xavier AGHINA – Orange
Rémi BAGUE – SCOR
Olivier DALOY - LVMH
Pierre DELORT – ANDSI
Thierry GAUCHET – Sanofi
Pierre HASTIR – Euro Disney
Philippe LESEIGNEUR – EDF
Philippe MARGAINE – CCI Vaucluse
Olivier PARENT – SPIE
Marc RAYMOND – Essilor
Stéphane ROYER – Axa
Betty SFEZ – Deleporte Wentz Avocats
Christophe VIATTEAU – Total

Ce document a été rédigé par Matthieu BOUTIN, CIGREF.

POUR TOUT RENSEIGNEMENT CONCERNANT CE RAPPORT, VOUS POUVEZ CONTACTER LE CIGREF AUX COORDONNEES CI-DESSOUS :

CIGREF, Réseau de Grandes entreprises
21, avenue de Messine 75008 Paris
Tél. : + 33.1.56.59.70.00
Courriel : contact@cigref.fr

Sites internet :
http://www.cigref.fr/
http://www.fondation-cigref.org/
http://www.histoire-cigref.org/
http://www.questionner-le-numerique.org
http://www.entreprises-et-cultures-numeriques.org

SOMMAIRE

1. SECURITE ET RISQUES NUMERIQUES POUR L'ENTREPRISE

La sécurité de l'information a toujours été une composante importante de la stratégie des entreprises, ne serait-ce que pour la protection des données confidentielles qu'elles détiennent. Mais si la sécurité était facilitée auparavant par une certaine autarcie du système d'information et que sa gestion en était donc confiée aux experts du domaine, il n'en est plus de même aujourd'hui.

Puisque le numérique a un caractère transversal dans l'entreprise, les risques liés ne sont pas circonscrits au seul périmètre des systèmes d'information. Le CIGREF a publié une étude[1] sur ce sujet en 2011, qui avait pour objectif d'en établir une cartographie. 8 familles de risques ont donc été identifiées : ressources humaines, dématérialisation des rapports humains, stratégie, contrôle des systèmes d'information, éthique et juridique, patrimoine numérique, marketing, et risques périphériques.

Certains risques sont localisés, comme les risques marketing qui sont principalement concentrés sur les relations avec les clients, et tous n'apparaissent pas au même moment. Alors que certains seront d'actualité tout au long de la vie de l'entreprise, comme ceux relatifs à la cybercriminalité, d'autres n'apparaissent qu'au moment du passage vers le numérique, pour s'estomper ensuite. C'est le cas du risque lié au manque d'adhésion des employés, ou celui lié à la concurrence entre supports de vente. Ces distinctions sont importantes lorsqu'il s'agit de chercher à faire de la prévention car les politiques de gestion des risques à court, moyen et long terme dépendent du moment où les risques sont susceptibles d'apparaitre.

La sécurité n'est donc plus limitée à un débat d'expert mais bien portée au plus haut niveau stratégique dans l'entreprise, car elle a un impact fort sur leur pérennité. L'atteinte aux données stratégiques et confidentielles peut en effet avoir des conséquences sur la survie même de l'entreprise.

Dans un contexte où l'externalisation des systèmes est de plus en plus courante, il ne faut pas oublier que la constitution d'une politique de sécurité des systèmes d'information passe par une analyse fine des risques. Dans ce cadre, toutes les données, et les traitements qui les concernent, ne nécessitent pas le même niveau de préoccupation, et seront donc traitées avec une considération sécuritaire adaptée. L'entreprise doit donc mettre en place les moyens juridiques et techniques nécessaires pour garantir la sécurité de son patrimoine.

[1] Les risques numériques pour l 'entreprise, CIGREF, mars 2011

Cette problématique est d'ailleurs traitée par un guide rédigé conjointement par le CIGREF, l'IFACI et l'AFAI sur la protection des données dans le Cloud[2]. Ce guide, à destination des dirigeants d'entreprises, a pour but d'aiguiller sur les réflexions à mener autour de la caractérisation des données selon leur degré de confidentialité et de leur externalisation possible on non dans les différents types de *Cloud* (interne/externe, public/privé).

Mais au-delà des moyens technologiques et organisationnels mis en œuvre dans les entreprises pour maitriser la sécurité liée à l'IT, le facteur humain, l'utilisateur du SI de l'entreprise, représente l'un des risques majeurs encourus. C'est également l'un des plus difficiles à appréhender et à maitriser.

Parce que chaque employé de l'entreprise a accès au système d'information de l'entreprise, et donc potentiellement à un certain nombre de données sensibles, la sécurité numérique en entreprise doit être portée par l'ensemble des collaborateurs. Tous ont un rôle important à jouer dans la protection de leur entreprise. C'est pourquoi il est nécessaire que la communication sur ce sujet soit portée par les plus hautes instances dirigeantes au sein de l'entreprise, pour que les bonnes pratiques de sécurité soient intégrées dans la culture et les valeurs de l'entreprise.

Les risques de cybercriminalité et de cyberterrorisme ont connu une augmentation de fréquence d'occurrence et de gravité au cours des deux dernières années. Sujet encore mal connu et ne remportant pas l'intérêt de la grande majorité des employés, il est primordial de trouver un moyen de l'aborder afin que tous soient sensibilisés.

[2] Cloud et protection des données : guide pratique à l'attention des directions opérationnelles et générales, CIGREF-AFAI-IFACI, mars 2013

2. APPORT DES *SERIOUS GAMES*

Le traitement des questions de sensibilisation, d'information et de formation des collaborateurs de l'entreprise à la question de la sécurité apparait donc comme primordial, et dans ce domaine, la quasi-totalité des moyens de formation a déjà été employée. Formations magistrales, mises en situation, *e-learning*, films de promotion…, tous ces moyens ont montré une efficacité limitée, que ce soit sur la taille de la population touchée par cette formation, et sur la retenue des messages par les auditeurs.

On considère que nous retenons différemment les choses selon le moyen utilisé :

- 10% de ce que nous lisons
- 20% de ce que nous entendons
- 30% des images que nous voyons
- 50% de ce que nous voyons ET entendons (films, démonstrations…)
- 70% de ce que nous disons (participation à une discussion, présentation…)
- 90% de ce que nous disons ET faisons (simulation d'une expérience réelle)

Le jeu semble alors être un moyen très pertinent pour faire évoluer les comportements des utilisateurs.

2.1. Qu'est-ce qu'un *Serious Game* ?

Les *Serious Games* sont des moyens ludiques pour aborder des aspects sérieux. Ils ont donc une finalité utilitaire, en utilisant les ressorts des jeux pour y parvenir. Nous en gardons la définition suivante :

> *« Application informatique, dont l'intention initiale est de combiner, avec cohérence, à la fois des aspects sérieux (Serious) tels, de manière non exhaustive et non exclusive, l'enseignement, l'apprentissage, la communication , ou encore l'information, avec des ressorts ludiques issus du jeu vidéo (Game) »* (Julian Alvarez, Thèse en Science de la communication et de l'Information, 2007)

Le *Serious Game* se trouve donc à mi-chemin entre le jeu vidéo et le simulateur, en prenant les dimensions ludiques du premier (facteurs de motivation) et la finalité sérieuse du second (métier, pédagogie, etc.).

Un *Serious Game*, pour être efficace, ne doit pas seulement « avoir un air ludique ». Il doit utiliser un certain nombre de ressorts issus du monde du jeu vidéo qui apporteront une forte motivation pour les utilisateurs : immersion, quêtes, missions, récompenses, suspense, dramaturgie. Les facteurs de motivation sont alors divers, qu'ils soient internes à la personne (intérêt personnel, curiosité, challenge, impact émotionnel) ou externes (obtention de compliments, amélioration des compétences…).

2.2. Le jeu au service de la formation

E-learning et *Serious Game* sont donc bien deux méthodologies de formation radicalement différentes. Le module de *e-learning* va se servir des ressorts d'une formation classique, à savoir une première partie didactique qui présente les connaissances à acquérir puis un contrôle à la fin. Le *Serious Game*, quant à lui, a une approche radicalement différente, basée sur le principe « essai-erreur ». L'apprenant intégrera d'autant mieux les messages clés qu'il se sera confronté aux différentes situations, se sera « trompé », et aura appris de ses erreurs (les conséquences des erreurs doivent alors être montrées). Le *Serious Game* de formation tire donc son intérêt non pas du résultat final mais du temps passé dessus et du nombre de situations rencontrées, en offrant une rejouabilité importante.

2.3. Enjeux des *Serious Games* pour l'entreprise

Pour une entreprise, les enjeux des *Serious Games* sont multiples : baisser le coût global de la formation (adaptation aux pays, moyens matériels), passer d'une pédagogie « passive » à une pédagogie « active », former sur des fondamentaux « métiers »… Plus que des jeux, ils constituent un nouveau mode d'apprentissage.

La perception des *Serious Game* est très bonne au sein de l'entreprise avec de très hauts niveaux de satisfaction. Il y a une forte attractivité pour ce moyen par rapport à la formation en distanciel : alors que 70% des apprenants ne terminent jamais les modules *e-learning*, 100% des apprenants vont jusqu'au bout du *Serious Game*[3]. La notion de « *scoring* » intégrée est importante car elle apporte un effet viral intense et incite les participants à se lancer dans une course au meilleur score. Cela peut d'ailleurs faire l'objet de challenges au sein de l'entreprise.

2.4. La sécurité numérique par le jeu

S'il est bien un sujet sur lequel la communication est difficile, c'est bien la sécurité numérique. Souvent considéré comme un empêcheur de tourner en rond, le responsable de la sécurité des SI obtient généralement des résultats mitigés sur les éléments de sensibilisation qu'il fait circuler au sein de l'entreprise. Face à un sujet aussi sérieux, le CIGREF considère que le jeu est un moyen efficace de véhiculer les messages clés autour des risques numériques. Il a donc cherché à développer un scénario de *Serious Game*, centré autour de situations reconnues comme étant à risques et adapté à l'ensemble des collaborateurs de l'entreprise. La question d'une formation plus « technique » n'est donc ici pas abordée, même si la possibilité de réaliser plusieurs épisodes de jeu est envisageable afin de faire le tour complet de la problématique.

[3] Chiffres issus d'une étude menée chez Renault en 2012

3. PRESENTATION DU SCENARIO ET REMARQUES GENERALES

Les grands principes du *Serious Game* sur la sécurité numérique reposent sur la mise en situation d'un joueur dans différents univers représentatifs de situations courantes de risques numériques (le Guide d'hygiène informatique élaboré par l'ANSSI a notamment été pris en référence afin de garder une cohésion globale avec les actions menées par l'Etat en ce sens).

Chaque situation comprend :

- Une mise en contexte
- L'arrivée d'un évènement
- Un choix multiple
- Le passage à la situation suivante, si le choix est bon
- Des explications claires, si le choix est mauvais

Le scénario proposé s'articule autour de quatre univers décrivant des situations spécifiques :

- En voyage
- Dans l'entreprise
- Devant son ordinateur
- Au domicile.

3.1. Constats

L'élaboration du scénario est partie de trois constats fondateurs :

- Les collaborateurs utilisent les systèmes d'information dans le cadre de leur vie professionnelle et personnelle
- Parmi les collaborateurs de nos sociétés, peu d'entre eux sont sensibilisés à la sécurité des systèmes d'information
- Pourtant les menaces courantes ciblent de plus en plus la crédulité des collaborateurs et les outils informatiques qu'ils utilisent.

3.2. Objectifs

Le scénario du *Serious Game* vise donc plusieurs objectifs pour l'entreprise :

- Faire prendre conscience aux collaborateurs de nos entreprises des risques encourus de par l'utilisation de nos systèmes d'information
- S'assurer qu'un maximum de nos collaborateurs adoptent de bonnes pratiques par le biais de formations professionnelles et ludiques (le collaborateur gagne en compétence tout en suivant une formation non rébarbative)
- S'assurer que les collaborateurs se reconnaissent dans les univers abordés en intégrant des contextes variés : en déplacement, dans la vie de tous les jours, à son domicile

- Permettre au collaborateur de mieux appréhender les risques numériques sans pour autant en faire prendre à son entreprise
- Pérenniser la sensibilisation aux risques numériques en incitant les collaborateurs à se confronter régulièrement à cet outil pédagogique.

3.3. Personnalisation – Paramétrage

La personnalisation des quatre univers aux identités graphiques des différentes entreprises auxquelles le *Serious Game* est destiné sera un élément clé d'appropriation de l'outil par les collaborateurs de l'entreprise. Par ailleurs, le jeu sera paramétrable pour s'adapter au contexte spécifique et à la politique de sécurité de chaque entreprise.

Parmi les éléments techniques importants, le jeu devant être utilisable par tous et à n'importe quel moment, il fonctionnera sur PC comme sur support mobile (tablette, *smartphone*), en mode *SaaS*. Il devra être multilingue (*a minima* français et anglais) et garantir l'accessibilité aux collaborateurs en situation de handicap.

3.4. Evolutivité

La sécurité des systèmes d'information est en constante évolution. Les menaces grandissent et de nouvelles font leur apparition constamment. Cela entraîne donc la nécessité de mettre à jour ce jeu régulièrement, par l'ajout de modules complémentaires dédiés.

3.5. Mesurabilité - Suivi et *reporting*

Le *Serious Game* devra permettre un suivi des performances et de la participation des collaborateurs (consultation de l'historique des participations, des scores, des temps passés dans le jeu, etc.) par un accès à des statistiques d'utilisation. Cela permettra d'assurer le suivi de la campagne de sensibilisation auprès des collaborateurs.

3.6. Fidélisation du joueur

Le jeu devra permettre aux collaborateurs de prendre conscience de leurs progrès en matière de compréhension des risques numériques en les matérialisant par différents niveaux de difficulté. Il faut garantir un certain niveau de rejouabilité qui offrira une meilleure captation des messages clés.

Les éléments clés de la session de jeu (situations rencontrées, bonnes pratiques, score…) seront restitués au joueur en fin de session, afin qu'il puisse garder une trace de son apprentissage. Le jeu doit comporter une fonction qui permettra au joueur de mesurer sa progression (points acquis, niveaux de jeu, …) et inclura une fonction « d'assistance » présentant des fiches d'aide (qui sont annexées à ce document).

4. UNIVERS DE JEU ET SCENARIOS

Cette section du document présente de manière détaillée les situations qui ont été retenues dans chaque univers, avec les propositions d'actions liées. La description des saynètes comprend ici la situation initiale, l'élément perturbateur et l'ensemble des choix proposés, avec l'effet de chacun de ces choix, selon la légende suivante :

: Action éliminatoire

: Action très risquée

: Action risquée

: Action attendue du collaborateur

4.1. En voyage

4.1.1. Raisons du choix de cet univers

- La mobilité est un facteur de risque de plus en plus avéré et dont l'impact est d'autant plus important
- La sensibilisation des travailleurs nomades permet d'assurer une meilleure propagation des messages / bonnes pratiques et ces collaborateurs constituent des cibles privilégiées
- Les cadres de l'entreprise étant souvent amenés à réaliser des déplacements professionnels, ils se sentiront d'autant plus concernés par ce scénario
- Cet univers nous permet d'aborder des situations qui ne se produisent pas ou peu au bureau.

4.1.2. Description des saynètes

- Le collaborateur est chez un partenaire
  - Le partenaire lui donne une clé USB
    - Il la branche
    - Il ne la branche pas
    - Il propose à son partenaire de prendre sa propre clé USB
  - Au moment du déjeuner, que faire de l'ordinateur portable ?
    - Il laisse la session non verrouillée et le poste en évidence pendant l'heure de déjeuner

- ✅ Il range le PC dans sa sacoche et s'assure que la salle ferme à clé avant d'aller déjeuner. Dans le cas contraire, il prend sa sacoche avec lui

- Le collaborateur est à l'hôtel
  - Il doit quitter sa chambre
    - 🛑 Il laisse son PC dans sa chambre en évidence sur le bureau
    - ⛔ Il laisse son PC dans sa chambre dans le coffre-fort
    - ✅ Il prend son PC avec lui

- Le collaborateur est à l'aéroport
  - Utilisation du point d'accès Wifi non sécurisé de l'aéroport
    - ✅ Il active son VPN[4] et envoie des documents confidentiels par sa messagerie professionnelle
    - ✅ Il ne se connecte pas à un point d'accès wifi public
    - ✅ Il n'a pas de VPN, mais a pris soin de chiffrer les documents auparavant en prenant soin de ne mentionner aucune information confidentielle dans le corps du mail
    - ⛔ Il envoie des mails sans avoir pris soin de les chiffrer auparavant
  - Pour passer le temps à l'aéroport, il souhaite installer des logiciels sur son smartphone / tablette/ PC
    - ⛔ Oui
    - ✅ Non
  - Il perd son terminal mobile ou une mémoire amovible pendant un déplacement
    - ✅ Il déclare immédiatement la perte du terminal ou de la mémoire amovible au service support de son entreprise
    - ⛔ Il attend d'être de retour au bureau pour déclarer la perte, à moins de l'avoir retrouvé(e) dans ses bagages
  - Alors qu'il travaille dans un lieu public, pour éviter le regard insistant et de travers de sa voisine
    - ✅ Il met son filtre écran
    - ✅ Il se déplace vers un autre siège
    - ✅ Il ferme son écran
    - ⛔ Il continue de travailler comme si de rien n'était

[4] Réseau Privé Virtuel (*Virtual Private Network* ou VPN)

- Dans un lieu public, un individu demande de charger son téléphone sur le port USB de son PC
  - ⛔ Il accepte de brancher son téléphone sur son port USB
  - ✔ Il n'accepte pas

- Le collaborateur est sur un site appartenant à son entreprise, mais qui n'est pas son site habituel
  - Il souhaite se connecter au réseau
    - ✔ Il branche son PC comme s'il était à son bureau
    - ✔ Il demande un accès WIFI invité et active son VPN
    - ✔ Il n'a pas confiance, et ne se branche pas sur ce réseau
  - Dans les réseaux WIFI accessibles, il détecte un réseau ouvert appartenant à un particulier, et un réseau appartenant à l'entreprise nécessitant un mot de passe
    - ⛔ Il se connecte sur le réseau ouvert du particulier
    - ✔ Il demande le mot de passe permettant de se connecter au réseau de l'entreprise, puis s'y connecte

- Le collaborateur doit partir dans un pays "à risques"
  - ✔ Il demande à son service informatique un "PC blanchi"
  - ✔ Il consulte les recommandations de l'ANSSI pour les voyageurs
  - ⛔ Il y va sans prendre de précautions particulières
  - ⛔ Il ne prend pas son matériel informatique puisqu'il se connectera depuis un cybercafé / un business center

4.2. Dans l'entreprise

4.2.1. Raisons du choix de cet univers

- Le choix d'un univers mettant en scène un collaborateur « type » permet d'assurer une meilleure appropriation par tous les joueurs
- Cet univers illustre les risques les plus courants, au quotidien
- Cet univers complète celui du collaborateur en mobilité.

4.2.2. Description des saynètes

- En route ou en déplacement à proximité de son entreprise, le collaborateur attend un mail important
  - ✘ Il demande à quelqu'un de lui prêter son PC pour regarder ses mails

- ✅ Il attend d'être de retour au bureau pour consulter sa messagerie
- ✅ Il ne regarde pas ses mails et appelle le bureau pour se tenir au courant

- Lors d'un court déplacement, le collaborateur utilise son smartphone ou sa tablette fournie par son entreprise pour consulter ses mails
  - Via le point d'accès wifi gratuit et ouvert
    - ✅ Il lance son client VPN
      - ✅ Il ouvre son mail
      - ✅ Il ouvre son webmail sécurisé en HTTPS
    - ⛔ Il ouvre son webmail non sécurisé en HTTP
  - Via le wifi protégé par un mot de passe de son opérateur téléphonique
    - ✅ Il lance son client VPN
      - ✅ Il ouvre son mail
      - ✅ Il ouvre son webmail sécurisé en HTTPS
    - ⛔ Il ouvre son webmail non sécurisé en HTTP
  - Via son abonnement 3G
    - ⛔ Il ouvre son webmail non sécurisé en HTTP
    - ✅ Il ouvre son webmail sécurisé en HTTPS

- Le collaborateur trouve une clé USB portant le logo de l'entreprise ou un autre périphérique USB dans le parking de l'entreprise
  - ✅ Il la ramasse et l'amène au service Sécurité
  - ❌ Il la ramasse et la branche sur son PC
  - ⛔ Il la laisse

- Le collaborateur assiste à la scène suivante :
  Une personne demande à rencontrer un collaborateur absent. Elle donne alors une clé USB à l'hôtesse d'accueil, et lui demande de la brancher sur son PC afin de transmettre un document à ce collaborateur
  - ✅ Il prévient le service de sécurité
  - ✅ Il dit à l'hôtesse de ne pas brancher la clé USB sur son PC
  - ❌ Il ne fait rien

- Le collaborateur reçoit un fournisseur dans une salle de réunion et ce dernier a besoin d'une connexion Internet pour réaliser une démonstration de son produit
  - ❌ Il lui permet de se connecter sur la prise réseau présente dans la salle

- ❌ Il lui donne un accès temporaire au réseau wifi de l'entreprise
- ✅ Il lui donne le SSID du réseau wifi utilisable par les visiteurs
- ✅ Il lui indique que c'est interdit

- Le collaborateur reçoit la visite de son auditeur aux comptes qui a besoin de se connecter sur le réseau de l'entreprise, pour avoir accès à la GED de la comptabilité afin de travailler sur certaines pièces comptables
  - ⛔ Il permet à l'auditeur d'utiliser son PC portable et de le connecter au réseau, car c'est un partenaire qu'il connait de longue date et auquel il fait totalement confiance
  - ⛔ Il lui permet d'utiliser une station de travail de l'entreprise (il le connecte avec son compte et son mot de passe)
  - ✅ Il appelle le support informatique pour demander un compte pour l'auditeur et lui permet d'utiliser une station de travail de l'entreprise

- Le collaborateur reçoit son neveu pour son stage de 3ème. Le neveu demande de pouvoir aller sur Internet pour consulter son Facebook (il possède un smartphone wifi)
  - ⛔ Il lui permet d'utiliser une station de travail de l'entreprise (il le connecte avec son compte et son mot de passe)
  - ⛔ Il lui donne un accès temporaire au réseau wifi qui permet d'accéder à Internet et il utilise son smartphone
  - ✅ Il lui donne le SSID du réseau wifi utilisable par les visiteurs qui permet d'accéder à Internet et il utilise son smartphone
  - ✅ Il demande au support informatique un compte et un mot de passe pour son neveu et lui indique une station de travail à partir de laquelle il pourra se connecter à Internet

- Le collaborateur est en charge d'un projet qui va nécessiter la présence d'un prestataire pendant plusieurs semaines sur le site. Ce prestataire, pour être efficace, a besoin d'utiliser son propre PC et d'avoir un accès à Internet
  - ⛔ Il lui permet de connecter son PC sur la prise réseau présente là où il travaille
  - ⛔ Il lui donne un accès temporaire au réseau wifi d'entreprise qui permet d'accéder à Internet
  - ✅ Il lui donne le SSID du réseau wifi utilisable par les visiteurs pour qu'il puisse se connecter à Internet

- ✅ Il appelle le support informatique pour demander un compte pour ce prestataire et lui permet d'utiliser une station de travail de l'entreprise pour se connecter à Internet

- Le collaborateur est en charge d'un projet qui va augmenter la productivité de l'entreprise de 500% (du moins c'est ce que dit le commercial) et le fournisseur qui recommande cet outil propose de venir l'installer provisoirement dans un des bureaux de l'entreprise. Il a besoin pour monter cette maquette de connecter un appareil sur le réseau
  - ⛔ Il lui permet de faire cette connexion car ce projet est suivi et approuvé par la direction générale
  - ⛔ Il débranche le câble d'un poste qui n'est pas utilisé pour lui permettre de se connecter au réseau
  - ✅ Il demande aux personnes en charge du réseau informatique de réaliser cette connexion

- Le responsable marketing du collaborateur lui demande de tester son intervention pour un prochain colloque. Il utilisera pour sa présentation une tablette wifi, une imprimante 3D wifi et un routeur wifi à brancher sur le réseau du colloque pour connecter le tout à Internet. Il doit vérifier que les appareils fonctionnent harmonieusement.
  - ⛔ Il connecte le tout sur le réseau de l'entreprise pour voir comment ça marche
  - ⛔ Il demande aux personnes en charge du réseau informatique de réaliser cette connexion sur le réseau d'entreprise
  - ✅ Il teste la configuration sur une Box indépendante du réseau de l'entreprise
  - ✅ Il se rend en avance sur le lieu de la présentation pour tester la configuration avant la présentation

4.3. Devant son ordinateur, à son bureau

4.3.1. Raisons du choix de cet univers

- Cet univers permet de montrer de manière lisible les fenêtres qui apparaissent sur l'écran d'un PC (vu de loin, ce serait illisible)
- Il permet également une bonne appropriation du contexte par le joueur qui se sent d'autant plus impliqué qu'il voit directement le contenu de l'écran

- Ceci est renforcé par le fait de ne pas montrer l'utilisateur : tous sont concernés par ce scénario, indépendamment de la fonction du joueur dans l'entreprise ou du contexte dans lequel il opère.

4.3.2. Description des saynètes

- On demande au collaborateur de changer son mot de passe Windows. Il choisit de mettre
  - ⛔ Son numéro de carte de crédit
  - ⛔ Le même que l'identifiant
  - ⛔ password02
  - ⛔ azertyqsdf
  - ⛔ jean-marie12031973
  - ⛔ Son mot de passe de messagerie perso qui est p2ssw0rd!
  - ✔ p2ssw0rd!
  - ✔ Au moins un chiffre, une lettre, un symbole et 8 caractères minimum

- On demande au collaborateur de changer son mot passe de l'outil de compta / ERP / ou autre outil métier. Il choisit :
  - ⛔ Le nom du département : supplychain2013
  - ⛔ Un mot de passe partagé avec l'ensemble de l'équipe
  - ⛔ Un mot de passe qu'il partage avec son *backup*
  - ✔ Un mot de passe propre qui est le même que son mot de passe Windows, à savoir p2ssw0rd!

- Pour mémoriser les mots de passe de ses applications et ses sites Web
  - ⛔ Il utilise un fichier Excel contenant ses mots de passe
  - ✘ Il utilise un fichier Excel zippé protégé par mot de passe contenant ses mots de passe
  - ✔ Mot de passe propre dans un coffre-fort à mot de passe
  - ✔ Il retient tous les mots de passe de tête

- Le collaborateur a une fenêtre d'alerte signalant que son PC est infecté
  - ✔ Il alerte le support
  - ✔ Il débranche le câble réseau
  - ⛔ Il demande à son collègue qui s'y connait

- Le collaborateur reçoit un mail « louche » (de *phishing*)
  - ❌ Il répond, ça a l'air tentant
  - ⛔ Il fait suivre à l'assistante ou aux collègues
  - ✔ Il le fait suivre à une adresse "report-spam@..."
  - ✔ Il le supprime
  - ✔ Il le signale au *helpdesk*, correspondant sécurité

- Le collaborateur reçoit une blague par mail contenant une pièce jointe
  - ⛔ Il le lit et ouvre le fichier attaché
  - ✔ Il le lit mais n'ouvre pas le fichier attaché ni ne clique sur un lien
  - ✔ Il supprime le mail

- Le collaborateur va prendre une pause café
  - ✔ Il verrouille sa session en enlevant le badge de son lecteur de carte à puce
  - ✔ Il verrouille sa session en appuyant sur « Windows + L »
  - ⛔ Il ne verrouille pas son PC car il en a juste pour quelques minutes

- Le collaborateur a besoin d'installer Adobe Acrobat ou un autre outil bureautique
  - ⛔ Il l'achète et essaie de l'installer (son collègue connait le mot de passe administrateur)
  - ⛔ Il le télécharge et essaie de l'installer
  - ✔ Il en fait la demande au support

- Le collaborateur s'apprête à quitter le bureau en fin de journée
  - ✔ Il arrête son PC
  - ✔ Il le verrouille
  - ⛔ Il le laisse se mettre en veille prolongée

- Quelqu'un demande son mot de passe au collaborateur
  - C'est un collègue
    - ⛔ Il lui donne car il est sympa
    - ⛔ Il lui donne, car c'est son chef ou sa secrétaire / son assistant
    - ✔ Il ne lui donne pas son mot de passe
  - C'est le support qui intervient physiquement
    - ✔ Il change son mot de passe pour "password123", et le rechangera lorsqu'ils rendront son PC

- ⛔ Il leur donne son mot de passe actuel

- C'est quelqu'un du support qui l'appelle par téléphone et lui demande son mot de passe
  - ✅ Il leur demande d'envoyer un email pour prouver qu'il s'agit bien du support ou leur propose de les rappeler lui-même
  - ⛔ Il leur donne son mot de passe actuel

4.4. Au domicile

4.4.1. Raisons du choix de cet univers

- Cet univers permet notamment d'illustrer les risques liés à l'apport de technologies numériques au travail par chaque collaborateur (« IT *Consumerization* ou BYOD – *Bring Your Own Device* ») ainsi que ceux ayant trait au travail à domicile
- Il montre en particulier les risques liés :
  - Au mélange de la vie privée et de la vie professionnelle des collaborateurs
  - A la difficulté de la valorisation de l'expérience professionnelle d'un collaborateur tout en assurant la confidentialité de ses travaux pour l'entreprise
  - A l'utilisation courante des réseaux sociaux dans l'entreprise
- Cet univers permet également une bonne appropriation du sujet par les joueurs, qui sont fréquemment confrontés à ces problématiques (chaque soir et chaque week-end!)

4.4.2. Description des saynètes

- Sur l'ordinateur portable de la société, le collaborateur reçoit une invitation à une conférence téléphonique sur un outil en ligne pour traiter une question professionnelle
  - ⛔ Il clique sur le lien, installe et ouvre le logiciel. (Le firewall se déclenche, un message d'alerte apparaît et bloque l'ouverture)
  - 🛑 Le collaborateur tente de désactiver le firewall, y parvient, le programme malveillant prend le contrôle de l'ordinateur qui se bloque infecté
  - ✅ Le collaborateur arrête la procédure et propose de passer par le téléphone professionnel, moins pratique mais autorisé
  - ✅ L'employé propose de passer par une solution de messagerie instantanée autorisée par l'entreprise

- Un partenaire demande au collaborateur de lui transmettre un fichier de travail stratégique pour qu'ils travaillent ensemble sur ce fichier
  - ⛔ Le collaborateur propose de déposer le fichier sur un DropBox et demande au partenaire si ce dernier détient un compte sur lequel il pourrait déposer le fichier.
  - ✔ L'employé suit la procédure de l'entreprise et dépose le fichier chiffré sur une version entreprise de "Dropbox"
    - ✔ Il donne le mot de passe par téléphone.
    - ✔ Il donne le mot de passe par un mail séparé et crypté

- Le partenaire propose au collaborateur de continuer à travailler chacun de son côté sur la future version du fichier
  - ✘ Il place son fichier dans Google Drive et le partage avec son partenaire
  - ⛔ Il envoie le fichier par messagerie personnelle et propose des allers-retours pour les mises à jour
  - ✔ Il chiffre puis envoie le fichier par messagerie personnelle et propose des allers-retours du document chiffré pour les mises à jour
  - ✔ Il utilise sa messagerie d'entreprise qui dispose d'une fonction de chiffrement pour les tiers partenaires

- La fille du collaborateur souhaite utiliser son PC professionnel à son domicile
  - ✔ Il le lui interdit
  - ⛔ Il lui laisse faire ce qu'elle veut
  - ⛔ Il a oublié de verrouiller son PC, elle peut y accéder librement
  - ✔ L'employé déverrouille son PC et lui laisse l'utiliser à condition qu'elle respecte quelques règles :
    - ✔ Elle n'installe aucun logiciel
    - ✔ Elle ne télécharge rien
    - ✔ Elle n'utilise pas sa messagerie professionnelle
    - ✔ Elle n'utilise pas les réseaux sociaux
    - ✔ Elle n'utilise pas de messagerie instantanée
    - ✔ Elle ne regarde aucun film en *streaming*
    - ✘ Elle peut installer les logiciels qu'elle veut du moment qu'elle les supprime ensuite
    - ✘ Elle fait ce qu'elle veut du moment qu'elle coupe le son

- ❌ Elle peut utiliser sa messagerie professionnelle du moment qu'elle n'écrit qu'à ses amis en précisant qu'elle est l'auteur des messages
- ❌ Parmi les réseaux sociaux, elle ne va que sur Facebook

- Le collaborateur met son CV à jour et enrichit sa fiche LinkedIn/Viadeo
  - ❌ Il y précise des détails sensibles mais professionnellement valorisants sur des projets qu'il a menés
  - ✅ Il limite les détails sur les projets qu'il a menés

- Après avoir travaillé sur sa présentation du lendemain depuis sa tablette
  - ❌ Il l'ajoute à son Google Drive pour y accéder le lendemain depuis son PC professionnel
  - ✅ Il le chiffre et l'envoie à son adresse mail professionnelle depuis sa messagerie personnelle
  - ✅ Il dépose sa présentation sur une clé USB chiffrée qu'il prendra avec lui le lendemain

5. FICHES CONSEIL : BONNES PRATIQUES ET RISQUES COUVERTS

Destinées à apparaître sous forme de « *pop-up* » au cours du jeu, les fiches Conseil regroupent quelques bonnes pratiques essentielles.

En mobilité

Bonnes pratiques

- Gardez votre poste de travail (ou autres *devices*) avec vous quel que soit le lieu où vous vous trouvez (ne faites pas confiance aux coffres-forts des hôtels par exemple)

Risques couverts

- Vol d'information

Dans un lieu public

Bonnes pratiques

- Ne consultez pas de données à caractère confidentiel
- N'abordez pas de sujets sensibles
- Utilisez des filtres de confidentialité sur vos écrans
- Si vous trouvez des périphériques USB, remettez-les à votre service sécurité

Risques couverts

- Vol d'information

Déplacement dans un pays « à risques»

Bonnes pratiques

- Prenez connaissance des recommandations mises à disposition par l'ANSSI

Risques couverts

- Vol d'information

Collaboration avec un partenaire

Bonnes pratiques

- Ne connectez que des périphériques de confiance à votre système
- N'utilisez que des plateformes sécurisées d'échange de fichiers, validées par votre entreprise, pour collaborer avec des tiers
- Ne transférez pas de documents professionnels vers votre messagerie personnelle

Risques couverts

- Vol d'information et infection virale

Connexion de visiteurs

Bonnes pratiques

- Ne connectez jamais une machine n'appartenant pas à votre entreprise directement au réseau de votre entreprise
- Proposez à vos interlocuteurs un accès au Wi-Fi Invités (s'il existe)

Risques couverts

- Vol d'information et infection virale

En quittant son poste de travail

Bonnes pratiques

- Verrouillez votre session de travail, fermez votre bureau à clef ou attachez votre poste de travail

Risques couverts

- Fraude et vol d'information

Installation de nouveaux logiciels

Bonnes pratiques

- Pour installer un logiciel sur votre poste de travail, contactez votre support utilisateur

Risques couverts

- Infection virale, conformité (licences logicielles) et instabilité du matériel informatique et des logiciels

Mise à jour des postes de travail

Bonnes pratiques

- Lorsque vous y êtes invité par votre système, redémarrez votre poste de travail (*a minima* une fois tous les quinze jours)

Risques couverts

- Infection de l'ordinateur et pénétration des systèmes de l'entreprise.

Mots de passe

Bonnes pratiques

- Utilisez un mot de passe complexe
- Utilisez un mot de passe différent pour chaque outil nécessitant une authentification (site web, ordinateur, sessions utilisateurs…)

- ✓ Ne partagez pas votre mot de passe avec un tiers (famille, collègue, etc.)

Risques couverts

- Usurpation d'identité

Détection d'anomalie sur les postes de travail

Bonnes pratiques

- ✓ En cas de d'activité suspecte sur votre ordinateur, contactez votre support utilisateur

Risques couverts

- Infection virale et vol d'information

Courriels suspects

Bonnes pratiques

- ✓ Supprimez tout mail suspicieux
- ✓ En parallèle, remontez cet incident au support utilisateur (remarque : le support peut demander à disposer du mail)

Risques couverts

- Infection virale et vol d'information

Bon usage des systèmes d'information professionnels

Bonnes pratiques

- ✓ Le matériel professionnel (poste de travail, portable, tablette, etc.) est uniquement à l'usage des collaborateurs de l'entreprise

Risques couverts

- Usurpation d'identité

6. PROCHAINES ETAPES

Aujourd'hui, un grand nombre d'entreprises sont convaincues par le bien-fondé de l'utilisation d'un *Serious Game* pour la sensibilisation à la sécurité numérique, et sont prêtes à continuer l'aventure.

Il s'agit maintenant, en partenariat avec le Comité Richelieu, de déterminer les parties prenantes qui seront impliquées dans la réalisation du *Serious Game* : État, financeurs publics et privés, éditeur de logiciel… L'objectif final est de pouvoir diffuser cet outil auprès des entreprises membres du CIGREF, mais également d'avoir la possibilité d'en faire un vecteur de communication sur les risques numériques auprès de l'ensemble des entreprises françaises (petites et grosses), et du grand public.

ANNEXE : PRECONISATIONS TECHNIQUES

Hébergement

Pour faciliter son déploiement, le *Serious Game* devra être accessible en mode « *Software As A Service* » (SaaS). Il pourra être hébergé soit chez un tiers de confiance, soit directement sur les infrastructures de l'entreprise.

Compatibilité et optimisation

Le *Serious Game* pourra s'intégrer aux intranets des entreprises, afin d'en faciliter l'accès au personnel de l'entreprise.

Il sera accessible sur le plus grand nombre possible de navigateurs et avec un minimum de pré requis techniques (*plugins* additionnels / matériels audio ou vidéo spécifiques, etc.).

Il est nécessaire que le jeu soit accessible facilement à l'ensemble des collaborateurs quels que soient les terminaux utilisés (poste de travail, tablette, etc.), en mobilité ou au bureau.

Qualité et pérennité

Les langages de programmation et outils utilisés pour les développements seront sélectionnés parmi les standards du marché, utilisés conformément à l'état de l'art.

Performance

Une attention toute particulière sera apportée aux performances (temps de réponse, nombre de joueur simultanés, …).

Sécurité

Le jeu devra être développé conformément aux meilleures pratiques en matière de sécurité des systèmes d'information (prévention des attaques par déni de service, des tentatives

d'intrusion ou de défiguration, etc.). En particulier les recommandations de l'ANSSI[5] et de l'OWASP[6] seront prises en compte.

Le jeu devra authentifier les joueurs conformément aux politiques de sécurité des entreprises, cette authentification devra être protégée (https).

Administration

Le jeu devra permettre un chargement par lot des comptes utilisateurs pour permettre aux entreprises de le déployer aisément.

Le jeu devra permettre aux participants de modifier leur code d'accès, leurs informations personnelles, etc.

Cette interface d'administration devra être disponible en plusieurs langues (*a minima* français / anglais).

Déclarations réglementaires

Les entreprises seront responsables de réaliser les déclarations réglementaires nécessaires (notamment auprès de la CNIL, G29 et des organismes étrangers similaires).

[5] http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-de-l-externalisation/externalisation-et-securite-des-systemes-d-information-un-guide-pour-maitriser.html

[6] http://www.owasp.org

CIGREF

21 avenue de Messine

75008 PARIS

Tel. : +33 1 56 59 70 00

Fax : +33 1 56 59 70 01

cigref@cigref.fr

www.cigref.fr