Règles du jeu des bonnes pratiques

- Contexte : Chaque joueur dispose d'un Système d'Information (S.I.) qu'il doit protéger au maximum contre diverses attaques durant la partie

- Objectif : Avoir en fin de partie le SI le mieux protégé (à titre indicatif : seuil de point minimum pour un SI protégé de 32 points). Le vainqueur est le joueur qui, à l'issue des 6 tours, a le plus grand nombre de points.

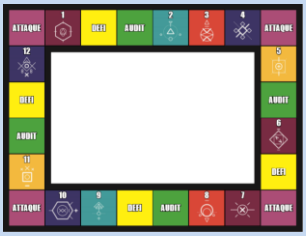
- Matériel :

> 1 Plateau de jeu (24 cases)
> 31 cartes défi
> 11 cartes attaques
> 1 dé
> 6 pions
> 1 maître du jeu
> liasse de billets

- Description du Plateau :

Plateau rectangulaire, composé de 24 cases :

- 12 cases "bonnes pratiques" (3 par côté)
- 4 cases attaques (une à chaque angle du plateau)
- 4 cases défi (une par côté)
- 4 cases audit



- Règles du jeu :

Phase d'initialisation :

- L'un des joueurs est désigné comme maître du jeu.
- Chaque joueur lance le dé pour connaître l'ordre de passage, de la plus grande valeur à la plus petite. En cas d'égalité, les joueurs concernés relancent le dé.
- Chaque joueur démarre en définissant son mot de passe administrateur correspondant à la première BP (sans qu'on lui indique le niveau de sécurité du mdp qu'il aura choisi). Il lui est ensuite demandé d'investir 300€ (déduits de son capital de départ de 1000€), il investit alors cet argent dans les BP de son choix parmi les Bonnes Pratiques 2, 3 et 4. (le prix des différents niveaux de sécurité est indiqué dans la partie "Métriques")
- Capital initial de 1000€
- 20 points de départ
- Avant de lancer le dé pour la première fois, tous les joueurs se placent sur le coin supérieur droit du plateau (entre la BP 4 et 5)

Les 12 Cases Bonnes Pratiques :

1- Mot de passe : Choisir avec soin et s'en souvenir pour toute la partie. Il sera amené à évoluer au fil du jeu surtout s'il manque de robustesse. Chaque changement nécessite un investissement. Il peut être changé si le joueur tombe sur la case Mot de passe ou bien lors d'un audit uniquement suite à une recommandation (pas possible de le changer lors d'un audit s'il est jugé suffisant). Ils seront classés en trois catégories : faible/bon/excellent).

2- Mises à jour : Le joueur devra faire attention à ses mises à jour. À chaque fois qu'un joueur finit un tour de plateau tous les logiciels seront obsolètes. Il faudra donc les mettre à jour. Le joueur peut décider de ne pas mettre à jour. Mais il peut tomber sur une attaque qui exploite les vulnérabilités (tout ceci sera détaillé dans les différents scénario). Celle-ci sera d'autant plus virulente que la version du logiciel est ancienne.

3- Connaissances de ses utilisateurs et prestataires : Adapter les comptes d'accès au S.I. à

l'initialisation, tous les collaborateurs de l'entreprise ont accès à un compte avec des droits administrateur. L'entreprise devra adapter ses comptes au fur et à mesure (arrivé de nouveaux collaborateurs/stagiaires avec moins de privilèges sur le SI/ département juridique/ressources humaines etc….)

4- Sauvegardes régulières : Un peu comme pour les màj régulières, chaque fois qu'un joueur finit un tour il faut sauvegarder les fichiers essentiels du S.I (liste et contacts des clients/ brevets/ fichiers juridiques etc…)

5- Accès Wi-Fi : initialiser le type de chiffrement (wep/wpa-es/wpa2). Au cours de la partie le joueur pourra soit faire évoluer le mdp, soit améliorer la protection sans fil en activant le pare-feu de la box par exemple ou encore penser à une architecture cloisonnée pour éviter la propagation d'une intrusion par les bornes wifi sur le reste des services du SI.

6- Smartphone : Installer des applications de sources sûres qui n'ont accès qu'aux données nécessaires. Protection avec un mot de passe lors du déverrouillage. Initialement, le joueur démarre avec un smartphone très peu protégé. (pas de verrouillage, applications nombreuses (dont celles du constructeur), Bluetooth activé, etc.)

7- Déplacements : Le scénario d'attaque prévoit pour cette B.P un déplacement pour le compte de l'entreprise avec des informations confidentielles. On jaugera la capacité du joueur à adopter des comportements qui ne mettent pas en danger ces données à l'aide d'une série de questions. Ses réponses seront classées en trois catégories (notamment : ne pas se connecter au Wifi public, ne pas laisser son ordinateur sans surveillance (ou sa session ouverte en son absence) --> mieux, utiliser un ordinateur dédié aux déplacements avec aucune donnée sensible dessus hormis ce qui est doit être présenté à un client, ne pas utiliser des clés USB prêtées par des clients ou des inconnus, etc.)

8- Prudence avec la messagerie : Encore une fois, il s'agira d'évaluer les bonnes pratiques adoptées concernant l'utilisation de la messagerie. On pourra éventuellement s'appuyer sur des exemples de mail de phishing et de mails "normaux" pour voir si le joueur est capable de distinguer les deux. Cette comparaison sera de plus en plus compliquée à établir à mesure que le jeu avance.

9- Téléchargements des programmes : Les logiciels et programmes devront provenir de sites d'éditeurs officiels. On pourra vérifier si les recommandations de l'ANSSI pour cette B.P sont suivies par le joueur sans les lui divulguer.

10- Paiement en ligne : Comme pour le phishing, on peut proposer des sites vitrines voleurs d'information bancaire et des sites normaux pour voir si le joueur parvient à les distinguer (notamment à l'aide d'indice (https/sécurité à deux facteurs etc…))

11- Séparation des usages professionnels et personnels : il est recommandé de séparer les usages personnels des usages professionnels. En effet, les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, ordiphone, etc.) personnels et professionnels. Il est alors intéressant de tester les réflexes de joueurs concernant cette bonne pratique.

12- Informations personnelles/identité numérique : une grande prudence est conseillée dans la diffusion des informations personnelles sur Internet. Les données laissées sur Internet nous échappent instantanément. Des personnes malveillantes sont alors en mesure d'user de l'ingénierie sociale pour nous nuire.

Cases attaques :

- Lorsqu'un joueur tombe sur une case attaque, il pioche une des 11 cartes attaque

(il y aura plus de 11 cartes dans le tas pour faire revenir des scénarios dans le jeu).

- Chaque carte propose un scénario d'attaques visant 3 des 12 bonnes pratiques (lors du premier tour, il ne s'agira que des 4 B.P initialisées 1/2/4/5).
- La virulence des attaques sera classée suivant 3 catégories la troisième étant la plus virulente. Une B.P protégée à ⅓ perdra face à une attaque de ⅔ ou 3/3. L'égalité signifie que le joueur est parvenu à résister à l'attaque.
- Si le joueur possède un système d'information capable de résister à 3 des attaques du scénario il gagne 3 points ; si son S.I. est vulnérable face à 1 des attaques il perd 2 points, s'il est vulnérable à 2 des attaques, il perd 3 points. Dans le cas où le joueur ne résiste à aucunes des attaques, il perd 4 points.
- On pourra également faire des attaques comparatives. Si deux joueurs se trouvent sur une case défi dans ce cas on compare leur SI suivant les mêmes B.P. Celui qui a le set des 4 B.P les plus fiables l'emporte et gagne 3 points et 100€ tandis que l'autre perd 3 points.

*N.S.= Niveau de sécurité (1, 2 ou 3)

Cases Défi :

- Lorsqu'un joueur tombe sur une case défi, il pioche une des 31 cartes défi.
- Un défi mettant à l'épreuve ses connaissances en cybersécurité lui est alors proposé. Il donne sa réponse au maître du jeu de manière que les autres joueurs n'entendent pas la réponse (afin que le défi puisse leur être proposé ultérieurement). Si le joueur relève le défi, et que le nombre de points en jeu n'est pas indiqué sur la carte, alors il choisit entre obtenir une récompense de 3 points ou bénéficier de 300€ supplémentaires.
- Des cartes défi spéciales permettent de poser des questions à l'ensemble des joueurs. Le premier qui répond emporte les points ou le montant. Cela permet d'ajouter de l'interaction.

Cases Audit :

- Un joueur ne pourra pas tomber deux fois de suite sur une case audit car elles sont séparées de plus de six cases.
- Elles permettent de formuler des recommandations suivant le niveau de sécurité du SI du joueur. Il peut demander un audit ciblé sur des B.P (100€/BP) ou un audit global (500€).
- Les recommandations seront fournies personnellement à chaque joueur pour que les autres ne puissent pas en bénéficier naturellement.

<u>Déroulement de la partie :</u>

Sur le plateau, les 12 cases bonnes pratiques ne sont indiquées que par des numéros. Les joueurs ignorent donc (au début au moins) la signification de chaque numéro. Cela ajoute un peu d'effet de surprise. On pourra leur demander de citer, à la fin de la partie, la signification de chaque case.

Le premier joueur désigné en phase d'initialisation commence en se plaçant sur le coin supérieur droit du plateau (entre la case 4 et 5) et lance le dé. Il avance son pion en conséquence et tombe sur l'une des cases décrites précédemment. Puis les autres le suivent. Le premier ayant achevé un tour rend obsolète les logiciels et sauvegardes. Dès lors une attaque portant là-dessus entraîne automatiquement une perte pour ces 2 B.P. Cela vaut pour les joueurs n'ayant pas fini leur tour.

Si un joueur fait un tour sans tomber sur une case attaque, il sera automatiquement renvoyé à la première case du plateau qui est une case attaque.

Chaque joueur a la possibilité au cours de la partie d'échanger des points contre de l'argent et

vice versa. La victoire finale dépendant du nombre de points, les joueurs devront effectuer les derniers échanges qu'ils souhaitent faire avant d'entamer leur 6ème et dernier tout, dès lors aucun échange ne sera possible. Pour l'échange 1 point = 150€.

Fin de la partie :

Le joueur avec le plus de points à l'issue des 6 tours l'emporte.

Métriques :

A chaque case "Bonne Pratique", le joueur fait le choix d'investir pour atteindre un meilleur niveau de sécurité afin de se protéger des attaques potentielles ou de rester au niveau initial le plus bas. 3 niveaux de sécurité sont disponibles.
Lorsque le joueur est sur une case BP, il peut donc choisir ou non d'investir, sachant que pour passer au Niveau de sécurité supérieur il doit dépenser 100€. Ainsi pour passer du NS1 au NS2 ou du NS2 au NS3 il paye 100€, et pour passer du NS1 au NS3 il paye 200€.

1 : Mot de passe : Faible moyen ou fort

- Le mot de passe fait au moins six caractères, mais ne contient ni chiffre ni majuscule alors, c'est un mot de passe *faible* ;
- Le mot de passe fait au moins six caractères et contient des chiffres et/ou des majuscules alors, c'est un mot de passe *moyen* ;
- Le mot de passe fait au moins huit caractères et contient des chiffres, des majuscules et au moins un caractère spécial alors, c'est un mot de passe *fort*.

2 et 4 : à chaque fin de tour les logiciels et sauvegardes deviennent obsolètes. Tomber sur l'une des cases BP correspondantes, vous permet de les mettre à jour. Niveau 1 : 2 versions de retard ou plus. Niveau 2 : 1 version de retard. Niveau 3 : Sauvegardes et logiciels sont à jours.

3 : A chaque nouveau tour un nouveau prestataire ou groupe d'utilisateur arrive. Le joueur peut dépenser de l'argent (qui représente le temps investi pour les intégrer au SI) afin de leur créer des comptes d'accès au S.I. avec des privilèges adaptés suivant leur fonction ou du fait qu'ils soient du service informatique ou non. Niveau 1 : 2 prestataires sont arrivés et n'ont pas les accès adaptés au SI. Niveau 2 : Un prestataire est arrivé sans que le SI de l'entreprise ne s'adapte et lui accorde ses privilèges spécifiques. Niveau 3 : Tous les utilisateurs du SI ont les droits/accès qui leur conviennent.

5 : Le wifi est sécurisé par défaut par une clé wep. Le joueur pourra l'améliorer lorsqu'il tombe sur la BP5, il aura alors le choix de rester à ce niveau de sécurité initial, ou d'investir pour acquérir une meilleure sécurité (un niveau 2 et 3 sont disponibles).

6 : Initialement il n'y a aucune protection sur le smartphone (mot de passe/chiffrement). Niveau 2 mot de passe de déverrouillage. Niveau 3 : mot de passe 6 chiffres, données chiffrées, applications de sources fiables.

7: Par défaut, utilisation des données professionnelles directement sur le terminal personnel. Naïveté (prêt de téléphone/ordinateur à de tierce personnes). Niveau 2 : utilisation de matériels différents. Niveau 3 : matériels différents + signes distinctifs + filtre de protection écran + mot de passes non pré-enregistrées.

8 : Par défaut, le joueur distingue mal un mail de phishing d'un mail professionnel ou personnel. Naïveté (clique sur les liens dans les mails, ouvre les pièces jointes). Niveau 2 : Distingue bien l'identité de l'expéditeur, désactive l'ouverture automatique de documents téléchargés, n'ouvre que les pièces jointes des expéditeurs connus. Niveau 3 : lance une analyse antivirus pour chaque pièce jointe, compare le lien écrit et le lien affiché

lorsqu'on passe la souris pour vérifier la cohérence.

9 : Par défaut, l'utilisateur télécharge des logiciels sur des sites peu sécurisés et parfois illégalement. Niveau 2 : S'assure qu'il est sur un site fiable (de préférence le site officiel de l'éditeur) et de confiance avant de télécharger un logiciel. Évite aussi les téléchargements illégaux notamment sur des sites de torrents peu fiables. Niveau 3 : Lance une analyse antivirus après chaque programme installé, n'installe pas de programme annexes souvent proposés lors d'une installation (sauf si nécessaire).

10 : Par défaut, ne procède à aucune vérification avant tout paiement en ligne. Niveau 2 : s'assure de la présence du cadenas dans la barre d'adresse avant d'entrer les coordonnées bancaires utiles au paiement. S'assure de la présence du "S" dans le https de l'adresse du site. Niveau 3 : Utilise la méthode d'envoi de code de confirmation par sms pour procéder à l'achat. Utilise une carte dédiée aux achats en ligne avec uniquement le montant nécessaire à l'achat.

11 : Par défaut les usages pro/perso sont liés. Niveau 2 : Les usages pro et perso sont séparées. Niveau 3 : Les usages pro et perso sont isolées et chiffrées.

12 : Par défaut, l'utilisateur fournit des informations personnelles dans les différents formulaires rencontrés et autorise le stockage d'information. Niveau 2 : Ne fournit que le strict minimum et uniquement les informations nécessaires sur les formulaires en ligne. Niveau 3 : N'autorise pas le partage ou stockage des données, fait attention aux informations divulguées sur les réseaux sociaux, vérifie régulièrement les paramètres de sécurité et confidentialité, utilise plusieurs adresses électroniques pour différentes activités sur internet.