**Règles du jeu des bonnes pratiques**

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

- Objectif : Avoir en fin de partie le SI le mieux protégé (seuil de point minimum : ). 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)

> 12 cartes défi

> 12 cartes attaques

> 1 dé

> 6 pions

> 1 liasse de billets

> 1 maître du jeu

- 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 :

Possibilité d’échanger des point en échange d’argent ( 5 points pour 300€) après chaque tour et vice-versa ou lors d’une case audit obligatoire.

Phase d’initialisation :

* L’un des joueur 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.
* 4 investissements à effectuer : Il faut choisir le mdp administrateur (100€) + Choisir si l’on fait une sauvegarde (100€) + Choisir si l’on fait une mise à jour des logiciels 100€ + choisir un type de sécurité wifi (100€).
* Capital initial de 1000€
* 20 points de départ

Les 12 ~~(commandements)~~ 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 joueur. 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 prêtés 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 :** Questions sur les bonnes pratiques. À creuser encore.

**12- Informations personnelles/identité numérique :** À creuser également.

Cases attaques :

* Lorsqu’un joueur tombe sur une case attaque, il pioche une des 12 cartes attaque (il y aura plus de 12 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 (en début de partie, 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 aucun 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.

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 à ce que les autres joueurs n’entendent pas la réponse (afin que le défi puisse leur être proposé ultérieurement). Si le joueur relève le défi, 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.

Déroulement de la partie :

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 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 finis 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.

Fin de la partie :

Le joueur avec le plus de point à l’issue des 6 tours l’emporte.

Métriques :

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 six 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.

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 faire des comptes SI avec des privilèges d’accès adaptés suivant qu’ils sont du service informatique ou non.

5 : Le wifi par défaut est sécurisé par défaut par une clé wep. Le joueur pourra l’améliorer lorsqu’il tombe sur la BP5

6 : 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 :

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.