Méthode de Formation : Sensibilisation à la Sécurité Informatique pour un Public Néophyte v0.2

Tiphaine Romand-Latapie

06/05/2015

Résumé

Ce document décrit une méthode de sensibilisation d'un public néophyte à la sécurité informatique. Cette méthode est basée sur l'utilisation d'un jeu de rôle, inventé par l'auteur. Le lecteur trouvera dans ce document les informations lui permettant de réaliser lui-même cette formation (soumis à autorisation de l'auteur).

1 Copyright

Joindre l'auteur :

`tiphaine.romand@orange.com`

`tiphaineRL@gmail.com`

2 Introduction

L'idée de cette formation est née de la nécessité de former un public opérationnel néophyte aux enjeux de la sécurité informatique. Plutôt que de rentrer dans un mécanisme de formation standard, basé sur la compréhension du contexte technique (qu'est-ce qu'un mot de passe, comment fonctionne un ordinateur etc.), qui, selon mon expérience, a tendance à ennuyer ou effrayer un public non informaticien, j'ai souhaité me concentrer sur les principes génériques de la sécurité informatique :

— La problématique de « faire confiance » à une entité/personne ;

— La notion de « défense en profondeur » ;

— Les motivations de l'attaquant ;

— La démystification de l'attaquant (qui n'est pas forcément un « hacker de génie ») ;
— Les notions de compromis entre contraintes opérationnelles et sécurité ;
— Les objectifs des équipes de sécurité (prévoir le comportement de l'attaquant, le prévenir ou le détecter) .

L'idée sur laquelle est basée cette formation est la suivante : les macro principes suivants sont les mêmes en sécurité physique et informatique :

— Nous sommes tous les jours confrontés à la notion de « faire confiance » à quelqu'un
— En sécurité physique, nous travaillons toujours dans le pire cas, nous traitons de plus les cas où la mesure de sécurité préliminaire est désactivée/inopérante
— L'attaquant est motivé par l'argent/l'idéologie etc.
— Les attaquants les plus répandus ne sont pas des génies du crime

La sécurité physique impose elle aussi des contraintes (fermer la porte à clé, port de badge obligatoire, contrôle avant de prendre l'avion, etc.) Les objectifs sont ici communs : prévoir le comportement d'un attaquant, le prévenir ou le détecter.

Or, les personnes néophytes sont beaucoup plus familières avec la sécurité physique que la sécurité informatique, autant dans leur vie professionnelle que personnelle. Tout le monde ferme sa porte à clé avant de sortir de chez soi, personne ne laisse rentrer n'importe qui chez lui, tout le monde a déjà eu à faire à des contrôles de sécurité, etc.

L'idée au cœur de la formation est donc de faire prendre conscience au public formé qu'il dispose déjà des bons réflexes et raisonnements, et de lui apprendre à les appliquer à la sécurité informatique, tout en dédramatisant cette dernière.

3 Le jeu de rôle

La formation est construite autour d'un jeu de rôle basé sur l'attaque et la défense d'un bâtiment.

3.1 Règles du Jeu

Le jeu se déroule avec un Animateur, appelé aussi « Maître du Jeu », une équipe d'attaquants et une équipe de défenseurs.

3.1.1 Description générale :

— Un immeuble de bureau dans une zone dense, avec parking souterrain et hélipad (piste d'atterrissage d'hélicoptère sur le toit). Un objet (tenant dans un sac à dos) de grande valeur, utilisé par des employés pendant la journée est stocké quelque part dans l'immeuble.
— Au début du jeu l'immeuble n'est pas sécurisé.
— Les attaquants proposent une attaque, les défenseurs une contre-mesure, et on recommence.

3.1.2 Règles et objectifs de l'équipe d'attaquants :

— Objectif : voler l'objet dans l'immeuble sans finir en prison

— Règles : budget illimité – nombre d'attaquants humains inférieur à dix - respecter les lois de la physique

3.1.3 Règles et objectifs de l'équipe de défenseurs :

— Objectif : empêcher le vol de l'objet ou récupérer de quoi faire arrêter les voleurs

— Règles : Budget illimité – personnel illimité – respecter les lois françaises et les lois de la physique – des gens doivent pouvoir travailler dans l'immeuble pendant la journée

3.1.4 Fin d'un scenario :

— Je conseille de terminer un échange (appelé « scenario ») lorsque les équipes arrivent à un point de blocage (tout le monde est mort, l'objet est détruit, les policiers sont là ...)

— Il est alors possible de passer à une nouvelle tentative (reprise à zéro) des attaquants. Dans ce cas : les défenseurs conservent toutes leurs mesures de protection.

— Dans le cas où les joueurs le souhaitent, ou si le maître du jeu souhaite relancer le jeu, il est également possible d'inverser les équipes (les attaquants deviennent défenseurs etc.)

3.1.5 Fin du jeu :

— Il n'y a pas de gagnant ni de perdant !

— Il est conseillé de faire plusieurs échanges ou « scenarii » dans une seule session, en ce cas, la fin du jeu est laissée à la discrétion de l'animateur (nous conseillons un jeu d'une durée de 40 à 60 minutes pour 6 personnes).

— Le jeu est suivi d'un débriefing par le formateur, permettant de mettre en exergue les notions souhaitées (voir la section consacrée au débriefing).

3.2 Concept des règles

3.2.1 Environnement

L'environnement du jeu (immeuble de bureau, zone dense, etc.) a été choisi pour maximiser le côté ludique et faciliter l'application à la formation :

— L'immeuble de bureau utilisable pendant la journée permet de travailler sur les compromis contrainte/sécurité et offre un environnement familier des joueurs.

  — Ne pas hésiter à personnaliser les détails du scénario avec l'environnement professionnel des joueurs : bâtiment de la société, objet de valeur correspondant à un produit phare de l'entreprise, etc. Cela permet une immersion et

implication des joueurs plus rapide (sans compter le plaisir à virtuellement perturber le quotidien professionnel).

- Le choix de la zone dense, de l'hélipad et du parking souterrain permet de renforcer le côté ludique (les attaquants peuvent imaginer creuser un tunnel, se poser en hélicoptère, sauter d'un immeuble à l'autre etc.) et de guider un peu les joueurs. Cela permet également de forcer la diversification des scenarii d'intrusion.
- Le choix de ne pas plus préciser l'environnement permet de laisser libre cours à l'imagination des joueurs, et de simplifier les règles.
- L'utilisation de l'objet pendant la journée permet d'éviter des mesures non constructives pour le jeu, du type « je coule l'objet dans un bloc de béton ».
- L'emplacement de l'objet est laissé libre, il peut évoluer au cours du jeu.
- Le fait de commencer sans sécurité est important :
  - Il permet de travailler sur l'empilement des mesures de sécurité et sur le principe selon lequel l'attaquant passe toujours par le point de moindre résistance ;
  - Les attaquants partent régulièrement du principe que l'immeuble « sans sécurité » comporte quand même des caméras de surveillance, des portes qui ferment à clé etc. Dans ce cas il n'est pas nécessaire de recadrer le jeu. En revanche, il est intéressant de faire réfléchir les joueurs sur ce sujet au cours du débriefing.
- Les échanges rapides permettent un jeu vivant et ludique.

3.2.2 Les règles et objectifs des attaquants :

- Un objectif simple, renvoyant aux films à gros budgets, facile à traduire en objectifs de sécurité informatique (entrée-sortie sans laisser de trace) ;
- Le budget illimité simplifie le jeu, tout en conservant la possibilité de discuter des aspects financiers lors du débriefing ;
- Le petit nombre de personnes physiques auquel a droit l'attaquant permet d'éviter les situations irréalistes du type « une armée de 300 personnes fait le siège du bâtiment » ;
- Le respect des lois de la physique permet encore une fois d'éviter des situations irréalistes et contraires à l'esprit du jeu (pas de téléportation/magie etc.).

3.2.3 Les règles et objectifs des défenseurs :

- Un objectif simple, renvoyant aux films à gros budgets, facile à traduire en objectifs de sécurité informatique (contrôle des entrées/sorties, ralentir l'attaquant etc.) ;
- Le budget illimité simplifie le jeu, tout en conservant la possibilité de discuter des aspects financiers lors du débriefing ;
- Le personnel illimité permet de compenser un peu le besoin de respecter les lois françaises, tout en permettant de faire un lien entre les mesures de protections parfois très chères mais inefficaces ;

— Le respect des lois de la physique permet encore une fois d'éviter des situations irréalistes et contraires à l'esprit du jeu (pas de téléportation/magie etc.) ;
— Le respect des lois du pays renvoie aux contraintes des ingénieurs en sécurité informatique, qui sont eux-mêmes limités par les lois du pays dans lequel ils pratiquent.

3.2.4 Qui perd gagne

Il n'y a pas de perdant ou de gagnant, même si les équipes de joueurs ont tendance à en vouloir un. Des règles permettant de désigner des gagnants/perdants complexifieraient inutilement le jeu. Le but des règles est globalement de favoriser les échanges ludiques entre joueurs, tout en faisant ressortir les notions dont le formateur a besoin pour que la formation atteigne son but.

3.3 Animation du jeu

Le jeu est animé par le(s) formateur(s), nommé "maître du jeu" dans la suite. Il est important de ne pas faire de trop grosses équipes. Je conseille 2 à 3 défenseurs et 2 à 3 attaquants. Au-delà de ce nombre, il devient très difficile pour le formateur de suivre les échanges et de les recadrer.

Le formateur commence par expliquer l'objectif du jeu et ses règles :

Objectif du jeu : faire prendre conscience aux élèves du travail des équipes de sécurité et du fait qu'ils possèdent déjà les bons réflexes : la formation doit leur donner les clés pour les appliquer à l'informatique.

3.3.1 Règles du jeu

Il est important de bien insister sur l'aspect « physique » du jeu. Dans certains groupes, les élèves, conscients d'être dans une formation à la sécurité informatique, cherchent immédiatement à « pirater » quelque chose. Il faut également bien préciser que pour les deux camps, l'objectif est double (empêcher/réaliser le vol ou le détecter), ceci pour permettre de faire émerger les notions d'usurpation d'identité, de traces etc. Enfin, il ne faut pas hésiter à insister sur les aspects juridiques du pays : les attaquants ont tous les droits, mais pas les défenseurs.

3.3.2 Déroulement du jeu

Dès le lancement du jeu, le formateur doit noter sur un support visible par les participants les différents échanges (cf. les exemples fournis dans ce document). En tant que Maître du Jeu, il est responsable du bon respect des règles, et peut limiter l'un ou l'autre des camps.

Il doit forcer les attaquants/défenseurs à détailler leurs actions dès que nécessaire :
— si quelque chose est verrouillé, on doit savoir par quel type de mesure (empreinte rétiniennes, empreintes digitales, badges, code, clé), et qui possède l'élément permettant de déverrouiller ;

— en cas par exemple de passage sur générateur de secours, il faut préciser ce que celui-ci alimente et le maître du jeu peut choisir de limiter le temps de fonctionnement du générateur de secours. Par exemple : un générateur de secours au fioul ne peut pas alimenter un système de sécurité complet d'un immeuble de bureau plus de quelques heures ;
— en cas de caméra de surveillance, il faut préciser si elles sont surveillées en temps réel, par qui et combien sont-ils etc.

La nécessité de préciser telle ou telle action est décidée par le maître du jeu, en fonction des enseignements qu'il souhaite tirer du jeu pendant le débriefing. Nous conseillons toutefois vivement de faire préciser les cas cités ci-dessus, ainsi que l'emplacement d'un PC footnotePoste de Commandement sécurité par exemple.

Tout ce qui n'est pas explicitement dit par les défenseurs ou les attaquants peut être interprété/détourné par le camp adverse. Si les défenseurs n'indiquent jamais avoir fermé les fenêtres, les attaquants peuvent considérer qu'elles sont ouvertes. Si les attaquants n'ont pas dit qu'ils étaient masqués, il faut considérer que les caméras de surveillance filment leurs visages etc.

Le maître du jeu peut orienter l'un ou l'autre des camps s'il trouve que le jeu ne va pas dans la bonne direction, ou si les échanges sont laborieux. Il peut rappeler par exemple les règles au moment opportun, comme dire à une équipe d'attaquants timides « je vous rappelle que vous n'avez pas à respecter les lois françaises, vous pouvez faire exploser la porte/tuer le garde ». L'objectif du maître du jeu est de faire ressortir dans le jeu (ou de repérer) les éléments lui permettant d'illustrer, lors du débriefing, les principes de base de la sécurité informatique.

Aucune comparaison/lien avec la sécurité informatique ne doit être réalisé pendant le jeu de rôle. Les liens sont effectués lors du débriefing.

3.3.3 Fin du jeu

Il est conseillé de terminer le scenario en cours dans les cas suivants :

— Les attaquants s'entêtent dans une direction alors que d'autres possibilités n'ont pas été explorées ;
— Le scenario en cours devient trop complexe ;
— Le scenario en cours devient irréaliste ;
— Le formateur souhaite inverser les équipes ;
— Les joueurs perdent en motivation (il est alors possible d'arrêter le jeu ou d'inverser les équipes)
— Le formateur a déjà toute la matière dont il a besoin pour son débriefing.

3.4 Exemple d'échange/scenario

Cet exemple a été observé au cours d'une des formations, à ce moment, le jeu durait déjà depuis 10 minutes.

Table 1 – Exemple de scenario

Attaquants	Défenseurs	Maître du jeu
Corruption de sous-traitants pour qu'ils réalisent eux-mêmes le vol		
	L'objet en utilisation reste en visibilité permanente de son utilisateur. Dès qu'il n'est plus utilisé, il est rangé dans un coffre-fort fermant à clé. Trois personnes ont chacune une clé : Le responsable du service de l'utilisateur de l'objet, l'utilisateur de l'objet et le directeur de la sécurité. On trace les actions des responsables de ces trois clés en permanence.	Qui possède la clé du coffre ?
Récupération du nom du directeur de la sécurité, phase d'observation pour connaître son emploi du temps. Vol avec violence permettant de récupérer la clé et de la donner au sous-traitant		
	Le coffre n'est pas en évidence	Mesure non effective : Le personnel d'entretien peut le trouver facilement.
	Vidéo Surveillance multi-écran. Un gardien 24/24 pour surveiller les écrans et un enregistrement. Un gardien est également présent à l'accueil	Attention, trop de caméras implique difficulté/impossibilité pour un humain de les surveiller en temps réel

Table 1 – Exemple de scenario

Attaquants	Défenseurs	Maître du jeu
Une femme de ménage distrait le gardien de la vidéo surveillance pendant que l'autre commet le vol		
	Formation accrue des gardiens (par la police, les forces spéciales etc.), enquête de moralité des sous-traitants	Il sera toujours possible de trouver un sous-traitant « faible », le gardien pourrait être malade, avoir besoin d'aller aux toilettes etc. Mais les attaquants ont « perdu » ! Les enregistrements vidéo sont revus et contiennent le visage de la femme de ménage
La femme de ménage se déguise dans les toilettes/La personne distrayant le gardien utilise un appareil permettant de détruire à distance les données sur disque dur (aimant)		
	Vidéo-Surveillance dans le couloir devant les toilettes et salle serveur protégée (au centre de l'immeuble, avec cage de faraday).	La caméra a été mise devant les toilettes suite à un recadrage du Maître du Jeu, la loi interdit de mettre des caméras dans les toilettes !
Débrancher la caméra		
	Alarme sonore et visuelle se déclenchant dans la loge du gardien en cas de dysfonctionnement/débranchement de caméra	Le Maître du Jeu déclare la fin du scenario, pour forcer l'équipe d'attaquant à passer à autre chose.

4 Le débriefing du jeu de rôle

4.1 Apprentissage des bons réflexes « communs »

Comme indiqué en introduction de ce document, les personnes néophytes ont déjà de bons réflexes, qui peuvent être appliqués aussi bien en sécurité physique qu'en sécurité informatique. Je conseille de présenter ces reflexes en sortie de jeu de rôle, en faisant le lien avec les scenarii apparus durant le jeu. Voici une liste non-exhaustive de bons réflexes à mettre en avant par le formateur :

— Ne pas « faire confiance » par défaut ;
— On vérifie les identités ;
— On ne donne pas la clé de sa maison/son code d'alarme/mot de passe à n'importe qui
— Cas des services d'urgence : donnez-vous votre clé « au cas où » ?
— Pourquoi donnerait-on son mot de passe au SAV ?
— On appelle la police/les services de sécurité en cas de suspicion d'activité malveillante
— On se pose les questions :
— « Quelqu'un a-t-il intérêt à attaquer mon bâtiment ? », « À quel point ? »
— Cette information/clé/badge serait-il utile à quelqu'un ?
— Que se passe-t-il en cas de dysfonctionnement ?

4.2 Grille de lecture des scenarii

Les éléments utilisés lors du jeu de rôle par les différents participants ont une correspondance facile avec la sécurité informatique. L'idée du débriefing est de réaliser ce lien entre le jeu et les aspects de la sécurité informatique sur lesquelles le formateur souhaite insister. La figure 1 présente une grille de lecture (non exhaustive) des éléments généralement utilisés par les joueurs et de ce qu'ils peuvent représenter dans le milieu de la sécurité informatique.

4.3 Points Communs et Divergences

Les points communs entre les sécurités physique et informatique ont déjà été présentés plusieurs fois au cours de ce document, nous les reprenons maintenant et indiquons les exemples types illustrant ces principes et apparaissant dans le jeu de rôle.

4.3.1 La problématique de « faire confiance » à une entité/personne

Très vite dans le jeu, les participants sont confrontés à la notion de contrôle d'accès. Vous verrez assez vite apparaître des notions de badge/vérification de cartes d'identité à l'accueil, ou d'attaquant se déguisant ou mentant pour accéder à l'immeuble. Il est important d'utiliser ces points pour faire réfléchir les participants à la notion de confiance,

Sécurité Physique	Sécurité Informatique
Clé/Badge	Mot de passe/carte à puce
Coffre/Porte blindée	Mesure technique de sécurité
Vidéo Surveillance	Supervision/logs/anti-virus
Destruction des enregistrements de vidéo surveillance	Destruction/Altération des logs
Coupure d'électricité/incendie	Denis de Service
Gardes/gardiens/personnel	Opérationnels
Déguisement/fausse carte d'identité	Usurpation d'adresse IP, usurpation d'identité
Observation, récupérer le nom d'un chef, une information ...	Social Engineering
Procédure d'urgence, générateur de secours, etc.	Résistance aux pannes, défense en profondeur, procédure SAV
Carte d'identité	Certificats
Utilisation par les attaquants d'une technologie spécifique (brouilleur, explosifs, drones etc.)	Utilisation d'exploit/de plateforme écrits par d'autres

FIGURE 1 – Grille de Lecture

d'identité et d'authentification. L'utilisation d'une fausse carte d'identité par l'attaquant est par exemple intéressante : qu'est ce qui nous permet de croire quelqu'un quand il décline son identité ? Cette notion est centrale dans tout système de sécurité. Le formateur peut également profiter de cette discussion pour parler des différentes possibilités :

- Biométrie
- PIN ou mot de passe
- Clé (qui peut être volée, perdue, copiée etc.)
- Carte d'identité, qui renvoie à la notion de faire confiance à une tierce partie (l'état dans la sécurité physique, une autorité de confiance dans la sécurité informatique)

Enfin, dans la plupart des sessions effectuées, les attaquants utilisent assez vite des mensonges/usurpation d'identité pour contourner des mesures de sécurité. Par exemple, dans une session, les attaquants récupéraient le nom d'un manager haut placé, et insistaient sur une livraison urgente à ce dirigeant à l'accueil. Ce genre de scenario est très utile pour illustrer le concept de social engineering. C'est enfin l'occasion de faire réfléchir les élèves sur la maxime « l'élément le plus faible est l'humain ».

4.3.2 La notion de « défense en profondeur »

Le principe de défense en profondeur, qui consiste à empiler les couches de sécurité et à traiter les cas où une couche est défaillante, apparait facilement lors du jeu de rôle. Par exemple, de façon systématique, les élèves proposent un contrôle d'accès à l'entrée

de l'immeuble, puis un contrôle d'accès accru à la pièce dans laquelle est stocké l'objet. Ils peuvent même rajouter un contrôle supplémentaire autour de l'objet dans cette pièce.

Le formateur se doit de mettre en avant ce comportement, et de faire remarquer aux élèves qu'il en est de même dans la sécurité informatique. C'est le moment de discuter avec eux des mesures de sécurité multiples, et de faire prendre conscience de leur intérêt. Nous entendons souvent, en tant qu'ingénieur en sécurité informatique des phrases du type « mais c'est dans le LAN, nous ne risquons rien », « mais là nous avons déjà tapé un mot de passe une heure avant, pourquoi un autre ? » Etc.

La multiplication du type de technologie (clé physique, badge, biométrie etc.) est aussi une façon de faire réfléchir les élèves sur les règles d'hygiène informatique (une clé/mot de passe par usage, etc.). Enfin, les différentes tentatives des attaquants permettent d'illustrer très bien la règle d'or selon laquelle le niveau de sécurité d'un système dépend du niveau de sécurité de son composant le plus faible.

4.3.3 Les motivations de l'attaquant

Les différents scenarii permettent au formateur d'illustrer la notion importante de motivation de l'attaquant (et du défenseur). Lorsque nous arrivons à des scenarii qui représentent plusieurs millions de d'euros, et des mois de préparation, la question se pose : l'objet en vaut-il la peine ? La même question peut être posée pour les défenseurs.

C'est également le moment de discuter du niveau de sécurité par rapport au niveau de l'attaquant, et de faire réfléchir les élèves aux questions au cœur de tout système de sécurité : que protège-t-on et contre qui ?

4.3.4 La démystification de l'attaquant (qui n'est pas un « hacker de génie »)

Une des notions les plus mal perçues par les néophytes est la diversité des profils d'attaquants informatique. L'imaginaire collectif dépeint une image de « génie » au fond d'une cave, or, comme en sécurité physique, il y a plusieurs types d'attaquants : si la porte ne ferme pas à clé, n'importe quel délinquant peut entrer dans l'immeuble. Lorsque le scenario devient complexe, nous sommes face à des attaquants extrêmement motivés ciblant un objectif bien défini.

La notion d'économie souterraine est également mal comprise :

— En sécurité physique les objets sont revendus ou « commandés » avant le vol. La même chose existe en sécurité informatique et les élèves doivent en prendre conscience ;

— De même qu'un attaquant « physique » va acheter des outils lui permettant de réussir son attaque (explosifs, brouilleurs radio, fausses carte d'identités etc.), l'attaquant informatique fait de même. Ce qui veut dire qu'il y a une économie liée à la découverte de ces outils (failles, exploit etc.) et à leur revente. C'est le moment de faire réfléchir les élèves sur les différents profils. N'importe qui peut appuyer sur le bouton d'un brouilleur radio, il faut en revanche des compétences techniques poussées pour le concevoir.

4.3.5 Les notions de compromis entre contraintes opérationnelles et sécurité

Pour cette notion, le formateur doit se concentrer sur les mesures mises en œuvre par les défenseurs, et des contraintes qu'elles impliquent pour les employés de la société ou la société elle-même. Le lien est alors assez facile à faire avec les contraintes de sécurité informatique.

Une partie intéressante à travailler est la présence dans les scenarii d'équipe de secours (police, armée, pompiers...) légitimes ou non. Demander aux élèves : donnent-ils accès à tout l'immeuble de façon systématique à toutes les équipes de secours « au cas où » ? Vérifient-ils la légitimité des services de secours ? Dans une des sessions, les attaquants s'étaient faits passer pour une équipe médicale d'évacuation par hélicoptère pour extraire l'objet volé. C'est le moment de discuter des accès SAV/service informatique etc. Des stockages de mot de passe en clair « au cas où le client l'oublie etc. ».

4.3.6 Les objectifs des équipes de sécurité (prévoir le comportement de l'attaquant, le prévenir ou le détecter)

Dans le jeu de rôle, le travail des défenseurs est facilité par rapport aux conditions réelles : les attaquants annoncent leur intention et leur objectif est connu. Le formateur peut profiter du débriefing pour mettre le doigt sur la difficulté des équipes de sécurité : elles doivent imaginer le comportement des attaquants et évaluer leurs possibles motivations. Le formateur peut également faire réfléchir sur les outils de supervisions de traces. Lorsqu'il n'est pas possible de prévenir le comportement d'un attaquant, il faut au minimum le détecter.

4.3.7 Divergences

Toute la sécurité physique n'est, bien sûr, pas transposable en sécurité informatique (et vice versa). Mais les différences, aussi essentielles soient-elles, sont finalement peu nombreuses sur le fond :

- Le facteur temps diffère énormément :
  - Par exemple : tester un mot de passe est bien plus rapide que tester une clé sur une serrure physique
- Le facteur géographique n'existe pratiquement plus :
  - L'attaquant n'a aucun besoin d'être physiquement présent pour mener l'attaque. La distance géographique n'a pas d'importance.
  - Il y a des exceptions à cette règle :
    - Les lois qui s'appliquent sont liées à la localisation physique des données volées ou altérées ;
    - Lors d'attaques de type signaux compromettants, radio ou hardware, la distance géographique peut redevenir un élément déterminant ;
- Ces deux changements d'échelle rendent les attaques de masse peu coûteuses et accessibles à tous ;

— Les traces exactes et facilement récupérables concernent les machines et plus difficilement les personnes physiques
  — Il peut être très difficile de remonter au coupable ;
  — L'attaquant peut se cacher derrière des machines de tierces parties non concernées ;
— Le vol est pratiquement impossible à détecter (copie informatique)
  — Les traces du vol peuvent être retrouvées si le système est correctement configuré ;
— Encore trop souvent, aucune sécurité basique n'est mise en place en informatique, alors que dans le monde physique, les gens mettent en œuvre au minimum une porte qui ferme à clé.

5 Annexe : exemple d'une session

Cette session a été réalisée avec cinq personnes (trois défenseurs, deux attaquants), elle a duré environ 50 minutes.

TABLE 2 – Exemple d'une session complète à 5 joueurs d'une durée de 50 minutes environ (hors débriefing)

Attaquants	Défenseurs	Commentaires	Parallèle sécurité informatique
Ouvre la porte, va chercher l'objet, ressort avec l'objet			Vol de données non protégées
	La porte est sécurisée par badgeuse et est fermée complètement après 20h. Si tentative d'effraction, alarme relié au commissariat		Protection par mot de passe, gestion des droits utilisateurs, supervision
Une femme séduit un employé et lui explique qu'elle a oublié son badge, l'employé la fait entrer (vol puis sortie)			Social engineering

TABLE 2 – Exemple d'une session complète à 5 joueurs d'une durée de 50 minutes environ (hors débriefing)

Attaquants	Défenseurs	Commentaires	Parallèle sécurité informatique
	L'objet est enfermé dans un coffre-fort à code. Seul le responsable du site dispose du code (il faut l'appeler pour utiliser l'objet). Le port du badge apparent est obligatoire dans l'entreprise, des agents de sécurité vérifient l'application de la consigne. Les salariés sont de plus sensibilisés sur le danger de laisser entrer un inconnu.	On remarque que la mesure est très contraignante pour l'entreprise (une seule personne pour l'accès à l'objet qui doit être utilisable)	Protection par mot de passe. Non partage des mots de passes. Logs et supervision. Sensibilisation
Déguisement en personnel d'entretien, entre avec un badge volé et un chariot qui contient un chalumeau. Ouvre le coffre au chalumeau, récupère l'objet, le met dans le chariot et ressort.			Usurpation d'identité, attaque par force brute

TABLE 2 – Exemple d'une session complète à 5 joueurs d'une durée de 50 minutes environ (hors débriefing)

Attaquants	Défenseurs	Commentaires	Parallèle sécurité informatique
	Il y a un détecteur de fumée dans la pièce. L'accès à la pièce est protégé par un système de reconnaissance rétinien.		Détection d'attaque. Biométrie
L'attaquant se pose en hélicoptère sur le toit de l'immeuble, puis utilise les conduits de climatisation jusqu'à la pièce. Descente "à la mission impossible" et vol du coffre. Sortie de l'immeuble, ouverture du coffre etc.			Attaque "Hors ligne", vol puis tentative de contournement de la mesure de sécurité.
	Le coffre est scellé dans le mur, il est de plus électrifié si le système de reconnaissance rétinien n'a pas validé l'entrée dans la pièce.		Interdiction d'attaque "hors ligne". Interdiction de toute action sans mot de passe
Coupure d'électricité			Denis de service/panne du système de sécurité

TABLE 2 – Exemple d'une session complète à 5 joueurs d'une durée de 50 minutes environ (hors débriefing)

Attaquants	Défenseurs	Commentaires	Parallèle sécurité informatique
	Groupe électrogène de secours maintenant les fonctions de sécurité de la pièce		Système de secours
L'attaquant fait chanter un employé ayant les accès à la pièce en prenant en otage sa famille. L'employé réalise le vol			Social engineering
	Des caméras sont présentes devant et dans la pièce, elles sont surveillées 24/24h par du personnel au PC Sécurité qui se trouve à l'extérieur du bâtiment.		Logs et supervision sur des serveurs dédiés
L'attaquant fait exploser le PC sécurité			Destruction, modification des logs

TABLE 2 – Exemple d'une session complète à 5 joueurs d'une durée de 50 minutes environ (hors débriefing)

Attaquants	Défenseurs	Commentaires	Parallèle sécurité informatique
	En cas d'explosion ou de coupure du PC sécurité, des équipes sont envoyées au PC sécurité et dans l'immeuble. Une alarme se déclenche en cas de coupure du lien de communication entre PC sécurité et batiment principal		Protection des logs, défense en profondeur (mécanisme de secours du mécanisme de secours)
Piratage des caméras de sécurité pour couper le flux vidéo			Attaque du système écrasant les logs
	Un capteur de mouvement est placé sur l'objet, en cas de mouvement, l'objet explose.	Refusé : l'objet doit être utilisable pendant la journée. non conforme avec la loi française.	En informatique, on appelle cette technique l'effacement d'urgence. En cas d'attaque détectée, les données sensibles sont effacées. Très contraignant
Intrusion en passant par les champs morts de la caméra et vol d'un badge pour entrée			

TABLE 2 – Exemple d'une session complète à 5 joueurs d'une durée de 50 minutes environ (hors débriefing)

Attaquants	Défenseurs	Commentaires	Parallèle sécurité informatique
	Tous les angles de caméras sont couverts et la surveillance se fait par une personne par caméra	Mesure très chère en personnel	Augmentation de la supervision et du personnel opérationnel
Cache caméra montrant une photo de l'emplacement			
	Un garde est présent à l'accueil et contrôle les entrées, des rondes sont de plus effectuées avec chiens de garde		
L'attaquant attaque les gardes et nourri les chiens pour les distraire			
	Toujours un contrôle rétinien, un ajout de contrôle d'empreinte pour accès à la salle.		Contrôle d'accès biométrique
Salarié infiltré (taupe) qui réalise le vol			
	Fouille systématique des employés du site	Mesure très contraignante (plusieurs secondes par employés, en horaire de pointe ...)	Contrôle permanent de l'ensemble du contenu des ordinateurs des employés (interdit)

TABLE 2 – Exemple d'une session complète à 5 joueurs d'une durée de 50 minutes environ (hors débriefing)

Attaquants	Défenseurs	Commentaires	Parallèle sécurité informatique
Utilisation d'un drone pour faire sortir l'objet			Exfiltration de données
	Fouille à l'entrée/sortie de la pièce.	Mesure très contraignante (plusieurs secondes par employé, en horaire de pointe ...)	
Meurtre du garde surveillant la pièce			
	Un antivol permet de détecter que l'objet est sortie du bâtiment, le site est verrouillé		Watermarking des données (moins efficace)
Déclenchement d'un incendie pour ouverture automatique des portes d'évacuation			Attaque des procédures de secours/d'urgence
	Géolocalisation de l'objet		
Utilisation de Papier aluminium pour empêcher la détection			
	Intervention de l'armée pour abattre le drone		
Plusieurs centaines de drones font diversion			

TABLE 2 – Exemple d'une session complète à 5 joueurs d'une durée de 50 minutes environ (hors débriefing)

Attaquants	Défenseurs	Commentaires	Parallèle sécurité informatique
Drones autoguidés, préprogrammés	Brouilleur radio pour empêcher le pilotage des drones		
	Brouillage des signaux GPS		
Passage par le sous-sol pendant que le drone sort un leurre de l'objet, sortie à 3 motos, seule l'une à l'objet			Diversion/surcharge de la supervision
	Des clous ont été mis sur a route lors du déclenchement de l'alarme. Porte blindée en sortie de parking		Toutes les notions attendues ont été exprimées, de plus, le scenario devient trop complexe. Arrêt du jeu.

