Pirate ta fac ! Ludification de séances de cours sur la sécurité des systèmes d'information

Pierre-Emmanuel Arduin, Benjamin Costé

Pirate ta fac !

Ludification de séances de cours sur la sécurité des systèmes d'information

Pierre-Emmanuel Arduin [1], **Benjamin Costé** [2]

1. *Université Paris-Dauphine, PSL, DRM UMR CNRS 7088*
   Place du Maréchal de Lattre de Tassigny, 75775 Paris Cedex 16, France
   pierre-emmanuel.arduin@dauphine.psl.eu
2. *Airbus Cybersecurity, Saint-Jacques-de-la-Lande, France*
   benjamin.b.coste@airbus.com

RÉSUMÉ. *La sécurité des systèmes d'information s'enseigne à l'instar de toute autre activité, c'est-à-dire au travers d'exercices pratiques tels que de l'analyse de logiciels malveillants, de la détection de hameçonnage, des défis de « capture du drapeau », etc. Ces activités transforment les étudiants en apprenants actifs et facilitent leur appropriation des concepts théoriques. Nous présentons dans cet article une approche d'enseignement originale induisant un engagement accru des étudiants à qui il a été demandé de pirater des ordinateurs et de manipuler des membres de l'université. Cette approche a notamment mené à une prise de conscience sur l'importance des menaces intérieures à la sécurité des systèmes d'information, mais a aussi et surtout maintenu l'enthousiasme et l'intérêt des étudiants.*

ABSTRACT. *Teaching cybersecurity is like any other teaching activity: it requires practical exercises such as malware analysis, phishing detection, "capture the flag" challenges, etc. These activities give students the opportunity to become active learners by testing theoretic concepts and applying them in a practical way. In this article, we present an original teaching approach inducing an increased engagement from students who were asked to hack devices and deceive people within the university. Such an approach has notably led to raise awareness on the importance of insider threats in cybersecurity, but also and above all has maintained the enthusiasm and interest of students.*

MOTS-CLÉS : *Cybersécurité, Capture du drapeau, Ludification, Menaces intérieures, Influence sociale, Motivation pour apprendre.*

KEYWORDS: *Cybersecurity, Capture the flag, Gamification, Insider threats, Social influence, Learning motivation.*

1. Introduction

La sécurité des systèmes d'information peut être appréhendée d'un point de vue technique et focalisée sur les menaces externes afin de prévenir les intrusions (Hansen *et al*., 2007) ou détecter les attaques par déni de service (Zhi-Jun *et al*., 2012).La littérature académique aussi bien que les professionnels observent qu'une menace majeure n'est ni technique ni externe, mais provient des employés à l'intérieur même des organisations (Hassandoust *et al*., 2020; Willison, Warkentin, 2013). Cette menace intérieure peut être intentionnelle ou non, malveillante ou non (Arduin, 2018; Leach, 2003; Loch *et al*., 1992; Warkentin, Willison, 2009), ce qui a conduit les professionnels, chercheurs et enseignants de l'enseignement supérieur à considérer la cybersécurité ou sécurité des systèmes d'information comme un phénomène social (McAlaney, Benson, 2020).

L'enseignement de la cybersécurité ne se réduit pas à l'enseignement de techniques de chiffrement/déchiffrement, d'analyse de réseau ou d'attaques par force brute. Venkatesh *et al*. (2003) ont montré que l'intention des individus de passer à l'acte est notamment déterminée par le fait qu'ils pensent que les autres individus soutiennent ou condamnent l'acte en question. Pour McAlaney, Benson (2020), cela démontre le besoin de comprendre comment non seulement les individus perçoivent les risques de cybersécurité, mais aussi comment ils pensent que les autres perçoivent ces risques. Dans cet article, nous approfondissons cette idée en présentant comment entretenir l'enthousiasme et l'investissement des étudiants lors de séances de cours sur la sécurité des systèmes d'information nécessitant une maîtrise de l'ingénierie aussi bien technique que sociale.

Dans la deuxième section de cet article, nous présentons les théories mobilisées : d'abord des concepts fondamentaux de la sécurité des systèmes d'information à partager avec les étudiants, menaces extérieures et intérieures, ensuite une revue de la littérature en pédagogie par la ludification. Dans la troisième section, nous présentons des scénarios conçus pour des cours de sécurité des systèmes d'information en deuxième année de master : d'abord une description des séances sur les menaces extérieures et intérieures, ensuite une description de l'exercice de capture du drapeau, enfin une discussion sur les limites et les implications éthiques de l'approche considérée dans ce travail. En effet, cet article vise à partager des scénarios pédagogiques ludiques pour enseigner la sécurité des systèmes d'information et stimuler la motivation des étudiants : pirate ta fac !

2. Concepts théoriques et revue de la littérature

Dans cette section, nous présentons d'abord les éléments cruciaux de la sécurité des systèmes d'information à partager avec les étudiants dans le cadre du cours considéré dans cet article : les menaces extérieures et intérieures à la sécurité des systèmes d'information. Ensuite, nous proposons des éléments de la littérature sur la ludification comme approche pédagogique.

2.1. Maîtriser les technologies, une condition préalable à la cybersécurité

Un système d'information (SI) n'est pas uniquement composé d'appareils technologiques ; il inclut également les humains (Reix, 2000) qui concourent activement à la sécurité du système global. Le SI est ainsi menacé à double titre : d'une part, les attaquants externes utilisent leurs propres ressources pour pénétrer puis compromettre le SI, d'autre part, les utilisateurs internes peuvent menacer intentionnellement ou non la sécurité du système. De plus, l'émergence de l'Internet des objets (IoT) (Atzori *et al*., 2010), du Bring Your Own Device (BYOD) (Thomson, 2012) et des modèles de confiance zéro (Ward, Beyer, 2014) renforce l'importance de considérer la sécurité des deux points de vue.

L'essor des appareils connectés de tous types (smartphones, assistants personnels intelligents, etc.) amène de nouvelles habitudes et un besoin croissant d'accès numérique. Étant connectés numériquement à presque chaque instant, nos données sont en même temps vulnérables. Les utilisateurs peuvent consolider la protection de ces nouveaux appareils de trois manières :

1. le recours à des produits payants d'éditeurs renommés tels que des antivirus, des réseaux privés virtuels (VPN), des pare-feu, des protections Web, etc. qui offrent un niveau de sécurité élevé (Ahvanooey *et al*., 2017).

2. l'utilisation de produits gratuits dont la contrepartie est leur faible efficacité. Il peut s'agir de versions de produits bien connus moins riches en fonctionnalités que leurs versions payantes ou de nouvelles solutions d'éditeurs à la conquête d'un marché. Cependant, il peut aussi s'agir de faux produits qui installent des *adwares* et/ou des *pop-ups* pour collecter (voire voler) des données personnelles en même temps qu'ils introduisent de nouvelles vulnérabilités (Wu *et al*., 2014).

3. la configuration personnalisée des périphériques sans recours à un logiciel de sécurité supplémentaire. Cela nécessite cependant une sensibilisation aux problématiques de sécurité et une connaissance approfondie de leurs aspects techniques. Par exemple, la plupart des gens laisse les interfaces sans fil activées, diffusant leurs données et encourageant les attaquants opportunistes. Ces derniers possèdent des compétences de niveau variable allant de débutants (souvent appelés « script kiddies ») à experts (Barber, 2001). En fonction des compétences des attaquants et de leur malveillance, l'appareil peut être inscrit dans une ferme de minage de Bitcoin (ou de Monero, ou de toute monnaie cryptographique) ou participera à une attaque par déni de service distribué (DDoS) (Antonakakis *et al*., 2017).

Chaque option comporte ses propres risques et la plupart des utilisateurs n'ont pas l'utilité de comprendre les éléments techniques sous-jacents bien qu'ils aient besoin de choisir les moyens de sécurité appropriés. En tant qu'informaticiens, les étudiants doivent comprendre quels sont les risques de leurs décisions, surtout lorsqu'ils mettent leurs compétences au service d'une entreprise dès lors que leurs décisions affectent plusieurs utilisateurs. De plus, les cybercriminels agissent différemment lorsqu'ils ciblent le SI des entreprises plutôt que les appareils personnels. Le cours que nous proposons vise à aider les étudiants à agir de manière appropriée pour surmonter

les risques personnels ou à l'échelle de l'entreprise. Dans cette optique, nous proposons de nous concentrer sur ces menaces externes à travers trois grands objectifs pédagogiques expliqués ci-après :

1. Le premier objectif est de penser comme un cybercriminel afin d'identifier et anticiper les vulnérabilités et les menaces. En effet, un esprit criminel n'est pas intuitif par nature car il contourne les outils ou les habitudes pour obtenir ce qu'il recherche. Les phreakers utilisaient un sifflet pour passer des appels téléphoniques gratuits (Mitnick, Simon, 2003), certains pirates utilisent des LED optiques pour exfiltrer les données d'ordinateurs isolés (Guri *et al*., 2016) ou même transforment les alimentations électriques en haut-parleurs (Guri, 2020). Les appareils peuvent ainsi être détournés de leur fonction première pour réaliser des actions non-désirées par les concepteurs voire strictement proscrites par ceux-ci. Le premier objectif de notre cours est de partager une telle idée avec nos étudiants.
2. Le deuxième objectif est que les étudiants puisse comparer leur approche avec celles d'attaquants réels. Ils apprennent par ce biais ce qui est réellement utilisé par les attaquants au travers d'exemples d'attaques réussies.
3. Le troisième objectif est de reconstruire une séquence d'événements et de trouver des éléments d'information sur un attaquant au travers de leur compréhension du modus operandi criminel.

Une juste appréciation des risques et des procédures criminelles est obtenue au cours de ce cours. Au fur et à mesure qu'ils acquièrent de nouvelles connaissances sur la cybersécurité et les moyens de pirater, nous avons observé une augmentation de l'implication, de l'estime de soi et du bien-être des élèves. Néanmoins, pour Seebruck (2015) notamment, il existe plusieurs motivations au piratage qui incluent un élément social : le piratage pour le prestige, le piratage idéologique connu sous le nom de hacktivisme, et les menaces internes qui peuvent être motivées par la vengeance.

2.2. Manager les individus, un besoin grandissant pour la cybersécurité

Les conséquences d'une attaque mises en évidence très tôt par Loch *et al*. (1992) restent les mêmes de nos jours : (1) divulgation d'informations monnayables, (2) modification ou (3) destruction d'informations sensibles et (4) déni de service, en entravant l'accès aux ressources. En particulier, ces auteurs ont souligné l'existence de menaces extérieures et intérieures pour la sécurité des SI (Fig. 1).

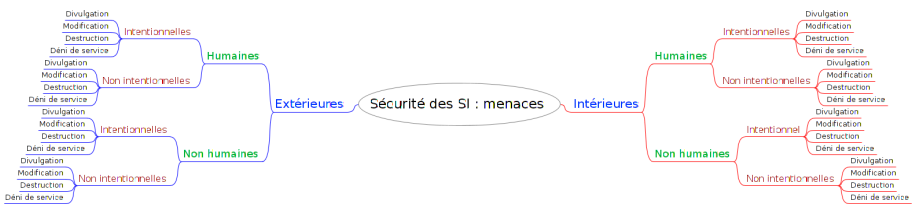

Figure 1. Taxonomie des menaces à la sécurité des SI (inspiré de Loch et al.*, 1992)*

Déterminer ce qui est « considéré comme juste » est un enjeu crucial dans le management de la sécurité des SI. Victor, Cullen (1988) ont par exemple proposé le concept de « climats de travail éthiques » pour définir la perception que les employés ont des valeurs, des politiques et des systèmes de récompense institutionnalisés. Il a été démontré que de tels climats de travail éthiques ont un impact sur le non-respect de la Politique de Sécurité des SI (PSSI) dans les entreprises (Gwebu *et al*., 2020).

Johnston, Warkentin (2010) ont noté que l'influence sociale a en effet un impact important sur les intentions des utilisateurs finaux en matière de sécurité. Pour Venkatesh *et al*. (2003), l'intention d'avoir un comportement en particulier dépend de la perception que vous avez que les autres soutiendront ou condamneront ce comportement. Dois-je faire part de mes doutes sur ce courriel suspect à mes collègues ? Dois-je faire confiance à cet assistant qui me presse de lui envoyer un fichier ? Des auteurs tels que Arduin (2021); Tsohou *et al*. (2015) ont montré que les biais cognitifs et culturels peuvent être activés de manière malveillante pour influencer les intentions des utilisateurs du SI quant à la sécurité.

Les menaces intérieures peuvent être classées selon deux dimensions : (1) le caractère intentionnel de la menace et (2) sa malveillance (Willison, Warkentin, 2013). Pour les employés utilisateurs d'un SI et constituant un point d'entrée dans le système, les menaces intérieures peuvent ainsi être (Arduin, 2018) :

1. *non-intentionnelles* : actions erronées d'employés inexpérimentés, négligents ou influencés ; par exemple, des clics inattentifs, des erreurs de saisie, des suppressions accidentelles de données sensibles, etc. (Stanton *et al*., 2005),

2. *intentionnelles et non-malveillantes* : actions délibérées d'employés ayant un bénéfice mais sans volonté de nuire ; par exemple, différer les sauvegardes, choisir un mot de passe faible, laisser les portes ouvertes lors de discussions sensibles, etc. (Guo *et al*., 2011),

3. *intentionnelles et malveillantes* : actions délibérées d'employés ayant la volonté de nuire ; par exemple, divulgation de données sensibles, introduction de logiciels malveillants, etc. (Shropshire, 2009).

Le cours que nous avons proposé intègre les aspects technologiques de la cybersécurité, tels que présentés dans la section 2.1, mais aussi les aspects sociaux et comportementaux de la cybersécurité s'appuyant sur ces trois catégories de menaces internes. En effet, la formation des individus est nécessaire pour contrer les attaques reposant sur des techniques d'ingénierie sociale et de manipulation (Campbell, 2019). Mitnick, Simon (2003) définissent l'ingénieur social comme étant un attaquant qui cible un utilisateur légitime duquel il obtient un moyen d'accès direct (droits d'accès, lien nuisible visité, etc.) ou indirect (informations vitales, relation de confiance, etc.) au système. Le contenu de la section 3 présente comment nos étudiants ont appris à penser en utilisant des techniques d'ingénierie sociale. Ils ont été impliqués dans le cours par la ludification des séances.

2.3. La ludification, un vecteur d'implication des étudiants dans l'enseignement

Si l'enseignement repose sur le partage des connaissances, il se heurte parfois à certaines difficultés : dans le cadre de l'enseignement en général et de l'enseignement supérieur en particulier, le désengagement induit par les méthodes pédagogiques traditionnelles est critiqué par des auteurs comme Siala *et al*. (2019). D'autres comme Mustar (2009) considèrent que les étudiants n'y sont pas assez remis en cause et que ces méthodes ne partagent pas les connaissances pratiques.

« J'entends et j'oublie, je vois et je me souviens, je fais et je comprends » : cette phrase, attribuée à Confucius au II^{e} siècle avant J.C., illustre bien l'idée du « *learning by doing* » formalisée par Kolb (1984). Cette idée est plutôt éloignée de l'apprentissage par frustration cognitive proposée par Cangelosi, Usrey (1970). Apprendre en agissant conduit non seulement à améliorer la pensée critique et les compétences de résolution pratiques (Kapp, 2012), mais aussi – et peut-être le plus important – la connaissance apprise devient « plus intéressante » (Tobias *et al*., 2014).

Des méthodes d'enseignement traditionnelles aux cours en ligne ouverts et massifs (MOOC), l'éventail des façons de partager les connaissances et d'enseigner est assez large. Si les MOOCs fournissent un contenu pédagogique en ligne et sont présentés comme permettant aux individus d'apprendre de manière autonome chez eux (Razmerita *et al*., 2019), il convient de rappeler que l'intention de rester dans le cours doit être mieux monitorée et analysée, ce qui a été particulièrement vrai pendant les confinements successifs dus au COVID-19 (Prenkaj *et al*., 2020).

Snyder (2018) a observé des expériences d'enseignement de la cybersécurité avec des *escape games*, des jeux d'évasion. Il a humblement conclu que ces expériences peuvent fonctionner – ou pas – mais que dans tous les cas les participants ont passé un bon moment. Bruguier *et al*. (2020) a identifié trois composants importants lors de la conception d'un jeu d'évasion pour l'enseignement de la sécurité matérielle : (1) l'importance du scénario, (2) la posture de l'enseignant et (3) le besoin d'un *debriefing*, une réunion-bilan. Silic, Lowry (2020, p. 131) vont plus loin lorsqu'ils proposent de définir la *gamification*, la ludification, de la sécurité comme un moyen de motiver les employés afin d'encourager l'apprentissage, l'efficacité et la conformité avec les initiatives de sécurité en utilisant des artefacts et des processus inspirés par le jeu.

La ludification de séances de cours sur la sécurité des systèmes d'information apparaît alors plutôt évidente face à la demande de Benson *et al*. (2019) de nouvelles méthodes facilitant l'appréciation collective des objectifs de sécurité. Même si une telle question a déjà été partiellement abordée à la fin des années 1990 avec la montée des *hackathons*, des événements intensifs de programmation informatique (Maaravi, 2020). Une étude réalisée par Briscoe, Mulligan (2014) conclut que les 150 répondants participent à des hackathons pour l'apprentissage (86%), le réseautage (82%), ou pour faire avancer le changement social (38%). En effet, ces auteurs rappellent que l'un des origines des hackathons est de hacker du code dans un but d'amélioration sociale.

3. Proposition : un cours « ludique » sur la sécurité des systèmes d'information

Plutôt que de former des experts en cybersécurité, le cours que nous proposons vise à assurer une compréhension fondamentale des concepts de sécurité des systèmes d'information les plus courants tout au long du cycle de vie de la sécurité : identification, protection, détection, réponse et récupération (NIST, 2018). Pour chaque partie, une brève description des problèmes rencontrés par les experts en cybersécurité est présentée, en s'appuyant aussi bien sur la littérature en la matière que sur nos propres expériences. Les bases de la cryptographie font également partie du cours. Chaque concept présenté est abordé aussi bien du côté attaquant (« équipe rouge ») que défenseur (« équipe bleue ») au regard des objectifs pédagogiques 1 et 3 (*cf.* section 2.1) ainsi que pour des raisons éthiques (Mirkovic, Peterson, 2014).

Le cours est organisé en trois parties successives. Trois cours magistraux pour commencer, sur les systèmes d'information, l'ingénierie sociale, les menaces intérieures, le cycle de vie de la sécurité et la cryptographie. Ces séances au contenu classique ne sont pas présentées dans cet article. S'ensuivent trois Travaux Dirigés (TD) répartis en deux thèmes : menaces extérieures et intérieures . Les étudiants choisissent eux-mêmes le thème qu'ils souhaitent suivre mais la répartition observée ces dernières années est plutôt équilibrée. Le cours se termine par un exercice de *Capture The Flag* (CTF), capture du drapeau, qui se tient en parallèle des séances de TD pour tous les étudiants et dont le contenu est détaillé dans la section 3.3.

3.1. De la maîtrise des technologies aux menaces extérieures

Après les cours théoriques, les étudiants sont répartis en groupes pour des cours dirigés. Chaque leçon pratique repose sur un scénario où les étudiants se voient confier un rôle de sécurité différent par rapport aux objectifs pédagogiques : tutoriel 1 – cybercriminel, tutoriel 2 – analyste des cybermenaces et tutoriel 3 – gestionnaire d'incidents. À la fin de chaque leçon, les étudiants doivent rédiger un rapport décrivant leur méthodologie. Les étudiants étant supposés novices en sécurité, leur sensibilisation aux problèmes de sécurité est privilégiée par rapport aux compétences techniques. Cela a une influence sur la conception des leçons : le premier scénario ne nécessite qu'une enquête sur le Web, le second nécessite une compréhension du vocabulaire techniques et le troisième nécessite des compétences techniques de base.

3.1.1. TD 1 – Hackons-le !

Dans le premier scénario, les élèves doivent imaginer un chemin pour compromettre un réseau commun, représenté sur la figure 2, comportant notamment une zone démilitarisée (DMZ) exposée sur Internet ainsi que différentes zones internes. Ils sont invités à s'inspirer du framework MITRE ATT&CK (Strom *et al.*, 2018) décrivant la méthodologie d'un attaquant. Ce framework est notamment utilisé en cas de détection d'attaque (Al-Shaer *et al.*, 2020) pour identifier les avancées des attaquants. Les exemples présentés sur le site du MITRE (cf https://attack.mitre.org/matrices/enterprise/) amènent les étudiants à découvrir plusieurs méthodologies d'attaquants.

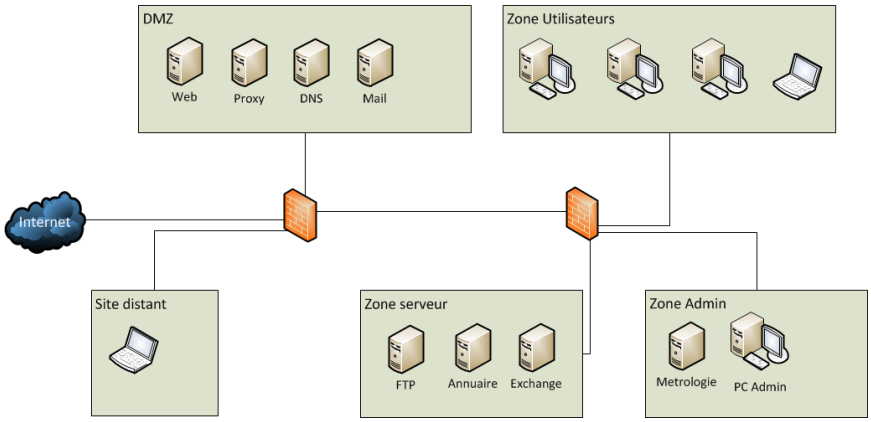

Figure 2. SI ciblé par les étudiants lors d'un TD sur les menaces extérieures

3.1.2. TD 2 – Connaître les attaquants

Dans le deuxième scénario, les étudiants se voient confier le rôle d'experts en Cyber Threat Intelligence (CTI). Chaque groupe doit analyser un rapport de menace différent, résumer la méthodologie employée par les attaquants et proposer des contre-mesures.

3.1.3. TD 3 – Trouvez le chat

Le troisième scénario est beaucoup plus technique. Les élèves doivent récupérer des éléments d'information sur un kidnappeur à l'aide de compétences en criminalistique numérique et en réponse aux incidents. Dans ce scénario, le chat de leur manager a été kidnappé (voir Fig. 3), et ils doivent trouver l'emplacement du kidnappeur et recouvrer les données secrètes chiffrées. Les étudiants reçoivent trois fichiers : des données secrètes chiffrées et deux demandes de rançon pour le chat et les données.

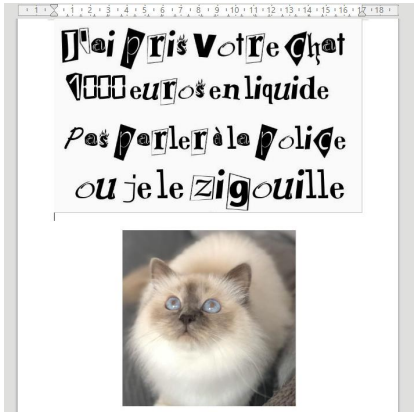

Figure 3. TD sur les menaces extérieures : demande de rançon avec données cachées.

Chaque fichier représente un défi différent : (i) le fichier de la rançon du chat contient l'emplacement probable du kidnappeur, caché dans les métadonnées ; (ii) Le deuxième fichier de rançon contient le mot de passe sécurisé qui est nécessaire pour déchiffrer les données secrètes (alias le troisième fichier) et qui ne peut être deviné ni forcé.

3.2. Du management des individus aux menaces intérieures

Les étudiants ayant choisi de rejoindre les TDs sur les menaces intérieures sont également répartis en groupes de quatre ou cinq personnes. Chaque séance aborde un cas spécifique de menace intérieure comme mentionné dans la section 2.2 : TD 1 – le non-intentionnel, TD 2 – l'intentionnel et non-malveillant et TD 3 – l'intentionnel et malveillant. À la fin de chaque séance, les étudiants rédigent un compte-rendu qui est évalué par l'enseignant et discuté en début de séance suivante.

3.2.1. TD 1 – Les menaces intérieures non-intentionnelles

Le premier TD est organisé en quatre temps : (i) les étudiants sont confrontés individuellement à des courriels de hameçonnage dans une salle d'expérimentation avec des murs de protection anti-copie (voir fig. 4.a), ils ne disposent d'aucune information sur la véracité des courriels et doivent indiquer les zones et éléments les amenant à faire confiance ou à se méfier ; (ii) les résultats de l'expérience sont discutés avec l'enseignant, en particulier les zones identifiées comme inspirant le plus la confiance et la méfiance (voir fig. 4.b) ; (iii) les étudiants passent ensuite en mode projet et doivent concevoir un courriel de hameçonnage « optimisé » en s'appuyant sur les résultats de l'expérience et expliquer leurs choix dans un compte-rendu écrit et noté (des exemples sont disponibles dans Arduin 2021) ; (iv) les travaux sont enfin présentés et discutés.

(a) (b)

Figure 4. TD sur les menaces intérieures – Hameçonne-moi si tu peux ! Murs anti-copie (a) et courriel de hameçonnage avec zones de confiance (b).

3.2.2. TD 2 – Les menaces intérieures intentionnelles et non-malveillantes

Pendant le deuxième TD, la classe est divisée en deux groupes : (A) le groupe des Responsables de la Sécurité des Systèmes d'Information (RSSIs) paranoïaques et

(B) le groupe des employés malins et paresseux, spécialistes des solutions de contournement et du moindre effort. Comme le lecteur l'aura peut-être compris, le groupe (A) représente les RSSIs déployant des Politique de Sécurité du Système d'Information (PSSIs) très contraignantes, tandis que le groupe (B) représente les employés contournant ces PSSIs et créant des menaces intérieures intentionnelles et non-malveillantes. Par exemple : imposer de changer son mot de passe à des fréquences farfelues peut conduire à les écrire sur des post-its, ou encore concevoir des procédures de sauvegarde complexes car trop sécurisées peut conduire à différer les sauvegardes, etc. Ce deuxième TD est organisé en trois temps : (i) une phase au cours de laquelle les étudiants du groupe (A) préparent des PSSIs complexes, très contraignantes, voire sciemment farfelues, alors que les étudiants du groupe (B) anticipent ces PSSIs singulières et comment ils pourraient les contourner, un compte-rendu qui sera noté est demandé avant de passer au temps suivant ; (ii) une phase de *battle*, confrontation au cours de laquelle des étudiants du groupe (A) vont avancer leurs PSSIs et des étudiants du groupe (B) exposer leurs solutions de contournement ; (iii) une phase de *débriefing*, discussion-bilan où les PSSIs et les solutions de contournement sont discutées.

3.2.3. TD 3 – Les menaces intérieures intentionnelles et malveillantes

Le troisième et dernier TD se concentre sur l'une des plus grandes craintes des RSSIs : les employés ayant des accès privilégiés qui deviennent des menaces intérieures intentionnelles et malveillantes. Durant ce TD, les groupes d'étudiants travaillent selon une procédure utilisée habituellement en *design thinking*, conception créative : la méthode DKCP (*Define, Knowledge, Concept, Project*) (Damart *et al.*, 2018). Les étudiants imaginent et conçoivent des pratiques parfois connues parfois inconnues où les utilisateurs deviennent intentionnellement des attaquants ayant la volonté de nuire. Après la phase individuelle de définition et de recueil de connaissances (D, K), les étudiants se mettent en groupe et échangent leurs idées pour proposer de nouveaux concepts (C) de menaces intérieures intentionnelles et malveillantes ; ils décrivent enfin la procédure comme s'il s'agissait d'un projet (P). À la fin du TD un compte-rendu est demandé, puis ces procédures sont présentées aussi bien que le processus de conception qui y a conduit. Une discussion-bilan vient conclure la séance, pendant laquelle les groupes sont invités à réfléchir aux contre-mesures possibles aux menaces identifiées.

3.3. L'exercice de capture du drapeau : accéder au sujet d'examen ?

La dernière partie de ce cours est conçue comme un défi de capture du drapeau (Snyder, 2018, voir section 2.3). Les étudiants doivent retrouver une partie de l'examen final cachée dans les murs de l'Université. Le défi est divisé en plusieurs parties, certaines étant communes à tous les groupes et certaines dépendant du groupe. Une cinquantaine d'étudiants en deuxième année de master MIAGE suivent ce cours chaque année. Ils ont été affectés au hasard à un groupe et plusieurs parties de l'examen final, les drapeaux, ont été cachées dans l'Université. Ainsi, tous les groupes ne cherchent pas un drapeau unique, mais deux ou trois groupes sont tout de même en

concurrence pour un même drapeau. Nous avons observé que certains groupes ont capturé plus d'un drapeau.

3.3.1. Partie 1 – Pirater un ordinateur portable (commun à tous les groupes)

Dans la première partie, un ordinateur portable est remis aux étudiants. Plusieurs vieux postes ont été récupérés au service informatique de l'Université et préparés en amont. Ceux-ci sont verrouillés et les étudiants n'ont aucun indice supplémentaire ni soutien de la part des enseignants. Tout comme une attaque réelle, ils doivent déverrouiller la session utilisateur afin de trouver des indices sur le lieu dans lequel se trouve leur drapeau cible, une partie du sujet d'examen. Rappelons que Bruguier *et al*. (2020, voir section 2.3) a mis en évidence trois composantes importantes de l'apprentissage par le jeu : (1) l'importance du scénario, (2) la posture de l'enseignant, et (3) le besoin d'un *débriefing*, une réunion-bilan. Comme le lecteur peut le deviner, l'importance du scénario était ici cruciale, tout comme la posture que nous avons adoptée lorsque nous avons demandé aux étudiants de pirater ces postes. Nous avons été très clairs depuis le début avec eux en leur expliquant que l'examen final sera très, très difficile et qu'ils pourraient en retrouver des parties que nous avions cachées à l'Université en découvrant des indices après avoir déverrouillé l'ordinateur portable. Bien sûr, ils ont été évalués sur la méthode qu'ils ont employée pour le faire. Le temps d'accès à l'ordinateur portable était limité par groupe et surveillé. Enfin, les groupes ont dû préparer un compte-rendu sur les vulnérabilités qu'ils ont exploitées, qu'elles soient extérieures ou intérieures. Il est important de souligner que bien que les étudiants soient totalement libres sur les méthodes à employer, il leur est rappelé que toute action entreprise dans le cadre de ce CTF relève de leur seule responsabilité.

Plusieurs indices ont été laissés comme un numéro de compte Twitter caché dans un faux code-barres que nous avons préparé (fig. 5.a) ou un indice donné par l'écran de verrouillage de Microsoft Windows après des essais infructueux (fig. 5.b). Une fois la session déverrouillée, une analyse stéganographique des fichiers des utilisateurs locaux était nécessaire pour révéler des adresses URL indiquant la cible suivante aux étudiants en fonction de leur numéro de groupe. Commence alors la deuxième phase : Le jeu virtuel de cette première partie de l'exercice de capture du drapeau, centré sur les aspects technologiques de la cybersécurité (voir section 2.1), devient un jeu réel, centré sur les aspects managériaux et comportementaux de la cybersécurité (voir section 2.2).

3.3.2. Partie 2 – Manipuler les individus (différent en fonction des groupes)

Les adresses URL découvertes dans la première partie donnent accès à différents défis selon les groupes et amènent les étudiants à rechercher des parties de l'examen final dans l'Université. Pour certains groupes, du code HTML caché contenait des informations sur une personne à retrouver. Pour d'autres, une page Web demandait un « identifiant administrateur » relativement trivial et facile à deviner. Certains groupes ont dû ouvrir des bureaux verrouillés avec des codes ou des clés (fig. 5.c). D'autres ont dû découvrir des dates de naissance de personnels de l'Université pour pouvoir accéder à des salles de conférence. Ensuite, une feuille de papier était cachée dans

(a) (b) (c)

Figure 5. Faux code-barres (a) et écran verrouillé (b) : pirater un poste. Serrure de porte avec code (c) : manipuler des employés.

le bureau ou la salle en question (derrière la porte, derrière une affiche de consignes incendie, sur le bureau, etc.). Les étudiants ont eu à exploiter des menaces intérieures (voir section 2.2) en incitant le personnel de l'Université à leur laisser accéder à des zones sécurisées. Là encore, le temps était limité depuis la fin de la première partie et ils ont dû préparer un compte-rendu noté sur les menaces qu'ils ont exploitées.

3.4. Discussion, limites et implications éthiques

L'approche pédagogique proposée ici repose évidemment sur du « *learning by doing* » (Kolb, 1984, voir section 2.3). Des auteurs comme Sagarin, Mitnick (2012) appelaient déjà il y a dix ans à une meilleure formation des internautes sur les techniques de manipulation employées par les attaquants. Pour d'autres comme Fiske, Taylor (2013), les individus ont tout simplement du mal à se lancer dans une réflexion approfondie et fatigante, ce qui les rend plus vulnérables aux armes d'influence en ligne (Muscanell *et al*., 2014) et rend nécessaire la formation à ce type de menace.

Nous avons observé avec des questionnaires de satisfaction en fin de cours que les étudiants étaient significativement satisfaits. Ils ont apprécié le challenge (« c'était particulièrement intéressant de trouver les indices tout seul ») et la formation technique (« peut-être approfondir un peu ce qui se passe sur le réseau, les ports, etc. »). L'ensemble des étudiants a apprécié le contrôle continu (« c'est une méthode d'évaluation qui me convient ») et nous avons même observé des étudiants partager leurs réponses ou utiliser des techniques d'ingénierie sociale sur d'autres étudiants ou du personnel administratif de l'Université, préalablement informé bien sûr mais sans détails sur l'exercice pour ne pas biaiser leur comportement.

Le risque de double usage de cette approche pédagogique ne peut pas être négligé (Rath *et al*., 2014). Même s'il existe un risque réel que des attaquants utilisent le matériau présenté dans cet article comme un guide pratique, nous considérons que les avantages en termes de formation l'emportent sur les risques. En effet, nous soutenons

que la formation des étudiants, des employés et des citoyens reste l'une des défenses les plus efficaces. Cette idée est d'ailleurs renforcée par l'explosion des cyberattaques utilisant l'ingénierie sociale du fait de l'épidémie de COVID-19 (Lallie *et al.*, 2020).

4. Conclusion

Dans cet article, nous avons proposé une approche pédagogique ludique pour des cours de sécurité des systèmes d'information renforçant l'idée que l'enseignement supérieur pouvait être le lieu d'expérimentations pédagogiques fertiles pour susciter et entretenir un engagement accru des étudiants : pirate ta fac !

Dans la deuxième section, nous avons présenté les menaces extérieures et intérieures à la sécurité des systèmes d'information, ainsi que des initiatives pédagogiques innovantes telles que la ludification. Dans la troisième section, nous avons présenté la structure du cours proposé, des travaux dirigés et l'exercice de capture du drapeau. Une discussion sur les limites et les implications éthiques de la pédagogie proposée est venue conclure le propos.

Pour des auteurs tels que Shah *et al*. (2019, p. 1128), la communauté universitaire doit s'efforcer de travailler avec toutes les parties pour offrir les meilleures pratiques. En effet, la nécessité de sensibiliser et de former les étudiants aux menaces de sécurité des systèmes d'information est plus que jamais cruciale : les individus sont connectés en permanence au système et constituent des points d'entrée sensibles aux armes d'influence en ligne (Muscanell *et al.*, 2014), ce à quoi il convient de les éduquer au plus tôt.

Bibliographie

Ahvanooey M. T., Li Q., Rabbani M., Rajput A. R. (2017). A survey on smartphones security: Software vulnerabilities, malware, and attacks. *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, n° 10, p. 30–45.

Al-Shaer R., Spring J. M., Christou E. (2020). Learning the associations of MITRE ATT&CK adversarial techniques. *ArXiv*.

Antonakakis M., April T., Bailey M., Bernhard M., Bursztein E., Cochran J. *et al*. (2017, août). Understanding the mirai botnet. In *26th USENIX security symposium (USENIX security 17)*, p. 1093–1110. Vancouver, BC, USENIX Association. Consulté sur https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

Arduin P.-E. (2018). *La menace intérieure*. ISTE Éditions.

Arduin P.-E. (2021). A cognitive approach to the decision to trust or distrust phishing emails. *International Transactions in Operational Research*, vol. à paraître.

Atzori L., Iera A., Morabito G. (2010, oct). The internet of things: A survey. *Computer Networks*, vol. 54, n° 15, p. 2787–2805.

Barber R. (2001, feb). Hackers profiled — who are they and what are their motivations? *Computer Fraud & Security*, vol. 2001, n° 2, p. 14–17.

Benson V., McAlaney J., Frumkin L. A. (2019). Emerging threats for the human element and countermeasures in current cyber security landscape. In *Cyber law, privacy, and security: Concepts, methodologies, tools, and applications*, p. 1264–1269. IGI Global.

Briscoe G., Mulligan C. (2014). Digital innovation: The hackathon phenomenon.

Bruguier F., Lecointre E., Pradarelli B., Dalmasso L., Benoit P., Torres L. (2020). Teaching hardware security: Earnings of an introduction proposed as an escape game. In *International conference on remote engineering and virtual instrumentation*, p. 729–741.

Campbell C. C. (2019). Solutions for counteracting human deception in social engineering attacks. *Information Technology & People*.

Cangelosi V. E., Usrey G. L. (1970). Cognitive frustration and learning. *Decision Sciences*, vol. 1, n° 3-4, p. 275–295.

Damart S., David A., Klasing Chen M., Laousse D. (2018, juin). Turning managers into management designers: an experiment. In *XXVIIème conférence de l'AIMS.* Montpellier, France.

Fiske S. T., Taylor S. E. (2013). *Social cognition: From brains to culture*. Sage.

Guo K., Yuan Y., Archer N., Connely C. (2011). Understanding nonmalicious security violations in the workplace: a composite behavior model. *Journal of Management Information Systems*, vol. 28, n° 2, p. 203-236.

Guri M. (2020). Power-supplay: Leaking data from air-gapped systems by turning the power-supplies into speakers. *arXiv preprint arXiv:2005.00395*.

Guri M., Hasson O., Kedma G., Elovici Y. (2016, dec). An optical covert-channel to leak data through an air-gap. In *2016 14th annual conference on privacy, security and trust (PST).* IEEE.

Gwebu K. L., Wang J., Hu M. Y. (2020). Information security policy noncompliance: An integrative social influence model. *Information Systems Journal*, vol. 30, n° 2, p. 220–269.

Hansen J. V., Lowry P. B., Meservy R. D., McDonald D. M. (2007). Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection. *Decision Support Systems*, vol. 43, n° 4, p. 1362–1374.

Hassandoust F., Techatassanasoontorn A. A., Singh H. (2020). Information security behaviour: A critical review and research directions. In *European conference on information systems, ECIS 2020.*

Johnston A. C., Warkentin M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, p. 549–566.

Kapp K. M. (2012). *The gamification of learning and instruction: game-based methods and strategies for training and education*. John Wiley & Sons.

Kolb D. A. (1984). Experience as the source of learning and development. *Upper Sadle River: Prentice Hall*.

Lallie H. S., Shepherd L. A., Nurse J. R. C., Erola A., Epiphaniou G., Maple C. *et al*. (2020, juin). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *ArXiv*, p. 1–20.

Leach J. (2003). Improving user security behaviour. *Computers & Security*, vol. 22, n° 8, p. 685–692.

Loch K. D., Carr H. H., Warkentin M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *Mis Quarterly*, vol. 16, n° 2, p. 173–186.

Maaravi Y. (2020). Using hackathons to teach management consulting. *Innovations in Education and Teaching International*, vol. 57, n° 2, p. 220–230.

McAlaney J., Benson V. (2020). Cybersecurity as a social phenomenon. In *Cyber influence and cognitive threats*, p. 1–8. Elsevier.

Mirkovic J., Peterson P. A. H. (2014, août). Class capture-the-flag exercises. In *2014 USENIX summit on gaming, games, and gamification in security education (3gse 14)*. San Diego, CA, USENIX Association. Consulté sur https://www.usenix.org/conference/3gse14/summit-program/presentation/mirkovic

Mitnick K., Simon W. (2003). *The art of deception: Controlling the human element of security*. John Wiley and Sons.

Muscanell N. L., Guadagno R. E., Murphy S. (2014). Weapons of influence misused: A social influence analysis of why people fall prey to internet scams. *Social and Personality Psychology Compass*, vol. 8, n° 7, p. 388–396.

Mustar P. (2009). Technology management education: Innovation and entrepreneurship at mines paristech, a leading french engineering school. *Academy of Management Learning & Education*, vol. 8, n° 3, p. 418–425.

NIST. (2018, apr). *Framework for improving critical infrastructure cybersecurity, version 1.1*. Rapport technique. National Institute of Standards and Technology.

Prenkaj B., Stilo G., Madeddu L. (2020). Challenges and solutions to the student dropout prediction problem in online courses. In *Proceedings of the 29th acm international conference on information & knowledge management*, p. 3513–3514.

Rath J., Ischi M., Perkins D. (2014). Evolution of different dual-use concepts in international and national law and its implications on research ethics and governance. *Science and engineering ethics*, vol. 20, n° 3, p. 769–790.

Razmerita L., Kirchner K., Hockerts K., Tan C.-W. (2019, 12). Modeling collaborative intentions and behavior in digital environments: The case of a massive open online course (mooc). *Academy of Management Learning & Education*.

Reix R. (2000). *Systemes d'information et management des organisations*. Paris, Vuibert.

Sagarin B. J., Mitnick K. D. (2012). The path of least resistance. *Six Degrees Of Social Influence: Science, Application, and the Psychology of Robert Cialdini*, p. 12.

Seebruck R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital investigation*, vol. 14, p. 36–45.

Shah M. H., Jones P., Choudrie J. (2019). Cybercrimes prevention: promising organisational practices. *Information Technology & People*.

Shropshire J. (2009). A canonical analysis of intentional information security breaches by insiders. *Information Management and Computer Security*, vol. 17, n° 4, p. 221-234.

Siala H., Kutsch E., Jagger S. (2019). Cultural influences moderating learners' adoption of serious 3d games for managerial learning. *Information Technology & People*.

Silic M., Lowry P. B. (2020, jan). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems*, vol. 37, n° 1, p. 129–161.

Snyder J. (2018). *A framework and exploration of a cybersecurity education escape room*. Thèse de doctorat non publiée, Brigham Young University.

Stanton J., Stam K., Mastrangelo P., Jolton J. (2005). Analysis of end user security behaviors. *Computers and Security*, vol. 24, n° 2, p. 124-133.

Strom B. E., Applebaum A., Miller D. P., Nickels K. C., Pennington A. G., Thomas C. B. (2018, juillet). *MITRE ATT&CK: Design and philosophy*. Rapport technique. MITRE CORP BEDFORD MA.

Thomson G. (2012, feb). BYOD: enabling the chaos. *Network Security*, vol. 2012, n° 2, p. 5–8.

Tobias S., Fletcher J. D., Wind A. P. (2014). Game-based learning. In *Handbook of research on educational communications and technology*, p. 485–503. Springer.

Tsohou A., Karyda M., Kokolakis S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & security*, vol. 52, p. 128–141.

Venkatesh V., Morris M. G., Davis G. B., Davis F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, p. 425–478.

Victor B., Cullen J. B. (1988). The organizational bases of ethical work climates. *Administrative science quarterly*, p. 101–125.

Ward R., Beyer B. (2014). Beyondcorp: A new approach to enterprise security. *;login:*, vol. 39, n° 6.

Warkentin M., Willison R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, vol. 18, n° 2, p. 101–105.

Willison R., Warkentin M. (2013). Beyond deterrence: an expanded view of employee computer abuse. *MIS Quartely*, vol. 37, n° 1, p. 1-20.

Wu F., Narang H., Clarke D. (2014). An overview of mobile malware and solutions. *Journal of Computer and Communications*, vol. 02, n° 12, p. 8–17.

Zhi-Jun W., Hai-Tao Z., Ming-Hua W., Bao-Song P. (2012). MSABMS-based approach of detecting ldos attack. *Computers & Security*, vol. 31, n° 4, p. 402–417.