CybeR&T : Ludification et micro-certification appliquées à la sensibilisation à l'hygiène informatique

Thierry Dumartin
Département Résaux et Télécommunications, *IUT La Rochelle*
La Rochelle, France
thierry.dumartin@univ-lr.fr

***Résumé*—Cet article présente un retour d'expérience de sensibilisation à l'hygiène informatique d'étudiants en première année de Bachelor Universitaire de Technologie Réseaux et Télécommunications. Nous expliquons comment nous avons organisé cette séquence pédagogique en créant « CybeR&T : le jeu que les DSI envient » et comment nous en sommes venus à créer une micro-certification reconnue par les entreprises.**

***Index Terms*—cybersécurité, ludification, open badge**

I. Introduction

Comme l'aurait énoncé Klaus Klages, « la plupart des problèmes informatiques se situent entre le clavier et la chaise ». Cette évidence devient d'autant plus flagrante lorsqu'on l'étend à la cybersécurité. En 2024, l'Unité Nationale Cyber évaluait le coût des cyberattaques en France à presque 120 milliards d'euros. 94% de ces malwares étaient distribués par e-mail et donc liés à une négligence humaine. Dans ces conditions, une sensibilisation de la population à l'hygiène informatique revêt un intérêt stratégique.

Les départements d'Institut Universitaire de Technologie (IUT) dispensant le Bachelor Universitaire de Technologie (BUT) Réseaux et Télécommunications (R&T) l'ont bien intégré. Ils forment les administrateurs réseaux et systèmes de demain et ils ont donc jugé primordial d'inclure dans leur programme national (PN) une sensibilisation à l'hygiène informatique et à la cybersécurité dès le début de la formation. Au département de La Rochelle, nous avons décidé d'approcher cette activité de manière ludique.

II. Le BUT : un paradigme qui change

Le BUT est un nouveau diplôme qui « repose sur une pédagogie entièrement repensée selon une approche par compétences » [1] qui remplace l'approche par objectifs jusque-là considérée comme vérité absolue.

A. L'approche par compétences

Définir de ce que représente une compétence n'est pas aisé. Pour cela, le système IUT s'en remet aux travaux de Georges et Poumay [2]. Ils s'appuient sur la définition de Tardif [3], pour qui, une compétence est « un savoir agir complexe prenant appui sur la mobilisation et la combinaison efficace d'une variété de ressources à l'intérieur d'une famille de situations ».

C'est donc dans l'action qu'une compétence se définit et non uniquement par la démonstration de l'acquisition d'un savoir. En ce sens, deux étudiants pourront démontrer la même compétence en utilisant des ressources différentes et en menant des actions différentes. La compétence dépasse donc le niveau du réflexe ou de l'automatisme. Mais comment faire pour mettre l'étudiant en situation de nous démontrer qu'il est compétent ?

B. Sur le chemin de la situation d'apprentissage et d'évaluation (SAÉ)

Jusqu'à présent, notre modèle d'enseignement s'articulait uniquement autour de trois axes : (i) cours magistraux (CM), (ii) travaux dirigés (TD) et (iii) travaux pratiques (TP), permettant aux étudiants d'acquérir des savoir-faire théoriques et pratiques. Cette organisation leur permet de construire des ressources internes mais nous comprenons rapidement que la démonstration de leur compétence ne pourra pas se faire dans ce contexte.

C'est donc ici qu'apparaît la nécessité des situations d'apprentissage et d'évaluation. À l'image de ce que pouvait préconiser Freinet avec l'expression libre, la SAÉ va placer l'étudiant au centre du processus d'apprentissage et lui permettre de faire la preuve de sa compétence. Pour cela, il faut le positionner dans des situations complexes qu'il pourrait rencontrer dans sa future vie professionnelle. Une SAÉ devra donc laisser beaucoup d'autonomie à l'étudiant tout en le confrontant à une problématique authentique qui lui permetta de combiner des ressources internes déjà acquises, et de découvrir et acquérir de nouvelles ressources. Et surtout, une SAÉ n'est pas scriptée, elle ne doit pas donner lieu à une réponse unique prédéfinie à l'avance par l'enseignant.

C. Ludification et jeu sérieux

On parle de ludification dès qu'une mécanique relevant du jeu est intégrée dans une séquence pédagogique (utilisation de clickers [4], scénarisation des TD ou des TP [5]). Le jeu sérieux représente une forme de ludification dont l'ambition est d'intégrer complétement le cours dans ses objectifs. Quelle que soit l'approche choisie, l'objectif reste d'améliorer l'engagement et la motivation des étudiants tout en leur faisant

oublier qu'ils apprennent. Nous devons essayer de les impliquer en les mettant en activité et en les rendant acteur de la séquence d'apprentissage. Et si cette séquence d'apprentissage se rapporte à une situation complexe authentique, nous aurons alors ludifié une SAÉ. Mais comment faire pour ludifier un apprentissage sans le dénaturer et en permettant aux étudiants d'acquérir des compétences ? Un rapide état de l'art des jeux de société ou vidéo nous permet d'énumérer facilement certains mécanismes essentiels comme les systèmes de points et de classement pour renforcer l'émulation ou le passage de niveaux et l'obtention de badges pour acquérir un statut ou une reconnaissance. Mais la création d'un jeu sérieux nécessite surtout de définir les critères suivants :

l'immersion qui permet aux étudiants d'incarner un personnage et de les mettre à distance avec la situation d'apprentissage,

le défi qui favorise l'implication des étudiants. Il est question ici de mettre de l'enjeu afin de pousser les étudiants à s'investir pleinement dans la situation d'apprentissage,

l'interaction qui favorise les échanges et contribue à la bonne dynamique du groupe,

la récompense qui permet de valoriser le travail accompli.

Ainsi, créer une SAÉ ludifiée nécessite de respecter un cadre structuré.

III. Application à la SAÉ1.01 : Se sensibiliser à l'hygiène informatique et à la cybersécurité

La SAÉ 1.01 est la première SAÉ du BUT R&T. Elle place l'étudiant en tant que professionnel R&T au sein d'une Direction des Systèmes d'Information (DSI). D'après le PN du BUT R&T [6], une des premières missions du technicien R&T est de sensibiliser le personnel de son entreprise aux règles d'hygiène informatique

A. Organisation de la SAÉ1.01

Nous nous interrogions sur la capacité de nos néo-bacheliers à être autonomes si tôt dans l'année. Nous avons donc cherché un moyen pour les motiver et les impliquer : l'approche par ludification. À la lecture des objectifs du PN et des contraintes liées à la mise en place d'une SAÉ, nous avons décidé d'initier un jeu de rôle. Les étudiants font partie de la DSI de l'entreprise SportE-Kom, spécialisée dans l'organisation de compétitions d'e-sport. En tant que technicien réseau, une de leurs missions est d'accueillir les nouveaux employés en les sensibilisant à l'hygiène informatique. Cette SAÉ est positionnée avant les vacances de Toussaint, après seulement quatre semaines de cours et se déroule sur cinq semaines (tel que décrit en Table I). Nos étudiants ayant encore très peu de recul par rapport à leur futur métier, nous avons commencé par une séance de TP entièrement guidée et encadrée. Cette première situation leur demande d'auditer le poste de travail d'un nouvel employé pour vérifier qu'il n'ait pas de comportements numériques à risque. Elle débouche sur une synthèse permettant de dresser une liste des principales règles d'hygiène informatique à respecter et de lancer la situation d'apprentissage complexe en autonomie. Lors de cette phase, par groupe de quatre, les étudiants vont alors créer un jeu sérieux qui devra permettre de sensibiliser le personnel de l'entreprise à l'hygiène informatique. Pour conclure, l'ultime séance de TP est encadrée par l'enseignant qui se positionne en maître de jeu, les étudiants jouant alors le rôle des employés. Elle permet de confronter les étudiants au travers de défis et d'évaluer les compétences acquises.

TABLE I
PLANNING DE LA SAÉ1.01 (HEURES PAR ÉTUDIANT)

Semaine	39	40	41	42	45
Cours		1 h			
TP	3 h				1 h 30
Projet		3 h	3 h	3 h	1 h 30

Notre organisation permet ainsi de :
- placer les étudiants dans une situation authentique, celle d'un technicien réseau chargé de former les employés d'une entreprise du monde numérique aux règles d'hygiène informatique,
- découvrir et d'acquérir de nouvelles ressources grâce à la séance de TP encadrée et à la séance de cours de synthèse,
- vérifier les compétences acquises lors de la séance finale de jeu,
- ne pas donner lieu à une réponse unique et prédéfinie à l'avance puisque chaque groupe d'étudiants devra faire preuve de créativité lors de l'élaboration du jeu sérieux.

B. Le TP de mise en situation

Pour ce TP, les étudiants se positionnent dans la peau d'un technicien réseau de l'entreprise SportE-Kom. Un nouveau développeur web, Jean Groseille, vient d'être recruté. Il a récupéré son poste de travail et signé la charte informatique. Les étudiants doivent auditer sa machine afin de découvrir si son comportement numérique ne pourrait pas nuire à la sécurité du système d'information (SI) de l'entreprise.

Chaque étudiant réalise individuellement le TP guidé. Il dispose de trois machines virtuelles (comme présenté en Fig. 1) : sa machine de technicien réseau, la machine de Jean ainsi que son serveur de développement.

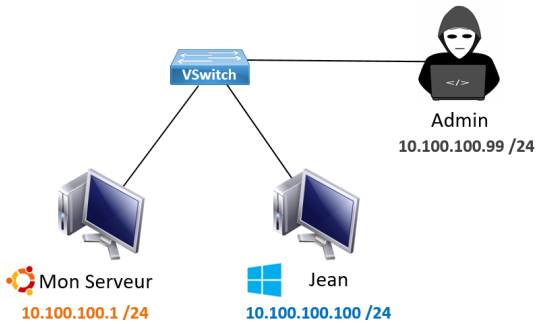

FIGURE 1. Maquette du TP de mise en situation

Le TP est adapté au niveau de néo-bacheliers et suit un processus simplifié de la *cyber kill chain* :

1) reconnaissance de la cible,
2) recherche et exploitation d'une vulnérabilité sur la cible,
3) intrusion sur la cible et exécution de code sur son système,
4) exfiltration des données de la cible.

Au cours de cette séance encadrée, les étudiants devront :

1) procéder à de la recherche d'informations en sources ouvertes sur le nom « Jean Groseille » :
   — découverte de la page Facebook publique de Jean,
   — récupération de ses informations personnelles,
   — création d'un dictionnaire de mots de passe susceptibles d'être utilisés par Jean.
2) énumérer les services actifs sur la machine de Jean. Ils repèreront le service *Remote Desktop Protocol* qui permet d'ouvrir un bureau distant sur une machine Windows.
3) procéder à une attaque par dictionnaire pour retrouver le mot de passe utilisé par Jean.
4) se connecter sur sa machine et l'auditer à la recherche de traces supplémentaires :
   — dans l'historique du navigateur Internet,
   — en utilisant un logiciel de récupération de données qu'ils auront installé (car Jean est administrateur de sa machine).

Ils y trouveront l'identifiant et le mot de passe permettant d'accéder au serveur de développement et pourront alors reproduire le même processus pour essayer de le compromettre. Ils en profiteront pour découvrir l'intérêt du chiffrement à travers la capture de trafic telnet et ssh en se connectant sur le serveur.

À la fin de ce TP, les étudiants seront invités à énoncer les règles d'hygiène informatique bafouées par Jean et à prendre les mesures de durcissement nécessaires :

— effacer l'historique et interdire la sauvegarde des mots de passe dans le navigateur Internet,
— gérer les mots de passe avec un gestionnaire de mot de passe,
— effectuer des sauvegardes régulières avec un outil de synchronisation,
— formater correctement son disque dur,
— chiffrer son disque dur,
— créer un utilisateur non-administrateur,
— vérifier l'utilisation de protocoles sécurisés lorsqu'on saisit un identifiant ou un mot de passe sur un réseau.

C. CybeR&T : le jeu que les DSI envient

À l'issue de la séance de TP, les étudiants auront donc une meilleure connaissance de ce que l'on nomme l'« hygiène informatique ». La séance de cours de synthèse sera l'occasion d'ouvrir vers les préconisations de l'ANSSI et de présenter les objectifs du projet. En effet, la formation du personnel d'une entreprise aux règles d'hygiène informatique est devenue un enjeu majeur de la cybersécurité. Pour cette partie de la SAÉ, les étudiants vont continuer à jouer leur rôle de technicien réseau. Ils devront concevoir du contenu pour un jeu sérieux permettant de sensibiliser les employés de SportE-Kom.

Le principe de CybeR&T est simple. Un maître de jeu supervise la partie. Il possède des cartes *Cyber Challenge* ainsi que les cartes *réponses* associées (qui auront été préalablement créées par les étudiants). Chaque équipe commence par tirer une carte *Cyber Challenge* qui se compose de quatre parties :

— un défi contextualisant des problématiques liées à l'hygiène informatique,
— la lettre M suivi d'un chiffre entre 2 et 5 précisant le nombre de menaces potentielles liées au défi,
— la lettre A suivi d'un chiffre entre 2 et 5 précisant le nombre d'actions préventives qu'il aurait fallu respecter pour éviter les problèmes liés au défi,
— la lettre R suivi d'un chiffre entre 2 et 5 précisant le nombre de remédiations à mettre en œuvre pour résoudre les problèmes liés au défi.

Chaque équipe dispose alors de dix minutes par carte pour retrouver les Menaces, les Actions préventives et les Remédiations de leur défi. C'est le maître de jeu qui donne le départ et l'arrêt du temps de recherche. Il récupère alors les propositions de chaque équipe afin qu'elles ne soient plus modifiées. Chaque équipe passe alors à tour de rôle pour présenter le résultat de ses réflexions et le maître de jeu les compare avec les réponses attendues. Elle marque des points pour chaque critère retrouvé (M, A et R). De son côté, l'équipe qui a créé la carte marque des points pour chaque réponse non trouvée et présente sur la *carte réponse*.

Notre idée est d'avoir ici une double approche. D'un côté, les étudiants sont acteurs de la conception du jeu en tant que technicien réseau de l'entreprise. Ils doivent donc imaginer des situations réalistes et pédagogues. Mais d'un autre côté, ils pourront aussi bénéficier de l'aspect ludique de leur réalisation en testant le jeu comme des employés nouvellement initiés. Cette mise en abîme est censée créer une émulation lors de la conception du jeu sérieux puisque chaque groupe sera confronté aux réalisations des autres équipes. Nous espérons ainsi qu'ils auront à cœur d'imaginer des cartes *Cyber Challenge* et des cartes *réponses* originales. Pour synthétiser notre approche, nous avons essayé de mettre en place une situation d'apprentissage :

— immersive positionnant l'étudiant dans son futur rôle de technicien réseau,
— générant un défi puisque chaque équipe devra essayer de trouver des situations suffisamment complexes pour piéger les équipes adverses mais dont elle devra connaître les réponses,
— interactive car il faudra que les étudiants travaillent de concert et partagent leurs idées afin de concevoir leurs cartes,
— motivante car chaque équipe pourra utiliser des ressources externes pour concevoir leurs défis ou pour se préparer à la séance de jeu,

— valorisant le travail accompli à travers le double système de comptage de points.

D. Evaluation et micro-certification

L'évaluation par compétence utilisée lors de cette SAÉ n'est pas abordée dans cet article. Néanmoins, à travers la réalisation des cartes *Cyber Challenge* puis en répondant aux défis des autres équipes, chaque étudiant doit prouver qu'il sait identifier :

— les cybermenaces portant sur un SI (M),
— les règles d'hygiène informatique à respecter pour ne pas être un danger pour le SI (A),
— les procédures à mettre en place sur le SI pour le maintenir ou le remettre en activité (R).

Nous sommes donc en capacité d'évaluer si nos étudiants sont compétents ou non. Néanmoins, nous nous demandions si notre approche ludifiée leur permettrait de répondre à une évaluation plus académique. Nous avons donc imaginé de leur faire passer une micro-certification « maison ». Elle prend la forme d'un QCM sur les règles d'hygiène informatique utilisant des questions comparables à celles que l'on peut trouver dans le MOOC de la SecNum Academie de l'ANSSI ou le programme « Introduction to Cybersecurity » de Netacad. Le certificat s'obtient à partir de 75% de bonnes réponses et est matérialisé par un Open Badge.

Un Open Badge est un certificat numérique prenant la forme d'une image intégrant des métadonnées dont l'organisme certificateur, les dates d'émission et de validité, les critères d'obtention, la description des compétences ou des savoir-faire validés, le nom du destinataire. Il peut être partagé sur des réseaux sociaux professionnels comme LinkedIn ou intégré à un CV ou un portfolio numérique. Il constitut la récompense finale de la séance ludifiée.

E. Résultats et perspectives

Cette SAÉ s'est déroulée sur cinq semaines en milieu de premier semestre, une période où l'on commence généralement à constater les premiers abandons et identifier les premiers étudiants en situation d'échec. La majorité de nos étudiants s'inscrivant en BUT R&T pour faire de la cybersécurité, la séance de TP a été particulièrement bien accueillie (« le meilleur TP de l'année » d'après plusieurs retours). La séance de synthèse a donné lieu à énormément d'échanges et de questions sur le sujet. L'idée de concevoir deux cartes de jeu les a tout de suite motivés. Les étudiants se sont tous pris au jeu et certains d'entre eux ont retrouvé un regain de motivation alors qu'ils commençaient à décrocher sur les enseignements plus « classiques ». Globalement, nous avons été très agréablement surpris par la qualité du travail produit. Les étudiants n'ont pas compté leur investissement. Ils ont fait appel à de nombreuses ressources externes afin de créer des cartes susceptibles de piéger les équipes adverses. Cela souvent était l'occasion d'aller au-delà du simple cadre de cette SAÉ et de vulgariser des notions qui seront traitées ultérieurement dans le programme (sur la cryptographie notamment). De plus, en les impliquant dans un travail de groupe très tôt dans l'année, nous avons pu contribuer à créer un esprit d'équipe plus rapidement.

L'obtention de l'Open Badge leur permet d'ouvrir leur premier portfolio numérique et d'enrichir leur CV. Après deux années d'expérimentation, 72 étudiants ont passé notre micro-certification et 69 (95,9%) ont obtenu plus de 75% de bonnes réponses, confirmant le sentiment de réussite de notre approche. Depuis cette année, notre micro-certification est portée par l'ensemble des départements R&T afin de lui donner une visibilité nationale. De plus, des entreprises liées à la cybersécurité ont reconnu la pertinence et la qualité des questions posées en endossant notre Open Badge. La gendarmerie nationale et ces entreprises semblent particulièrement intéressées pour l'utiliser dans leurs activités de sensibilisation. Nous avons aussi pu échanger avec le groupe cybermalveillance de l'ANSSI qui travaille sur la création d'un jeu sérieux de sensibilisation à destination des TPE et PME, confirmant la pertinence de l'authenticité de notre approche

IV. Conclusions

De notre point de vue, la ludification est sans conteste un levier très intéressant pour motiver et impliquer des néo-bacheliers. Mais elle implique une scénarisation et une mise en situation importante de la part de l'enseignant. Il faut impérativement que celui-ci soit partie prenante du scénario et du jeu de rôle pour que les apprenants s'impliquent en retour. Tout cet investissement se voit néanmoins récompensé au travers de l'engagement des étudiants dans la création du jeu et de leur motivation à gagner ou à piéger les équipes adverses... et cela représente déjà une belle victoire !

La matérialisation de leurs acquis par l'intermédiaire d'une micro-certification est une réussite et a permis de valider la cohérence de notre approche. L'intérêt d'acteurs professionnels de la sensibilisation à l'hygiène informatique lui ouvre des perspectives dépassant le simple cadre de nos objectifs pédagogiques initiaux et représente une énorme plus-value pour nos étudiants.

Références

[1] "Le Bachelor Universitaire Technologique," https://www.iut.fr/le-but-et-ses-specialites, accédé : 20/01/2025.

[2] F. Georges and M. Poumay, "Rédiger le référentiel de compétences du bachelor universitaire de technologie - guide d'accompagnement à la rédaction du référentiel de compétences du b.u.t. en contexte d'apc," June 2020, accédé : 20/01/2025. [Online]. Available : https://orbi.uliege.be/bitstream/2268/252906/1/IMPRIMER_%20Guide_competences_ADIUT_FINAL.pdf

[3] J. Tardif, *L'évaluation des compétences : documenter le parcours de développement*. Chenelière éducation, 2006.

[4] N. Fortino and F. Payan, "Une pédagogie interactive en R&T grâce aux boîtiers de vote électronique," in *Workshop pédagogique R&T (Réseaux & Télécommunications)*, 2014. [Online]. Available : https://hal.science/hal-02010312

[5] P.-E. Arduin and B. Costé, "Pirate ta fac ! Ludification de séances de cours sur la sécurité des systèmes d'information," in *INFORSID 2022 - INFormatique des Organisations et Systèmes d'Information et de Décision*, 2022, pp. 125–140. [Online]. Available : https://hal.science/hal-03960042

[6] "Programme National BUT Réseaux & Télécommunications," https://www.enseignementsup-recherche.gouv.fr/sites/default/files/2023-12/r-seaux-et-t-l-communications-30876.pdf, accédé : 20/01/2025.