# CyberEdu, ou l'ambition de former à la sécurité tous les acteurs du numérique

Olivier Levillain [1]

Depuis plusieurs années, on entend régulièrement des annonces, en France ou à l'étranger, affirmant que les besoins en sécurité du numérique sont immenses et qu'il faut former plus d'experts en cybersécurité. Bien que ce constat soit avéré, il est important de comprendre que la sécurité du numérique ne doit pas reposer uniquement sur des experts. Chaque acteur de la chaîne des systèmes d'information (administrateur, développeur, chef de projet, etc.) doit se sentir concerné et être impliqué, afin que la sécurité soit prise en compte tout au long des projets et de la vie des systèmes. On parle parfois de « *security by design* ».

Ainsi, tout administrateur réseau devrait savoir que les adresses réseau source d'un paquet peuvent être trivialement modifiées. Cela permettra d'éviter que le filtrage par adresse MAC soit vu comme un mécanisme de défense absolu. De manière similaire, tout développeur devrait avoir quelques notions concernant les vulnérabilités logicielles classiques, telles qu'un débordement de tampon (*buffer overflow* en anglais), ainsi que les moyens de s'en protéger (en effet, demander aux utilisateurs d'un site Internet de ne pas utiliser certains caractères dans leur mot de passe n'est pas une solution acceptable).

Développer chez les étudiants cet état d'esprit, cultiver ce réflexe du questionnement, susciter la curiosité face au monde du numérique, c'est la base de la sécurité.

1. Secrétaire adjoint de l'association CyberEdu, responsable du centre de formation de l'ANSSI.

## CyberEdu, une démarche initiée par l'ANSSI

La démarche CyberEdu, initiée en 2013 par l'agence nationale de la sécurité des systèmes d'information (ANSSI), a pour objectif d'introduire des notions de sécurité dans l'ensemble des formations du numérique en France. Deux grandes actions ont été lancées par l'ANSSI pour CyberEdu : d'une part la réalisation et la mise à disposition de supports de cours destinés aux enseignants du supérieur en informatique souhaitant intégrer des éléments de sécurité dans leurs interventions et d'autre part la tenue de colloques réunissant des enseignants du supérieur en informatique et des experts de l'ANSSI.

Ces travaux ont été plus particulièrement menés par le centre de formation à la sécurité des systèmes d'information (CFSSI), avec l'appui des équipes techniques de l'ANSSI. Le CFSSI propose aux agents des fonctions publiques et aux militaires français des formations en SSI sur des sujets allant du panorama de la SSI à la cryptologie, en passant par l'analyse de risques ou l'audit. Un des objectifs de CyberEdu pour le CFSSI était de toucher un public plus large.

## Les supports de cours CyberEdu

L'université européenne de Bretagne (qui regroupe 28 établissements d'enseignement supérieur et de recherche) et Orange ont remporté l'appel d'offre de l'ANSSI pour la fourniture des supports pédagogiques. Ces supports ont été mis à la disposition de tous les enseignants souhaitant utiliser ces ressources pour leurs cours [2] et comportent :

— un guide pédagogique, qui présente la démarche et propose d'expliquer quelques grands principes. Parmi ceux-ci, citons l'importance de ne pas traiter la sécurité comme un module à part, mais d'intégrer ce sujet, de le tisser autant que faire se peut au sein des cours existants ;

— un ensemble de planches de présentation, qui est un cours prêt à l'emploi d'une durée de 20 heures environ. Il est à destination des étudiants de niveau licence / DUT / BTS, pour leur donner les notions de base, le vocabulaire nécessaire à la compréhension des enjeux de sécurité et pour présenter succinctement l'organisation de la cybersécurité en France ;

— des fiches sur différents sujets pour les enseignants au niveau master : les systèmes d'exploitation, le réseau, le développement logiciel, l'authentification et les composants électroniques. L'objectif est de proposer à l'enseignant de tisser au cœur de son cours l'étude d'un sujet lié à la sécurité.

2. https://www.ssi.gouv.fr/administration/formations/cyberedu/contenu-pedagogique-cyberedu/

Ces documents ont été publiés sous licence Creative Commons Attribution (CC-BY). Cela permet à tous les enseignants le souhaitant de les réutiliser et de les adapter librement, y compris pour une utilisation commerciale, à la condition de rappeler la paternité des documents originaux (le projet CyberEdu).

## Les colloques

Entre 2014 et 2017, cinq colloques ont été organisés par l'ANSSI pour les enseignants du supérieur en informatique afin de leur présenter la démarche et d'échanger sur l'intégration de la sécurité dans leurs cours. Plus d'une centaine de personnes venues de toute la France ont ainsi assisté à ces colloques.

Ces rencontres ont été l'occasion de partager le point de vue de l'ANSSI avec les enseignants. En plus de son objectif principal, CyberEdu a d'autres vertus qui peuvent intéresser les enseignants adhérant à la démarche. Tout d'abord, les sujets touchant à la sécurité sont plébiscités par les étudiants (encore plus depuis leur médiatisation auprès du grand public) ce qui aide à capter leur attention. Ensuite, pour comprendre un problème de sécurité, il est généralement nécessaire de bien comprendre le fonctionnement du sujet auquel le problème se rattache. Ainsi, la compréhension des vulnérabilités que peuvent introduire un débordement de tampon requiert des connaissances précises sur la représentation mémoire d'un processus.

Chaque colloque, d'une durée de trois jours, a été l'occasion d'aborder aussi bien des sujets techniques (systèmes d'exploitation, réseau, développement, notions de cryptographie) que juridiques et ont également permis de présenter quelques retours d'expériences.

## L'association

Après cette première phase (2013-2016) menée par l'ANSSI, quelques limites de cette approche ont été constatées. D'une part, il semblait important d'associer durablement des enseignants à cette démarche, puisque ce sont eux les relais au cœur du dispositif. D'autre part, les colloques ont jusqu'à présent été uniquement organisés à Paris, pour des raisons logistiques.

Afin de répondre à ces limitations, l'ANSSI a proposé d'impliquer les enseignants dans la démarche, en commençant par ceux qui avaient suivi les colloques. C'est pourquoi, le 17 mai 2016, l'association CyberEdu a été fondée. Son objectif est de reprendre le flambeau en lien avec l'ANSSI. L'agence continuera en effet de s'impliquer dans la démarche CyberEdu via une participation à divers groupes de travail de l'association.

L'association a pour vocation de porter les missions suivantes :

— maintenir à jour les documents existants et en proposer de nouveaux ;
— proposer des colloques sur l'ensemble du territoire ;

— offrir un forum d'échanges entre spécialistes et non spécialistes de la sécurité ;
— labelliser des formations « CyberEdu » (voir section suivante).

L'association est jeune, mais ces différentes activités se structurent depuis quelques mois. L'actualité de l'association peut être suivie sur le site de l'association [3].

***L'esprit sécurité ?***

*Pour les spécialistes du domaine de la sécurité, certaines habitudes deviennent une seconde nature. Il leur est ainsi naturel d'étudier le comportement d'un programme face à des stimuli non prévus dans la spécification. En effet, l'attaquant n'est pas tenu de respecter les règles du jeu.*

*Même si CyberEdu n'a pas pour objectif de former des spécialistes en sécurité du numérique (mais la démarche peut toujours susciter des vocations !), il est néanmoins nécessaire de détruire certains mythes et d'en finir avec le côté parfois magique de l'informatique.*

*En réseau, un exemple classique est la capture de paquets réseau. Il est en effet toujours intéressant de découvrir la réaction des étudiants face à la quantité de données qui circulent en clair sur le réseau ! Sans cette prise de conscience, comment espérer qu'un administrateur comprenne l'importance des protocoles de sécurité ?*

*Lors du développement d'une application, l'objectif premier est évidemment de livrer un produit fonctionnel dans les délais impartis. Cependant, il arrive trop souvent que les développeurs oublient de tester le comportement de leur application face à des arguments invalides. Il s'agit pourtant d'une source classique de failles de sécurité. Si un utilisateur normal n'a aucune raison d'ajouter un caractère guillemet (") dans le champ* login*, un attaquant essaiera certainement d'introduire de tels caractères, considérés comme spéciaux par de nombreux moteurs de base de données (on parle d'injections SQL, une vulnérabilité très connue, et décrite jusque dans la BD en ligne* xkcd*,* `https://www.xkcd.com/327/`*).*

*L'esprit sécurité, c'est se poser des questions qui vont au-delà du fonctionnel !*

3. `https://www.cyberedu.fr`

## Le label CyberEdu

Afin de mettre en avant les formations incluant des contenus d'initiation à la sécurité du numérique, l'association a lancé au printemps 2017 un dispositif de labellisation.

Le processus de labellisation est le suivant [4] :

— les organismes de formation intéressés remplissent un formulaire et le transmettent par voie électronique. Le formulaire décrit en particulier les contenus de sensibilisation et d'initiation à la sécurité du numérique inclus dans la formation candidate ;

— le dossier est instruit par l'association, qui vérifie que la demande est complète, et peut demander des précisions sur les contenus dispensés ;

— si le label est accordé, l'association publie les informations correspondant à la formation sur son site web ;

— pendant la durée de validité du label, l'organisme de formation s'engage à dispenser les contenus décrits dans le formulaire, selon des dispositions décrites dans une charte.

Attention, ce label, qui sera géré et décerné par l'association, concerne les formations de *non-spécialistes* en sécurité, et ne doit pas être confondu avec le label SecNum*edu*, délivré par l'ANSSI aux formations de *spécialistes* en sécurité du numérique.

## Le futur de CyberEdu

Quelles extensions sont envisagées pour la démarche CyberEdu ? Au-delà des informaticiens, ou plus généralement des acteurs du numérique, il serait en effet logique de s'adresser à des enseignants d'autres disciplines, de communiquer notre message à d'autres populations (professions libérales, acteurs du monde de la santé par exemple), ou encore d'étendre la démarche à l'enseignement secondaire.

Mais avant cela, il faut pérenniser le travail réalisé auprès des enseignants du supérieur dans le domaine du numérique !

Pour la suite, restez à l'écoute sur `cyberedu.fr` !

4. `https://www.cyberedu.fr/pages/labellisation/`