CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Sensibilisation et initiation à la cybersécurité

Le projet CyberEDU

24/03/2016

UNIVERSITÉ DE RENNES 1

ENSSAT LANNION

Patrick ERARD, Ingénieur de recherche, IMT

- Une démarche nécessaire:
  - Pour nos enseignants
  - Pour nos étudiants / la formation tout au long de la vie
  - Pour nos entreprises : l'intelligence économique
  - Pour notre rayonnement
- Un porteur de projet: l'ANSSI
  - Opérateur historique de la SSI en France
  - Un CFSSI musclé, référent en terme de formation des personnels des administrations
  - Une volonté au plus haut de l'état
- Un consortium au départ :
  - Orange Business Services et l'UEB
  - UBO, UBS, Rennes 1, Télécom-Bretagne, Ecole Normale Supérieure Rennes, INSA de Rennes
  - Des béta testeurs :
    - ENSSAT, cours de sensibilisation
    - Rennes 1, cours Système d'exploitation

Les 3 phases de CyberEDU

- Phase 1 : 3 thématiques essentielles et des problèmes évidents
  - Réseau : une gestion des flux qui pose question
    - Des fiches vues comme une progression
  - Systèmes d'exploitation : des systèmes souvent mis à jour…
    - Des thématiques essentielles : gestion de la mémoire / des processus
    - Des systèmes fondamentalement différents : Unix, Windows, BSD…
  - Programmation : il faut que ça marche… mais combien de temps ?
    - Des fiches dans le prolongement de « Mind your language(s) »
    - Une difficulté d'entrer dans les langages…
- Phase 2 : une tranche conditionnelle
  - Des fiches sur la Cybersécurité et Composants Embarqués
  - Des fiches sur l'Authentification
- Phase 3 : création de la communauté CyberEDU
  - Une association d'enseignant spécialistes et non spécialistes cybersécurité
  - Production d'autres fiches : cryptographie, bases de données, Web…
  - Echanges constructifs, y compris avec les spécialistes de l'ANSSI

CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Sensibilisation et initiation à la cybersécurité

Retour d'expérience

24/03/2016

UEB

UNIVERSITÉ DE RENNES 1

ENSSAT LANNION

Jean-Christophe PETTIER, Dir. ENSSAT Bretagne

- **Public** d'élèves-ingénieurs de 1ère année, second semestre
  - spécialités sous statut étudiant en électronique, informatique, **optronique**
  - cours non obligatoire, 20h, 2h/sem de mars à mai, 28 étudiants
  - 4 "modules" (chapitres) avec quizz fourni, découpés en 2 parties
    1) notion de base
    2) hygiène informatique

    } les 3 spécialités

    3) réseau et applicatifs
    4) gestion dans les organisations

    } Informatique + qques Electronique
- **L'enseignant**
  - vierge de toute connaissance particulière cyber-sécurité
    - a assisté séminaire 3j à l'ANSSI en novembre
    - Q/R avec contractant Orange avant chaque module
  - a délivré plusieurs cours sur Systèmes d'Exploitation ← atout
  - proximité avec le Service informatique ← atout
  - envie de délivrer un cours dans un cadre en lien avec l'actualité
- Choix **pédagogiques** :
  - délivrer des compléments de compréhension (fonctionnement Internet, chiffrement)
  - lecture coupures presse en lien avec l'actualité de la semaine
  - favoriser l'interaction pendant le cours (car petit effectif)

Appétence des étudiants

- **Curiosité** sur un sujet d'actualité, veulent (très subjectivement) :
  - savoir si la cyber-délinquance relève du fantasme ou de la réalité ?
  - **comprendre** ← une **difficulté** majeure car il est rarement possible de développer des mécanismes d'attaque autrement que dans les grandes lignes
- **Inquiétude** sur leur propre vulnérabilité
  - très **touchés** par le suicide d'étudiants consécutifs à des chantages sur réseaux sociaux
- Très friands **d'anecdotes**
  - attaques relayés dans les media
  - pratiques du service informatique de l'Ecole
- N'ont pas forcément conscience des **conséquences** de la transformation numérique de la société
  - le **virtuel** peut avoir des **incidences** dans la vie réelle
  - enjeux de protection de la **vie privée**

Les supports

- sont fortement structurés :
  - 4 modules divisés
    - en 3 à 5 sections divisés
      - jusqu'à une dizaine de sous-sections
  - des exemples ← en nombre significatif mais je pense qu'il pourrait en être ajoutés
- livrés avec un quizz à la fin de chaque module ← indispensable de procéder à des sollicitations tous les 2-3 CM
- peuvent être délivrés en 20h avec compléments, exemple :
  - premier quizz préparatoire "à blanc"
  - 5 vidéos de 5 min sur le fonctionnement d'Internet
  - petite dizaine de planches sur le chiffrement asymétrique
- des messages "à retenir" encadrés
- des redites ← mais l'enseignement doit aussi parfois être basé sur la répétition et c'est même indispensable sur **messages prescriptifs forts**
- une **crédibilité** "**professionnelle**" apporté par les "logos" :

orange™ Business Services

⇨ **peu de travail préparatoire**, limité à l'envie de "creuser le sujet" pour se sentir à l'aise face à d'éventuelles questions

Difficultés

- étudiants sont un **public qui n'a pas connaissance des réalités** de l'administration d'un parc de machines :
  - tâches à accomplir
  - commandes

  } la mention de possibilités techniques ne leur parlent pas vraiment (ex : centralisation de l'authentification)
- **contenu très souvent descriptif** sur lequel il y a peu à expliquer

  ⇨ à admettre d'autorité, pas le plus simple à délivrer pour un enseignant...

  ⇨ l'emploi fréquent d'**anecdotes**, si possible lié au quotidien des étudiants, est essentiel
- **même support** pour informaticiens généralistes et potentiellement futurs administrateurs (de nombreux sujets sur l'administration !)

Bilan partiel

- cours délivré à près de 90% à ce jour
- 1er questionnaire "de satisfaction" en ligne, anonyme sur modules ouverts à tous après 1ere moitié **1) notion de base & 2) hygiène informatique**
  - ⇨ taux de retour ~50 % , éléments principaux :
    - 70% ont "*le sentiment d'avoir globalement compris le module"*
    - 54% le "*recommanderaient"*, 46% "*ne se prononcent pas"* mais aucun le *"déconseille"* ! ← objectif "à moitié" rempli, pas de rejet, explicable par public optronique
    - 8% ont découvert "*significativement"*, 80% entre "*raisonnablement"* et "*modérément*"
    - 38% "*se comporteront différemment*", 40% "*ne changeront rien*" ← attention, certains étudiants m'ont paru déjà bien "affutés"
    - 84% "*ont été intéressés*"
    - 72% ont trouvé la forme "*bien adapté*" et "*au bon niveau*"
    - 100% de satisfecit sur évaluation par quizz !

Expérimentation CyberEDU
Systèmes d'exploitation

Bilan

CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Systèmes d'exploitation

Retour d'expérience

24/03/2016

UNIVERSITÉ DE RENNES 1

ENSSAT LANNION

Isabelle PUAUT Professeur Université de Rennes 1

- Cours concerné
  - Cours avancé système d'exploitation niveau M1
  - Volume de cours 80h/annuel : CM, TD, TP
  - Bases sécurité dans le cours : droits d'accès
- Profil des étudiants
  - Parcours « système et réseaux », étudiants ayant un goût pour le « bas niveau » et le « technique »
  - Demandeurs d'enseignements sécurité système

Fiches proposées

- Thématiques
  - Droits spéciaux Linux
    - Droits SUID/SGID, utilisation, failles de sécurité associées, remèdes (30 mn)
  - Eléments de sécurité et virtualisation
    - Virtualisation de systèmes, vulnérabilités connues, remèdes
- Forme
  - Fiche Word ou PDF à analyser et assimiler par la formateur

Bilan global

- Globalement positif
  - Contenu jamais introduit sans CyberEDU
  - Fiches établies en fonction du contenu du cours
  - Tissage d'éléments de sécurité apprécié
  - Renouvellement prévu l'année prochaine
- Points à améliorer
  - Forme des fiches, adaptation au public
  - Réception des fiches / calendrier du cours

Bilan fiche « droits spéciaux »

- Format de la fiche
  - Positif : longueur adaptée, facile à assimiler
  - Négatif : pas assez « prêt à l'emploi » (PPT)
    - ½ journée de montage pour 20 mn de présentation
- Contenu de la fiche
  - Complet sur le sujet
  - Niveau de technicité un peu en deçà de ce qu'attendaient l'enseignant et les étudiants

Bilan fiche « droits spéciaux »

- Avis des étudiants à la suite du cours
  - Positifs : donne des éléments de culture générale
  - Négatif :
    - Manque de moyen de voir les failles de sécu associées « de bout en bout »
    - Auraient apprécié plus de pratique (TP)
    - Un peu trop basique pour le M1
    - Un script en PDF n'est pas adapté, corrigé par la suite
  - Auraient préféré voir des débordements de buffer et l'ASLR

Bilan fiche « virtualisation »

- Contenu de la fiche
  - Très complet, de nombreuses annexes permettant d'aller plus dans le détail
- Format de la fiche
  - Très loin du « prêt à l'emploi »
  - Contenu trop volumineux, pas assez synthétique : délai court, période de surcharge
- Cette fiche n'a pas été jouée
  - Remplacement par exposé « Buffer Overflow »

Fiche alternative « Buffer Overflow »

- Initiative 10kstudents http://10kstudents.eu/
  - Supports pédagogiques « clé en main »
  - Trois niveaux de public joués : « grand public », « informaticien moyen », « informaticien expert »
  - Exercices intégrés
- Bilan
  - Positif : facile à prendre en main, niveau de technicité modulable, très apprécié des étudiants
  - Négatif : aurait mérité des travaux pratiques

CyberEdu

La sécurité par l'enseignement supérieur des NTIC

La communauté c'est vous…

24/03/2016

UNIVERSITÉ DE RENNES 1

ENSSAT LANNION

CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Merci de votre attention

ueb

Université de Rennes 1

ENSSAT Lannion

Télécom Bretagne

Institut Mines-Télécom

rennes

université de bretagne occidentale

UBS Université de Bretagne-Sud

INSA Rennes