Syllabus pour le cours de sensibilisation et initiation à la Cybersécurité

CyberEdu

CyberEdu

La sécurité par l'enseignement supérieur des NTIC

Ce document pédagogique a été rédigé par un consortium regroupant des enseignants-chercheurs et des professionnels du secteur de la cybersécurité.

Version 1.1 — Février 2017

Table des matières

1 Introduction, prérequis **3**

1.1 Objectifs 3

1.2 Prérequis pour les étudiants 3

1.3 Prérequis pour les formateurs 3

1.4 Structure de la sensibilisation 3

2 Contenu de la sensibilisation **3**

1 Introduction, prérequis

1.1 Objectifs

L'objectif de ce cours est de sensibiliser aux menaces et enjeux et d'initier aux principaux concepts de la cybersécurité. Il s'agit de présenter un guide de bonnes pratiques applicables à l'ensemble des professionnels de l'informatique, qu'ils soient en formation ou en activité.

1.2 Prérequis pour les étudiants

Cette initiation est ouverte à tous. Les connaissances de base suivantes faciliteront la compréhension des étudiants, mais ne sont pas impératives :
- Connaissances de base sur les systèmes d'information (biens, fonctionnement, etc.) ;
- Connaissances de base sur le fonctionnement technique des réseaux, des systèmes d'exploitation et des applications (ces connaissances de base seront surtout utiles pour le module 3).

1.3 Prérequis pour les formateurs

Le support est principalement autoporteur, i.e. les diapositives contiennent toutes les informations nécessaires pour faire passer les messages souhaités. Certaines diapositives font également l'objet de commentaires complémentaires (à l'attention du formateur) lorsque le support nécessite une explication supplémentaire avant de le diffuser aux étudiants. Le formateur devrait posséder les compétences suivantes :
- Connaitre le fonctionnement des systèmes d'information ;
- Connaitre le fonctionnement technique et l'architecture des réseaux, des systèmes d'exploitation et des applications.

Il n'est pas demandé au formateur de maitriser le domaine de la sécurité, toutefois être curieux et attentif aux problématiques sécurité présente un avantage certain pour être en mesure de présenter clairement les sujets abordés dans ce cours.

1.4 Structure de la sensibilisation

Module 1	Cybersécurité : notions de base	5 heures
Module 2	Les règles d'hygiène informatique	6 heures
Module 3	Cybersécurité : les aspects réseaux et applicatifs	4 heures
Module 4	La gestion de la cybersécurité au sein d'une organisation	3 heures

Chaque module se termine par un quizz permettant d'évaluer ce que les étudiants ont retenus des enseignements. Un ensemble de références vers des ressources complémentaires (sites Web, documents, statistiques, etc.) est également fourni pour les formateurs et étudiants qui souhaiteraient approfondir certains sujets de cybersécurité.

2 Contenu de la sensibilisation

Ce chapitre détaille les quatre modules d'enseignement, en précisant les objectifs, les thèmes abordés et une estimation de la durée de chacun de ces thèmes.

Module 1	Cybersécurité : notions de base
Durée	5 heures
Objectifs	– Comprendre les motivations et le besoin de sécurité des systèmes d'information – Connaitre les définitions de base et la typologie des menaces

- **Les enjeux de la sécurité des S.I.** - (30 minutes)
  - La nouvelle économie de la cybercriminalité
  - Les impacts sur la vie privée
  - Quelques exemples d'attaques
- **Propriétés de sécurité** - (30 minutes)
  - Disponibilité, Intégrité, Confidentialité, Preuve/Traçabilité
  - Exemples de mécanismes offrant des propriétés de sécurité
- **Présentation des notions de menaces, vulnérabilités, attaques** - (1 heure 15)
  - Notions de « Vulnérabilité », « Menace », « Attaque »
  - Exemple de vulnérabilité lors de la conception d'une application
  - Illustration de l'exploitation d'une vulnérabilité
- **Panorama de quelques menaces** - (1 heure 15)
  - Les principales sources de menaces
  - Hameçonnage & ingénierie sociale
  - Fraude interne
  - Intrusion informatique
  - Virus informatique
  - Déni de service
- **Le droit des T.I.C. et l'organisation de la sécurité en France** - (1 heure)
  - L'organisation de la sécurité en France
  - Le contexte juridique
  - Le droit des T.I.C.
  - Dispositif juridique français de lutte contre la cybercriminalité
  - Protection des données à caractère personnel
- *Quizz partie 1 (notions de base à connaitre)* - (30 minutes)

Module 2	Les règles d'hygiène informatique
Durée	6 heures
Objectifs	– Appréhender et adopter les règles d'hygiène de base de la cybersécurité, pour les organisations et les individus

Présentation les règles d'hygiène informatique pour le monde de l'entreprise, accompagné d'exemples pratiques et complété par des recommandations applicables par le grand public [1].

- **Connaître le S.I** - (25 minutes)
  - Identifier et inventorier les composants du SI
  - Types de réseau et interconnexion
- **Maîtriser le réseau** - (1 heure 20)
  - Sécuriser le réseau interne
  - Accès distant
  - Sécuriser l'administration
  - Wifi
- **Sécuriser les terminaux** - (1 heure 10)
  - Applications et mises à jour logicielles et systèmes
  - Protéger contre les codes malveillants
  - Protéger les données
  - Durcir les configurations
- **Gérer les utilisateurs** - (1 heure 40)
  - Gestion des privilèges
  - Mots de passe et autres moyens d'authentification
  - Sensibilisation des utilisateurs
- **Sécuriser physiquement** - (20 minutes)
- **Contrôler la sécurité du S.I.** - (35 minutes)
  - Contrat de maintenance, d'assurance, de support
  - Surveiller et superviser et gérer les incidents de sécurité
  - Plan de secours
  - Audit
- *Quizz partie 2 (recommandations et bonnes pratiques pour chacun) - (30 minutes)*

1. Les exemples et les recommandations « grand public » intégreront notamment le wifi personnel ou dans les lieux publics, comment réagir face au spam et au phishing, la prise de conscience de la communication de données personnelles, la sécurisation de son ordinateur personnel, la bonne utilisation du navigateur et du « cadenas jaune », la sauvegarde de données, etc. Ces sujets seront traités en filigrane des règles d'hygiène.

Module 3	Cybersécurité : les aspects réseaux et applicatifs
Durée	4 heures
Objectifs	– Comprendre les vulnérabilités inhérentes aux mécanismes réseaux et applicatifs couramment utilisés – Connaitre le panorama des solutions techniques de sécurité

- **La sécurité des protocoles IP, ICMP, TCP, UDP** - (15 minutes)
  - Présentation synthétique des faiblesses inhérentes à ces protocoles
- **Revue d'architectures réseaux (sécurisation)** - (1 heure 15)
  - Pare-feu
  - Répartiteur de charge
  - Anti-virus
  - IDS/IPS (Intrusion Detection & Prevention Systems)
  - VPN (Virtual Private Network) IPsec et SSL
  - Segmentation
  - Exemple pratique de sécurisation d'un réseau
- **Cryptographie** - (1 heure 30)
  - Vocabulaire relatif à la cryptographie
  - Un peu d'histoire (Chiffrement de César, Machine Enigma)
  - Présentation des concepts de chiffrement (symétrique, asymétrique, chiffrement, hashage, signature électronique, certificats et tokens)
  - Présentation des applications pratiques de la cryptographie dans les services et usages quotidiens
- **La sécurité des applications Web** - (30 minutes)
  - Usurpation d'identité via les cookies
  - Injection SQL
- *Quizz partie 3 (mécanismes techniques à connaitre) - (30 minutes)*

Module 4	La gestion opérationnelle de la cybersécurité au sein d'une organisation
Durée	3 heures

Objectifs	– Appréhender les méthodes et normes de prise en compte de la sécurité :
	  – de façon globale au sein d'une organisation dont l'activité est supportée par un système d'information
	  – de façon plus unitaire au sein des projets, une activité étant gérée en mode projet
	– Comprendre et anticiper les difficultés couramment rencontrées dans la gestion de la sécurité dans une organisation
	– Présenter les filières métiers de la cybersécurité dans l'environnement d'exercice de leur fonction au sein des organisations

- **Intégrer la sécurité au sein d'une organisation à travers une présentation synthétique de la famille des normes ISO/IEC 27000, notamment** - (45 minutes)
  - Préambule de présentation du chapitre
  - Panorama des normes ISO 27000
  - Système de Management de la Sécurité de l'Information (27001)
  - Code de bonnes pratiques (27002)
  - Gestion des risques (27005)
  - Classification des informations
  - Gestion des ressources humaines
- **Intégrer la sécurité dans les projets** - (45 minutes)
  - Préambule de présentation du chapitre
  - Prise en compte de la sécurité dans le cycle de vie d'un projet
  - Contre-exemple de prise en compte en fin de développement
  - Approche par l'analyse et le traitement du risque
  - Plan d'action SSI : la défense en profondeur
- **Les difficultés couramment rencontrées dans la prise en compte de sécurité** - (30 minutes)
  - Compréhension insuffisante des enjeux
  - Implication nécessaire de la direction
  - Difficulté de faire des choix en toute confiance
  - Arbitrage délicat entre commodité et sécurité
  - Suive l'évolution des technologies
  - Frontières floues entre sphères professionnelle, publique et privée
- **Présentation de métiers liés à la cybersécurité** - (30 minutes)
  - Positionnement des métiers au sein des organisations
  - Cartographie des métiers et compétences
  - Profils et carrières
  - Perspectives d'embauche
- *Quizz partie 4 (l'organisation de la sécurité) - (30 minutes)*

Ce document pédagogique a été rédigé par un consortium regroupant des enseignants-chercheurs et des professionnels du secteur de la cybersécurité.

Version 1.1 — Février 2017