Formation et SSI

Éric Jaeger, ANSSI/SDE/CFSSI

Colloque ARCSI du 25 janvier 2014, École Militaire

Plan

Parmi les missions de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un service à compétence nationale créé par le décret n° 2009-834 du 7 juillet 2009

- Autorité nationale en matière de SSI, à ce titre [. . .] elle assure la formation des personnels qualifiés dans le domaine de la SSI
- L'ANSSI favorise la prise en compte de la sécurité dans les développements des TIC

Site web : `www.ssi.gouv.fr`

Le centre de formation à la SSI

La sous-direction expertise (SDE) de l'ANSSI doit notamment favoriser l'élévation de compétences [...] par la formation [...] ; le centre de formation à la SSI (CFSSI), qui lui est rattaché, développe et met en œuvre la politique formation de l'ANSSI

- Recensement des titres cybersécurité de niveau master
- Relations avec les établissements de formation cybersécurité
- Stages SSI au profit des agents de l'Administration
- Formation « Expert en Sécurité des Systèmes d'Information »
- Intégration de la SSI dans les formations en informatique

Site web : `www.ssi.gouv.fr/cfssi`

Plan

Cybersécurité

- état recherché [...] permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données [...] et des services
- fait appel à des techniques de sécurité des systèmes d'information [...] et sur la mise en place d'une cyberdéfense [*i.e.*] d'un ensemble de mesures techniques et non techniques

Vision fonctions ou sécurité (1/3)

Exemple d'une question visant non pas à évaluer des connaissances mais à mettre en évidence différents « modes » de pensée

> *Parmi les commandes suivantes, lesquelles sont susceptibles (sans redirection) de provoquer la destruction de données d'un fichier ?*
>
> `ls` ☐ `cd` ☐ `cp` ☐ `cat` ☐ `rm` ☐ `mv` ☐

Au moins deux lectures

- Fonctionnelle : la question est interprétée « *Comment détruire les données d'un fichier ?* », la réponse donnée se limite à `rm`
- Sécurité : si on cherche à protéger les données, les commandes dangereuses sont `rm` mais aussi `cp` et `mv`

Vision fonctions ou sécurité (2/3)

Un autre exemple dans le domaine des protocoles réseaux

- Un paquet *IP* comporte les adresses source et destination
- Un courriel comporte les champs `TO` et `FROM`
- ...

Dans une vision fonctionnelle, il faut rendre le service (acheminer l'information), seule la destination est importante

Dans une vision sécurité, il est facile de comprendre que les informations relatives à l'émetteur ne sont ni exploitées, ni vérifiées

- *Spoofing* d'adresse *IP*
- Falsification du champ `FROM` pour un courriel

Vision fonctions ou sécurité (3/3)

Un dernier exemple concernant les formats de fichiers compressés

Deux façons d'appréhender un logiciel de décompression

- Bon fonctionnement : le logiciel doit décompresser correctement les fichiers compressés
- Robustesse : aucun comportement indésirable ne peut être provoqué par un fichier forgé (incohérent)

Ces deux approches sont distinctes [1] qu'il s'agisse de spécifier, de développer ou encore de tester le logiciel

1. et en réalité complémentaires...

Quelques orientations

Ces exemples techniques révèlent que la sécurité est souvent orthogonale aux considérations fonctionnelles usuelles

Dans ces conditions, une formation à la sécurité des systèmes d'information quelles que soient ses ambitions devrait veiller à

- Encourager le développement d'une vision sécurité
- Aborder tous les domaines, techniques ou non
- Être cohérente
- Proposer une approche en profondeur (ce qui nécessite une réelle culture dans les domaines connexes)

Ces différents points sont à apprécier en fonction du contexte et des métiers (tout en limitant les dérives ≪ offensives ≫)

Plan

Responsable SSI en administration centrale

Stage de 5 jours pour sensibiliser aux problématiques liées à la SSI et aborder les principales notions, réglementations et mesures, afin de faire prendre conscience de l'importance de la fonction RSSI et fournir des méthodes utiles à la fonction

- Stratégie : enjeux, architecture gouvernementale
- Planification : réglementation (dont RGS), principes, PSSI, RSSI dans les projets, gestion du risque
- Réalisation : mesures pratiques, externalisation, labellisations
- Vérification : CERT, journaux, traitement des incident, audits
- Amélioration : nouveaux risques, tableaux de bord, guide GISSIP, exercices

Plan

Le titre ESSI

Le titre « Expert en sécurité des systèmes d'information » (ESSI) est enregistré [2] comme titre de niveau I au Registre national des certifications professionnelles (RNCP)

- Successeur du BESSSI
- L'enregistrement nécessite la formalisation d'un référentiel métier, dont une version détaillée est publiée sur le site de l'ANSSI sous l'intitulé « Architecte référent en SSI »

Il n'est délivré que par le directeur général de l'ANSSI mais est accessible *via* trois parcours actuellement

- Formation ESSI délivrée par le CFSSI
- À certains ingénieurs diplômés de Télécom SudParis
- Validation des acquis de l'expérience (VAE)

2. En réalité, la demande de renouvellement est en cours de traitement

Référentiel métier ESSI (1/2)

1 Connaître et formaliser les besoins de sécurité

(a) Être conscient des enjeux de la sécurité et prendre en compte toutes les dimensions de la problématique SSI

(b) Être capable de mener, de manière formelle, l'analyse d'un projet relatif à un système d'information complexe afin d'identifier les besoins en sécurité, les menaces et les risques, et d'en déduire les objectifs de sécurité

(c) Être capable de conseiller ou de convaincre un donneur d'ordre dans le domaine de la SSI

2 Élaborer un dispositif technique répondant aux besoins de sécurité

(a) Comprendre les problématiques de sécurité, notamment connaître et savoir identifier les risques liés à un système d'information par domaine ou de manière globale

(b) Comprendre les forces et faiblesses des produits de sécurité, notamment ceux mettant en œuvre des mécanismes cryptographiques

(c) Être capable de définir une solution technique pour défendre un système d'information selon les grands axes de la défense en profondeur

(d) Être capable de faire des recommandations relatives à la SSI auprès d'un spécialiste technique d'un système d'information

Référentiel métier ESSI (2/2)

3 Savoir estimer et faire estimer le niveau de sécurité d'un dispositif ou système d'information

(a) Estimer soi-même le niveau de sécurité d'un système d'information

(b) Connaître les différentes modalités d'un audit et savoir le préparer

(c) Savoir prendre en compte les résultats d'un audit, élaborer et conduire un plan d'action

(d) Savoir établir une démarche d'homologation et bien la conduire

4 Gérer la sécurité d'un système d'information

(a) Être un interlocuteur auprès des acteurs du projet, des spécialistes informatiques, des administrateurs et des RSSI

(b) Maintenir le niveau de sécurité du système d'information, adapté aux contraintes métier

(c) Savoir formaliser les documents SSI

(d) Savoir veiller sur les dernières vulnérabilités, menaces et produits de sécurité et savoir les analyser

(e) Évaluer les impacts d'une vulnérabilité ou d'une menace

(f) Savoir détecter et gérer un incident de sécurité

La formation ESSI du CFSSI

Une formation gratuite, réservée aux agents de la fonction publique et aux militaires (habilités), d'une durée de 13 mois

- Un enseignement de 7 mois, 650 heures de cours et TP
- Un stage de 6 mois en milieu professionnel

Autant que possible, le CFSSI veille à ce que la formation ESSI

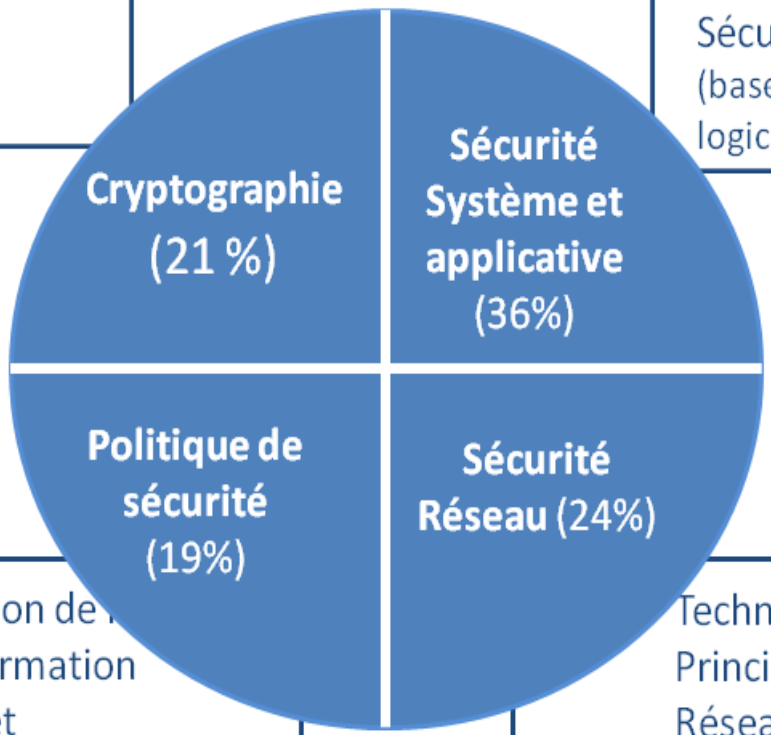
- Encourage le développement d'une vision orientée sécurité
- Propose une approche en profondeur
- Soit cohérente
- Aborde les multiples domaines de la sécurité

En pratique, elle est dense et ambitieuse

Programme de la formation ESSI

Cryptographie
Mathématiques
IGC

Sécurité système
Sécurité applicative
(base de donnée, sécurité logicielle, ...)



Système de gestion de
sécurité de l'information
Gestion SSI Projet
Droit, réglementation, normes
Analyse de risque, EBIOS
Audit théorie et pratique
Système de détection
Traitement des incidents de sécurité

Technologie IP
Principaux protocoles
Réseaux opérateurs
Architecture « classifiée »
Architecture Web
Protocole d'authentification
Réseau sans fil
Pratiques

Plan

Quelques préalables

Communication du conseil des ministres, 25 mai 2011

> *La SSI sera incluse dans les formations supérieures, en commençant par les formations scientifiques et techniques, afin que l'ensemble des étudiants acquièrent un socle commun de connaissances et de bonnes pratiques dans ce domaine.*

Discours de Patrick Pailloux, conférence de clôture des Assises de la SSI 2011

> *J'appelle les écoles d'ingénieurs et les universités à inclure dans leurs formations les règles d'hygiène informatique élémentaires. Un projet informatique rendu avec des mots de passe en dur mérite zéro. Là encore nous allons publier un certain nombre de recommandations.*

Quelques préalables

Feuille de route du Gouvernement sur le numérique, 28 février 2013

> *Un volet SSI sera intégré à toutes les formations supérieures aux métiers du numérique.*

Livre blanc sur la défense et la sécurité nationale, avril 2013

> *Il importe également d'accroître le volume d'experts formés en France et de veiller à ce que la sécurité informatique soit intégrée à toutes les formations supérieures en informatique.*

Enjeux

Ne pas faire reposer la sécurité que sur des experts, en s'assurant que chaque acteur du SI soit concerné et impliqué

- Prévenir l'apparition des vulnérabilités plutôt que d'attendre de l'infrastructure qu'elle apporte des réponses (palliatives)
- Élever le niveau de vigilance et la pertinence des réactions face à des incidents

Idéalement, chaque formation supérieure en informatique en France devrait donc intégrer la cybersécurité

- S'assurer que tout informaticien ait suivi une sensibilisation, une initiation ou une formation au niveau approprié
- Il ne s'agit pas de former des experts en sécurité !

Orientations

Quelques points délicats, parmi d'autres

- Quels sont les sujets à aborder, pour quel auditoire ?
- Comment les intégrer dans un contexte très contraint ?
- Proposer des modules dédiés ou adapter l'existant ?

Principales orientations envisagées

- Convaincre plutôt que (tenter d')imposer
- Travailler avec les établissements de formation
- Élaborer et proposer guides pédagogiques, supports, *etc.*
- Traiter la question de la formation des enseignants

L'ANSSI devrait prochainement communiquer et publier en ce sens

Merci pour votre attention

Avez-vous des questions ?