PSSI, SMSI : de la théorie au terrain

Plan

- Introduction : nécessité de la SSI
- Problématiques en SSI
- Cadre légal, réglementaire, normes
- Pilotage de la SSI : de la théorie au terrain
- Expérience SSI à Subatech
- Perspectives

Nécessité de la SSI

- L'impact d'une atteinte au système d'information est potentiellement grave :
  - Légal : responsabilité des tutelles engagée
  - Financier : perte de matériel ou de données coûteuses, voire impossible à reconstruire, perte de brevets
  - Image de marque du labo et des tutelles, compétition scientifique
  - Atteinte à des personnes
  - Activités de l'unité paralysées

Nécessité de la SSI (2)

- Enjeux par catégorie :
  - Disponibilité :
    - données, applications
    - serveurs, réseau
    - infrastructure : alimentation électrique, climatisation
  - Intégrité (données, systèmes)
  - Confidentialité (données)
  - Imputation, non-répudiation (preuves)

Approche par les risques

- L'approche par les risques (analyse de risques) est naturelle et préconisée
  - Savoir quoi protéger (actifs/assets)
  - Connaître les menaces
  - Estimer l'impact et la probabilité d'occurence
  - Liste de scénarii avec valeur de risques
- L'analyse de risques est mentionnée dans la loi
  - Preuve formelle d'un effort de sécurisation dans le cadre d'une obligation de moyens

Problématiques en SSI (1)

- SSI traditionnelle : réaction des ASR face à leur propre perception des risques
  - Pragmatique mais pas forcément alignée sur les risques réels
  - Peut oublier de prendre en compte les besoins des utilisateurs
  - Peut sous-estimer le facteur humain (mesures essentiellement techniques)
  - N'implique pas la direction (pourtant responsable de la SSI)
  - Risque d'oublier les aspects d'organisation et de sécurité de l'information au delà du SI.

Problématiques en SSI (2)

- Un contexte de plus en plus difficile :
  - Nomadisme et confusion des sphères professionnelles et privées
  - Des applications complexes (sécurité navigation Web par ex.)
  - Des parties du SI qui échappent au contrôle du service informatique, intrusion de matériels non gérés (BYOD)
  - Une offre alléchante d'applications/logiciel « gratuits » mais peu ouverts voire carrément suspects
  - Moyens humains et financiers toujours plus limités
  - Cyber-criminalité de plus en plus organisée
  - Concurrence économique internationale

Cadre légal, réglementaire

- Exigences légales :
  - Loi informatique et libertés
  - Conservation des traces
  - [...]
- Dispositions au niveau de l'Etat
  - PPST, RGS, PSSI-E
- Dispositions SSI des tutelles
  - Chartes, chiffrement, recommandations

Outils, méthodes, normes

- Les méthodes d'analyse de risques :
  - MEHARI, EBIOS
- Normes :
  - ISO27001
- Méthodes de « management »
  - Pilotage de type PDCA (*) de la SSI : le SMSI

(*) PDCA : Plan – Do – Check - Act

Le SMSI comme outil de pilotage

- Objectif : alignement des mesures sur la stratégie du labo et des tutelles, sur les risques, les exigences légales et réglementaires
- Principaux processus (7 à 9 selon les normes) :
  - Analyse de risques
  - Traitement du risque (plan d'action, mesures)
  - Contrôle de l'efficacité des mesures
- Fonctionnement cyclique
- Pas exclusivement une affaire d'informaticiens
- Analogue à une démarche « qualité »

De la théorie au terrain :
Au pied du mur !

- EBIOS, SMSI et ISO27001 : trop lourd pour un labo ?
- Analyse de risques : Exhaustivité ? Généricité ? Sur les actifs les plus précieux/exposés ?
- Court-circuiter l'analyse de risques par une sélection de mesures de sécurité « qui tombent sous le sens » ?
- Mise en oeuvre des mesures : comment évaluer l'état de mise en oeuvre ?
- Référentiel de mesure ISO27002 : formulation trop généraliste ? Comment relier à la réalité ?
- Evaluer l'efficacité des mesures ?

L'essentiel en quelques points

- Rechercher les actifs qui sortent de l'ordinaire et les traiter spécifiquement (analyse de risques limitée)
- Pour le reste, démarche générique
- Plan d'action des choses à corriger ou améliorer
- Rendez-vous annuel pour un regard critique sur le travail de l'année passée
- Lien avec la direction (rendez-vous annuel ?)
- Enregistrements (incidents SSI)
- Documentation minimale : CR réunion annuelle, plan d'action

Expérience SSI à Subatech

- Historique
  - Oct.2009 : Décision directeur de créer un comité de pilotage de la SSI animé par le CSSI (6 personnes)
  - [2010-2011] : Analyse de risques et validation (Fev.2013) par la direction d'un plan de traitement des risques
  - [2011-2012] : Rédaction, validation et publication (Avr.2012) de la PSSI
  - [Sep.2013] : DdA : liste de mesures destinées à couvrir les risques identifiés (80 mesures sur 133 de ISO27002)
  - En cours : Mise en oeuvre des mesures (estimation de l'état de mise en oeuvre) et indicateurs

Calendrier annuel SSI

- Période de référence : 1er Decembre – 30 Novembre
- Réunion annuelle de réexamen début décembre (basée sur 3 rapports : opérationnel, contexte et pilotage)
- => Nouveau plan d'action de l'année
- Rapport d'activité du CPSI remis à la direction et demande de rendez-vous annuel en début d'année (Janvier)
- [Projet] Séminaire interne SSI sur les incidents/résultats de l'année précédente (Février)
- Reste de l'année : mise en oeuvre du plan d'action Réunions mensuelles ~1h30

Expérience SSI à Subatech

- Difficultés rencontrées
  - Analyse de risques : estimation des impacts et probabilité, sentiment d'arbitraire, influence du résultat
  - Compréhension mesures ISO et rapprochement avec nos propres mesures
  - Comment évaluer l'état de mise en oeuvre d'une mesure ISO ?
  - Capacité à réexaminer les risques, prendre en compte les changements

Anatomie d'une règle ISO27002

10.4.1 Mesures contre les codes malveillants

Mesure

Il convient de mettre en oeuvre des mesures de détection, de prévention et de récupération pour se protéger des codes malveillants ainsi que des procédures appropriées de sensibilisation des utilisateurs.

Préconisations de mise en oeuvre

Il convient de fonder la protection contre les codes malveillants sur les logiciels de détection/réparation de code malveillant, la sensibilisation à la sécurité et les mesures adéquates de gestion des modifications et de l'accès au système. Il convient d'envisager les directives suivantes:
a) établir une politique formelle prohibant l'utilisation de logiciels non autorisés (voir 15.1.2);
b) établir une politique formelle indiquant les mesures de protection qu'il convient de prendre pour se protéger des risques liés aux fichiers et logiciels obtenus aussi bien depuis ou via les réseaux externes que sur tout autre support;
c) mener des réexamens réguliers des logiciels et du contenu des données des systèmes traitant des processus critiques pour l'activité; il convient de conduire une enquête formelle sur la présence de tout fichier non approuvé ou de modifications non autorisées;
d) l'installation et la mise à jour régulière, comme mesure de précaution ou tâche de routine, des logiciels de détection/réparation de code malveillant pour analyser les ordinateurs et les supports; il convient que les contrôles réalisés comprennent les tâches suivantes:
1) vérification avant usage de l'absence de code malveillant dans tout fichier stocké sur un support électronique ou optique, ou reçu via les réseaux;
2) vérification avant usage de l'absence de code malveillant dans les pièces jointes et les fichiers téléchargés; il convient de mener cette vérification à différents endroits, par exemple sur les serveurs de messagerie électronique, les ordinateurs de bureau et à l'entrée du réseau de l'organisme;

Document Mise en oeuvre

ISO 10.4.1

Références:
DdA
Analyse de Risques : R02 ,R03,R18,R19,R20,R43,
Mesures : Mes14,Mes41,Mes71,Mes20,Mes55,Mes120,Mes122,Mes123

Mise en oeuvre

Ref	Mesure	Retenu	Etat
10.4.1-01	Prohiber l'utilisation de logiciels non autorisés	Oui	OK
10.4.1-02	Protection contre les fichiers et logiciels obtenus via réseau ou périphériques USB (clés, disques, etc.). Antivirus	Oui	OK
10.4.1-03	Détecter sur les systèmes critiques les modifications anormales	Oui	WARNING
10.4.1-04	Installation et mise à jour régulière anti-virus	Oui	OK
10.4.1-05	Signalement par les utilisateurs des anomalies de comportement	Oui	OK
10.4.1-06	Prévoir la récupération (dispo/données) en cas d'attaque virale	Oui	OK
10.4.1-07	La veille technologique sur les vulnérabilités et les virus	Oui	OK
10.4.1-08	La vérification des sources d'information	Oui	OK
10.4.1-09	La combinaison de deux mécanismes anti-virus différents	Oui	WARNING
10.4.1-10	L'adoption de règles quant à la connexion de supports externes	Oui	WARNING
10.4.1-11	Sensibilisation utilisateur à la protection du poste de travail	Oui	OK
10.4.1	Etat de mise en oeuvre (calcul 2)		73%

Document Mise en oeuvre (2)

Détail de la mise en oeuvre

10.4.1-01 - Prohiber l'utilisation de logiciels non autorisés

L'interdiction d'installer des logiciels provenant de sources non sûres doit apparaître clairement au niveau de la Charte Inforamtique et de la Politique de Sécurité (PSSI). C'est le cas (PSSI paragraphe 7.5.4). Le personnel doit être conscient de cette interdiction, y compris les nouveaux arrivants.
Etat : OK

Indicateurs

- Permettent d'apprécier l'efficacité d'une mesure
- Généralement basés sur des enregistrements

Indicateurs (2)

2. Tableau des indicateurs

Période : du 1/12/2012 au 30/11/2013
Situation au : 30/11/2013

Ref	Libellé	Valeur	Statut
ENR-0011	Une réunion de réexamen du SMSI s'est tenue il y a moins d'un an	14/12/2012	OK
ENR-0021	Le CPSI s'est réuni régulièrement durant l'année précédente	10	OK
ENR-0022	La participation des membres du CPSI est soutenue	77%	OK
ENR-0023	Existence d'un CR pour chaque réunion	100%	OK
ENR-0024	Rapport d'Activité de l'année précédente	Vrai	OK
ENR-0025	Réunion avec la direction	Vrai	OK
ENR-003	Nombre d'incidents	32	
ENR-0031	Nombre de vols ou de pertes de supports de données	3	
ENR-0032	Nombre de compromissions d'origine virale	9	
ENR-0041	Taux d'ordinateurs portables chiffrés	35%	WARN
ENR-0042	Nombre de mots de passe de plus de 2 ans	70	CRIT
ENR-0051	Nombre de messages de sensibilisation envoyés	7	OK
ENR-0052	Nombre de formations « nouveaux entrants »	0	CRIT
ENR-0053	Nombre de séminaires de sensibilisation SSI	1	OK

Expérience SSI à Subatech

- Bilan et état actuel
  - Meilleure implication du personnel (à travers les membres du CPSI), de la direction
  - Prise de conscience que la sécurité dépend plus du comportement des utilisateurs que des techniques mises en oeuvre par le service informatique => sensibilisation !
  - Tentative d'intégrer un volet SSI à chaque nouveau projet du laboratoire
  - Des documents de référence pour les ASR (politique écrite, procédures)
  - Crédibilité renforcée en interne et en externe (réseaux RSSI CNRS, partenaires)

Perspectives

- Des PSSI au niveau de l'Etat et des tutelles :
  - PSSI-CNRS : PSSI Générale, PSSI-Opérationnelle pour les laboratoires : essentiellement une Déclaration d'applicabilité
- Mettre en oeuvre les mesures et prouver qu'on l'a fait
- Mesure de l'efficacité
- La sensibilisation des utilisateurs reste le défi le plus important

Questions ?

Liens :

Site RSI CNRS (ARESU/Securité) :
https://aresu.dsi.cnrs.fr/spip.php?rubrique16

ISO27000
http://fr.wikipedia.org/wiki/ISO/CEI_27001

SMSI
http://en.wikipedia.org/wiki/Information_security_management_system
(l'article en anglais est plus élaboré)