Pilotage de la SSI et PSSI-CNRS

Jean-Michel BARBET, Laboratoire Subatech

Journées Informatiques IN2P3/IRFU Paris Novembre 2021

Plan

- Un peu d’histoire :
  - Formation SIARS 2009 : Management de la SSI : SMSI
  - Création du CPSI au laboratoire Subatech
  - Premiers travaux (analyse de risques, PSSI)
  - Analyse de risques ?
- Les éléments clé du pilotage de la SSI
- PSSI-CNRS
- Sensibilisation
- Adaptation
- Conclusion

Formation SIARS 2009

- Déclinaison en région d'une formation nationale
- Roscoff septembre 2009 (R.Longeon, F.Morris and al.)
- EBIOS [1], normes ISO 27000, SMSI [2]
- Démarche très formelle et très lourde
- Des points intéressants, néanmoins :
  - Périmètre et formalisation des rôles
  - l'amélioration continue (roue de Deming)
  - Les traces écrites et l'auditabilité

Création du CPSI

Subatech

Laboratoire de physique subatomique et des technologies associées

Unité Mixte de Recherche 6457
École des Mines de Nantes - IN2P3/CNRS - Université de Nantes

Le Directeur Jacques Martino	**NOTE**	Le 26 octobre 2009

Objet : mise en place du comité en charge du pilotage de la sécurité de l'information (CPSI)

Notre laboratoire est un établissement classé ERR (Etablissement à Régime Restrictif) compte tenu des activités nucléaires qui y sont poursuivies, et des collaborations que nous avons développées.

Ce classement nous impose un certain nombre de devoirs liés à la sécurité en général, et informatique en particulier. Sur ce dernier point j'ai décidé que cette sécurité informatique était le mieux placée sous la houlette du CNRS et des prescriptions associées.

Dans ce cadre, il nous est demandé de mettre en place une politique précise et bien définie de sécurité informatique (et de l'information), sous la responsabilité d'un agent bien identifié.

Comme CSSI (correspondant pour la sécurité des systèmes d'information) j'ai nommé, avec son accord, Jean-Michel Barbet. Pour définir la PSSI (politique...) associée à notre laboratoire, il m'a proposé la mise en place d'un comité (CPSI) dont la mission sera de faire vivre la politique de sécurité des systèmes d'information, et de m'en proposer au fil de l'eau les inflexions requises.

[...]

Le CPSI

- Objectif 1 : Rédiger la PSSI du laboratoire
- Objectif 2 : « Piloter » la SSI au laboratoire
- Impliquer diverses catégories de personnel
- Petit groupe : 6 personnes : chercheurs, ITA, service SMART, direction, service informatique
- Réunions mensuelles
- Espace web intranet pour le laboratoire
- Espace documentaire privé (web) pour le CPSI

Le CPSI dans l'intranet labo

Laboratoire SUBATECH - Sécurité de l'Information
[Intranet] Pages réservées aux membres du Laboratoire SUBATECH

Sécurité de l'Information

Note: L'accès aux liens précédés de la mention *[prive]* est réservé aux membres du Comité CPSI.

Conformément à la politique de sécurité de l'information du CNRS, il est demandé au Laboratoire de définir et mettre en oeuvre sa propre politique dans ce domaine. La direction du laboratoire s'est engagée dans ce sens en nommant un Correspondant pour la Sécurité des Systèmes d'Information (CSSI) [1]. Le pilotage de la Sécurité de l'Information au laboratoire a été confiée à un comité nommé Comité de Pilotage de la Sécurité de l'Information (CPSI) [2].

Comité de Pilotage de la Sécurité de l'Information

Le Comité à pour tâches :

1. Conduire une étude visant à définir la Politique de Sécurité des Systèmes d'Information du Laboratoire (PSSI),
2. Faire évoluer cette politique au cours du temps.

Le comité se compose actuellement (depuis avril 2016) de :

1. Mickaël Bailly (SMART)
2. Jean-Michel Barbet (CSSI)
3. Jean-Luc Beney (Directeur technique)
4. Stéphane Bouvier (Service Electronique)
5. Khalil Chawoshi (Service Informatique)
6. Philippe Pillot (Chercheur)

Avancement du projet

Mars 2021 : Décision de mise en oeuvre de la PSSI CNRS [11]
Janvier 2021 : Le CPSI travaille sur une nouvelle PSSI CNRS [10]
Octobre 2017 : Une nouvelle version de la PSSI (v1.2) a été validée par le directeur
Février 2016 : Une nouvelle version de la PSSI (v1.1) a été validée par le directeur
11 Mai 2012 : La PSSI v1.0 validée par le directeur et a été présentée au conseil du laboratoire.

Documents Validés

- **Politique de Sécurité des Systèmes d'Information (PSSI)**
- **[New]** Sous-Politique : Politique de sécurité de l'information pour les télétravailleurs
- **[New]** Sous-Politique : Accès au Système d'Information depuis Dispositifs Nomades Personnels

Le CPSI dans l'intranet labo

- Responsabilités
- Fiche A4 Fr/En
- Présentations
- Rapports activité
- Textes de référence

- Sous-Politique : Gestion des Acces au Systeme d'Information
- Sous-Politique : Gestion des Incidents
- Sous-Politique : Sauvegarde
- Sous-Politique : Chiffrement
- Politique du Système de Management de la Sécurité de l'Information (SMSI)
- Fiches Responsabilités SSI
- Fiche A4 Information SSI

Présentations

- Séminaire: *Cybersécurité: Apprenez à vous protéger des menaces* Régis Dubrulle, Octobre 2021
- Séminaire *Sécurité et vie privée sur le web: le navigateur web* Vincent Mazenod, 27 Novembre 2020
- Séminaire *Messagerie électronique et sécurité* Benoit Delaunay, 8 Février 2019
- Séminaire *Vol de votre ordinateur portable : prévenir, réagir, surmonter* Mariangela Settimo, 1er Décembre 2017
- Séminaire *Offres et utilisation des espaces de stockage informatique* Jean-Luc Béney, 8 Juin 2017
- Séminaire *Certificats Electroniques* Jean-Michel Barbet, 8 Décembre 2016
- Séminaire *La sécurité des systèmes de l'information: Tout dépend de vous!* par Thierry Mouthuy, 2 Décembre 2015
- Présentation Charte CNRS 2014, 30 Avril 2015
- Séminaire *Mon Mobile, moi et mon boulot* par Serge Bordères, 9 Décembre 2014
- Responsabilités SSI réunion chefs de groupe, 24 Octobre 2013
- CPSI, Journées du Labo, St-Jean de Monts, Juin 2013
- Présentation PSSI au Conseil de Laboratoire, 11 Mai 2012
- Sécurité Informatique, Journées du Labo, Guidel, Mai 2011

Activité

- Rapport d'Activité du CPSI 2020
- Rapport d'Activité du CPSI 2019
- Rapport d'Activité du CPSI 2018
- Rapport d'Activité du CPSI 2017
- Rapport d'Activité du CPSI 2016
- Rapport d'Activité du CPSI 2015
- Journal de l'activité du CPSI depuis sa création

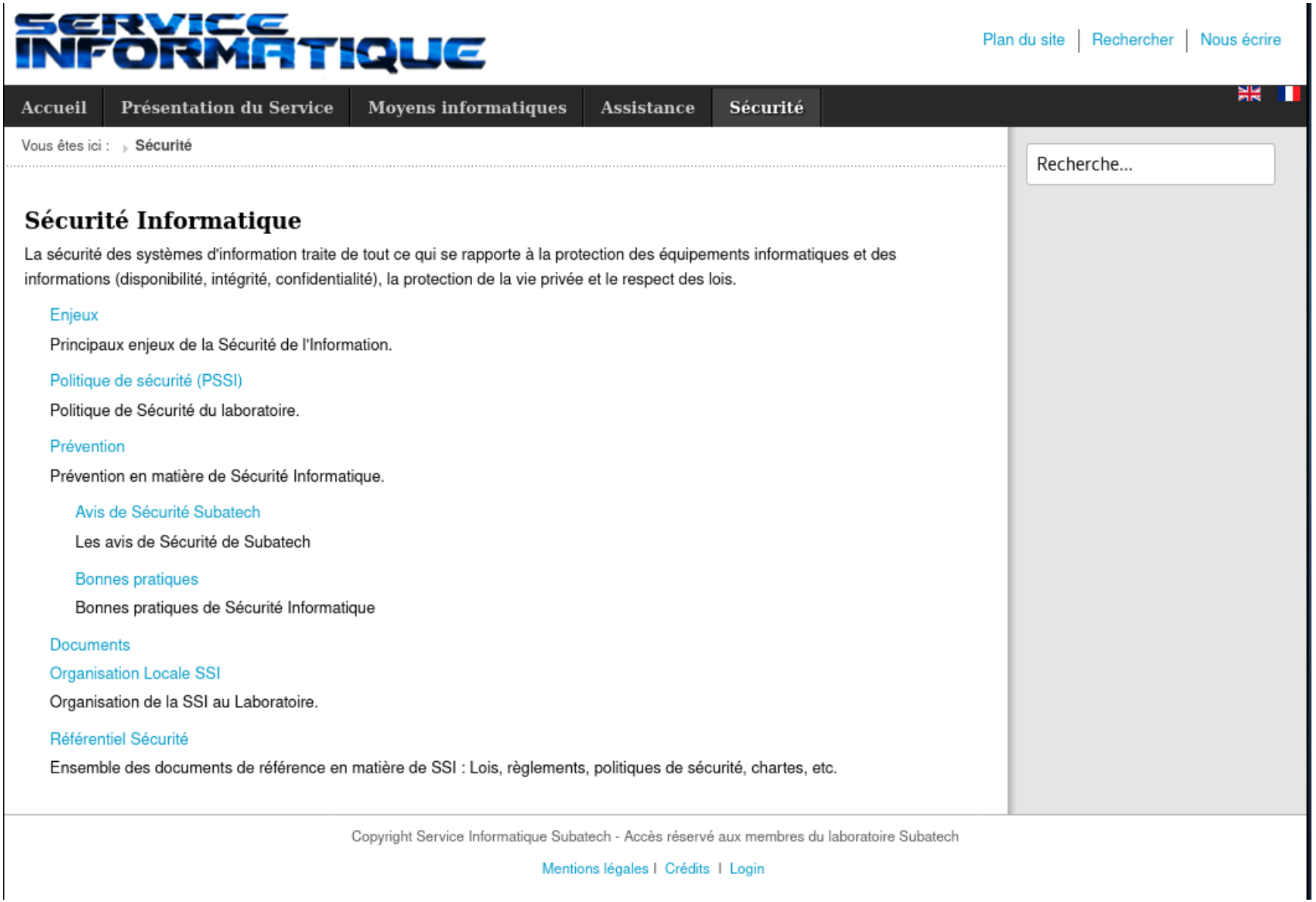
Références

- [1] Décision DEC131018DR17 : Nomination CSSI Subatech
- [2] Note de Service Mise en place du Comité CPSI
- [3] Pages Sécurité sur l'Intranet du Service Informatique
- [4] Décision DEC133249DAJ : Approbation Charte SSI CNRS 2014
- [5] Charte SSI CNRS 2014 Français
- [6] CNRS ISS Charter 2014 English
- [7] NOT15YDSI-RSSIC sur le Chiffrement (21 décembre 2012)
- [8] Courrier aux DU sur le chiffrement des ordinateurs et protection des smartphones professionnels (30 novembre 2018)
- [9] Note 20191220 relative aux annuaires des sites internet institutionnels du CNRS
- [10] Mise en oeuvre de la PSSI du CNRS (A.Petit PDG CNRS Octobre 2019)
- [11] Décision de mise eu oeuvre de la PSSI du CNRS et niveau de sensibilité, conseil de laboratoire du 9 Mars 2021

Zone de travail du comité CPSI

[prive] Zone Reservee aux membres du CPSI

Service informatique



Piloter la SSI = SMSI ?

- Un « système de management » (concept ISO 9000)
- Basé sur 7 processus :
  - Pilotage
  - Analyse de risques
  - Traitement du risque
  - Conformité
  - Incidents
  - Sensibilisation
  - Documentation

La Roue de Deming et l'amélioration permanente…

- Application de « la roue de Deming [3] » à chaque processus

Espace de travail du CPSI

[CPSI] Documentation du SMSI

L'accès à cette zone est strictement réservée aux membres du CPSI

---

26 Janvier 2015 : bascule de la documentation sur la nouvelle organisation suivant les processus du CPSI.

Raccourcis pour l'acces aux principaux documents :

- Reunions
- Actions

Name	Last modified	Size	Description
Parent Directory		-	
01-Pilotage/	09-Sep-2016 15:25	-	
02-Analyse-Risque/	29-Apr-2019 09:34	-	
03-Traitement-Risque/	08-Aug-2019 16:55	-	
04-Controle-Efficacite/	09-Jan-2019 11:13	-	
05-Gestion-Incidents/	10-Sep-2019 16:19	-	
06-Formation-Sensibilisation/	25-Apr-2014 11:46	-	
07-Documentation-Preuves/	22-Jan-2019 10:52	-	

Premiers travaux

- Définir le « périmètre du SMSI » !
- La méthode EBIOS préconise de réaliser une « analyse de risques »
- Il fallait dans un premier temps identifier les éléments à protéger (assets)
- Le CPSI a donc procédé à une enquête auprès des groupes de recherche et services au laboratoire
  - Discussion à « bâtons-rompus » avec les responsables d'équipes et de services. Objectif : identifier des besoins spécifiques de sécurité mais finalement, a permis de faire prendre conscience de la valeur de certaines données !

Analyse de risques ?

- Comment conduire une analyse de risques ?
  - Se focaliser sur des risques les plus partagés par les différentes entités (génériques), au risque de tomber dans des lieux communs, mais permet de travailler pour l'ensemble du laboratoire
  - Se focaliser sur les besoins spécifiques d'une équipe, service ?
  - Le CPSI a estimé que l 'analyse « générique » couvrait la majorité des besoins et qu'il pourrait être conduit des études complémentaires
  - La théorie : risque = probabilité de réalisation d'une menace * impact. Etablissement de tableaux (abaques).

Analyse de risques : exemples

R02 Poste de travail fixe (M26S1) : L'exécution d'un ver ou virus rend un grand nombre de postes de travail fixes indisponibles pendant plus de 24 heures.	
Mesures préconisées :	
Mes14	Les utilisateurs sont sensibilisés à la protection de leur poste de travail
Mes12	Les utilisateurs ont des droits limités et ne peuvent pas installer d'applications
Mes41	Les postes sont équipé d'un antivirus à jour
Mes20	Protéger le SI des tentatives d'intrusion ou virus venant de l'extérieur
Mes73	La connexion de supports externes est réglementée ou encadrée
Risque avec les Mesures préconisées : 5	

R01 Services critiques et postes de travail fixe (M12S2) : Pas d'alimentation électrique (tout le labo) pendant plus de 24 heures.	
Mesures préconisées : Néant	
Risque avec les Mesures préconisées : 6	
Mesures supplémentaires :	
Mes2	Il convient de protéger les matériels et les services essentiels des coupures longues de l'alimentation électrique (groupe électrogène par exemple)
Risque avec les mesures supplémentaires : 5	

Analyse de risques : décisions

Plan de traitement des risques

Risque	Décision (1)
R01: Pas d'alimentation électrique (tout le labo) pendant plus de 24 heures.	Maintien
R02: L'exécution d'un virus rend un grand nombre de postes de travail fixes indisponibles pendant plus de 24 heures.	Réduction
R03: L'exécution d'un virus rend un grand nombre de postes de travail portables indisponibles pendant plus de 24 heures.	Réduction
R04: Panne matérielle sur un serveur d'authentification	Réduction

[…]

Par la suite, décision de réduction du risque R01

Analyse de risques : décisions

Mesures à ajouter à la Déclaration d'Applicabilité

Référence	Mesure
Mes401	Mise en oeuvre d'un onduleur sur chacune des arrivées électriques des salles machines
Mes402	Double alimentation sur deux lignes différentes pour tous les serveurs critiques et réseau
Mes403	Contrôle régulier du fonctionnement des onduleurs et doubles alimentations
Mes404	Détection et alarmes pour les évènements sur les onduleurs et alimentation
Mes405	Procédures écrites permettant d'arrêter rapidement les services, les moins critiques en premier afin de prolonger l'autonomie des onduleurs jusqu'à 30mn
Mes406	Dispositif automatique d'arrêt des services non-critiques dans le but de prolonger la durée d'alimentation secourue jusqu'à couvrir si possible la plage d'horaires non ouvrés.
Mes407	Groupe électrogène de secours pour les services critiques

Au final sur l'analyse de risques

- Exercice intéressant
- Mais trop consommateur de temps
- Quelle précision ? Honnêteté de la démarche ?
- A permis toutefois de poser les bonnes questions
  - Risque d'indisponibilité jugé inacceptable = installation d'un groupe électrogène, décision validée par la suite (coupures fréquentes et pertes de matériel coûteux dans d'autres établissements sur le même campus)
- Des analyses de risques plus ciblées par la suite (serveur web, copieurs multifonctions,...)

PSSI

- GT CNRS CAPSEC (2006)[4]
- Travaux IN2P3 (2006)
- Groupe de travail CNRS GT-PSSI (Fin 2012)
- Première PSSI Subatech (2012)
- PSSI-CNRS [5] publiée Nov 2019 (message d'A.Petit)
  - Politique Générale (objectifs, périmètre, organisation,…)
  - Politique Opérationnelle (services|unités)
- La PSSI de l'État comme référence
- Utilité d'une déclinaison locale ?
  - De la PSSI peut-être pas, mais nécessité du pilotage :

« Chaque unité doit produire et conserver les documents et enregistrements permettant de surveiller, contrôler la gestion de la SSI. »

Pilotage de la SSI

- Définir le périmètre d'application de la SSI
- Identifier les exigences réglementaires (lois, chartes, réglements, exigences de la PSSI)
- Estimation de l'état de conformité (règles PSSI-CNRS)
- Plan d'action pour réduire les écarts
- Collecte des mesures , recherche d'indicateurs
- Prise en compte des changements et des nouveaux projets
- Mise en place du processus de révision/amélioration

Pilotage : les éléments clé

- Cycle d'amélioration permanente (PDCA) :
  - Réunion de « réexamen »
  - Un plan d'action
  - Réunions régulières (mensuelles ?)
- Lien avec la direction
- Information et sensibilisation du personnel
- Traces écrite, preuves, documents

Adaptation

- Le contexte de la SSI (menaces, choses à protéger, exigences,…) évolue en permanence
- De nouvelles réglementations ou références voient le jour (PSSI CNRS)
- Le dispositif SSI du laboratoire doit s'adapter
- D'où la nécessité du pilotage de la SSI et d'un dispositif PDCA tel que le prévoit le SMSI
- La réunion annuelle de réexamen est primordiale

PSSI CNRS

PSSI-CNRS/Règles

Légende:

Travail pas commencé
Travail en cours
Analysé, mise en oeuvre < 50% : Règle pas en place
Analysé, mise en oeuvre ≥ 50% < 80% : A améliorer ?
Analysé, mise en oeuvre ≥ 80% : Règle OK

Liste des règles sur securite-si.cnrs.fr

Politique de Sécurité de l'Etat (PSSIE)

Règles de niveau 1

Code	Directive	Responsable	Mise en oeuvre	Niv.
AUT-1	Seuls les comptes individuels (non partagés) sont autorisés pour l'identification préalable à l'accès aux ressources informatiques (postes de travail, systèmes d'information, etc.)	KH	90%	1
AUT-2	Toute action d'autorisation d'accès d'un utilisateur à une ressource des SI, qu'elle soit locale ou nationale, doit s'inscrire dans le cadre d'un processus d'autorisation formalisé qui s'appuie sur le processus d'entrée et de sortie du personnel	SB	100%	1
AUT-4	La gestion des moyens d'authentification des utilisateurs sur les SI doit se faire suivant les recommandations nationales	KH	92%	1
AUT-5	Lorsque les moyens de contrôle d'accès personnels d'un utilisateur aux informations doivent être rendus accessibles aux administrateurs, l'utilisateur doit en être informé et ces informations doivent être transmises et stockées de façon sécurisée	-	-	1
CNF-1 CNF-2 CNF-3 CNF-4	Le DU est responsable de l'application des procédures liées à la mise en œuvre de la réglementation relative au traitement automatisé des données à caractère personnel réalisés sur des systèmes qui sont sous la responsabilité de l'unité	JL	?	1
CNF-6	Le DU doit mettre à disposition de l'audit interne du CNRS, du RSSI du CNRS, du RSSI de la DR dont il dépend tout document permettant de juger du niveau d'application des règles de sécurité des SI dans l'unité	JM	100%	1
EXP-9	Les systèmes doivent être maintenus à jour et les correctifs de sécurité appliqué	-	-	1
EXP-CNF-1	Le parc logiciel de l'unité est géré et permet notamment un suivi de l'attribution des logiciels au personnel	-	-	1
EXP-CNF-3	La configuration logicielle des matériels utilisés par le personnel doit être sécurisée suivant les recommandations nationales spécifiques à chaque type de matériel, OS, et usage	-	-	1
EXP-RES-6	La prise de main à distance sur le poste de travail d'un utilisateur ne doit se faire que suivant une procédure sécurisée en suivant les directives nationales	-	-	1
GRH-1.3	Les personnes qui ne font pas partie du personnel doivent prendre connaissance des règles SSI de l'unité avant toute connexion au SI de l'unité	-	-	1
GRH-1	Le personnel entrant dans l'unité doit être accueilli suivant une procédure d'accueil formalisée qui inclut la prise de connaissance de la charte SSI et des règles élémentaires de sécurité informatique avant l'ouverture des accès sur le SI	MB	-	1
GRH-2	Le personnel sortant de l'unité doit être connu de l'équipe informatique qui applique une procédure de départ formalisée incluant la fermeture des droits sur le SI et la restitution des matériels appartenant à l'unité	-	-	1

PSSI CNRS

PSSI-CNRS/AUT-4

Categorie: Authentification et contrôle d'accès: ***La gestion des moyens d'authentification des utilisateurs sur les SI doit se faire suivant les recommandations nationales***

Référence : AUT-4-implementation

Directives

Quelques règles à appliquer...

Etat de mise en oeuvre

Code	Directive	Responsable	Mise en oeuvre
AUT-4-01	Le mot de passe initial ou les fichiers « clefs » initiaux doivent être transmis de manière sûre, en évitant par exemple une transmission en texte clair dans un message électronique	SINFO	100%
AUT-4-02	Lorsque les utilisateurs doivent changer leur mot de passe, il convient que le mot de passe initial soit temporaire et suffisamment sécurisé (difficile à deviner) et que les utilisateurs soient forcés de le changer à la première connexion	SINFO	100%
AUT-4-03	Les sequestres sont stockés de manière sûre, par exemple dans une zone chiffrée	SINFO	100%
AUT-4-04	Mettre en oeuvre les recommandations de l'ANSSI [2]	SINFO	100%
AUT-4-05	Contrôle de la robustesse des mots de passe et changement périodique	SINFO	100%
AUT-4-06	Sequestre des clés de chiffrement	SINFO	100%
AUT-4-07-01	Les authentifiants permettant l'administration des ressources des SI doivent être placés sous séquestre et tenus à jour	SINFO	100%
AUT-4-07-02	Tout accès d'administration à une ressource informatique doit pouvoir être tracé et permettre de remonter à la personne exerçant ce droit	SINFO	100%
AUT-4-08-01	L'accès à toute ressource non publique doit nécessiter une identification et une authentification individuelle de l'utilisateur	SINFO	100%
AUT-4-08-02	Dans le cas de l'accès à des données sensibles, des moyens d'authentification forte doivent être utilisés	SINFO	0%
AUT-4-08-03	Le contrôle d'accès doit être géré et s'appuyer sur un processus formalisé en cohérence avec la gestion des ressources humaines	SINFO	100%
AUT-4-09	Les informations d'authentification (mots de passe d'accès aux SI, clés privées liées aux certificats électroniques, etc.) doivent être considérées comme des données sensibles	SINFO	100%
AUT-4	**Etat global de mise en oeuvre**	SINFO	**92%**

Contrôle/Indicateurs [1]

AUT-4-05

IND-0042 : nombre de mots de passe de plus de 2 ans.
Règles de complexité de smots de passe dans Active-Directory

Commentaires

La plupart de ces mesures se traduisent par des directives pour différents acteurs autours du SI du laboratoire. Voir le document : DOC-Mise-en-oeuvre-PSSI-CNRS-v10.pdf

AUT-4-01

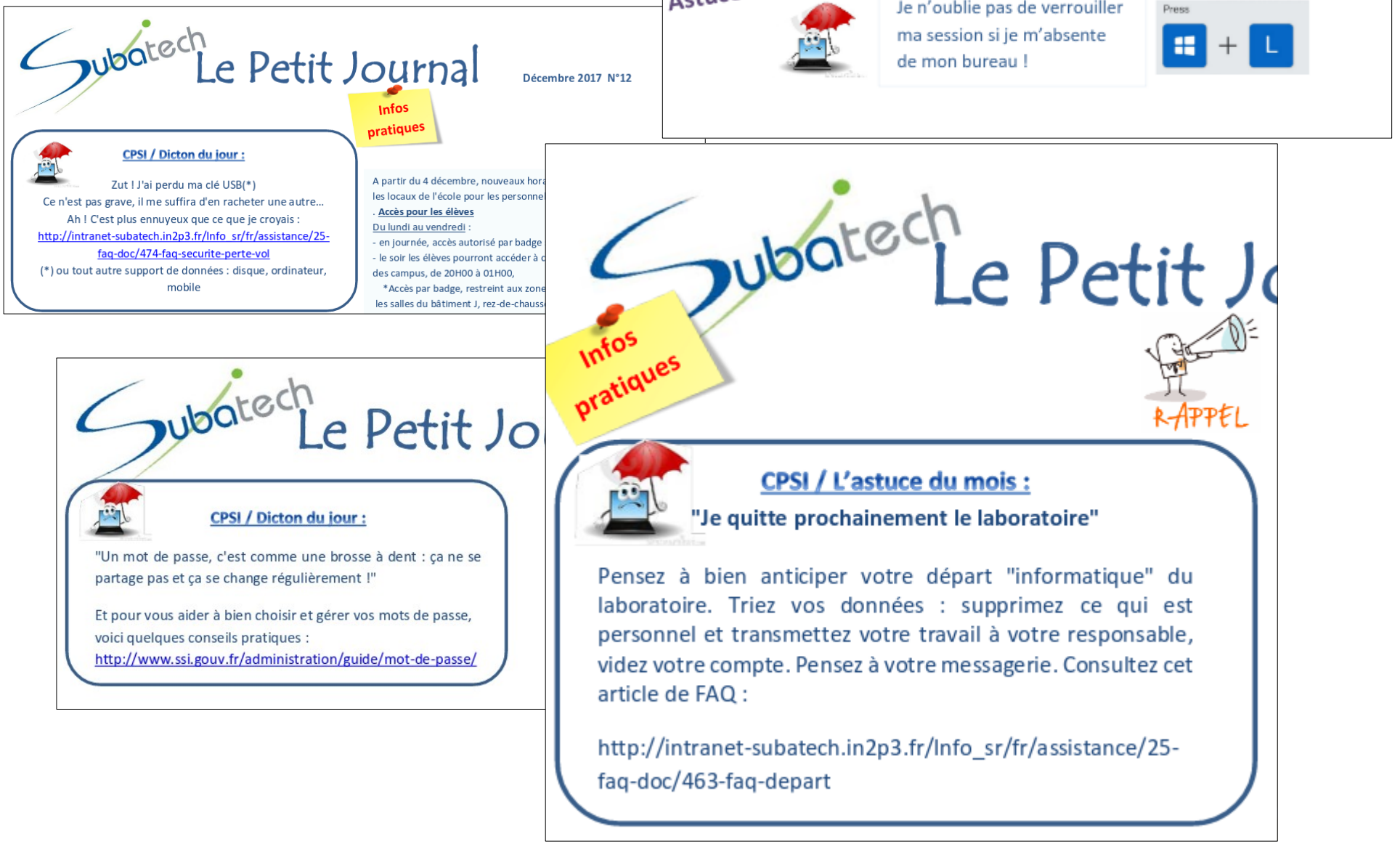
Transmission directe (de main à main) du service informatique à l'utilisateur via document papier refermé. Alternativement, si à distance, transmission du mot de passe en plusieurs parties via des canaux différents.

[...]

Sensibilisation

- Les utilisateurs sont la principale cible des pirates pour s'introduire dans un SI (techniques d'ingénierie sociale)
- De même, pour la protection des données, les utilisateurs jouent un rôle clé
- Le sensibilisation des utilisateurs est donc une priorité
- Reconnaître les points particuliers nécessitant une action de sensibilisation
- Comment procéder ? (séminaires, mails, com. interne)
- Sensibiliser les nouveaux entrants
- « Formation » SSI obligatoire (comme au CERN) ?

Sensibilisation



Subatech Le Petit Journal

Décembre 2017 N°12

Infos pratiques

CPSI / Dicton du jour :

Zut ! J'ai perdu ma clé USB(*)
Ce n'est pas grave, il me suffira d'en racheter une autre...
Ah ! C'est plus ennuyeux que ce que je croyais :
http://intranet-subatech.in2p3.fr/Info_sr/fr/assistance/25-faq-doc/474-faq-securite-perte-vol
(*) ou tout autre support de données : disque, ordinateur, mobile

A partir du 4 décembre, nouveaux hora
les locaux de l'école pour les personne
. **Accès pour les élèves**
Du lundi au vendredi :
- en journée, accès autorisé par badge
- le soir les élèves pourront accéder à c
des campus, de 20H00 à 01H00,
*Accès par badge, restreint aux zone
les salles du bâtiment J, rez-de-chauss

Astuce CPSI

Je n'oublie pas de verrouiller ma session si je m'absente de mon bureau !

Press + L

Subatech Le Petit Jo

CPSI / Dicton du jour :

"Un mot de passe, c'est comme une brosse à dent : ça ne se partage pas et ça se change régulièrement !"

Et pour vous aider à bien choisir et gérer vos mots de passe, voici quelques conseils pratiques :
http://www.ssi.gouv.fr/administration/guide/mot-de-passe/

Subatech Le Petit Jo

Infos pratiques

RAPPEL

CPSI / L'astuce du mois :

"Je quitte prochainement le laboratoire"

Pensez à bien anticiper votre départ "informatique" du laboratoire. Triez vos données : supprimez ce qui est personnel et transmettez votre travail à votre responsable, videz votre compte. Pensez à votre messagerie. Consultez cet article de FAQ :

http://intranet-subatech.in2p3.fr/Info_sr/fr/assistance/25-faq-doc/463-faq-depart

Sensibilisation : séminaires

Séminaire tout public

jeudi 14 octobre 2021 à 14:00

Amphi Georges CHARPAK

Apprenez à vous protéger des cybermenaces en 2021

Régis Dubrulle

ANSSI Région Pays de la Loire

La transformation numérique, source d'incroyables opportunités, génére de nouveaux risques : les cyberattaques. Ce type d'attaque comme celle sur la ville d'Angers en janvier 2021 se multiplient considérablement entraînant des dysfonctionnements informatiques critiques dans les organismes. Pour faire face, il est aujourd'hui important de bien comprendre les dernières menaces et adopter les bonnes mesures d'hygiène numérique.
Ce webinar, après une présentation de l'état de la menace, abordera l'écosystème des attaquants puis présentera un ensemble de bonnes pratiques à suivre qui vous serviront dans votre vie professionnelle mais aussi personnelle.

Subatech

Des services bien attractifs !

Il y a longtemps qu'on s'en doute !!!

Présentations

- Séminaire: *Cybersécurité: Apprenez à vous protéger des menaces* Régis Dubrulle, Octobre 2021
- Séminaire *Sécurité et vie privée sur le web: le navigateur web* Vincent Mazenod, 27 Novembre 2020
- Séminaire *Messagerie électronique et sécurité* Benoit Delaunay, 8 Février 2019
- Séminaire *Vol de votre ordinateur portable : prévenir, réagir, surmonter* Mariangela Settimo, 1er Décembre 2017
- Séminaire *Offres et utilisation des espaces de stockage informatique* Jean-Luc Béney, 8 Juin 2017
- Séminaire *Certificats Electroniques* Jean-Michel Barbet, 8 Décembre 2016
- Séminaire *La sécurité des systèmes de l'information: Tout dépend de vous!* par Thierry Mouthuy, 2 Décembre 2015
- Présentation Charte CNRS 2014, 30 Avril 2015
- Séminaire *Mon Mobile, moi et mon boulot* par Serge Bordères, 9 Décembre 2014
- Responsabilités SSI réunion chefs de groupe, 24 Octobre 2013
- CPSI, Journées du Labo, St-Jean de Monts, Juin 2013
- Présentation PSSI au Conseil de Laboratoire, 11 Mai 2012
- Sécurité Informatique, Journées du Labo, Guidel, Mai 2011

Conclusion

- Plus de 10 ans d'existence du CPSI à Subatech
- Un investissement important, surtout au début (lourdeur de l'analyse de risques) mais devenu raisonnable
- L'expérience acquise dans le pilotage a permis le suivi des exigences du CNRS (chiffrement par ex.) et facilite actuellement la prise en compte de la PSSI du CNRS
- L'existence du CPSI renforce la confiance des partenaires (tutelles, bailleurs de fonds, clients du service de métrologie)
- La SSI est un projet qui doit impliquer l'ensemble du personnel. La sensibilisation est très importante, le rôle des responsables de groupes et du service RH également

Références

[1] Système de Management de la Sécurité de l'Information (SMSI) :
https://fr.wikipedia.org/wiki/Syst%C3%A8me_de_management_de_la_s%C3%A9curit%C3%A9_de_l%27information

[2] EBIOS
https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/

[3] Roue de Deming :
https://fr.wikipedia.org/wiki/Roue_de_Deming

[4] CAPSEC
https://halshs.archives-ouvertes.fr/halshs-00096276/document

[5] PSSI CNRS
https://securite-si.cnrs.fr/pssi/

[6] « *SMSI/PSSI Pilotage de la SSI vers un régime permanent* »
réunion du Groupe Sécurité IN2P3, 2012 :
https://indico.in2p3.fr/event/6806/contributions/39410/attachments/31788/39019/securite-PSSI.pdf

[7] PSSI, SMSI : de la théorie au terrain
Présentation JI2014 :
https://indico.in2p3.fr/event/9954/contributions/51390/attachments/41646/51590/present-SSI-JMB-JI2014.pdf

Backup Slides