

Pilotage de la sécurité des Systèmes d'Information (SSI)

Comité de Pilotage de la SSI (CPSI) à Subatech
Un retour d'expérience après 14 ans d'existence

Jean-Michel BARBET, Laboratoire Subatech

Séminaire SSI Laboratoire Subatech Novembre 2023

Plan

- Origine du CPSI
- Premiers travaux (analyse de risques, PSSI)
- Prise en compte de la PSSI du CNRS
- Les éléments clé du pilotage de la SSI
- Sensibilisation et culture SSI
- Conclusion

Origine du CPSI

- Formation nationale SIARS CNRS
- Déclinaison en région à Roscoff septembre 2009 (R.Longeon, F.Morris and al.)
- EBIOS, normes ISO 27000, SMSI
- Démarche très formelle et très lourde
- Des points intéressants, néanmoins :
 - Périmètre et formalisation des rôles
 - Le concept d'amélioration continue
 - Les traces écrites et l'auditabilité

SIARS: Sécurité Informatique Administrateur Réseau et Systèmes

EBIOS :Expression des besoins et identification des objectifs de sécurité [1]

SMSI : Système de Management de la Sécurité de l'Information [2]

Piloter la SSI selon ISO27000

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



Roue de Deming ou cycle PDCA : Méthode de gestion de la qualité [3]

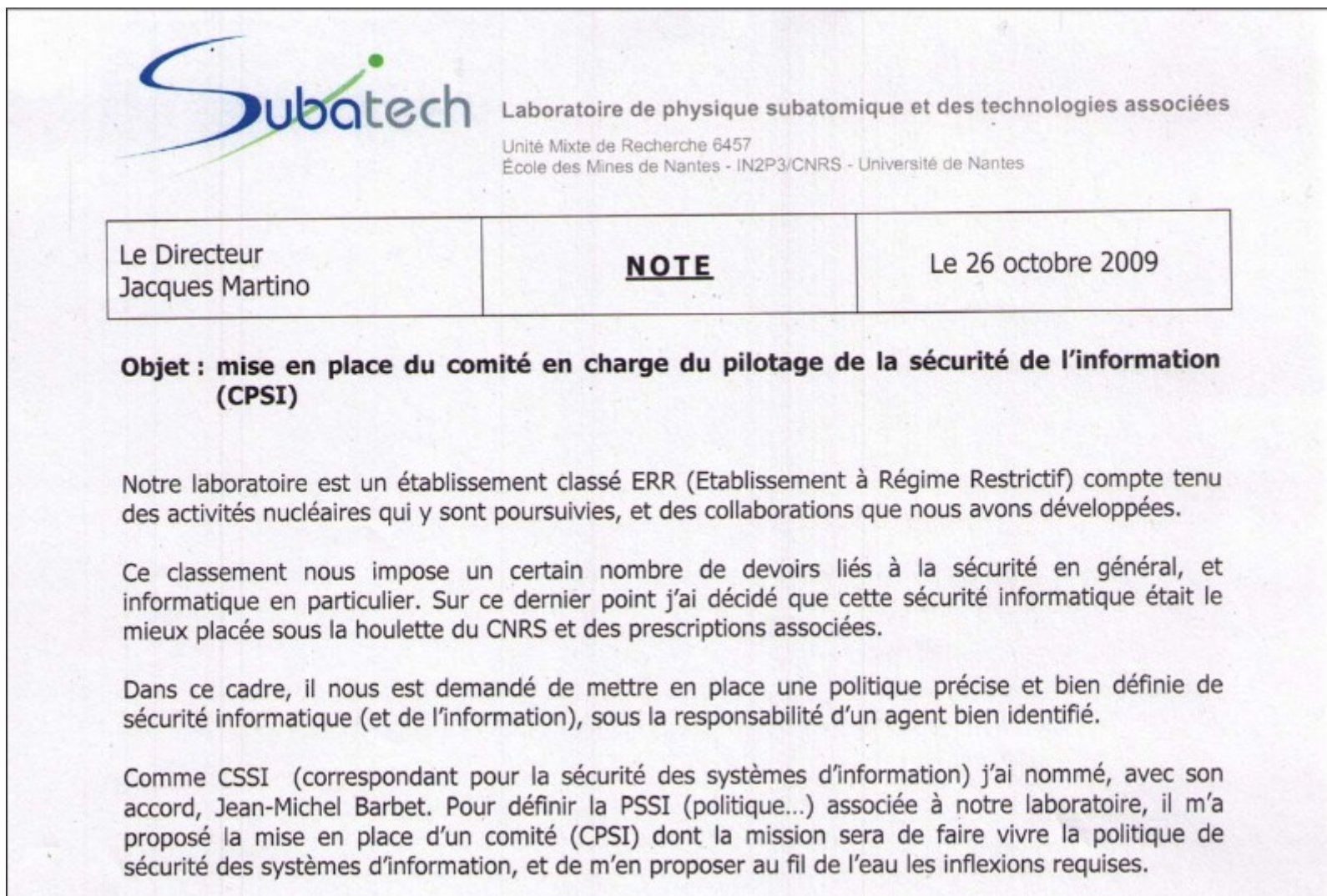
Pilotage de la SSI

- Définir le périmètre d'application de la SSI
- Identifier les exigences réglementaires (lois, chartes, règlements, PSSI applicable)
- Estimation de l'état de conformité (règles PSSI)
- 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 :
 - Réunion de « réexamen »
 - Un plan d'action
 - Réunions régulières (mensuelles ?)
- Lien avec la direction
- Information et sensibilisation du personnel
- Traces écrite, preuves, documents

Création du CPSI



[...]

Le CPSI

Objectifs :


- Rédiger la PSSI du laboratoire
- « Piloter » la SSI au laboratoire
- Impliquer les diverses catégories de personnel

Fonctionnement :

- 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

<http://intranet-subatech/cpsi/>

 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 a 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 juillet 2022) de :

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

Avancement du projet

Mars 2023 : Nouvelle version de la Politique du SMSI (v2.0) validée par le directeur

Octobre 2021 : Une nouvelle version de la PSSI (v1.3) a été validée par le directeur

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

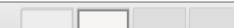
Février 2016 : Une nouvelle version de la PSSI (v1.1) a été validée par le directeur

11 Mai 2012 : La PSSI v1.0 validée par le directeur et a été présentée au conseil du laboratoire.

Documents de Politiques

- [Politique du Système de Management de la Sécurité de l'Information \(SMSI\)](#)
- [Politique de Sécurité des Systèmes d'Information \(PSSI\)](#)

 Sécurité de l'Information — Mozilla ...

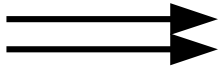


Documents de Politiques



- [Politique du Système de Management de la Sécurité de l'Information \(SMSI\)](#)
- [Politique de Sécurité des Systèmes d'Information \(PSSI\)](#)
- [Sous-Politique : Politique de sécurité de l'information pour les télétravailleurs](#)
- [Sous-Politique : Accès au Système d'Information depuis Dispositifs Nomades Personnels](#)
- [Sous-Politique : Gestion des Accès au Système d'Information](#)
- [Sous-Politique : Gestion des Incidents](#)
- [Sous-Politique : Sauvegarde](#)
- [Sous-Politique : Chiffrement](#)

Autres Documents



- [\[New\] Données Informatiques](#)
- [Fiches Responsabilités SSI](#)
- [Fiche A4 Information SSI](#)

Présentations

- [Présentation Management de la SSI au Conseil de Laboratoire le 13 Mars 2023](#)
- [Projet de Groupe de Travail : Résilience à une cyber-crise, Réunion CES, 25 Octobre 2022](#)
- [Présentation dispositif SSI CNRS et Labo au Conseil de Laboratoire le 10 Mars 2022](#)
- [Séminaire: Cybersécurité: Apprenez à vous protéger des menaces Régis Dubrulle, Octobre 2021](#)
- [Séminaire Sécurité et vie privée sur le web: le navigateur web Vincent Mazonod, 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](#)
- [Présentation SSI CNRS nouveaux entrants, R.Longeon, 2 Octobre 2007](#)

Activité

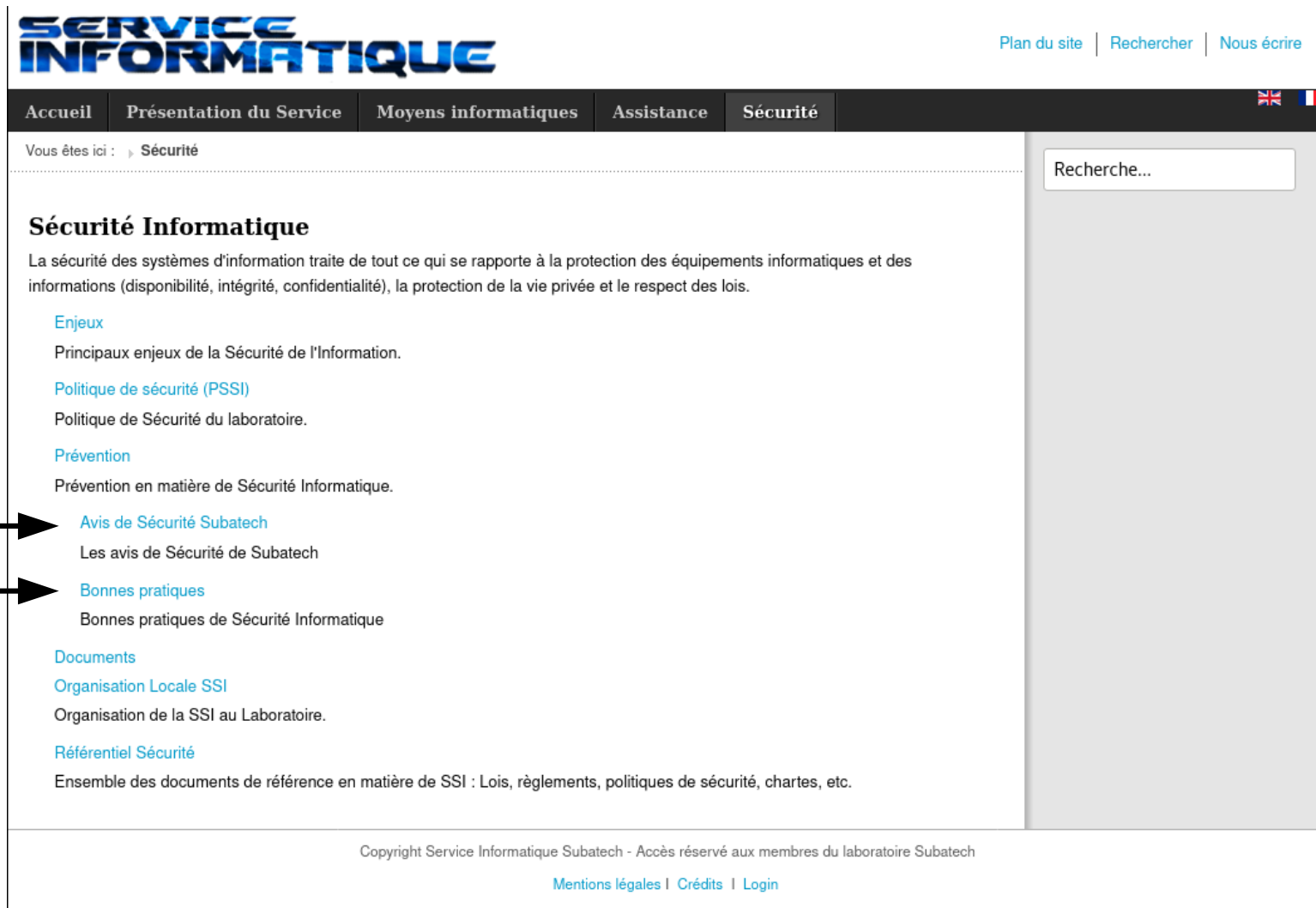
- [Rapport d'Activité du CPSI 2022](#)
- [Rapport d'Activité du CPSI 2021](#)
- [Rapport d'Activité du CPSI 2020](#)
- [Rapport d'Activité du CPSI 2019](#)
- [Rapport d'Activité du CPSI 2018](#)
- [Rapport d'Activité du CPSI 2017](#)
- [Rapport d'Activité du CPSI 2016](#)
- [Rapport d'Activité du CPSI 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 en oeuvre de la PSSI du CNRS et niveau de sensibilité, conseil de laboratoire du 9 Mars 2021](#)
- [\[12\] PSSI de l'Etat \(PSSIE: Circulaire 38641\)](#)

Service informatique

http://intranet-subatech/Info_sr/fr/securite



SERVICE INFORMATIQUE [Plan du site](#) | [Rechercher](#) | [Nous écrire](#)

Accueil | Présentation du Service | Moyens informatiques | Assistance | **Sécurité** 

Vous êtes ici : [Sécurité](#)

Recherche...

Sécurité Informatique

La sécurité des systèmes d'information traite de tout ce qui se rapporte à la protection des équipements informatiques et des informations (disponibilité, intégrité, confidentialité), la protection de la vie privée et le respect des lois.

- [Enjeux](#)
Principaux enjeux de la Sécurité de l'Information.
- [Politique de sécurité \(PSSI\)](#)
Politique de Sécurité du laboratoire.
- [Prévention](#)
Prévention en matière de Sécurité Informatique.
- [Avis de Sécurité Subatech](#)
Les avis de Sécurité de Subatech
- [Bonnes pratiques](#)
Bonnes pratiques de Sécurité Informatique
- [Documents](#)
 - [Organisation Locale SSI](#)
Organisation de la SSI au Laboratoire.
 - [Référentiel Sécurité](#)
Ensemble des documents de référence en matière de SSI : Lois, règlements, politiques de sécurité, chartes, etc.

Copyright Service Informatique Subatech - Accès réservé aux membres du laboratoire Subatech

[Mentions légales](#) | [Crédits](#) | [Login](#)

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'accès aux principaux documents :

- [Reunions](#)
- [Actions](#)

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 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 (2010-11)

Analyse de risques : bilan

- Exercice intéressant
 - 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 !
- 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,...)

Démarches PSSI CNRS et IN2P3

- Groupe de travail CNRS CAPSEC (2006) [4]
- Groupe de travail IN2P3 (2006)
- Groupe de travail CNRS GT-PSSI (Fin 2012)
- Première PSSI Subatech (2012) [8]
- PSSI du CNRS [5] publiée en Nov 2019
 - Politique Générale (objectifs, périmètre, organisation,...)
 - Politique Opérationnelle (services|unités)
- La PSSI de l'État comme référence
- Utilité d'une déclinaison locale ?
 - Document 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. »

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
- La 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



Le Petit Journal

Décembre 2017 N°12

Infos pratiques

CPSI / Dictionnaire 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-perde-vol
(*) ou tout autre support de données : disque, ordinateur, mobile

A partir du 4 décembre, nouveaux horaires des locaux de l'école pour le personnel

Accès pour les élèves

Du lundi au vendredi :

- en journée, accès autorisé par badge
- le soir les élèves pourront accéder à certains des campus, de 20H00 à 01H00,

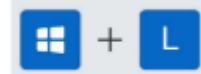
*Accès par badge, restreint aux zones des salles du bâtiment J, rez-de-chaussée

Astuce CPSI



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

Press



Le Petit Journal

Infos pratiques

CPSI / Dictionnaire 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/>



Le Petit Journal

Infos pratiques

R-APPEL

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



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, génère 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.

Des services bien attractifs !



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

Journées du Laboratoire, 20–21 Juin 2013, CPSI

14/18

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 Mazonod, 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](#)

Culture SSI

- La SSI n'est pas uniquement le problème du CPSI et du service informatique
- Tous les membres du laboratoire ont un rôle à jouer
 - En tant qu'utilisateur des moyens informatique
 - Dans la maîtrise des données (organisation, placement, protection)
 - Pour alerter en cas de « choses » anormales
 - En tant que responsable de service ou d'équipe pour la gestion des arrivées, des départs, du renouvellement des accès

Conclusion

- Environ 14 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 l'implémentation et 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] EBIOS

<https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/>

[2] 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

[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/>

[8] Présentation PSSI Subatech au conseil de laboratoire, mai 2012 :

<http://intranet-subatech/cpsi/pssi-conseil-labo.pdf>