LA SÉCURITE DES SYSTÈMES D'INFORMATION (SSI),

élément indispensable pour une protection efficace du potentiel scientifique et technique (PPST) d'une entreprise

HFDS Bercy

Protéger ses savoirs, savoir-faire contre l'espionnage et la destruction de données, est une préoccupation essentielle de toute entreprise soucieuse de préserver son potentiel économique actuel et futur.

La PPST est une politique publique qui permet de l'accompagner dans sa démarche de protection et de sécurisation de ses données sensibles.

En adhérant à ce dispositif, l'entreprise accède à une protection géographique par la création de zone (s) à Régime restrictif (ZRR) incluant la protection de ses systèmes d'information par la mise en place de mesures adaptées à sa taille et à son activité, au travers de sa politique de sécurité des systèmes d'information (PSSI).

Les grandes lignes du dispositif PPST

1 une opportunité d'élévation globale du niveau de sécurité.

2 une protection « géographique »: la ZRR est constituée d'un espace (bureau, étage, bâtiment) dont l'accès est réglementé et nécessite une autorisation d'accès.

3 Une PSSI avec un accompagnement des services de l'État.

Les grandes lignes de la PSSI

Face aux risques et menaces multiples qui pèsent sur elle, l'entreprise doit élaborer un document qui matérialise sa PSSI. Ce document de référence SSI reflète la vision stratégique du chef d'établissement et son engagement à garantir un niveau de SSI optimal. Elle est évolutive car elle doit prendre en compte les transformations du contexte de l'entreprise (changement d'organisation, évolution des activités, etc.) et des risques (réévaluation de la menace, variation des besoins de sécurité, des contraintes et des enjeux).

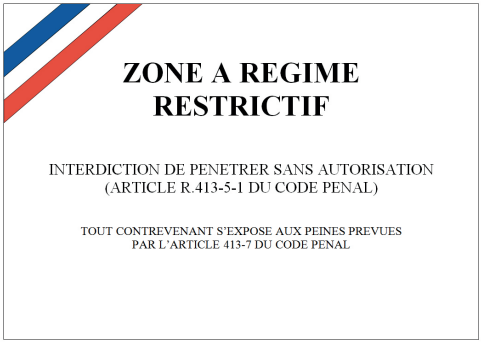
Enfin, la PSSI est également un instrument de sensibilisation et de communication, une fois validée et pour être opposable, elle doit être diffusée à l'ensemble du personnel (utilisateurs, sous-traitants, prestataires, etc.). Sa diffusion permet de responsabiliser chaque utilisateur, qui s'engage personnellement dans la démarche d'amélioration continue de la SSI (charte informatique, attribution d'objectifs liés à la sécurité, etc.).

Les acteurs

Au sein de l'entreprise, le chef d'établissement nomme un responsable de la ZRR, et un responsable de la SSI (RSSI), interlocuteurs privilégiés du service du haut fonctionnaire de défense et de sécurité (HFDS) des ministères économiques et financiers. Le HFDS accompagne l'entreprise pour la mise en place des ZRR, pour le contrôle d'accès aux informations protégées par la ZRR et pour l'élaboration de sa PSSI en s'appuyant sur les recommandations de l'ANSSI.

En conclusion, outre les grandes lignes déjà évoquées, le dispositif PPST permet l'application de sanctions pénales dissuasives pour toute personne qui rentrerait dans une ZRR sans autorisation (accès locaux mais aussi SI). Pour l'entreprise déjà engagée dans un processus de protection de son potentiel, les coûts inhérents à l'entrée dans le dispositif PPST sont maîtrisés (pancartes à poser sur les accès à la zone).

Pour en savoir plus et disposer de précisions supplémentaires relatives au dispositif PPST/PSSI, se reporter à la rubrique « Pour aller plus loin » en annexe, page 4.



ANNEXE

A qui et à quoi peut servir la PSSI ?

La PSSI s'adresse à l'ensemble du personnel de l'entreprise (direction, intervenants IT, personnels administratifs, techniques et commerciaux, ouvriers,...) ainsi qu'aux tiers (fournisseurs, clients, sous-traitants, opérateurs de maintenance, etc.).

La PSSI sert :

1 au chef d'établissement, en protégeant les systèmes d'information sensibles, indispensables à la pérennité des activités de l'entreprise ;

2 aux professionnels de la sécurité/sûreté, qui, dans le cadre d'une bonne gouvernance qu'elle permet, voient définies leurs fonctions et leurs missions ;

3 aux intervenants IT, qui doivent prendre des décisions au quotidien et qui ont besoin de référentiels ;

4 à l'ensemble du personnel (toutes catégories confondues), afin que chaque utilisateur adopte les bons réflexes au quotidien concernant les principes de sécurité de l'entreprise, dans le but de réduire les incidents de sécurité et les coûts associés, et soit responsabilisé pour une démarche d'amélioration continue de la SSI.

Comment élaborer sa PSSI ?

Elle est élaborée par des professionnels de la SSI qui devront au préalable réaliser une analyse de risque afin d'identifier, notamment, les informations les plus « critiques » pour la survie de l'entreprise.

Une méthodologie pour effectuer cette analyse de risques est disponible en libre téléchargement sur le site web de l'ANSSI :

www.ssi.gouv.fr/entreprise/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

Quel est le contenu de la PSSI ?

Elle permet de fixer des objectifs en matière :

1. d'organisation et de gouvernance : par exemple identifier et désigner les acteurs et les responsables SSI.

2. de ressources humaines : par exemple, sensibiliser, rédiger une charte d'application SSI et gérer les arrivées et départs du personnel.

3. de gestion des biens, de la sécurité du poste de travail et du réseau : par exemple, élaborer une cartographie des systèmes d'information.

4. d'intégration de la SSI dans le cycle de vie des systèmes d'information : par exemple, apprécier, traiter et communiquer sur les risques relatifs à la sécurité des systèmes d'information ainsi que gérer dynamiquement les mesures de protection, tout au long de la vie du système d'information.

5. de sécurité physique : par exemple, assurer la sécurité physique des locaux abritant les systèmes d'information et des centres serveurs.

6. de sécurité des réseaux : par exemple, établir une cartographie des réseaux et des interconnexions de l'entité, en particulier des réseaux sans-fil.

7. d'architecture des systèmes d'information : par exemple, mettre en place une architecture sécurisée des centres informatiques.

8. d'exploitation des systèmes d'information : par exemple, surveiller et configurer les ressources informatiques, gérer les autorisations et contrôles d'accès logiques.

9. de sécurité du poste de travail : par exemple, « durcir » les configurations des postes de travail en protégeant les utilisateurs et en sécurisant la téléphonie ainsi que les copieurs multifonctions.

10. de sécurité du développement des systèmes : par exemple, prendre en compte la sécurité dans le développement des systèmes d'information, des logiciels et sécuriser les applications à risque.

11 de traitement des incidents : par exemple, partager l'information (alertes, incidents) dans le respect des règles de prudence.

12 de continuité d'activité : par exemple, se doter de plans de continuité d'activité et les tester.

13 de conformité, audit, inspection, contrôle : par exemple, effectuer des contrôles et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

POUR ALLER PLUS LOIN

- Guide des bonnes pratiques de l'informatique (ANSSI / CGPME)

http://www.ssi.gouv.fr/uploads/2015/03/guide_cgpme_bonnes_pratiques.pdf

- Instruction interministérielle n°901/SGDSN/ANSSI : une nouvelle étape dans la protection des SI sensibles

http://circulaires.legifrance.gouv.fr/index.php?action=afficherCirculaire&hit=1&retourAccueil=1&r=39217

- Passeport de conseils aux voyageurs

http://www.ssi.gouv.fr/IMG/pdf/passeport_voyageurs_anssi.pdf

- Guide d'hygiène informatique à destination des responsables informatiques

http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

- Politique de sécurité des systèmes d'information de l'État à destination des responsables informatiques

http://www.ssi.gouv.fr/uploads/2014/11/pssie_anssi.pdf

D'AUTRES ENCORE :

- http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/

Fiches de sécurité économique (D2IE) :
http://www.intelligence-economique.gouv.fr/methodes-et-outils/la-securite-economique-au-quotidien

- Normes ISO relatives à la sécurité des systèmes d'information (famille des normes ISO/CEI 2700x) :

http://www.iso.org/fr/

Pour les entreprises intéressées par le dispositif PPST et qui relèvent du périmètre des ministères économiques et financiers : se référer au décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation, à l'arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation et à la directive ministérielle en date du 22 novembre 2012, disponible auprès du HFDS.

POUR PLUS DE RENSEIGNEMENTS

Contacter le service
du haut fonctionnaire de défense et de sécurité (HFDS)
bâtiment le Valmy – 18 avenue Léon Gaumont
75977 Paris Cedex 20.

ppst.hfds@finances.gouv.fr

Téléphone: 01.57.53.26.42