SANTÉ

SANTÉ PUBLIQUE

MINISTÈRE DES AFFAIRES SOCIALES
ET DE LA SANTÉ

Secrétariat général des ministères
chargés des affaires sociales

Délégation à la stratégie des systèmes
d'information de santé (DSSIS)

Service spécialisé du haut fonctionnaire
de défense et de sécurité (SHFDS)

Instruction n° SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information (« plan d'action SSI ») dans les établissements et services concernés

NOR : *AFSZ1629742J*

Date d'application : immédiate.

Validée par le CNP le 18 novembre 2016. – Visa CNP 2016-167.

Catégorie : directives adressées par le ministre aux services chargés de leur application, sous réserve, le cas échéant, de l'examen particulier des situations individuelles.

Résumé : enjeux de la sécurité des systèmes d'information de santé et demande aux ARS de diffuser le plan d'action SSI.

Mots clés : sécurité des systèmes d'information – SSI.

Références :

Arrêté du 1er octobre 2015 portant approbation de la politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales ;

Guide d'hygiène informatique, version 1.0 de janvier 2013 et autres guides publiés par l'Agence nationale de sécurité des systèmes d'information ;

Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) publiée sur le site de l'Agence des systèmes d'information partagés de santé ;

Introduction à la sécurité des systèmes d'information, guide pour les directeurs d'établissement de santé, publié en novembre 2013 par le ministère chargé de la santé.

Annexe :

Plan d'action SSI.

La ministre des affaires sociales et de la santé
à Mesdames et Messieursles directeurs généraux des agences régionales de santé.

La présente instruction a pour objectif de présenter le plan d'action sur la sécurité des systèmes d'information (« Plan d'action SSI ») et les modalités de sa mise en œuvre dans les établissements de santé, les laboratoires de biologie médicale, les centres de radiothérapie et les centres d'imagerie et de radiologie publics et privés. Dans la suite du document ils sont tous désignés sous le terme générique de « structure ».

Ce plan a été élaboré en concertation avec les acteurs concernés de la sphère sanitaire et médico-sociale.

Le plan d'action SSI a été annoncé par la ministre des affaires sociales et de la santé lors de son intervention du 3 octobre 2016 sur la sécurisation des sites hospitaliers.

1. Enjeu

Les incidents liés à la sécurité des systèmes d'information se multiplient dans le monde. Selon l'éditeur Symantec, la France serait entrée en 2015 dans le top 10 des pays les plus touchés par le piratage informatique. Le cabinet de conseil Pricewaterhouse Coopers publie que le nombre de cyber-attaques recensées a progressé de 38 % dans le monde en 2015, et 51 % en France. Tous les secteurs d'activités sont concernés. La sphère santé et médico-sociale n'est pas épargnée : selon un article récent[1], sur le deuxième trimestre 2016, les cybercriminels ont concentré leurs efforts sur le domaine particulièrement sensible et rentable de la santé. En effet, près de 90 % des attaques ransomware sur cette période ont visé des établissements de santé dans le monde. Dans ce secteur, les incidents liés à la sécurité des systèmes d'information peuvent avoir un impact direct sur la sécurité des soins. Ils peuvent également avoir, comme ailleurs, un impact économique[2]. Leur traitement est donc une priorité pour les pouvoirs publics et pour tous les producteurs de soins.

2. Réglementation applicable

Un certain nombre de textes applicables en matière de sécurité des systèmes d'information ont été publiés ces dernières années :

- la Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI-MCAS), déclinaison de la politique de sécurité des systèmes d'information de l'État (PSSI-E), a été approuvée par arrêté ministériel du 1er octobre 2015 ;
- les premiers éléments (guides pratiques et référentiels) de la Politique de sécurité des systèmes d'information de santé (PGSSI-S) ont été publiés dès 2013. Certains référentiels de la PGSSI-S seront rendus opposables dès 2017 ;
- des guides sont publiés par l'Agence nationale de sécurité des systèmes d'information (ANSSI), tels le « guide d'hygiène informatique » d'octobre 2012 ;
- le Programme hôpital numérique, piloté par la DGOS, intègre des exigences en matière de sécurité des SI qui constituent des prérequis ;
- par ailleurs, un guide pour les directeurs d'établissement de santé « Introduction à la sécurité des systèmes d'information », a été publié en novembre 2013. Il est en cours d'actualisation ;
- le guide d'auditabilité des systèmes d'information précise, quant à lui, les besoins de sécurité nécessaires à la certification des comptes des établissement de santé ;
- l'accrédidation des laboratoires de biologie médicale pose des exigences en matière de sécurité des systèmes d'information.

3. Objectif du plan d'action SSI

Le plan d'action (en annexe de la présente instruction) vise à opérer une mise à niveau minimale de la sécurité des systèmes d'information dans toutes les structures concernées, au sein desquelles la défaillance des outils numériques représente un haut niveau de criticité (probabilité/impact).

Le plan d'action SSI ne se substitue pas aux obligations de sécurité que doivent mettre en place les structures mais il propose un calendrier à 6, 12 et 18 mois de réalisation de mesures prioritaires en termes d'efficacité par rapport, notamment, au risque de piratage informatique. Le niveau 1 de priorité permet de diminuer le risque de manière significative, avec des mesures dont la mise en œuvre ne doit pas poser de difficulté majeure, pour des gains importants en matière de sécurité. Le document constitue un fil conducteur. La plupart des structures y retrouveront naturellement des actions qu'elles ont déjà mises en place, ou dont la mise en place est en cours.

4. Action des ARS

L'importance de l'enjeu exige une action forte de sensibilisation par les ARS auprès des acteurs concernés, afin d'assurer la diffusion du plan d'action et sa prise en compte effective. Il vous appartient dans ce cadre de mettre en œuvre les modalités qui vous paraissent les plus appropriées pour obtenir le niveau de mobilisation attendu. Dans tous les cas, l'association effective des représentants régionaux des établissements et structures concernés est un pré-requis. Vous voudrez bien tenir informé de façon trimestrielle le SG/HFDS des actions que vous aurez entreprises et des résultats obtenus.

---

[1] https://www.lexsi.com/securityhub/ransomware-a-bonne-sante/

[2] À titre d'exemples, une intrusion avec mise hors service des systèmes d'information d'une ARS pendant 24 h a engendré des coûts d'intervention par un prestataire de l'ordre de 10 000 €, la perte de productivité est estimée à près de 40 000 €, soit un total de 50 000 € ; un cryptovirus en EHPAD a coûté 50 000 € en coûts directs d'intervention et coûts indirects ; un piratage du standard d'un centre hospitalier a généré une surfacturation de téléphonie de l'ordre de 40 000 €.

Toute question sur la présente instruction est à adresser aux boites fonctionnelles suivantes du ministère chargé de la santé :

Direction générale de l'offre de soins (DGOS) :
DGOS-PF5@sante.gouv.fr

Services du haut fonctionnaire de défense et de sécurité :
HFDS-SSI@sg.social.gouv.fr

Je vous saurais gré de bien vouloir me tenir informé de toute difficulté rencontrée dans la mise en œuvre de la présente instruction.

Pour la ministre et par délégation :
Le secrétaire général
des ministères chargés des affaires sociales,
P. Ricordeau

ANNEXE

1. **Mesures de priorité 1 à mettre en place dans les 6 mois**

Gestion des ressources humaines (RH)

La fonction sécurité des systèmes d'information est identifiée et prise en charge par la direction. Cette fonction est éventuellement mutualisée entre plusieurs entités, notamment dans le cadre d'un GHT.

Mise en œuvre d'une charte utilisateur annexée au règlement intérieur de la structure.

Organisation (ORG)

Réalisation et tenue à jour d'une cartographie/d'un inventaire des ressources informatiques sous la responsabilité de la structure (postes de travail, serveurs, équipements actifs, équipements biomédicaux…) s'appuyant sur un outillage adapté.

Établissement d'une procédure de signalement et de traitement des incidents de sécurité SI au sein de la structure en vue de la mise en œuvre de l'obligation de signalement des incidents graves de sécurité des systèmes d'information en application de l'article L. 1111-8-2 du code de la santé publique.

Gestion du poste de travail (PC)

Équipement de tous les postes de travail par un antivirus, les postes nomades étant équipés d'un pare-feu local.

Gestion des comptes utilisateurs (USER)

Sécurisation des comptes par mots de passe robustes et renouvelés périodiquement.

Gestion des sauvegardes (SAUV)

Mise en œuvre de sauvegardes régulièrement testées.

2. **Mesures de priorité 2 à mettre en place dans les 12 mois**

Organisation (ORG)

Établissement d'une procédure formelle d'appréciation du risque avant toute mise en production d'un SI (homologation).

Gestion du poste de travail (PC)

Versions maintenues des systèmes d'exploitation[1].

Organisation du maintien en conditions de sécurité de l'ensemble des systèmes numériques (postes de travail, serveurs, équipements actifs, équipements biomédicaux…) notamment en appliquant les mises à jour proposées par les éditeurs et constructeurs.

Gestion des réseaux (RES)

Identification et protection de tous les accès à Internet et de télémaintenance.

Sécurisation du wifi, séparation des réseaux professionnels et des réseaux invités.

Gestion des comptes utilisateurs (USER)

Mise en œuvre d'une gestion des comptes utilisateurs avec profils et droits différentiés selon le principe du moindre privilège (utilisateur, prestataire, administrateur…).

Gestion des ressources humaines (RH)

Identification des actions de formation SSI et inscription d'au moins une action de sensibilisation à la SSI dans le plan de formation annuel des personnels de la structure.

[1] Il peut paraître urgent de mettre à jour les postes de travail dans leur dernière version de système d'exploitation mais une migration de parc est toujours un projet assez complexe. C'est pourquoi cette action est en priorité 2 et non en priorité 1. Toutefois elle doit être largement entamée dès les 6 premiers mois.

3. **Mesures de priorité 3 à mettre en place dans les 18 mois**

Gestion des réseaux (RES)

Cloisonnement du réseau de la structure par grandes familles d'usage (administration, paie, plateau technique...) et par niveaux de sécurité homogènes.

Définition des modalités d'enregistrement et d'analyse des traces d'accès.

Gestion des contrats de sous-traitance SI (PRESTA)

Encadrement contractuel de tous les accès par des prestataires au réseau de la structure et vérification des clauses de réversibilité.

Organisation (ORG)

Réalisation et tenue à jour d'une analyse de risque SI de la structure ; définition et mise en œuvre du plan d'action associé, ces 2 éléments étant validés par les instances de gouvernance de la structure.

Engagement de la direction sur la réduction d'un nombre limité de risques chaque année.

4. **Liste thématique des mesures et références réglementaires et documentaires associées**

LISTE	RÉFÉRENCES
Gestion du poste de travail [PC] Équipement de tous les postes de travail par un antivirus, les postes nomades étant équipés d'un pare-feu local Versions maintenues des systèmes d'exploitation Organisation du maintien en conditions de sécurité de l'ensemble des systèmes numériques (postes de travail, serveurs, équipements actifs, équipements biomédicaux…) notamment en appliquant les mises à jour proposées par les éditeurs et constructeurs	PSSI-MCAS - 1er octobre 2015 PGSSI-S : Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social - Mai 2015 - V1.0 ANSSI : Guide d'hygiène informatique - Version 1.0 - Janvier 2013
Gestion des comptes utilisateurs [USER] Sécurisation des comptes par mots de passe robustes et renouvelés périodiquement Mise en œuvre d'une gestion des comptes utilisateurs avec profils et droits différentiés selon le principe du moindre privilège (utilisateur, prestataire, administrateur…)	PSSI-MCAS - 1er octobre 2015 ANSSI : Guide d'hygiène informatique - Version 1.0 - Janvier 2013 ANSSI : Recommandations de sécurité relatives aux mots de passe - 5 juin 2012 COFRAC : Guide technique d'accréditation pour l'évaluation des systèmes informatiques en biologie médicale - SH GTA 02
Gestion des réseaux [RES] Identification et protection de tous les accès à internet et de télémaintenance Sécurisation du wifi, séparation des réseaux professionnels et des réseaux invités Cloisonnement du réseau de la structure par grandes familles d'usage (administration, paie, plateau technique…) et par niveaux de sécurité homogènes Définition des modalités d'enregistrement et d'analyse des traces d'accès	PSSI-MCAS - 1er octobre 2015 PGSSI-S : Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social - Mai 2015 - V1.0 ANSSI : Guide d'hygiène informatique - Version 1.0 - Janvier 2013 COFRAC : Guide technique d'accréditation pour l'évaluation des systèmes informatiques en biologie médicale - SH GTA 02
Gestion des contrats de sous-traitance SI [PRESTA] Encadrement contractuel de tous les accès par des prestataires au réseau de la structure et vérification des clauses de réversibilité	PSSI-MCAS - 1er octobre 2015 PGSSI-S : Règles pour les interventions à distance sur les SI de santé - Décembre 2014 - V1.0
Gestion des sauvegardes [SAUV] Mise en œuvre de sauvegardes régulièrement testées	PSSI-MCAS - 1er octobre 2015 PGSSI-S : Règles de sauvegarde des SI de Santé - Décembre 2014 - V1.0 PHN : Guide des indicateurs des prérequis et des domaines prioritaires du socle commun du programme hôpital numérique - Avril 2012 COFRAC : Guide technique d'accréditation pour l'évaluation des systèmes informatiques en biologie médicale - SH GTA 02
Gestion des ressources humaines [RH] La fonction sécurité des systèmes d'information est identifiée et prise en charge par la direction. Cette fonction est éventuellement mutualisée entre plusieurs entités, notamment dans le cadre d'un GHT Mise en œuvre d'une charte utilisateur annexée au règlement intérieur de la structure Identification des actions de formation SSI et inscription d'au moins une action de sensibilisation à la SSI dans le plan de formation annuel des personnels de la structure	PSSI-MCAS - 1er octobre 2015 PGSSI-S : Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social - Mai 2015 - V1.0 PHN : Boite à outils pour l'atteinte des prérequis - Fiche pratique n°6 : fiche de poste type d'un RSSI et description des fonctions d'un référent sécurité du système d'information PHN : Boite à outils pour l'atteinte des prérequis - Fiche pratique n° 7 : charte-type d'accès et d'usage du système d'information HAS : Manuel de certification des établissements de santé V2010 - Critère 5.b Sécurité du système d'information COFRAC : Guide technique d'accréditation pour l'évaluation des systèmes informatiques en biologie médicale - SH GTA 02

LISTE	RÉFÉRENCES
Organisation [ORG] Réalisation et tenue à jour d'une cartographie/d'un inventaire des ressources informatiques sous la responsabilité de la structure (postes de travail, serveurs, équipements actifs, équipements biomédicaux…) s'appuyant sur un outillage adapté Établissement d'une procédure de signalement et de traitement des incidents de sécurité SI au sein de la structure en vue de la mise en œuvre de l'obligation de signalement des incidents graves de sécurité des systèmes d'information en application de l'article L. 1111-8-2 du code de la santé publique Établissement d'une procédure formelle d'appréciation du risque avant toute mise en production d'un SI (homologation) Réalisation et tenue à jour d'une analyse de risque SI de la structure ; définition et mise en œuvre du plan d'action associé, ces 2 éléments étant validés par les instances de gouvernance de la structure Engagement de la direction sur la réduction d'un nombre limité de risques chaque année	PSSI-MCAS - 1er octobre 2015 PGSSI-S : Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social - Mai 2015 - V1.0 PHN : Guide des indicateurs des prérequis et des domaines prioritaires du socle commun du programme hôpital numérique - Avril 2012 COFRAC : Guide technique d'accréditation pour l'évaluation des systèmes informatiques en biologie médicale - SH GTA 02