ÉDITION SPÉCIALE
SÉCURITÉ DE L'INFORMATION

NEWSLETTER **THÉMATIQUE** N°5

Mai 2017

Guide des bonnes pratiques pour la sécurité du système d'information

Sensibilisation et formation

“ Comme d'autres agences nationales, l'Agence eSanté lance la publication d'une newsletter spécifique à la sécurité de l'information. Au travers d'une série d'articles spécifiquement destinés au monde de la santé luxembourgeoise, nous allons distiller les bonnes pratiques pour le management de la sécurité de l'information et les procédures de traitement en interne des données à caractère personnel.

Didier Barzin
Responsable Pôle RSSI

Chaque établissement de santé est différent, de par sa taille, l'organisation de son système d'information, la nature des services offerts par son système d'information. Il n'est dès lors pas possible de rédiger un Système de Management de la Sécurité de l'Information qui conviendrait exactement à chaque structure de soins, à moins de rendre homogène tous les établissements de santé.

Cette série d'articles se veut être un guide pour la mise en place dans les établissements de santé d'un embryon d'un système de management de la sécurité couvrant les spécificités de ces établissements et traitant également les aspects liés à la protection des données. Nous aborderons entre autres, les aspects organisationnels et techniques, la sécurité de l'exploitation et des communications, la gestion de la relation avec les tiers et les sous-traitants …

Il est primordial de définir et de mettre en place des procédures de sécurité de l'information qui permettent de répondre en termes de conformité à la fois aux mesures attendues au niveau de la sécurité du système d'information que celles pour garantir la conformité aux lois et aux règlements - d'une façon plus large à l'échelle européenne - en ce qui concerne la protection des données à caractère personnel.

Julien Sassela
Chargé
Protection Données

La mise en place de ces mesures de sécurité et leur contrôle régulier sous le principe des quatre yeux permettent de remettre en cause les processus, et de coller au plus proche de la réalité l'évaluation et l'étude d'impact au sens large. Ce processus continu doit permettre d'éviter la majeure partie des incidents de sécurité et de prévenir d'éventuelles vulnérabilités du système d'information.

Cette dynamique de protection au sens large se fonde sur l'importance de la relation étroite et du travail en adéquation permanente entre, au niveau interne, le Responsable de sécurité des systèmes d'informations de santé (RSSI) et le Chargé de la protection des données (ou DPO, Data protection officer). Ce guide a pour objectif principal de décrire le périmètre de ces relations ainsi que les mécanismes et interactions entre ces deux postes clés permettant de garantir un haut niveau de conformité. ”

Guide n°1

Sensibilisation à la sécurité de l'information

Il est important de sensibiliser les équipes soignantes aux bonnes pratiques de sécurité informatique. Chaque soignant est un maillon à part entière de la chaîne de sécurité des systèmes d'information. À ce titre, dès son arrivée dans l'établissement, il doit être informé des enjeux de sécurité, des règles à respecter, des bons comportements et des mesures d'hygiène de sécurité des systèmes d'information à adopter, à travers des actions de sensibilisation et de formation.

Ces formations doivent être régulières et adaptées aux soignants ciblés. Elles peuvent prendre différentes formes (mails, affichage, réunions, espace intranet dédié, etc.) et devraient aborder au minimum les sujets suivants :

- les objectifs et enjeux que rencontre l'établissement en matière de sécurité des systèmes d'information ;
- les informations considérées comme sensibles ;
- les réglementations et obligations légales ;
- les règles et consignes de sécurité régissant l'activité quotidienne : respect de la politique de sécurité, non-connexion d'équipements personnels au réseau de l'établissement, non-divulgation de mots de passe à un tiers, non-réutilisation de mots de passe professionnels dans la sphère privée et inversement, signalement d'événements suspects, etc. ;
- les moyens disponibles et participant à la sécurité du système : verrouillage systématique de la session lorsque l'utilisateur quitte son poste, outil de protection des mots de passe, etc.

La direction de l'établissement doit communiquer sur l'importance de la sécurité de l'information au travers du bulletin d'information de l'établissement, d'une note de service, …

Pour renforcer ces mesures, l'élaboration et la signature d'une charte des moyens informatiques précisant les règles et consignes que doivent respecter les équipes soignantes peut être envisagée.

Cette charte doit être communiquée à tout le personnel soignant et revue régulièrement par le responsable de la sécurité de l'information et la direction de l'établissement.

Formation des équipes techniques

Il est important de former les équipes opérationnelles en charge de la gestion des équipements assurant la sécurité des systèmes d'information. Il faut s'assurer que ces équipes opérationnelles comprennent leurs responsabilités et qu'elles soient compétentes pour remplir les fonctions que l'établissement leur confie.

Les équipes opérationnelles ont des accès privilégiés au système d'information. Elles peuvent, par inadvertance ou par méconnaissance des conséquences de certaines pratiques, réaliser des opérations génératrices de vulnérabilités. Citons par exemple l'affectation de comptes disposant de trop nombreux privilèges par rapport à la tâche à réaliser, l'utilisation de comptes personnels pour exécuter des services ou tâches périodiques, ou encore le choix de mots de passe peu robustes donnant accès à des comptes privilégiés.

À intervalles réguliers, il faut vérifier la définition des postes et le plan de formation suivi par chaque membre de ces équipes. Les équipes opérationnelles sont appelées à maintenir des contacts réguliers avec les groupes de spécialistes en sécurité de l'information. Le Luxembourg possède de nombreuses organisations très actives en matière de sécurité de l'information, telles qu'entre autres :

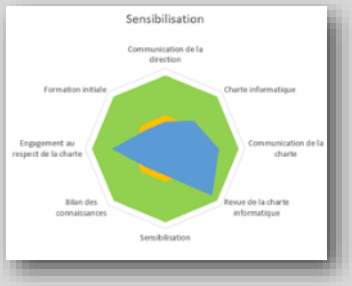
- Le Club de la Sécurité de l'Information – Luxembourg (CLUSIL)
- Le Club de Professionnels de la Sécurité de l'Information (CPSI)
- SecurityMadeIn.lu qui organise une fois par mois un déjeuner-conférence autour de la cybersécurité.

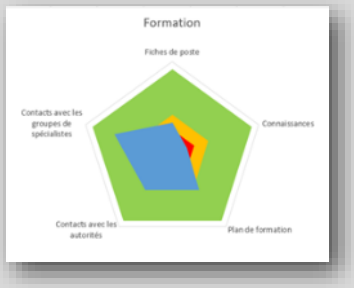
Ces organismes sont l'endroit idéal pour discuter des sujets pertinents et actuels de grand intérêt, partager des informations pertinentes pour l'amélioration de la sécurité et du travail opérationnel quotidien, et faire face à l'écosystème local de la cybersécurité.

Citons ici également la conférence Hack.lu, organisée annuellement au Luxembourg et qui en est à sa 13ème édition cette année. Cette conférence rassemble de nombreux spécialistes de la sécurité de l'information qui viennent présenter des applications concrètes et/ou échanger au sujet de la sécurité informatique, de la protection de la vie privée, de la technologie de l'information et de ses implications culturelles/ techniques sur la société.

Tableaux de bord

Le responsable de la sécurité de l'information est tenu de mesurer à intervalles réguliers l'efficacité des mesures mises en place. Il le fait par moyen d'un tableau de bord, qu'il présente à la direction périodiquement et sur base duquel il tire des conclusions et met en place des plans de remédiation afin d'améliorer ces indicateurs lors de la prochaine évaluation.





Il se doit de conserver des informations documentées permettant de prouver que la sécurité est planifiée, réalisée, contrôlée et ajustée afin d'améliorer sans cesse la qualité du Système de Management de la Sécurité de l'Information.

Références

- ISO/CEI 27001 - Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences
- ISO/CEI 27002 - Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information
- Club de la Sécurité de l'Information – Luxembourg (CLUSIL) - www.clusil.lu
- Club de Professionnels de la Sécurité de l'Information (CPSI) – www.cpsi.lu
- Security Made In Luxembourg – www.SecurityMadeIn.lu
- Hack.lu 2017 - www.hack.lu

Sensibilisation

Les questions qu'il faut se poser

- La direction de l'établissement communique-t-elle sur l'importance de la sécurité de l'information au travers de son bulletin d'information interne ?
- Existe-t-il une charte informatique dans l'établissement destinée au personnel soignant ?
- La charte est-elle communiquée au personnel soignant lors de sa prise de fonction ?
- La charte informatique est-elle revue annuellement par le RSSI et la direction de l'établissement ?
- Un bilan des connaissances en matière de sécurité de l'information est-il réalisé à la fin de chaque session d'apprentissage et de formation pour évaluer les acquis ?
- Quel pourcentage d'employés se sont engagés formellement à suivre la charte informatique de l'établissement ?
- Quelle est la date de la dernière campagne de sensibilisation à la sécurité de l'information destinée aux professionnels de santé de l'établissement? Une évaluation de l'impact de cette campagne a-t-elle été réalisée ?
- Quand les professionnels de santé ont-ils été informés pour la dernière fois du contenu de la charte informatique ?
- Existe-t-il un plan de formation à la sécurité de l'information que le personnel soignant reçoit lors de son arrivée dans l'établissement ?

Formation

Les questions qu'il faut se poser

- Des fiches de postes décrivant des rôles et responsabilités des équipes techniques sont-elles établies ?
- Les connaissances nécessaires à la réalisation de ces tâches sont-elles définies et réévaluées ?
- Un plan de formation continue est-il en place afin de maintenir les connaissances nécessaires à la réalisation de ces tâches ?
- A quelle fréquence l'établissement a-t-il des contacts avec les autorités pour évoquer les aspects relatifs à la sécurité de l'information ou de la protection des données à caractère personnel ?
- A quelle fréquence l'établissement a-t-il été en contact avec des groupes de spécialistes en matière de sécurité de l'information ?