40 règles « d'hygiène informatique » pour assurer la sécurité informatique d'un cabinet/service d'imagerie médicale

Le système d'information (RIS, PACS, internet, …) est au cœur de l'organisation de tout cabinet/service d'imagerie médicale.
C'est un structurant fondamental du fonctionnement du centre d'imagerie.
Mais il nécessite le respect de règles de sécurité.
Il est de la responsabilité des dirigeants de vérifier que les mesures de protection adaptées sont mises en place et opérationnelles. Elles doivent faire l'objet d'une politique de sécurité écrite, comprise et connue de tous. L'application de ces règles doit être régulièrement vérifiée.
Parmi ces mesures, il existe des mesures techniques simples, qualifiées « d'hygiène informatique » car elles sont la transposition dans le monde numérique de règles élémentaires de sécurité sanitaire.
Nous les détaillons ici.

Cet article est rédigé sur la base du document « Guide d'hygiène informatique » publié par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), Version 1.0 - Janvier 2013, sites internet : www.ssi.gouv.fr et www.securite-informatique.gouv.fr

Règle n°1 : Disposer d'une cartographie précise de l'installation informatique et la mettre à jour dès que nécessaire.
Cette cartographie doit préciser :
- la liste des matériels (en précisant le modèle) et des logiciels (en précisant la version utilisée),
- l'architecture réseau sur laquelle sont identifiés les points névralgiques (il est nécessaire d'inventorier tous les accès Internet et toutes les interconnexions avec les réseaux partenaires).

Attention : cette cartographie ne doit pas être stockée sur le réseau qu'elle représente car il s'agit de l'un des éléments que l'attaquant va rechercher en premier lieu en cas d'intrusion.

Règle n°2 : Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour. Ce point concerne principalement les services administratifs, financiers, …
Attention : faire attention aux utilisateurs qui disposent d'un poste non administré par le service informatique.

Règle n°3 : Rédiger et appliquer des procédures de conduite à tenir en cas d'arrivée et de départ des utilisateurs (personnels, stagiaires, …).
Il faut s'assurer que les droits sont appliqués au plus juste.
Il est important que les droits affectés à une personne soient révoqués lors de son départ.

Règle n°4 : Limiter le nombre d'accès Internet du cabinet/service au strict nécessaire. Il est très important de connaitre exactement le nombre de postes ayant accès à Internet.

Règle n°5 : Interdire la connexion d'équipements personnels au système d'information du cabinet/service (tablettes, smartphones, lecteurs MP3, clefs USB).
Ils sont difficilement maitrisables car ce sont les utilisateurs qui décident eux-mêmes du niveau de sécurité de leurs équipements.

Cette règle est souvent mal vécue. Cependant, il faut savoir que statistiquement, 10% des équipements sont compromis par un code malveillant générique. En cas de travail à distance nécessaire, le cabinet/service doit fournir les moyens professionnels pour permettre de tels usages.
Le transfert de messages des messageries professionnelles vers les messageries personnelles doit être interdit.

Règle n°6 : Connaitre les modalités de mise à jour de l'ensemble des composants logiciels utilisés et se tenir informé des vulnérabilités de ces composants et des mises à jour nécessaires.
Une mise à jour du logiciel ne peut être téléchargée que du site de l'éditeur.

Règle n°7 : Définir une politique de mise à jour et l'appliquer strictement. Il est primordial de définir :
- les éléments à mettre à jour,
- les responsabilités des différents acteurs de cette mise à jour,
- les moyens de récupération et de qualification des mises à jour.

Règle n°8 : Identifier nommément chaque personne ayant accès au système.
L'objectif de cette règle est de supprimer les comptes et accès génériques et anonymes.

Règle n°9 : Définir des règles de choix et de dimensionnement des mots de passe (cf. fiche « règles d'utilisation des mots de passe »).

Règle n°10 : Mettre en place des moyens techniques permettant de faire respecter les règles relatives à l'authentification. Par exemple :
- blocage des comptes tous les 6 mois si le mot de passe n'est pas changé,
- blocage de toute configuration du poste qui permettrait le démarrage du poste dans un mode « sans mot de passe »,
- vérifier que les mots de passe choisis ne soient pas faciles à trouver.

Règle n°11 : Ne pas conserver les mots de passe en clair dans les fichiers sur les systèmes informatiques. Ne pas utiliser les mécanismes automatiques « se souvenir du mot de passe ».

Règle n°12 : Renouveler systématiquement les éléments d'authentification par défaut sur les équipements (commutateurs réseau, routeurs, serveurs, imprimantes).

Règle n°13 : Privilégier lorsque cela est possible une authentification forte par carte à puce.

Règle n°14 : Mettre en place un niveau de sécurité homogène sur l'ensemble du parc informatique.

Règle n°15 : Interdire techniquement la connexion des supports amovibles sauf si cela est strictement nécessaire.

Règle n°16 : Utiliser un outil de gestion de parc informatique permettant de déployer des pratiques de sécurité et les mises à jour sur les équipements.

Règle n°17 : Gérer les terminaux nomades selon une politique de sécurité au moins aussi stricte que celle des postes fixes.

Règle n°18 : Interdire dans tous les cas où cela est possible, les connexions à distance sur les postes clients.

Règle n°19 : Chiffrer les données sensibles, en particulier sur les postes nomades et les supports potentiellement perdables (en cas de perte ou de vol par exemple).

Règle n°20 : Auditer régulièrement la configuration de l'annuaire central (il convient de vérifier si les droits d'accès sont correctement positionnés).

Règle n°21 : Mettre en place des réseaux cloisonnés. Pour les postes ou les serveurs contenant des informations importantes, créer un sous-réseau protégé par une passerelle d'interconnexion spécifique.

Règle n°22 : Eviter l'usage d'infrastructure sans fil (WIFI). Si l'usage ne peut être évité, cloisonner le réseau d'accès WIFI du reste du système d'information.

Règle n°23 : Utiliser systématiquement des applications et des protocoles sécurisés :
- à éviter : les réseaux telnet, FTP, POP, SMTP, http, …
- à remplacer par leurs équivalents sécurisés : SSH, SFTP, POPS, SMTPS, HTTPS, …

Règle n°24 : Sécuriser les passerelles d'interconnexion avec Internet. Il faut permettre un cloisonnement entre l'accès Internet, la zone de service (DMZ) et le réseau interne.

Règle n°25 : Vérifier qu'aucun équipement du réseau ne comporte d'interface d'administration accessible depuis Internet. Cette règle concerne les imprimantes, les serveurs, les routeurs, les commutateurs réseau.

Règle n°26 : Définir concrètement les objectifs de la supervision des systèmes et des réseaux.
Les problèmes suivants doivent être traités dans les 24 heures :
- connexion d'un utilisateur hors de ses horaires habituels de travail ou pendant une absence déclarée,
- transfert massif de données vers l'extérieur du cabinet/service,
- tentative de connexions successives ou répétées sur un service,
- tentative de connexions sur un compte non actif,
- tentative de contournement de la politique de sécurité : utilisation d'un service interdit, connexion non autorisée à un service…).

Règle n°27 : Définir les modalités d'analyse des évènements journalisés. Il faut vérifier en particulier les deux points suivants :
- analyse de la liste des accès aux comptes de messagerie des personnes clé du cabinet/service,
- analyse des accès aux machines ou aux ressources sensibles du cabinet/service.

Règle n°28 : Interdire tout accès à l'internet depuis les comptes de l'administration.

Règle n°29 : Utiliser un réseau dédié à l'administration des équipements ou au moins un réseau logiquement séparé du réseau des utilisateurs.

Règle n°30 : Ne pas donner aux utilisateurs de privilège d'administration. Ne faire aucune exception.

Règle n°31 : N'autoriser l'accès à distance au réseau du cabinet/service, y compris pour l'administration du réseau, que depuis des postes du cabinet/service qui mettent en œuvre des mécanismes d'authentification forte et qui protègent intégrité et la confidentialité des échanges à l'aide de moyens robustes.

Règle n°32 : Utiliser impérativement des mécanismes robustes de contrôle d'accès des locaux.

Règle n°33 : Protéger rigoureusement les clés permettant l'accès aux locaux et les codes d'alarme.
Les règles suivantes doivent être appliquées :
- récupérer systématiquement les clefs ou les badges d'un employé à son départ définitif du cabinet/service,
- changer régulièrement les codes de l'alarme,
- ne jamais donner de clef ou de code d'alarme à un prestataire externe sauf s'il est possible de tracer les accès et de les restreindre techniquement à des plages horaires définies.

Règle n°34 : Ne pas laisser de prises d'accès accessibles au réseau interne dans des endroits ouverts au public.
Attention :
- aux imprimantes ou photocopieuses entreposées dans les couloirs,
- aux écrans d'affichage diffusant des flux d'informations,
- aux caméras de surveillance,
- aux téléphones,
- aux prises réseau dans une salle d'attente.

Règle n°35 : Définir les règles d'utilisation des imprimantes et des photocopieuses :
- utiliser des imprimantes disposant d'un mécanisme d'impression nécessitant la présence physique du demandeur pour démarrer l'impression,
- détruire en fin de journée (dans les broyeuses) tous les documents oubliés sur l'imprimante ou la photocopieuse,
- prévoir des procédures de recyclage ou de destruction pour les supports informatiques en fin de vie.

Règle n°36 : Disposer d'un plan de reprise et de continuité de l'activité informatique tenu régulièrement à jour et décrivant comment sauvegarder les données essentielles du cabinet/service.

Règle n°37 : Mettre en place une chaine d'alerte et de réaction connue de tous les intervenants. Tous les interlocuteurs doivent pouvoir s'adresser à un interlocuteur référent en cas d'incident.

Règle n°38 : Ne jamais se contenter de traiter l'infection d'une machine sans tenter de saisir comment le code malveillant a pu s'installer, s'il a pu se propager ailleurs dans le réseau et quelles informations ont été manipulées.
Quelles sont les questions à se poser ? :

- nature du poste compromis : y en a-t-il d'autres du même type, exposés aux mêmes menaces ?
- quelles sont les informations auxquelles l'attaquant a pu avoir accès ?
- le poste compromis a-t-il communiqué avec d'autres postes ou serveurs ?

En cas de compromission et afin de faciliter le travail des équipes d'investigation, il est possible de :

- ne pas éteindre électriquement les machines infectées pour préserver les informations disponibles en mémoire,
- réaliser ou faire réaliser des copies de mémoires et des disques durs des machines infectées,
- réinstaller intégralement la machine après copie des disques durs. Ne jamais se contenter d'une simple restauration ou d'un nettoyage.

Règle n°39 : Sensibiliser les utilisateurs aux règles d'hygiène informatique élémentaires :

- non contournement de la politique de sécurité,
- verrouillage systématique de la session si l'utilisateur quitte son poste,
- non connexion d'équipements personnels,
- non divulgation des mots de passe,
- non réutilisation des mots de passe professionnels dans la sphère privée,
- signalement des évènements suspects.

Il est fortement conseillé de rédiger une charte informatique.

Règle n°40 : Faire réaliser des audits de sécurité périodique (au moins une fois par an). Chaque audit doit être associé à un plan d'actions.