GOUVERNEMENT
Liberté
Égalité
Fraternité

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

LA CYBERSÉCURITÉ POUR LES ESSMS EN 13 QUESTIONS

OCTOBRE 2022

ÉDITOS

Le numérique est devenu incontournable dans notre système de santé. Il permet le décloisonnement et une meilleure coordination des professionnels. Il favorise les innovations thérapeutiques et organisationnelles. Il replace l'individu au cœur des organisations de soin. Paradoxalement, les flux croissants et l'échange nécessaire d'informations sont autant de prises de risque pour la sécurisation des données et donc *in fine* pour la prise en charge des individus.

Le virage numérique amorcé par Ma Santé 2022 est en phase d'être relevé. Il nécessite aujourd'hui plus que jamais une gouvernance solide et une utilisation contrôlée.

La menace est réelle comme en témoignent de récents évènements. Face à cela, il n'est plus possible de faire de la cybersécurité une variable d'ajustement des systèmes d'information en santé.

Le secteur social et médico-social doit être en mesure de pouvoir comprendre, évaluer, anticiper et maîtriser ces risques, qui sont *in fine* une exposition pour la qualité des soins et des accompagnements et pour la confiance des utilisateurs.

Le volet numérique du Ségur de la santé a prévu une enveloppe de 2 milliards d'euros d'investissements pour accélérer la numérisation des établissements de santé et médico-sociaux. L'ambition est de permettre d'accompagner leur transition numérique, moderniser les systèmes d'information existants, renforcer leur interopérabilité et leur sécurité.

Les outils de la sécurité numérique ne manquent pas, mais ces derniers perdent toute efficacité s'ils ne sont pas parfaitement intégrés, si l'un des nombreux maillons de la chaîne est fragilisé ou défaillant.

Nous nous félicitons de la parution du Guide Cybersécurité spécialement appliqué au secteur social et médico-social qui propose aux acteurs des recommandations concrètes, claires et simples.

Notre préoccupation commune étant et devant rester le patient – le résident – le bénéficiaire, nous avons à cœur de soutenir chaque organisation, quel que soit sa maturité numérique, afin que la cybersécurité soit l'engagement de tous. Nous voulons ainsi que l'investissement collectif permette de limiter la vulnérabilité de leur système et soit au service de la qualité des soins et des accompagnements grâce à une gouvernance solide en la matière, tout en protégeant les droits et données des personnes.

Jean-Christophe Combe,
ministre des Solidarités, de l'Autonomie
et des Personnes handicapées

François Braun,
ministre de la Santé et de la Prévention

L'augmentation des cyberattaques nous impose une résilience de plus en plus importante. Le secteur social et médico-social, qui vit sa transformation numérique, doit être en mesure de se protéger, et de faire face, au même titre que le secteur sanitaire. C'est dans cette ambition que l'Agence du Numérique en Santé (ANS) se mobilise au quotidien.

Régulatrice, elle produit les référentiels et les guides de la Politique Générale de la Sécurité des Systèmes d'Information en santé (PGSSI S), elle définit les exigences cyber de la doctrine du numérique en santé, et gère le schéma de certification des hébergeurs de données de santé.

Aussi, elle héberge le CERT Santé qui apporte un appui aux établissements et services sociaux et médico-sociaux (ESSMS) dans la veille sur les menaces cyber et la réponse à un incident de sécurité des systèmes d'information.

Enfin, dans le cadre de son programme de transformation, l'ANS a souhaité « aller vers » ses bénéficiaires. La nouvelle gouvernance de l'ANS, intégrant les Agences Régionales de Santé (ARS) et les Groupements Régionaux d'Appui au Développement de la e-santé (GRADeS) a souhaité instruire la cybersécurité dans un groupe de travail dédié. Plusieurs chantiers ont été menés dont l'un sur les actions de sensibilisation dans le secteur social et médico-social. Ces travaux ont rassemblé l'ensemble des parties prenantes du secteur pour travailler à ce guide, pensé pour les directeurs des ESMS et les référents SI.

Adapté au besoin du secteur, ce guide livre de manière pédagogique les clés fondamentales de l'hygiène informatique et des gestes à connaitre en cas d'incident. Il permet de participer pleinement à la démarche de protection de l'ESSMS pour l'ensemble des professionnels du secteur, en répondant à leurs questions sur les techniques d'hameçonnage et les moyens pour les éviter, mais aussi sur les premiers gestes à adopter dans le cas d'un incident. La force réelle de toute démarche de cybersécurité est constituée par un collectif humain informé et responsable !

Annie Prévot, directrice générale de l'Agence du Numérique en Santé

Le secteur social et médico-social est en pleine transformation. Cette transformation doit favoriser l'émergence d'une société plus inclusive et relever le défi de la logique « domiciliaire ». Elle vise à garantir à chaque personne un accompagnement souple, modulaire et construit au regard de ses attentes. À la Caisse nationale de solidarité pour l'autonomie (CNSA), nous sommes convaincus que le développement du numérique au service des personnes et des professionnels est une opportunité pour répondre à ces enjeux.

Dès 2019, la CNSA a initié le programme ESMS Numérique. Il a été amplifié grâce aux crédits du Ségur de la Santé. À travers ce programme, la CNSA appuie méthodologiquement et financièrement les établissements et services du secteur dans l'informatisation de leur « cœur de métier ». Informatiser le cœur de métier des ESSMS, c'est informatiser le dossier des usagers.

Ces dossiers comportent des données médicales et personnelles sensibles. Il est donc indispensable de sensibiliser et de mobiliser les gestionnaires de structures aux enjeux de la cybersécurité. C'est une condition *sine qua non* d'un développement du numérique réussi.

Ce guide a été construit pour et avec le secteur. Il doit permettre aux gestionnaires, quels que soient leur niveau d'équipement et leurs ressources informatiques, de franchir une première étape pour mieux sécuriser les données de leurs usagers et de sensibiliser leurs équipes aux mesures d'hygiène informatique.

Virginie Magnant, directrice de la Caisse nationale de solidarité pour l'autonomie (CNSA)

SOMMAIRE

INTRODUCTION

Historiquement peu informatisé, le secteur social et médico-social fait aujourd'hui l'objet d'un fort développement des usages numériques, encouragé par les pouvoirs publics, et le tournant de longue date qu'a pris la société comme nos usagers.

L'accélération du numérique vise à proposer un parcours cohérent et sans rupture grâce à un partage d'informations fluide entre les différents acteurs. La disponibilité du système d'information et l'intégrité des données des usagers et des professionnels sont des enjeux majeurs pour garantir un **accompagnement sécurisé dans le secteur social et médico-social.** La mise en œuvre d'actions de cybersécurité est un des moyens pour répondre à ses besoins.

Elle est définie comme un ensemble de moyens utilisés pour assurer la sécurité des systèmes et des données informatiques d'une organisation.

Le secteur social et médico-social est confronté aux risques cybersécurité, pouvant impacter le quotidien des professionnels de santé mais aussi mettre en péril la prise en charge du patient. Depuis ces dernières années, la cybersécurité est un enjeu indispensable pour transformer notre système de santé en toute confiance.

Ce guide présente, en treize questions, des mesures accessibles pour une protection globale de l'Établissement et Services sociaux et médico-sociaux (ESSMS). Certaines recommandations relèvent des bonnes pratiques, d'autres requièrent un investissement plus important. **Elles vous permettront d'accroître votre niveau de sécurisation et de sensibiliser vos équipes aux bons gestes à adopter.**

En l'absence de préparation, lorsque l'incident survient, il est déjà trop tard. N'attendons pas que le pire arrive. Ensemble, soyons tous cybervigilants !

ARTICULATION AVEC L'OBSERVATOIRE MaturiN-SMS

L'Observatoire MaturiN-SMS (Maturité Numérique pour les secteurs du social et du médico-social) a pour objectif d'accompagner les établissements et services sociaux et médico-sociaux dans leur montée en maturité en matière de numérique. Il va permettre d'outiller les acteurs, via un système d'indicateurs à paliers, pour mesurer leur maturité numérique afin de l'améliorer. À ce titre, il contient plusieurs indicateurs relatifs à la cybersécurité : le lien a été fait avec les questions du guide pour vous mettre de mesurer facilement votre niveau de maturité sur chacune des thématiques.

SYNTHÈSE

ACTIONS PRIORITAIRES À RÉALISER

1. Connaissez-vous suffisamment votre parc informatique ?

- **Inventorier :**
  - les équipements et services
  - les logiciels utilisés
  - les données et traitements de données
  - les droits et les accès
  - les interconnexions

2. Effectuez-vous des sauvegardes régulières ?

- **Identifier les données à sauvegarder**
- **Déterminer le rythme des sauvegardes**
- **Choisir le ou les supports à privilégier pour la sauvegarde**
- **Évaluer la pertinence du chiffrement des données**

3. Appliquez-vous régulièrement les mises à jour ?

- **Utiliser des solutions matérielles et logicielles maintenues**
- **Activer la mise à jour automatique des logiciels et des matériels**

4. Utilisez-vous un antivirus ?

- **Déployer un antivirus sur tous les équipements**
- **Centraliser la gestion des antivirus**

5. Avez-vous implémenté une politique d'usage de mots de passe robuste ?

- **Formaliser des exigences en matière de complexité des mots de passe**
- **Définir des fréquences régulières de changement des mots de passe**

6. Avez-vous activé un pare-feu ?

- **A minima, activer le pare-feu préinstallé sur le poste de travail et son paramétrage par défaut**
- **Installer sur tous les postes de travail un pare-feu local (qu'il soit intégré au système d'exploitation ou qu'il soit une solution logicielle tierce)**

7. Comment sécurisez-vous votre messagerie ?

- Sensibiliser les professionnels
- Proscrire la redirection de messages professionnels vers une messagerie personnelle
- Disposer d'un système d'analyse antivirus
- Activer le chiffrement de la couche de transport (Transport Layer Security-TLS)

8. Comment séparez-vous vos usages informatiques ?

- Créer des comptes utilisateurs dédiés à chaque salarié et ne disposant pas de privilège d'administration
- Au départ d'un collaborateur, faire l'inventaire de ses accès et les révoquer

9. Comment maîtrisez-vous le risque numérique lié au nomadisme des professionnels ?

- Sauvegarder régulièrement ses données
- Conserver son matériel informatique
- Réduire voire supprimer l'utilisation des clés USB

10. Comment vous informez-vous ? Comment sensibilisez-vous vos collaborateurs ?

- Formaliser une charte informatique
- Prévoir des formations à la cybersécurité

11. Savez-vous comment réagir en cas de cyberattaque ?

- Organiser des exercices de crise cybersécurité
- En cas d'incident, déconnecter son équipement ou SI d'internet mais ne pas éteindre ou modifier les ordinateurs et matériels affectés par l'attaque
- Porter plainte

12. Avez-vous fait évaluer la couverture de votre police d'assurance cyber ?

- Contacter son assurance en vue de souscrire à une clause permettant de se prémunir de certains risques d'origine numérique (cyber malveillance, cyberattaques)

13. Maîtrisez-vous les risques numériques liés à vos relations avec des tiers ?

- Identifier et décrire dans les contrats les missions confiées à des tiers
- Formaliser des exigences de sécurité et les annexer au contrat avec les prestataires
- Identifier les membres de l'organisation assurant le lien avec les fournisseurs
- Documenter les moyens mis en œuvre par les prestataires pour respecter les exigences de sécurité

QUESTION 1

CONNAISSEZ-VOUS suffisamment VOTRE PARC INFORMATIQUE ?

Pour protéger son système d'information, tout ESSMS doit dans un premier temps inventorier son système d'information : son matériel, ses logiciels utilisés, ses données et les traitements associés. De cet inventaire découle l'identification de mesures de protection adaptées.

Inventorier les équipements et services

Plusieurs équipements sont à inventorier : ordinateur (et ses périphériques), mobile multifonction (smartphone), tablette, serveur local et serveur distant (hébergeur du site web et messagerie, services en ligne), périphériques (box, clés 4G, imprimantes, etc.). **Cet inventaire permet d'identifier les biens critiques à protéger pour sécuriser l'activité de l'ESSMS.**

L'inventaire doit **lister toutes les informations utiles :** nom du matériel, fabricant, numéro de série, modèle, système d'exploitation, fournisseur et date d'achat, lieu d'utilisation et type d'utilisation (poste dédié ou partagé), fin de garantie, numéro du contrat de maintenance, date du renouvellement du poste à prévoir, date de la dernière maintenance, etc.

Des logiciels et applications permettent de gérer plus facilement l'inventaire du parc informatique.

Inventorier les logiciels

L'inventaire des logiciels permet de **disposer de l'ensemble des informations relatives à chaque logiciel :** noms, fonctions principales, version, éditeur, présence sur le parc informatique, utilisateurs, dernière formation et utilisateurs concernés, etc.

Il faut s'assurer d'être en possession de licences d'utilisation valides, en nombre suffisant. Elles sont indispensables aussi bien du point de vue des **obligations légales, que pour la maintenance.**

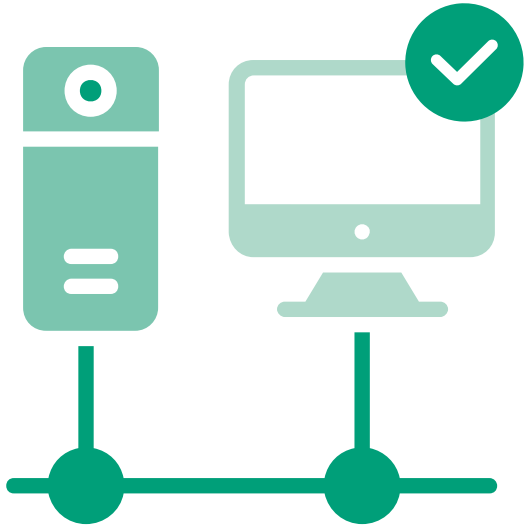
Inventorier les données et traitements

L'inventaire des données et traitements doit permettre de répondre aux questions suivantes :

- quelles sont les données et traitements susceptibles **d'affecter la prise en charge des usagers** ou d'interrompre l'activité en cas de perte ou d'altération ?
- quelles sont **les données sensibles** et celles soumises à des **obligations légales** ? Où sont conservées les données sensibles (dont les données de santé) ?

Inventorier les accès

Il s'agit de déterminer, comme le préconise le Règlement Général sur la Protection des Données (RGPD), **qui se connecte au système d'information et selon quelles modalités :** catégorie de



l'accédant (administrateur, utilisateur, invité), moyen d'accès (connexion locale ou distante).

Cet inventaire permettra de **contrôler les droits d'accès** et de vérifier qu'aucun accès indu n'est maintenu (ancien employé, ancien prestataire) afin de **limiter la surface d'exposition aux menaces.**

Inventorier les interconnexions avec l'extérieur

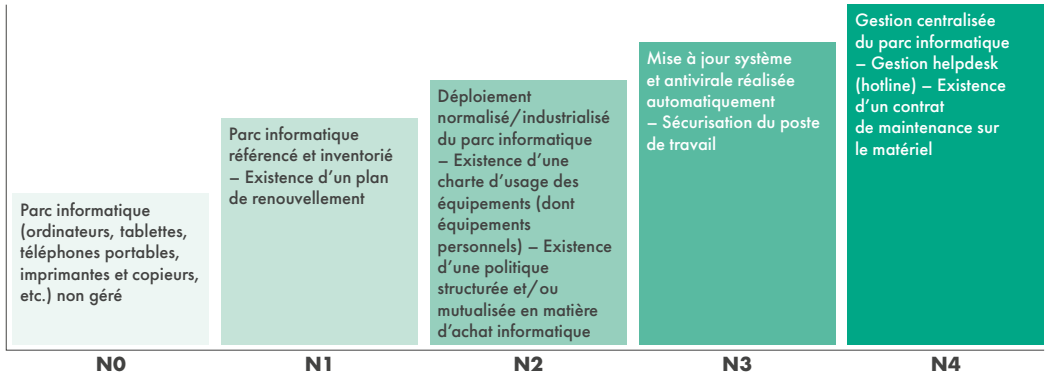
Tout accès Internet, depuis ou vers un prestataire ou un partenaire, doit être inventorié. Des règles de filtrage et de surveillance adaptées pourront y être associées.

Mettre régulièrement à jour les différents inventaires

Ces cinq inventaires doivent être **mis à jour régulièrement** (au moins deux fois par an) pour présenter une image relativement proche du réel et rester un outil de suivi et de contrôle. Ce bilan régulier permet **d'aider au choix des solutions numériques adaptées à l'ESSMS, d'identifier les points de sécurisation** et, le cas échéant, de fournir un état des lieux détaillé qui aidera le prestataire sollicité pour cette tâche. Il sera aussi très utile pour les professionnels qui interviendront en réponse à un incident en cas de compromission réelle. **Le Délégué à la Protection des Données (DPD)** peut éventuellement être un soutien et une ressource à solliciter dans ce travail.

LIEN AVEC LES INDICATEURS DE L'OBSERVATOIRE SIN MS

GESTION DU PARC INFORMATIQUE



POUR EN SAVOIR PLUS

- Cartographie du système d'information – guide d'élaboration en 5 étapes

QUESTION N°2

EFFECTUEZ-VOUS DES SAUVEGARDES RÉGULIÈRES ?

Effectuer des sauvegardes régulières permet une reprise plus rapide des activités opérationnelles en cas d'incident, notamment en cas d'attaque par rançongiciel.

Identifier les données à sauvegarder

Après l'inventaire du matériel, il est nécessaire de déterminer quelles données sont essentielles à la poursuite de votre activité. Il peut s'agir de données personnelles (relatives à l'usager ou aux professionnels), financières, administratives, etc.

Ainsi, plusieurs modalités de sauvegarde doivent être mises en œuvre en fonction du type de données sauvegardées (nature, criticité, volume,...). L'ESSMS doit définir une politique de gestion et de suivi des sauvegardes.

Déterminer le rythme de vos sauvegardes

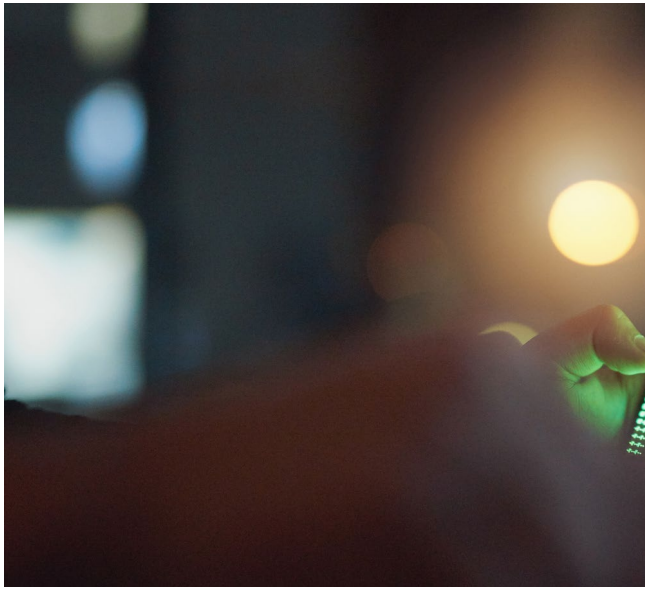
La fréquence des sauvegardes est à définir en lien avec le volume de données numériques produites sur un temps donné.

La règle « 3 – 2 — 1 » peut ainsi être mise en œuvre :

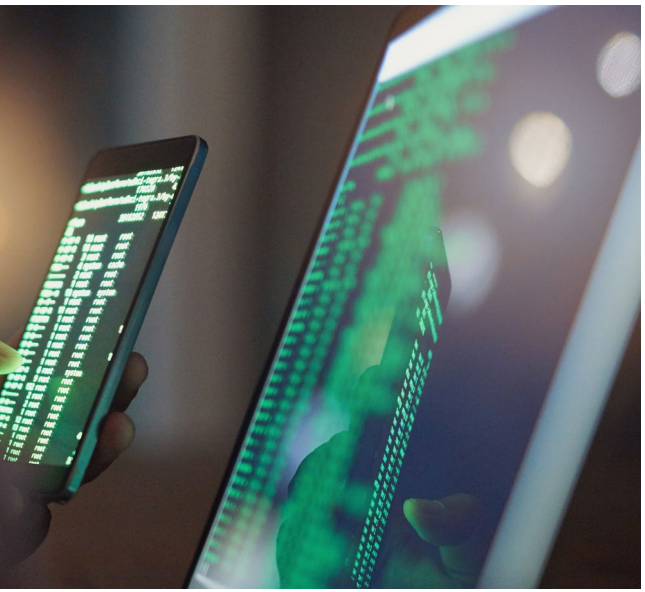
- des sauvegardes (idéalement 3 exemplaires) effectuées périodiquement : la période entre deux sauvegardes correspond à la perte que vous êtes prêts à accepter ;
- des tests de restauration complets des données pour vérifier le bon état de fonctionnement de vos supports (idéalement 2 distincts) et la bonne réalisation des sauvegardes ;
- une copie de sauvegarde protégée, déconnectée physiquement du système informatique et géographiquement éloignée pour parer tout sinistre local (incendie, dégât des eaux...).

Choisir le ou les supports à privilégier pour votre sauvegarde

Il peut s'agir d'un disque dur externe à accès limité, à déconnecter du système d'information à l'issue de la sauvegarde ou d'une sauvegarde dans un



« cloud sécurisé », voire des deux pour les données les plus précieuses. Le support physique présente l'avantage d'être à l'abri d'une intrusion informatique, mais pas à l'abri d'un vol, d'une destruction, d'une connexion à un appareil attaqué, ou d'un dysfonctionnement. Les « cloud » proposés aussi bien par les fournisseurs d'accès que par les éditeurs permettent une automatisation simple des sauvegardes mais sont plus exposés aux risques d'intrusion ou de panne. Quelle que soit votre préférence de support, toute sauvegarde, une fois effectuée, doit faire l'objet d'un test pour vérifier son intégrité et sa viabilité lors d'une restauration.



Il est impératif de recourir à un prestataire qui propose un hébergement adapté aux types de données conservées : en cas d'hébergement de données de santé, l'hébergeur doit ainsi être certifié hébergeur de données de santé (HDS).

Évaluer la pertinence du chiffrement des données

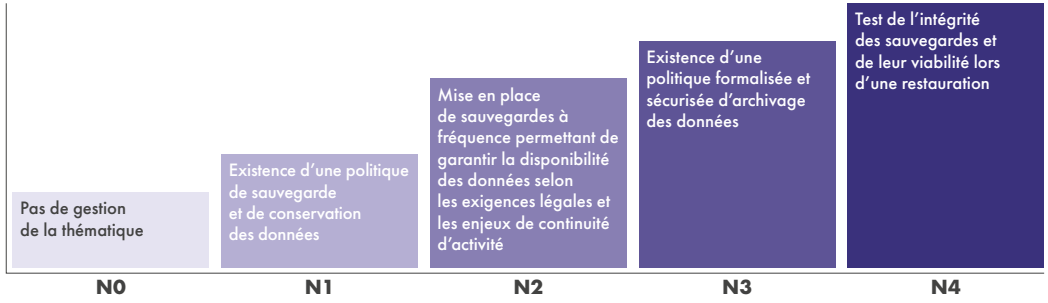
Le chiffrement des données avant leur sauvegarde est une pratique recommandée. Elle concerne en priorité le stockage dans un service de type « cloud » : en cas d'accès illégitime au cloud, les données restent protégées. Le choix de l'opérateur pour le « cloud », les modalités de stockage des données et les conditions d'accès et d'authentification seront autant de points de vigilance à vérifier.

Respecter le cadre juridique

Les données dites « personnelles », qu'elles soient relatives aux employés ou aux usagers, nécessitent des mesures de protection renforcées pour garantir le respect des exigences issues duRèglement Général sur la Protection des Données (RGPD). Les dispositifs juridiques de protection et de conservation des données s'appliquent quels que soient les objectifs du stockage (traitement ou sauvegarde). Qu'il s'agisse d'obligations fiscales ou de protection des données personnelles, appliquez les mêmes mesures à vos sauvegardes qu'à votre système d'information.

LIEN AVEC LES INDICATEURS DE L'OBSERVATOIRE SIN MS

POLITIQUE DE SAUVEGARDE ET CONSERVATION DES DONNÉES



POUR EN SAVOIR PLUS

- Pourquoi et comment bien gérer ses sauvegardes ?
- RGPD : de quoi parle-t-on ?
- Référentiel relatif aux traitements de données à caractère personnel mis en œuvre dans le secteur social et médico-social
- Documents de référence sur la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)

QUESTION N°3

APPLIQUEZ-VOUS RÉGULIÈREMENT LES MISES À JOUR ?

La majorité des attaques ciblent des **vulnérabilités publiques et documentées pour prendre pied sur les systèmes d'information :** les pirates informatiques comptent soit sur la négligence des utilisateurs soit sur la vulnérabilité d'un service exposé sur Internet (pare-feu, messagerie, etc.).

Il est indispensable **d'effectuer les mises à jour** des systèmes d'exploitation et de tout logiciel dès la mise à disposition des correctifs de sécurité par leurs éditeurs.

Utiliser des solutions matérielles et logicielles maintenues

Par habitude, par négligence ou par souci d'économies, il peut être tentant de **conserver un matériel ou un logiciel au-delà de son « cycle de vie »,** c'est-à-dire après la période pendant laquelle son fabricant ou son éditeur garantit son maintien en conditions de sécurité. Tout matériel ou logiciel qui ne peut plus être mis à jour doit être **mis au rebut ou désinstallé.**

Activer la mise à jour automatique des logiciels et des matériels

Les mises à jour du système d'exploitation et de tous les logiciels utilisés doivent être effectuées dès que possible, à chaque mise à disposition d'un correctif par leurs éditeurs. **Cela est d'autant plus important pour tous les matériels exposés sur Internet.**

Il est recommandé d'activer les fonctions de **mise à jour automatique** proposées par les éditeurs.

En complément, des **mises à jour hors calendrier** peuvent survenir en cas de détection d'une vulnérabilité, et devront être **appliquées dès que possible.**

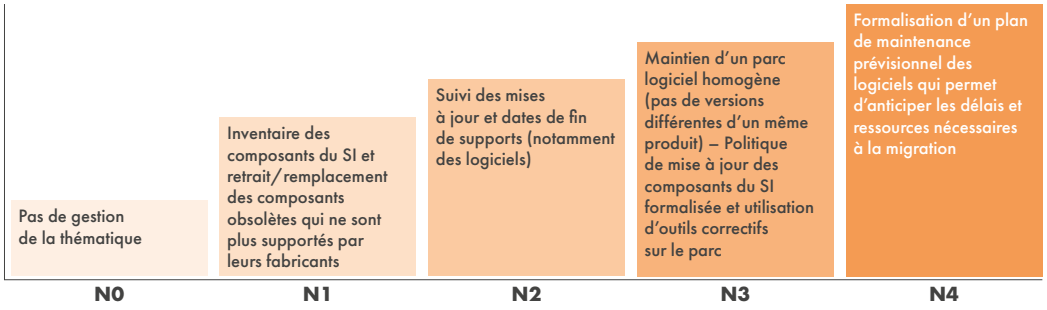
Si vous recourez à un sous-traitant, **assurez-vous qu'il effectue bien le maintien en condition de sécurité des systèmes numériques** utilisés dans votre ESSMS. Nous vous recommandons **d'exiger cette pratique dans vos contrats de sous-traitance.**

POUR EN SAVOIR PLUS

- Guide d'hygiène informatique
- Externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques
- Pourquoi et comment bien gérer ses mises à jour ?

LIEN AVEC LES INDICATEURS DE L'OBSERVATOIRE SIN MS

POLITIQUE DE MISE À JOUR



QUESTION 4

UTILISEZ-VOUS UN ANTIVIRUS ?

Déployer un antivirus sur tous les équipements

Les antivirus sont très utiles à la protection des moyens informatiques : ils peuvent dans la majorité des cas **bloquer une attaque par rançongiciel et réduire le risque de compromission.** Un antivirus doit être déployé sur tous les équipements, en priorité ceux connectés à Internet (postes de travail, serveurs de fichier, etc.). **Un antivirus protège des menaces connues,** qui évoluent très rapidement : des centaines de milliers de codes malveillants apparaissent chaque jour.

Ainsi, il faut **tenir à jour le logiciel en lui-même** et sa base de données de signatures. Cette base de données est l'élément qui permet l'identification de programmes et fichiers malveillants : sans mise à jour fréquente, la protection offerte par l'antivirus s'en trouve très rapidement amoindrie.

Les antivirus commerciaux proposent une mise à jour automatique, et un scan automatique des espaces de stockage : il est indispensable de procéder à l'activation de ces mécanismes dans les paramètres.

Par ailleurs, lors de l'achat d'un antivirus, il peut être préconisé, en fonction de vos usages, de **souscrire aux fonctionnalités complémentaires** proposées par de nombreux éditeurs logiciels tels qu'un pare-feu, un filtrage Web, un VPN, des outils anti-hameçonnage et de renforcement de la sécurité des transactions bancaires.

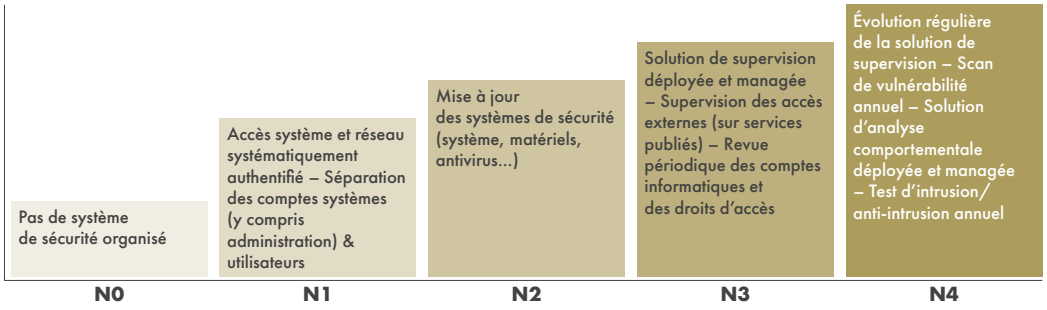
Enfin, il est recommandé de mettre en œuvre une **gestion centralisée des antivirus** afin de pouvoir assurer un suivi et un contrôle du bon déploiement de ceux-ci sur l'ensemble des équipements à disposition et utilisés.

POUR EN SAVOIR PLUS

- Les antivirus – Assistance aux victimes de cybermalveillance

LIEN AVEC LES INDICATEURS DE L'OBSERVATOIRE SIN MS

SÉCURITÉ SYSTÈME & RÉSEAU HARDWARE (SYSTÈME & RÉSEAU)



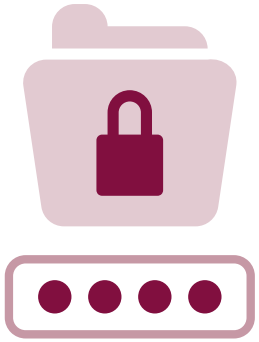
QUESTION N°5

AVEZ-VOUS IMPLÉMENTÉ UNE POLITIQUE D'USAGE DE MOTS DE PASSE ROBUSTES ?

Choisir des mots de passe robustes

De nombreuses attaques sur Internet sont facilitées par l'utilisation de mots de passe trop simples, réutilisés ou partagés entre plusieurs utilisateurs. Les attaques contre des mots de passe peuvent être de différentes natures : par force brute (l'attaquant tente le plus grand nombre de combinaisons possibles), par dictionnaires (l'attaquant tente les mots de passe les plus courants), de type « ingénierie sociale » (test des informations personnelles après les avoir récupérées sur les réseaux sociaux : prénoms de vos proches ou surnoms de vos animaux de compagnie), à partir d'éléments déjà disponibles en ligne (ex : à partir d'une base de données mal sécurisée d'un fournisseur).

Par ailleurs, une attaque contre les mots de passe au sein d'un ESSMS est susceptible d'impacter l'organisme gestionnaire ainsi que ses partenaires. De même, votre courriel pourrait être utilisé par l'attaquant pour adresser des courriels malveillants à vos contacts professionnels afin de les inciter à faire des actions dangereuses à leur insu (comme cliquer sur un lien vers un site Internet compromis) : **on parle d'hameçonnage** (ou phishing en anglais).



Qu'est-ce qu'un mot de passe robuste ?

L'Agence National de la Sécurité des Systèmes d'Information (ANSSI) recommande un minimum de 9 caractères pour les services peu critiques (dont la compromission ne donnerait accès à aucune information personnelle, financière et n'impacterait pas le fonctionnement de l'organisation) et **un minimum de 14 caractères pour les services critiques** (dont la compromission donnerait l'accès à des données de santé de l'usager).

Un mot de passe robuste comporte :

- capitales
- minuscules
- chiffres
- caractères spéciaux.

Il ne doit comporter aucun élément personnel (tel qu'une date de naissance ou un prénom). Il est possible d'avoir recours à une phrase de passe (passphrase en anglais) en choisissant aléatoirement un certain nombre de mots. Les passphrases sont souvent plus longues que les mots de passe « classiques », mais sont aussi pour certains utilisateurs plus simples à mémoriser.

Définir une bonne politique de mots de passe

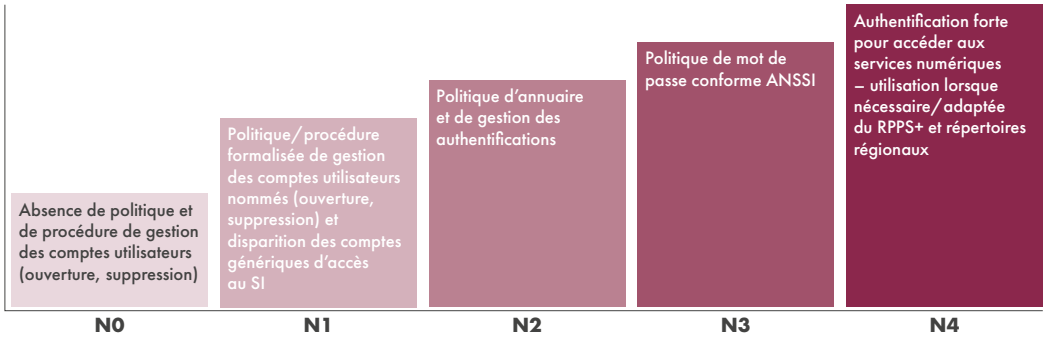
Il est impératif d'utiliser des mots de passe différents pour chaque service nécessitant. Il convient en particulier de ne jamais utiliser un même mot de passe pour sa messagerie personnelle et sa messagerie professionnelle. L'outil « coffre-fort » vous permet de générer des mots de passe robustes et les garder en mémoire grâce à la sauvegarde d'un fichier chiffré accessible uniquement par un seul et unique mot de passe. Il est recommandé d'utiliser un coffre-fort certifié par l'ANSSI (https://www.ssi.gouv.fr/entreprise/produits-certifies/produits-certifies-cspn/#category_3).

Le succès d'une bonne politique de mots de passe nécessite une sensibilisation des utilisateurs aux risques liés au choix d'un mot de passe qui serait trop facile à deviner. **Il est fortement recommandé d'activer une authentification multi-facteurs pour les applications qui gèrent des données de santé (exemple : Dossier Usager Informatisé).** L'authentification multi-facteurs permet de renforcer la sécurité de l'accès à vos comptes grâce à l'ajout d'un ou de plusieurs facteurs d'authentification : par exemple, un code reçu par mail ou par SMS. Il est recommandé d'activer cette authentification secondaire dès qu'elle vous est proposée.

L'authenfication unifiée (pour les référents Système d'Information – SI)

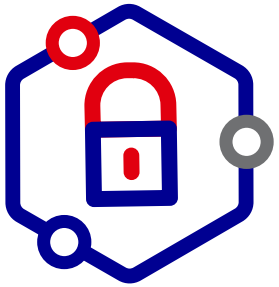
Pour les ESSMS qui disposent de nombreuses solutions logicielles centralisées (messagerie, services Web internes, etc.), **l'activation d'un service d'authentification unifié (type *Single Sign-on*) permet de simplifier et de renforcer les mécanismes d'authentification.** Ce type de service permettra notamment le blocage des comptes à l'issue de plusieurs échecs de connexion, la désactivation des options de connexion anonyme (comptes « invité ») et la mise en place d'une politique robuste des mots de passe sur les serveurs d'authentification.

LIEN AVEC LES INDICATEURS DE L'OBSERVATOIRE SIN MS
IDENTITÉ DE L'UTILISATEUR (PROFESSIONNEL)



POUR EN SAVOIR PLUS

- Pourquoi et comment bien gérer ses mots de passe ?
- Recommandations relatives à l'authentification multi facteur et aux mots de passe
- Sensibilisation à la sécurité des mots de passe
- Documents de référence sur la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)
- Qu'est-ce que Pro Santé Connect (PSC) ?



Pro Santé Connect (PSC)

Pro Santé Connect (PSC) est un fédérateur d'identité proposé par les pouvoirs publics (à l'instar de France Connect). Il permet aux professionnels :

- de s'identifier aux services de santé raccordés à PSC via un moyen d'identification unique ;
- de passer d'un service numérique à un autre sans devoir se réidentifier ;
- de centraliser et homogénéiser des données d'authentification, au bénéfice de la sécurité face aux fuites ou aux attaques.

À compter du 1er janvier 2023, **l'implémentation de PSC sera obligatoire pour les différents services numériques en santé.** Les identités fournies proviennent de l'Annuaire Santé, lui-même alimenté par les répertoires RPPS et FINESS. Pro Santé Connect permet de s'authentifier facilement et de manière sécurisée à tous les services raccordés de la e-santé, avec les moyens d'authentification qui conviennent le mieux aux professionnels de santé..

Rapprochez-vous de votre éditeur de votre solution de DUI pour connaître le calendrier d'intégration de PSC sur vos outils.

QUESTION 6

AVEZ-VOUS ACTIVÉ UN PARE-FEU ? EN CONNAISSEZ-VOUS LES RÈGLES DE FILTRAGE ?

Un pare-feu local est un logiciel installé sur l'ordinateur de l'utilisateur qui protège **principalement contre des attaques provenant d'Internet.** Il permet de ralentir ou limiter l'action d'un acteur malveillant ayant réussi à prendre le contrôle d'un poste de travail. Les attaquants tentent souvent **d'élever leurs privilèges pour prendre le contrôle du SI et d'étendre leur intrusion aux autres postes** de travail. **L'activation du pare-feu** sur chaque poste de travail **rend plus difficile ce déplacement latéral.**

Comment procéder ?

POUR LE DIRECTEUR

Sans connaissance informatique particulière, l'activation d'un pare-feu préinstallé sur le poste de travail et son paramétrage par défaut (qui bloque toute connexion entrante), constituent un premier niveau de protection. Ce pare-feu est une fonction disponible sur la plupart des systèmes d'exploitation grand public. Des pare-feux sont également commercialisés en complément de suites logicielles antivirales.

POUR LE REFERENT SI

Un pare-feu individuel (qu'il soit intégré au système d'exploitation ou une solution logicielle tierce) doit être installé sur tous les postes de travail. Il est recommandé d'assurer l'homogénéité des configurations et de la politique de filtrage des flux. Une politique de filtrage minimale permet de :

- boquer tous les flux non strictement nécessaires (en particulier les connexions entrantes depuis Internet) ;
- journaliser les flux bloqués.

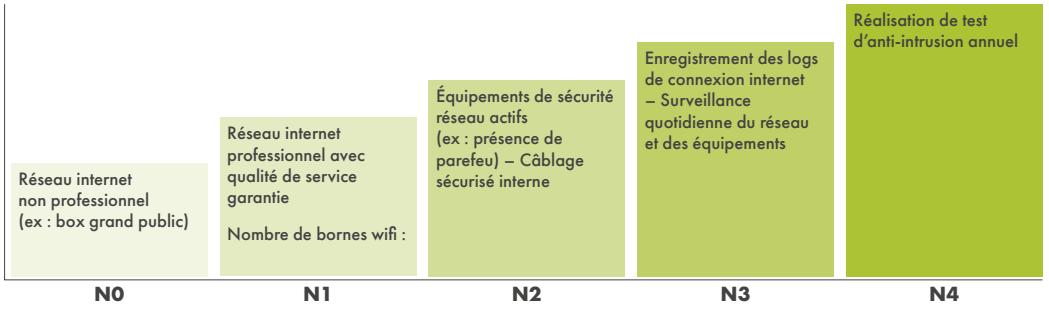
En plus d'un pare-feu individuel, **il est recommandé de mettre en place un pare-feu physique** pour chaque lieu géographique/bâtiment ayant son propre accès à internet. Un ESSMS

doit déployer des pares-feux physiques en priorité pour protéger l'interconnexion du SI à Internet, voire, pour les entités les plus matures en matière de sécurité ou disposant d'une masse critique, pour segmenter le réseau interne en zones ayant des niveaux différents de sensibilité et d'exposition aux menaces (zone des postes de travail utilisateurs, zone des serveurs internes, zone des serveurs exposés sur Internet, etc.).

S'agissant de l'interconnexion à Internet, elle se traduira idéalement par **la mise en œuvre d'une zone « démilitarisée » (DMZ),** constituée de pare-feux mais aussi de services de rebond, principalement pour la messagerie et la navigation Web.

Pour une configuration adaptée à vos usages, **n'hésitez pas à recourir aux services d'un prestataire informatique labellisé ExpertCyber.** Une mise en relation est proposée par le site Cybermalveillance.gouv.fr.

LIEN AVEC LES INDICATEURS DE L'OBSERVATOIRE SIN MS
ACCÈS RÉSEAU ET SÉCURITÉ DU RÉSEAU



POUR EN SAVOIR PLUS

- Recommandation pour choisir des pare-feux maîtrisés dans les zones exposées à internet

QUESTION 7

COMMENT SÉCURISEZ-VOUS VOTRE MESSAGERIE ?

POUR LE DIRECTEUR

La messagerie est le principal vecteur d'infection du poste de travail. En un clic, vous pouvez être victime d'hameçonnage (ou phishing en anglais), pour s'en prémunir, quelques reflexes à adopter :
L'expéditeur est-il connu ? Une information de sa part est-elle attendue ? Le lien proposé est-il cohérent avec le sujet évoqué. En cas de doute, une vérification de l'authenticité du message par un autre canal (téléphone, SMS, etc.) auprès de l'émetteur est nécessaire. **La sensibilisation des employés des ESSMS à identifier ces tentatives est primordiale.**

Par ailleurs, la redirection de messages professionnels vers une messagerie personnelle est à proscrire car cela constitue un vecteur de fuite irrémédiable d'informations de l'entité.

POUR LE RÉFÉRENT SI

Que l'entité héberge ou fasse héberger son système de messagerie, elle doit s'assurer :

- de disposer **d'un système d'analyse antivirus en amont des boîtes aux lettres** des utilisateurs pour prévenir la réception de fichiers infectés ;
- de mettre en place certains protocoles pour **vérifier l'authenticité et l'intégrité des courriels** (Sender Policy Framework – SPF, DomainKeys Identified Mail – DKIM, etc.) ;
- **de l'activation du chiffrement TLS des échanges** entre serveurs de messagerie ainsi qu'entre les postes utilisateurs et les serveurs hébergeant les boîtes de messagerie électronique.

Pour se prémunir d'escroqueries connues (exemple : demande de virement frauduleux) **des mesures organisationnelles** doivent être appliquées strictement.

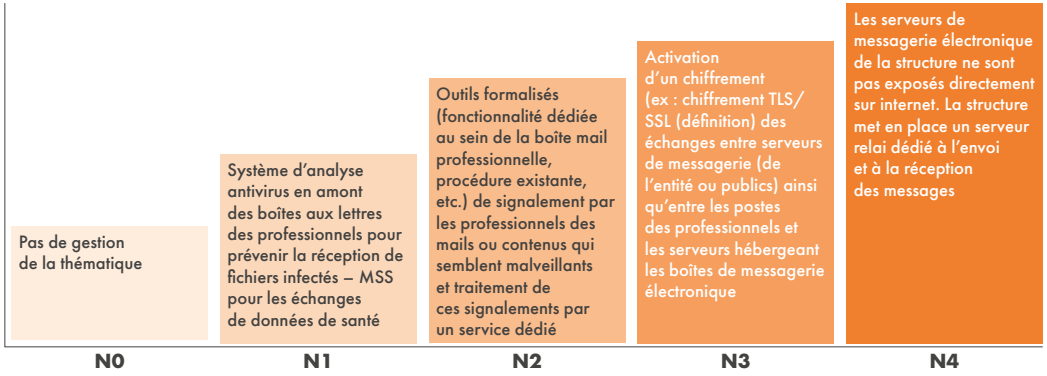
Il est souhaitable de ne **pas exposer directement sur internet les serveurs de messagerie électronique d'entreprise.** Dans ce cas, un serveur relai dédié à l'envoi et à la réception des messages doit être mis en place en cas de coupure d'Internet.

POUR EN SAVOIR PLUS

- Les 5 réflexes à avoir lors de l'ouverture d'un courriel
- Fiche réflexe : que faire en cas d'hameçonnage ?
- Recommandations de sécurité relatives à la couche transport (TLS)
- Guide ANSSI : recommandations relatives à l'interconnexion d'un système d'information à internet

LIEN AVEC LES INDICATEURS DE L'OBSERVATOIRE SIN MS

SÉCURISATION DE LA MESSAGERIE



QUESTION 8

COMMENT SÉPAREZ-VOUS VOS COMPTES ET VOS USAGES INFORMATIQUES ?

L'interconnexion des outils informatiques avec Internet présente un certain nombre de risques, notamment :

- l'exfiltration de données depuis l'ESSMS vers Internet, portant ainsi atteinte à leur confidentialité voire à la réputation de l'ESSMS si elles sont diffusées ;
- l'intrusion depuis Internet pour porter atteinte à l'intégrité ou la disponibilité du SI ;
- l'usurpation d'identité ;
- le détournement du SI de l'ESSMS pour des usages frauduleux ou délictueux.

Comment diminuer l'exposition à ces menaces ?

Le premier principe d'hygiène repose sur la création de comptes utilisateurs dédiés à chaque employé et ne disposant pas de privilège d'administration. Ceci permet de limiter le risque d'installation de codes malveillants.

Seuls les comptes utilisateur doivent être utilisés pour la navigation sur Internet : de très nombreuses attaques sont causées par une navigation effectuée depuis un compte doté de privilèges administrateur, ce qui facilite grandement la tâche d'un attaquant pour prendre le contrôle complet de l'ordinateur. **Les comptes d'administration doivent être utilisés uniquement pour configurer les équipements ou installer des logiciels. Les comptes et les privilèges administrateur doivent être tenus à jour : quand un employé quitte l'ESSMS, il convient de faire l'inventaire de ses accès et de tous les révoquer, de telle sorte que lui-même ou un tiers ne puisse plus y accéder.** Par ailleurs, l'idéal est de posséder un ordinateur uniquement dédié à sa pratique professionnelle, sans usage personnel et familial. Cependant en cas d'usages multiples sur une seule et même machine, il est alors recommandé de créer des comptes utilisateur pour chacun d'entre eux.

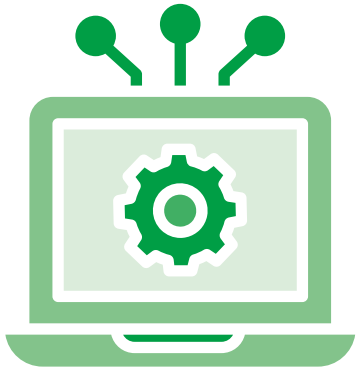
Ces cloisonnements d'usages sont faciles à implémenter. Ils permettent de contrer l'exécution arbitraire d'un certain nombre de programmes malveillants.

Depuis un mobile multifonctions ou une tablette, les tâches d'administration et de cloisonnement s'effectuent d'une autre manière : **il faut limiter les autorisations données à chaque application pour chacune de leurs utilisations et télécharger les applications uniquement depuis les marchés officiels** ou le site Internet des éditeurs.

POUR LE REFERENT SI

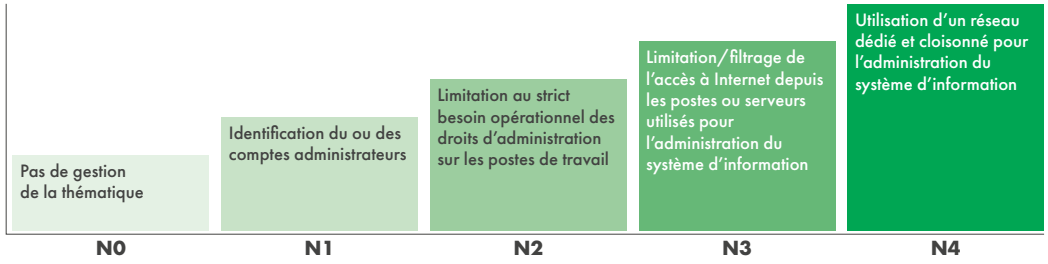
Pour les ESSMS possédant un grand nombre de collaborateurs et disposant d'un réseau informatique de plusieurs machines, il est recommandé de respecter les mesures suivantes :

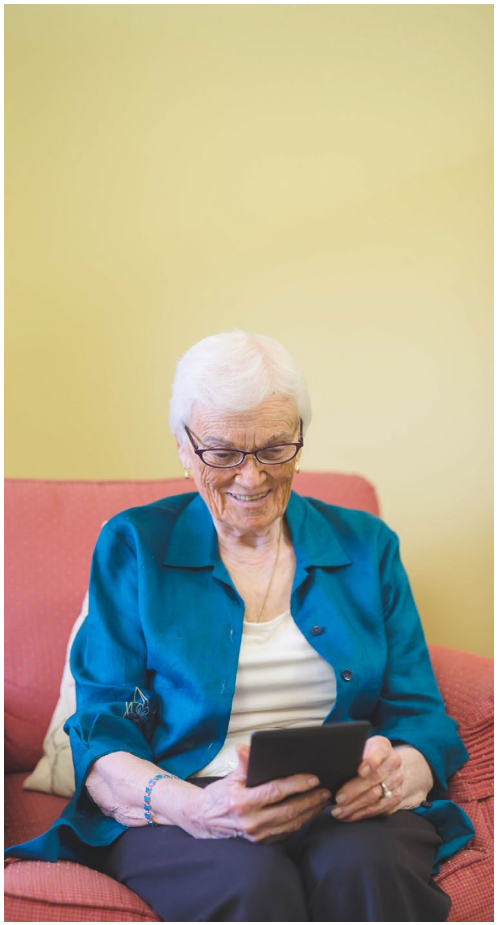
- **les connexions entre les postes des utilisateurs doivent être interdites par défaut :** si un poste est infecté par un code malveillant, ce cloisonnement évite la propagation directe sur l'ensemble des autres postes ;
- en matière d'administration du SI, **les postes et les comptes d'administration doivent être dédiés à cet usage ;**
- si les ressources de l'ESSMS s'y prêtent, les activités numériques de l'établissement doivent être **cloisonnées en différentes zones réseaux** par des dispositifs de filtrage physiques ou virtualisés (zone des serveurs internes, zone des serveurs exposés sur Internet, zone des postes de travail utilisateurs, zone d'administration, zone système industriel, etc.). Il est recommandé de vous faire **accompagner par des professionnels** de l'informatique pour bénéficier de l'architecture sécurisée adaptée à votre système d'information et à la nature de vos données.



LIEN AVEC LES INDICATEURS DE L'OBSERVATOIRE SIN MS

SÉCURITÉ DE L'ADMINISTRATION





POUR EN SAVOIR PLUS

- Recommandations relatives à l'interconnexion d'un système d'information à internet
- Recommandations relatives à l'administration sécurisée des systèmes d'information
- Apprendre à séparer ses usages pro-perso

QUESTION N°9

MAÎTRISEZ-VOUS LE RISQUE NUMÉRIQUE LIÉ AU NOMADISME DES PROFESSIONNELS ?

L'utilisation d'ordinateurs portables, de mobiles multifonctions ou de tablettes facilite le nomadisme pour les professionnels ainsi que le transport et l'échange de données. Le renforcement du télétravail a également augmenté le recours à des solutions de mobilité. Tout en facilitant la continuité d'activité, ces usages présentent néanmoins des risques que vous pouvez éviter.

Sécuriser la mobilité numérique

Plusieurs actions sont à prévoir en amont d'un déplacement pour sécuriser la mobilité :

- sauvegardez vos données pour les retrouver en cas de perte ou de vol des équipements ;
- vérifiez que vos mots de passe ne sont pas pré-enregistrés ;
- dans la mesure du possible, procéder au chiffrement de vos données les plus sensibles ou de l'ensemble du disque dur ;
- dans le cas où vous devez accéder à distance aux systèmes d'information de l'ESSMS, prévoyez l'installation d'un logiciel de connexion à distance de type VPN (virtual private network) afin de protéger vos communications.

Avoir les bons réflexes durant les déplacements

Plusieurs bonnes pratiques sont recommandées :

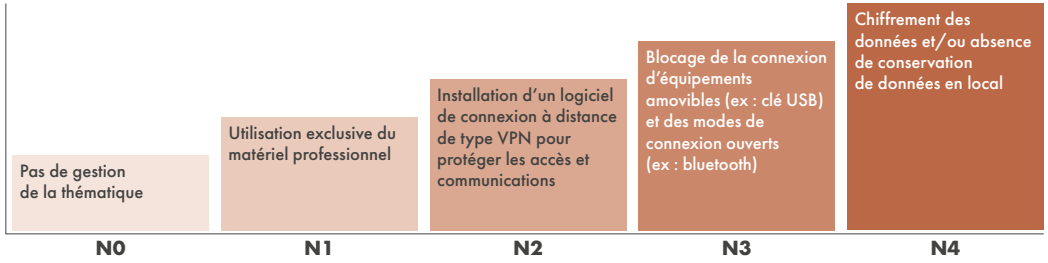
- gardez vos appareils, supports et fichiers avec vous ;
- informez votre ESSMS en cas de perte ou de vol de votre matériel ;
- refusez la connexion d'équipements appartenant à des tiers à vos propres équipements (ordiphone, clé USB, baladeur, etc.).

POUR EN SAVOIR PLUS

- Bonnes pratiques à l'usage des professionnels en déplacement
- Recommandations sur le nomadisme numérique

LIEN AVEC LES INDICATEURS DE L'OBSERVATOIRE SIN MS

RISQUE NUMÉRIQUE ET MOBILITÉ



QUESTION n°10

COMMENT VOUS INFORMEZ-VOUS ? COMMENT SENSIBILISEZ-VOUS VOS COLLABORATEURS ?

Pour le directeur : s'informer

Sans avoir de compétences particulières en informatique ni beaucoup de temps à y consacrer, il est possible de **prendre connaissance de recommandations concernant les bonnes pratiques,** d'alertes sur les menaces en cours et d'informations sur les mises à jour logicielles disponibles en suivant les actualités publiées par le **dispositif Cybermalveillance.gouv.fr.** Ce suivi ne nécessite aucune compétence informatique particulière.

Par ailleurs, **les agences régionales de santé (ARS), les Groupements Régionaux d'Appui au Développement de la e-Santé (GRADeS) et les collectifs SI** proposent régulièrement des conseils et accompagnements sur le sujet de la sécurité numérique. Des webinaires et de nombreuses ressources documentaires sont disponibles sur leurs sites internet.

Enfin l'Agence nationale de l'appui à la performance (Anap) et l'Agence du Numérique en Santé (ANS) produisent des guides pratiques et informatifs abordant les enjeux de cybersécurité pour les ESSMS. Des webinaires et de nombreuses ressources documentaires sont disponibles sur leurs sites internet.

POUR EN SAVOIR PLUS

- Actualité – Cybermalveillance
- CERT-Santé – Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques

Pour le référent SI : s'informer et sensibiliser

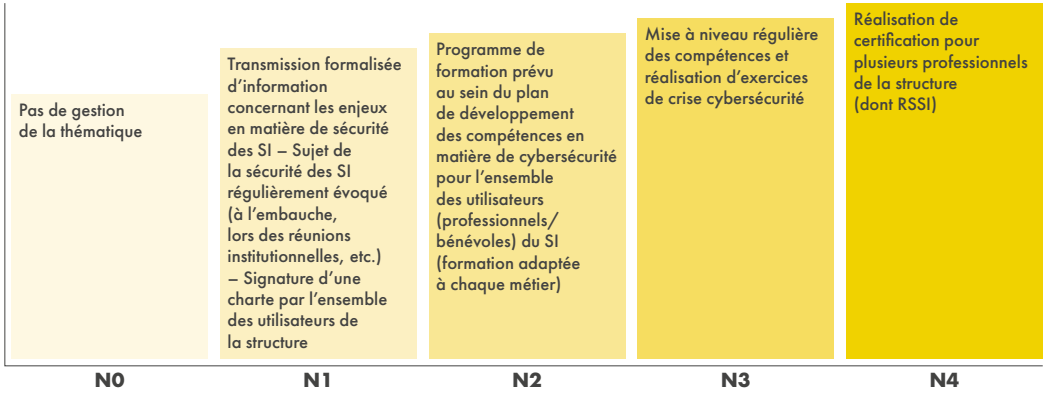
Pour aller plus loin, **une veille technique relative aux campagnes d'attaques et aux vulnérabilités** est également effectuée par la cellule de veille, d'alerte et de réponse aux attaques informatiques de l'Agence du Numérique en Santé (ANS), **le CERT-SANTE.** Elle conviendra plus particulièrement aux référents SI dotés d'un service informatique.

En parallèle, pour les référents SI, il est préconisé d'informer et de sensibiliser régulièrement le personnel aux bonnes pratiques de sécurité et aux principales menaces qui peuvent affecter la structure. Avoir une bonne hygiène informatique peut se traduire par la mise en place d'actions internes, telles qu'une charte informatique, diffusions régulières de messages internes, newsletters, etc.

La déclaration d'incidents doit être encouragée et, pour ce faire, une réponse non coercitive doit être privilégiée. Il s'agit de **responsabiliser les utilisateurs** face à des menaces évolutives et non de les sanctionner (sauf en cas d'action délibérée) afin d'éviter une sous-déclaration des incidents. Pour rappel, **la déclaration d'incident est obligatoire pour les ESSMS** depuis l'ordonnance du 19 novembre 2020. Le décret n° 2022-715 du 27 avril 2022 relatif aux conditions et aux modalités de mise en œuvre du signalement des incidents significatifs ou graves de sécurité des systèmes d'information vient également apporter des précisions.

LIEN AVEC LES INDICATEURS DE L'OBSERVATOIRE SIN MS

SENSIBILISATION ET INFORMATION DES UTILISATEURS (PROFESSIONNELS/BÉNÉVOLES) EN MATIÈRE DE SÉCURITÉ DES SI



QUESTION n° 11

SAVEZ-VOUS COMMENT RÉAGIR EN CAS DE CYBERATTAQUE ?

Se préparer à l'incident

Les ESSMS ont tout avantage à **identifier préalablement des prestataires spécialisés** dans la réponse aux incidents de sécurité.

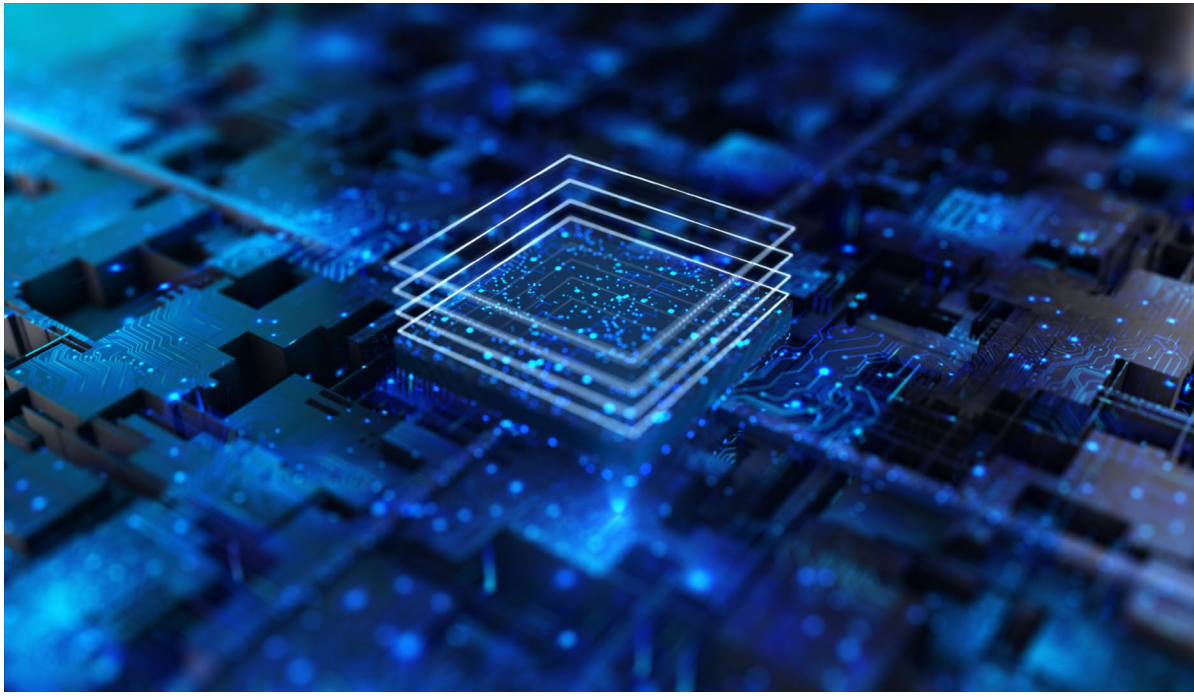
Le CERT Santé apporte ainsi un appui en cas d'incident de sécurité des systèmes d'information. Il assure une mission de prévention et d'alerte face aux menaces de cybersécurité et partage différentes recommandations pour minimiser les effets en cas de cyberattaque.

En parallèle, il est également possible de contacter **votre ARS ou votre GRADeS :** leurs experts peuvent vous orienter vers une assistance appropriée.

En cas d'incident avéré cas d'incident avéré

Le premier réflexe à avoir en cas d'incident concernant un système d'information est de déconnecter son équipement ou son système d'information d'entreprise d'Internet. Pour un équipement individuel, cela peut se traduire par le retrait de la prise ou la désactivation des services WiFi. Pour un SI de l'ESSMS, l'action peut être menée sur l'équipement réseau ou le pare-feu. Cela évitera une fuite éventuelle de données.

N'éteignez pas, ni ne modifiez, les ordinateurs et matériels affectés par l'attaque : ils seront utiles aux enquêteurs.



En cas de rançongiciel, ne payez jamais la rançon demandée : des solutions de déchiffrement existent et vous serez assistés par des gardiens de la paix.

Vos sauvegardes vous permettront de retrouver une activité normale (*cf. Question n° 2*). Il est recommandé d'ouvrir une main courante pour tracer les actions et événements liés à l'incident, (l'heure et la date de l'action ou de l'événement, le nom de la personne à l'origine de cette action ou ayant informée sur l'événement, la description de l'action ou de l'événement). La tenue d'une main courante régulièrement alimentée tout au long de l'incident va considérablement faciliter l'intervention du prestataire et la résolution du problème.

Pour un ESSMS, il convient de concevoir et de déployer un dispositif de communication

relatif à l'incident. Ce dispositif doit être proposé par le référent communication (en lien avec les experts techniques) et porté par la direction. La charte informatique peut également informer les collaborateurs de la bonne attitude à avoir en cas d'incident avéré.

Aspects juridiques

Le décret nº 2022-715 du 27 avril 2022 relatif aux conditions et aux modalités de mise en œuvre du signalement des incidents significatifs ou graves de sécurité des systèmes d'information prévoit pour les ESSMS une obligation de signalement à l'Agence du Numérique en Santé (ANS) des incidents « significatifs ou graves » de sécurité

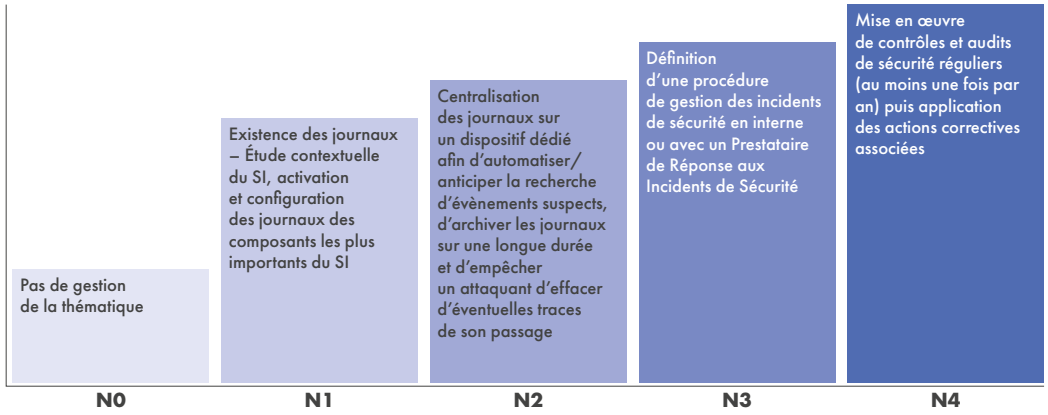
informatique. **La déclaration doit être réalisée via le Portail de signalement des événements sanitaires indésirables.** Cette obligation de déclaration doit permettre aux autorités compétentes (ANSSI, CNIL, CERT-Santé) d'éviter la propagation des cyberattaques à d'autres ESSMS.

Si un incident implique des données personnelles et présente un risque pour les droits et libertés des personnes, **l'ESSMS doit également informer la CNIL.** En cas de risque élevé, l'ESSMS doit également notifier les personnes concernées par l'incident.

Il est essentiel de porter plainte. Vos matériels affectés et vos journaux seront très utiles aux enquêteurs.

LIEN AVEC LES INDICATEURS DE L'OBSERVATOIRE SIN MS

SUPERVISION, AUDIT DU SI, ANTICIPATION DES INCIDENTS



POUR EN SAVOIR PLUS

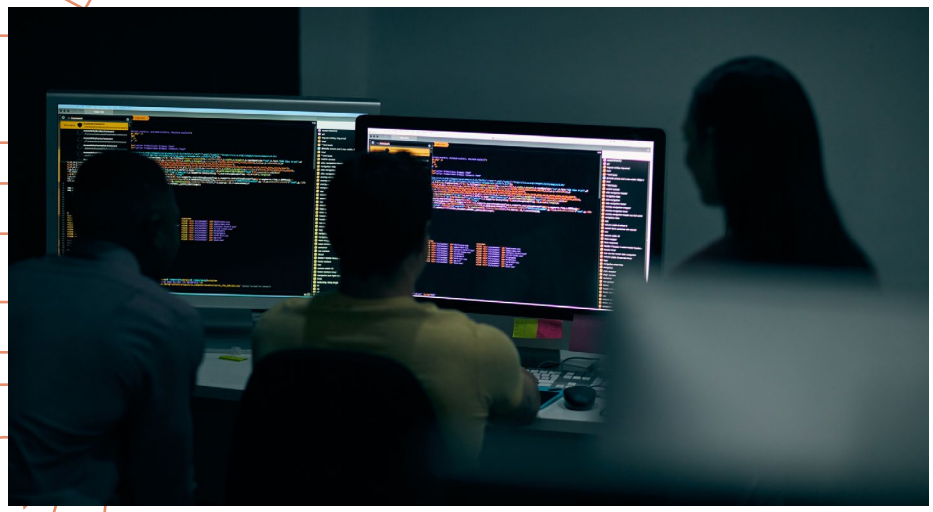
- Attaques par rançongiciels, tous concernés – comment les anticiper et réagir en cas d'incident ?
- Gouvernement – information risques cybercriminalité
- CNIL – Notifier une violation de données personnelles

QUESTION N° 12

AVEZ-VOUS FAIT ÉVALUER LA COUVERTURE DE VOTRE POLICE D'ASSURANCE AU RISQUE CYBER ?

Les sociétés d'assurance proposent de plus en plus des clauses permettant de se prémunir de certains risques d'origine numérique afin d'accompagner les entreprises victimes de cybermalveillance ou de cyberattaques. L'assurance fournit, en cas de sinistre, une assistance juridique ainsi qu'une couverture financière du préjudice (matériel, immatériel, etc.).

Selon les contrats, **différents types de protections** peuvent être proposés : usurpation d'identité, garanties contre une perte d'exploitation, accompagnement juridique pour une déclaration d'atteinte aux données personnelles, prise en charge d'un accompagnement technique pour la restauration du système d'information après une cyberattaque. À ce titre, dans le cadre de leur mission de certification des comptes annuels, les commissaires aux comptes recommandent de plus en plus la souscription de ce type de protection.

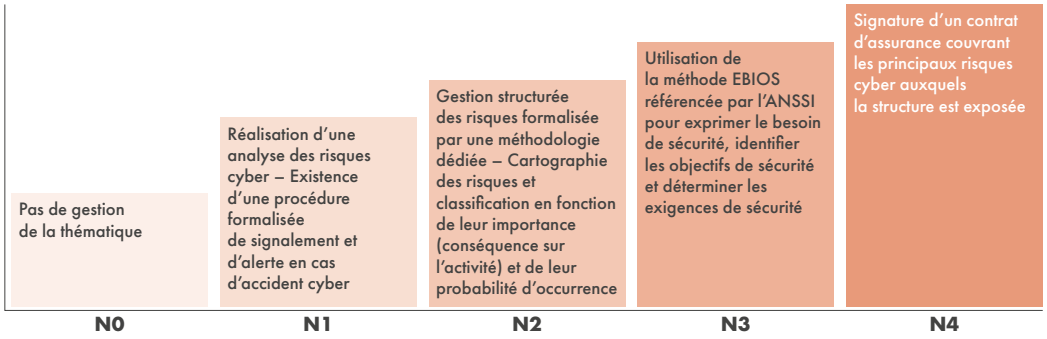


Ces clauses assurantielles peuvent se traduire dans **les contrats d'assurance classique ou prendre la forme d'une police d'assurance « cyber » spécifique,** bien que ce dernier marché reste encore à développer, en particulier en matière de jurisprudence concernant l'activation ou non des clauses d'exclusion.

Il est important de vérifier auprès de sa police d'assurance les modalités de protection proposées afin d'évaluer la faisabilité d'y souscrire. **Étant donné la forte externalisation des systèmes d'information du secteur social et médico-social, il est indispensable de demander aux prestataires, éditeurs de solution et hébergeurs, la couverture de leur police d'assurance en la matière.** Les opérateurs du secteur social et médico-social ont également l'enjeu de **faire évoluer les contrats signés avec les prestataires** sur le sujet de la couverture des risques cyber afin que les prestataires tiennent compte de la couverture des risques dans leur offre de service.

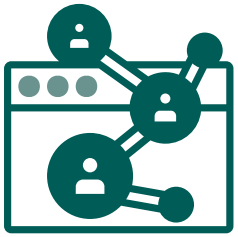
LIEN AVEC LES INDICATEURS DE L'OBSERVATOIRE SIN MS

ANALYSE DE RISQUE ET POLICE D'ASSURANCE RISQUE CYBER



QUESTION 13

MAÎTRISEZ-VOUS LES RISQUES NUMÉRIQUES LIÉS À VOS RELATIONS AVEC DES TIERS ?



Le recours à un fournisseur extérieur pour les prestations informatiques implique à l'organisation de mettre en place un niveau de sécurité homogène et maîtrisé, les mêmes exigences de sécurité s'appliquent en interne. Pour exemple, l'exposition d'un éditeur de logiciel à une cyberattaque est susceptible d'impacter les données sensibles d'une structure.

Rédiger des contrats qui incluent des exigences précises pour lesquelles les tiers s'engagent les tiers s'engagent :

- identifier et décrire dans le contrat les missions et activités confiées au tiers afin de formaliser la répartition des responsabilités. Le contrat doit spécifier l'objet, la durée et la finalité du traitement et les obligations des parties ;
- formaliser des exigences, notamment pour la protection et l'usage des données à caractère personnel, dans une attestation et annexer ce document au contrat pour que les tiers signent et s'engagent systématiquement à respecter les éléments de l'attestation ;
- pour le volet de la protection des données, le contrat doit contenir des dispositions relatives à la confidentialité des données personnelles confiées, des contraintes minimales en matière d'authentification, les conditions de restitution et/ou destruction des données en fin de contrat, les règles de gestion et de notification des incidents.

Deux points de vigilance concernant les contrats :

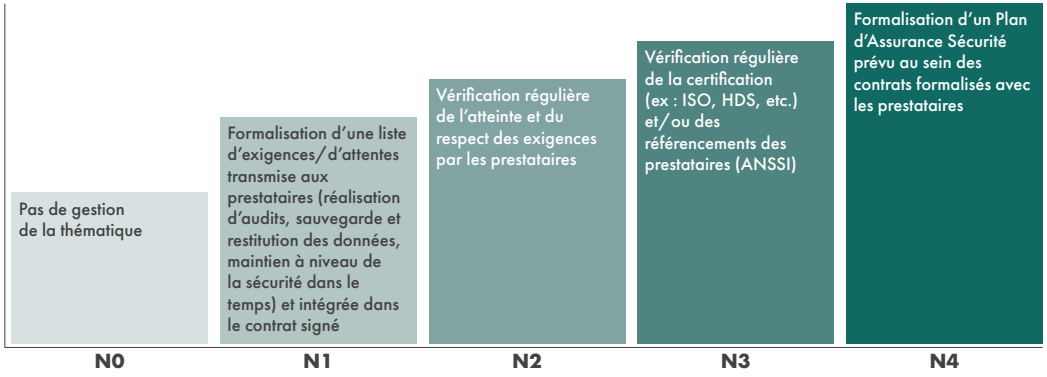
- il faut faire attention aux contrats standards proposés par des tiers puisque ces derniers peuvent fixer des modes de traitements des données ne respectant pas la législation ;
- les enjeux de sécurité sont d'autant plus importants pour les tiers fournissant des prestations informatiques. Il faut donc accroître le niveau de vigilance et les exigences en matière de sécurité pour ces fournisseurs.

Suivre et évaluer le respect des exigences de sécurité par les tiers le respect des exigences de sécurité par les tiers :

- lorsque tout ou partie de la gestion du système d'information est confiée à des tiers, cartographiez les périmètres d'intervention des différents prestataires ;
- identifiez les membres de la structure qui assurent le lien avec les tiers et précisez dans leurs missions le suivi du respect des exigences de sécurité du SI par les tiers ;
- documentez les moyens mis en œuvre par les tiers pour garantir le respect des engagements de sécurité (audits de sécurité, visité d'installation, politique de sécurité des systèmes d'information, etc.).

LIEN AVEC LES INDICATEURS DE L'OBSERVATOIRE SIN MS

GESTION DE LA SÉCURITÉ EN LIEN AVEC LES PRESTATAIRES



POUR EN SAVOIR PLUS

- Sécurité : gérer la sous-traitance

GLOSSAIRE

Chiffrement – Déchiffrement
Codage de l'information rendant incompréhensible son contenu pour ceux qui ne possèdent pas l'algorithme et la clé de décodage. Le chiffrement est mis en œuvre dans le but d'assurer un certain niveau de confidentialité des données. Il ne faut pas confondre le chiffrement avec la compression des données.

Compromission
Intrusion dans un système ayant pour conséquence la divulgation, la modification, ou la destruction d'informations confidentielles.

Filtrage (de contenu) Web
Technique qui bloque et filtre l'accès à des contenus web inappropriés ou dangereux. Il est ainsi possible pour une entreprise d'empêcher ses employés de visiter des sites de spam connus.

GRADeS/Groupement Régional d'Appui au Développement de a e-Santé
Les GRADeS assurent une expertise e-santé pour les territoires et accompagnent les professionnels de santé dans la transition numérique sur leur métier. Ils garantissent la finalité d'améliorer la qualité des soins, le respect de la sécurité et de la confidentialité des données de santé et le développement des usages de services numériques de santé en région.

Hacking
Utilisation non autorisée ou tentative de tromper ou de passer outre des mécanismes de sécurité sur un ordinateur ou un réseau.

Hameçonnage (Phishing)
Méthode de fraude par usurpation d'identité. Elle permet au pirate d'obtenir les identifiants et mot de passe de sa victime pour réaliser des opérations bancaires ou des achats.

L'attaque passe généralement par courrier électronique dont l'apparence fait croire qu'il vient d'un organisme connu et l'invite à se connecter directement ou indirectement au site de sa banque qui est en fait un site pirate déguisé. On peut en général détecter une attaque par hameçonnage en lisant attentivement l'URL du lien.

Hygiène informatique
Parmi les mesures techniques que les entités publiques ou privées doivent prendre pour garantir la sécurité de leurs systèmes d'information, on qualifie les plus simples et élémentaires d'entre elles d'hygiène informatique, car elles sont la transposition dans le monde numérique de règles élémentaires de sécurité sanitaire.

Pare-feu
Logiciel ou matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données.

Rançongiciel
Technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement.

Rebond
Méthode de connexion via un ordinateur pour ensuite se connecter à une tierce machine.

Système d'Information/SI
Ensemble des moyens (organisation, acteurs, procédure, systèmes informatiques) nécessaires au traitement et à l'exploitation des informations dans le cadre d'objectifs définis au niveau de la stratégie de l'établissement, des métiers, de la réglementation.

Virtual Private Network/VPN
Protocole réseau permettant d'étendre un réseau local en traversant un autre réseau, le plus souvent Internet.
Les trames sont encryptées sur le réseau tiers, qui ne sert que de support.
On peut utiliser le VPN pour effectuer une liaison sécurité entre une personne distante et un intranet entreprise par exemple.

Zone Démilitarisé/DMZ
Zone tampon d'un réseau d'entreprise, située entre le monde extérieur (par exemple internet) et le réseau interne. Les pares-feux actuels intègrent généralement trois interfaces réseau :
Un pour l'intranet (zone privée), un pour l'internet (passerelle) et enfin un pour la DMZ (zone publique).
Les plus anciens ne comportent généralement que deux interfaces réseau (internet/intranet).

REMERCIEMENTS

La cybersécurité se construit avec tout l'écosystème.
Acteurs institutionnels, nationaux, régionaux, établissements et professionnels.

Ce document est le fruit d'un travail collectif.

MERCI à tous pour votre engagement et votre disponibilité !

Agence Nationale d'Appui à la Performance (ANAP)

Agence nationale de la sécurité des systèmes d'information (ANSSI)

Agence du Numérique en Santé (ANS)

Les Agences Régionales de Santé (ARS)

Caisse nationale de solidarité pour l'autonomie (CNSA)

Collectifs Système d'Information Médico-Social

Délégation Ministérielle du numérique en Santé (DNS)

Groupement Régional d'Appui au Développement de la e-Santé (GRADeS)

Haut fonctionnaire de défense et de sécurité (HFDS)

esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'Agence du Numérique en Santé et s'informer sur l'actualité de la e-santé.

@esante_gouv_fr

linkedin.com/company/agence-du-numerique-en-sante

Rejoignez-nous

welcometothejungle.com/fr/companies/agence-du-numerique-en-sante

ANS – Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50 du lundi au vendredi
(hors jours fériés) de 8 h 30 à 13 h et de 14 h à 17 h

AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici