Journées Nationales
13 & 14 octobre 2022

Réussir ensemble le virage numérique dans le médico-social

LE MÉDICO-SOCIAL
ENGAGÉ
POUR LA E-SANTÉ

1.6 La cybersécurité pour les ESSMS en 13 questions

La cybersécurité pour les ESSMS en 13 questions

Salle 2.06

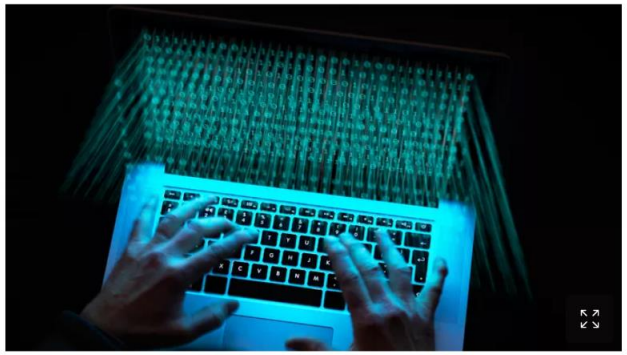
LE MÉDICO-SOCIAL ENGAGÉ POUR LA E-SANTÉ

L’actualité et cybersécurité

Un Ehpad victime d'une cyberattaque dans l'Eure

Par Le Figaro avec AFP
Publié le 24/08/2022 à 16:50, mis à jour le 24/08/2022 à 16:57

Écouter cet article 00:00/01:48



C'est la deuxième cyberattaque visant un établissement de santé en quelques jours. *Andrew Brookes/Westend61 / stock.adobe.com*

Nouvelle carte Vitale : attention à l'arnaque par SMS !

Publié le 22 avril 2022 - Direction de l'information légale et administrative (Premier ministre)

Vous avez reçu un message par SMS de l'Assurance maladie vous demandant de renouveler ou de mettre à jour votre carte Vitale ? Attention, vous faites l'objet d'une tentative d'arnaque ! *Service-Public.fr* vous explique cette arnaque et vous indique les moyens de s'en protéger.

Crédits : © Fizkes - stock.adobe.com

Une arnaque par SMS

Au Costa Rica, des hackers russes menacent l'équilibre du pays tout entier

Depuis mi-avril, toutes les administrations du pays d'Amérique centrale sont visées par des cyberattaques, paralysant une bonne partie de la société.

Cyberattaque contre un hôpital de l’Essonne : les hackers ont diffusé des données de santé

Le groupe de hackers, qui avait orchestré en août une cyberattaque contre le Centre hospitalier sud-francilien, à Corbeil-Essonnes, a commencé vendredi à diffuser des données. Elles « semblent concerner » des usagers, le personnel et des partenaires, précise l'hôpital, qui a refusé de payer la rançon demandée.

Ouest-France
Avec AFP.
Modifié le 25/09/2022 à 10h54
Publié le 25/09/2022 à 10h17

Abonnez-vous

ÉCOUTER
LIRE PLUS TARD
PARTAGER
NEWSLETTER LA MATINALE

Le Centre hospitalier sud-francilien de Corbeil-Essonnes avait été victime d'une cyberattaque en août. | JOEL SAGET

[Enquête] Caen. Cyberattaque : et maintenant ?

Informatique. La Ville de Caen a été victime d'une cyberattaque lundi 26 septembre. Quels enseignements faut-il en tirer ? Comment réagir ? Éléments de réponse.

Publié le 05/10/2022 à 12h30

Pourquoi la cybersécurité en 13 questions ?

Constat : la documentation autour de la cybersécurité est nombreuse mais il y a très peu voire pas du tout de document à destination du secteur social et médico-social.

Objectif : adapter des documents existants pour les mettre à disposition du secteur

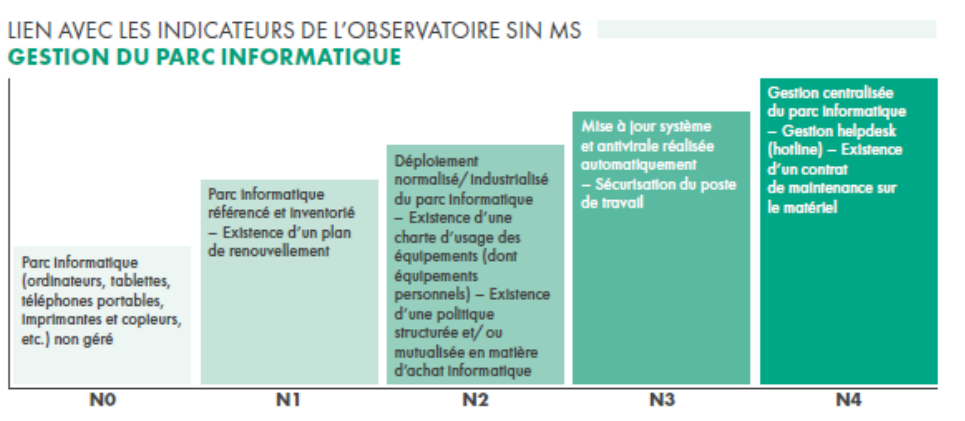
Le premier document adapté est un document de l'ANSSI : la cybersécurité pour les TPE/PME en 12 questions

? Sauriez-vous identifier la question bonus pour le secteur social et médico-social ?

LE MÉDICO-SOCIAL
ENGAGÉ
POUR LA E-SANTÉ

Question n°1 - CONNAISSEZ-VOUS suffisamment VOTRE PARC INFORMATIQUE ?

- Les équipements et services
- Les logiciels
- Les données et traitements
- Les accès
- Les interconnexion avec l'extérieur



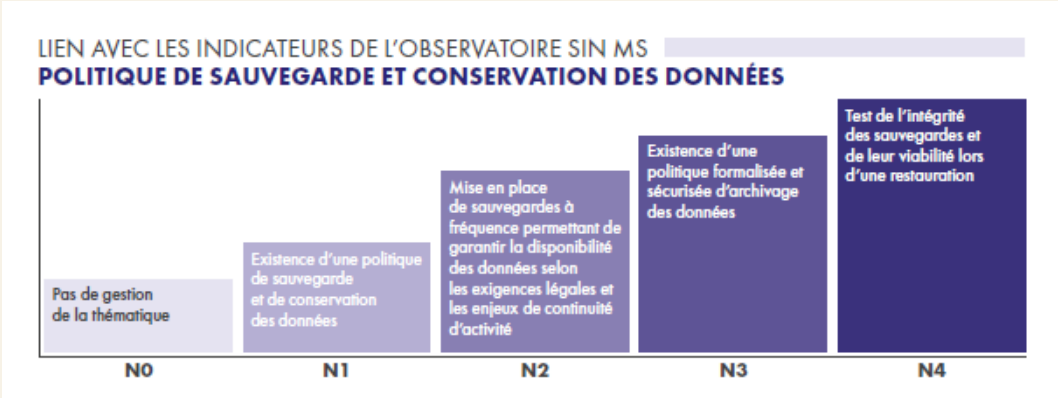
A quoi ça sert ?

- Aider au choix des solutions numériques adaptées à l'ESSMS,
- Identifier les points de sécurisation et, le cas échéant,
- 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 MÉDICO-SOCIAL ENGAGÉ POUR LA E-SANTÉ

Question n°2 - EFFECTUEZ-VOUS DES SAUVEGARDES RÉGULIÈRES ?



- Identifiez les données à sauvegarder
- Déterminez le rythme de vos sauvegardes
- Choisissez-le ou les supports à privilégier pour votre sauvegarde
- Évaluez la pertinence du chiffrement des données
- Respectez le cadre juridique

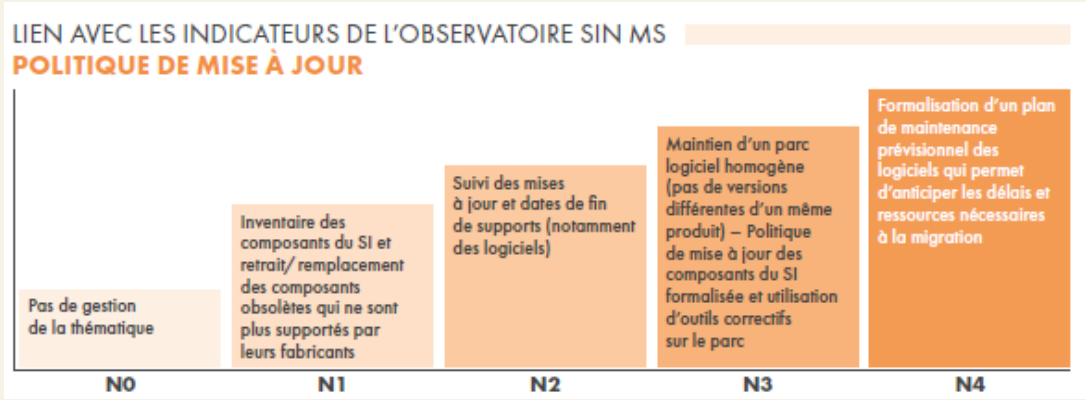
A quoi ça sert ?

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

LE MÉDICO-SOCIAL ENGAGÉ POUR LA E-SANTÉ

Question n°3 - APPLIQUEZ-VOUS RÉGULIÈREMENT LES MISES À JOUR ?

- Utilisez des solutions matérielles et logicielles maintenues
- Activez la mise à jour automatique des logiciels et des matériels



A quoi ça sert ?

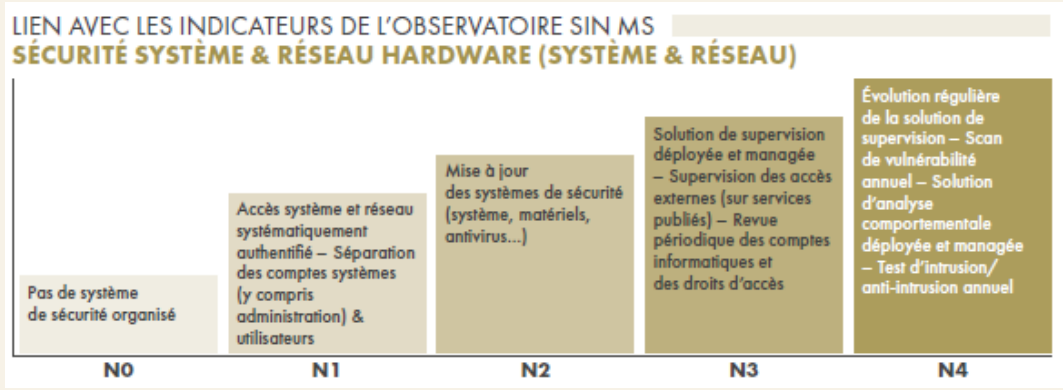
La majorité des attaques ciblent des vulnérabilités publiques et documentées pour prendre pied sur les systèmes d'information : les pirates informatiques comptent soit sur la négligence des utilisateurs soit sur la vulnérabilité d'un service exposé sur Internet (pare-feu, messagerie, etc.).

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.

LE MÉDICO-SOCIAL ENGAGÉ POUR LA E-SANTÉ

Question n°4 - UTILISEZ-VOUS UN ANTIVIRUS ?

- Déployez un antivirus sur tous les équipements
  - Il doit être déployé sur tous les équipements, en priorité ceux connectés à Internet (postes de travail, serveurs de fichier, etc.)
  - 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
  - Une gestion centralisée des antivirus



A quoi ça sert ?

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.

LE MÉDICO-SOCIAL ENGAGÉ POUR LA E-SANTÉ

Question n°5 - AVEZ-VOUS IMPLÉMENTÉ UNE POLITIQUE D'USAGE DE MOTS DE PASSE ROBUSTES ?

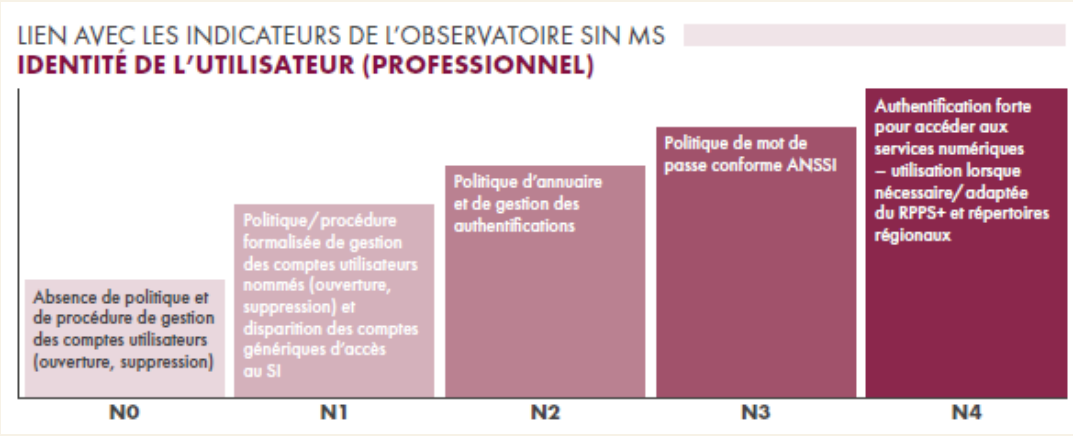
- Choisissez des mots de passe robustes
  - Qu'est-ce qu'un mot de passe robuste ?

L'Agence National de la Sécurité des Systèmes d'Information (ANSSI) recommande un minimum de **9 caractères** pour les services peu critiques et un minimum de **14 caractères** pour les services critiques (dont la compromission donnerait l'accès à des données de santé de l'usager).

- Définissez une bonne politique de mots de passe
  - Mise en place double authentification
  - Mise en place SSO

A quoi ça sert ?

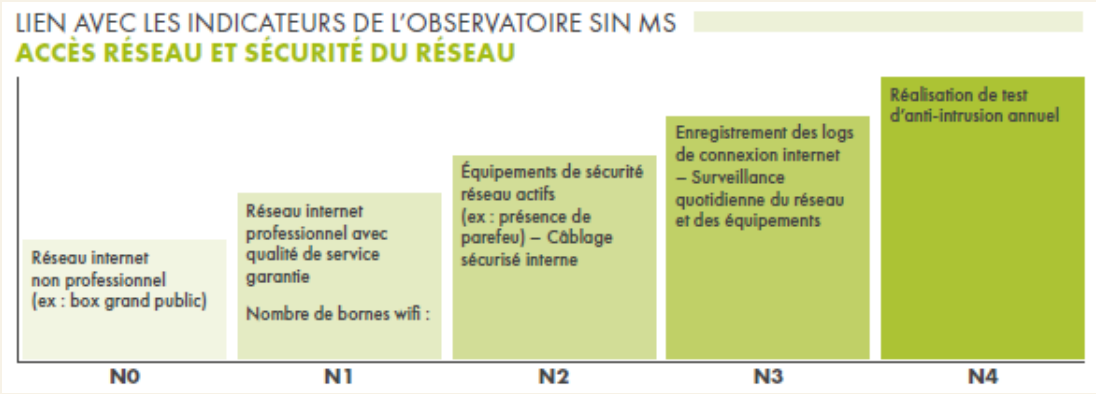
Une attaque contre les mots de passe au sein d'un ESSMS est susceptible d'impacter l'organisme gestionnaire ainsi que ses partenaires. De même, votre courriel pourrait être utilisé par l'attaquant pour adresser des courriels malveillants à vos contacts professionnels afin de les inciter à faire des actions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



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Question n°6 - AVEZ-VOUS ACTIVÉ UN PARE-FEU ? EN CONNAISSEZ-VOUS LES RÈGLES DE FILTRAGE ?

- Activez le pare-feu préinstallé sur le poste de travail
- 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.
- 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.



Différence entre Pare-feu et antivirus ?

le pare-feu surveille et filtre les paquets entrants et sortants tandis que l'antivirus effectue une opération d'analyse qui se fragmente en trois étapes (détection, identification et suppression).

A quoi ça sert ?

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.

LE MÉDICO-SOCIAL ENGAGÉ POUR LA E-SANTÉ

Question n°7 - COMMENT SÉCURISEZ-VOUS VOTRE MESSAGERIE ?

La sensibilisation des professionnels des ESSMS à identifier les tentatives d'hameçonnage (ou phishing en anglais) est primordiale :

- 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.

Il existe aussi des moyens techniques pour sécuriser sa messagerie :

- 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
- de l'activation du chiffrement des échanges entre serveurs de messagerie (de l'entité ou publics) ainsi qu'entre les postes utilisateurs et les serveurs hébergeant les boîtes de messagerie électronique.

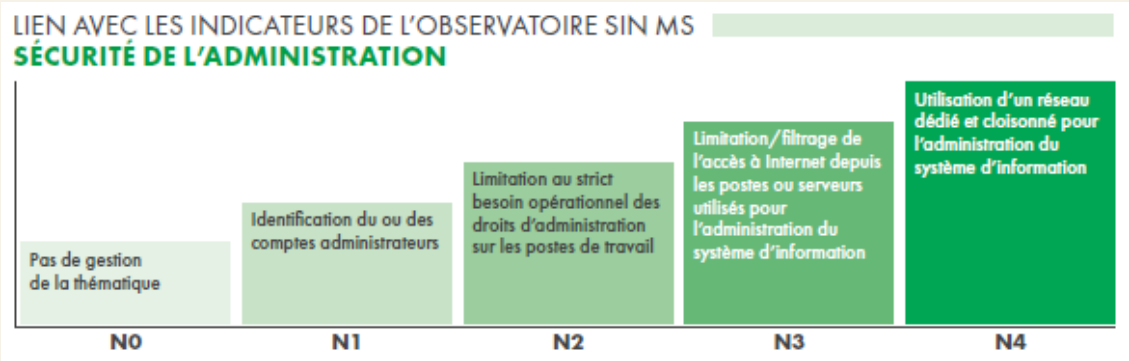
A quoi ça sert ?

La messagerie est le principal vecteur d'infection du poste de travail. C'est la première porte d'entrée pour un attaquant. Sa protection est primordiale .

LE MÉDICO-SOCIAL ENGAGÉ POUR LA E-SANTÉ

Question n°8 - COMMENT SÉPAREZ-VOUS VOS COMPTES ET VOS USAGES INFORMATIQUES ?

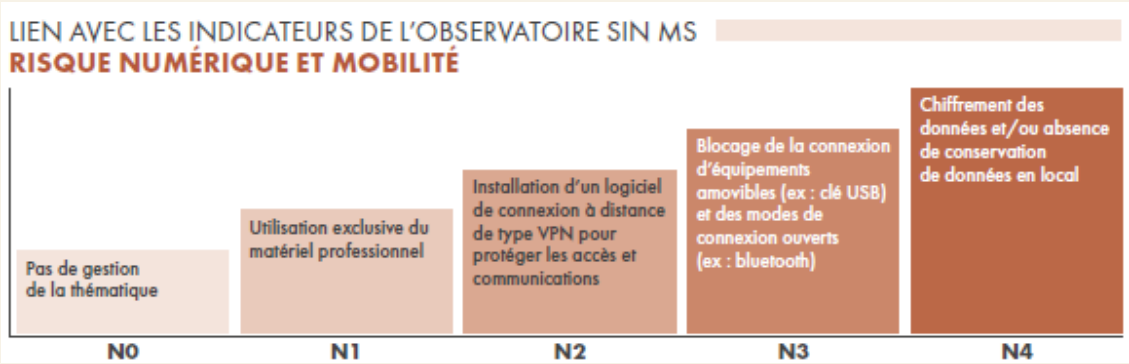
- Le premier principe d'hygiène repose sur la création de comptes utilisateurs dédiés à chaque employé et ne disposant pas de privilège d'administration.
- Les comptes et les privilèges administrateur doivent être tenus à jour : quand un employé quitte l'ESSMS, il convient de faire l'inventaire de ses accès et de tous les révoquer, de telle sorte que lui-même ou un tiers ne puisse plus y accéder.
- 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.



LE MÉDICO-SOCIAL ENGAGÉ POUR LA E-SANTÉ

Question n°9 - MAÎTRISEZ-VOUS LE RISQUE NUMÉRIQUE LIÉ AU NOMADISME DES PROFESSIONNELS ?

- 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.



A quoi ça sert ?

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.

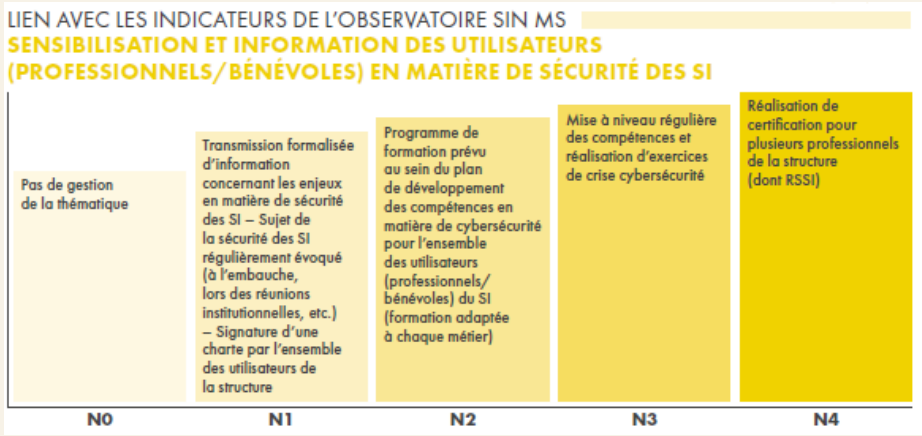
LE MÉDICO-SOCIAL ENGAGÉ POUR LA E-SANTÉ

Question n°10 - COMMENT VOUS INFORMEZ-VOUS ? COMMENT SENSIBILISEZ-VOUS VOS COLLABORATEURS ?

Pour s'informer et sensibiliser, plusieurs sources disponibles :

- Les ARS, GRADeS et les collectifs SI 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.
- L'ANSSI, l'ANS et l'ANAP produisent de la documentation à destination du secteur ou plus globalement sur la cybersécurité
- Il existe une veille plus technique réalisée par le CERT Santé (Computer Emergency Response Team Santé).

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…



A quoi ça sert ?

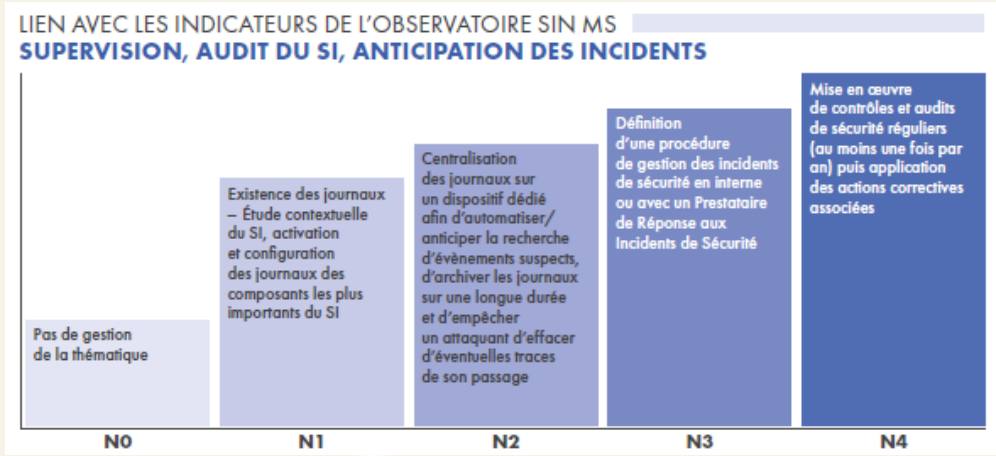
La cybersécurité est une affaire collective et commence par les utilisateurs : un professionnel informé et sensibilisé est la meilleure façon pour se protéger.

LE MÉDICO-SOCIAL ENGAGÉ POUR LA E-SANTÉ

Question n°11 - SAVEZ-VOUS COMMENT RÉAGIR EN CAS DE CYBERATTAQUE ?

- Identifiez préalablement des prestataires spécialisés dans la réponse aux incidents de sécurité : CERT Santé, ARS-GRADeS
- En cas d'incident :
  - 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
  - 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
- Concevoir et de déployer un dispositif de communication relatif à l'incident.

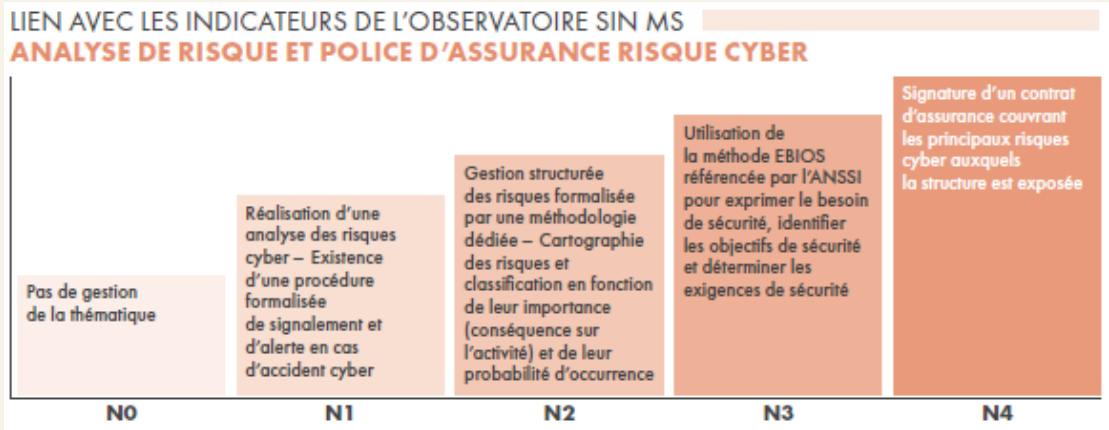
La déclaration d'incident est obligatoire pour les ESSMS depuis l'ordonnance du 19 novembre 2020. Le Décret n° 2022-715 du 27 avril 2022 relatif aux conditions et aux modalités de mise en œuvre du signalement des incidents significatifs ou graves de sécurité des systèmes d'information



LE MÉDICO-SOCIAL ENGAGÉ POUR LA E-SANTÉ

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.
- Ces clauses assurantielles peuvent se traduire dans les contrats d'assurance classique ou prendre la forme d'une police d'assurance « cyber » spécifique.
- Etant donné la forte externalisation des systèmes d'information du secteur médico-social, il est indispensable de demander aux prestataires, éditeurs de solution et hébergeurs, la couverture de leur police d'assurance en la matière.



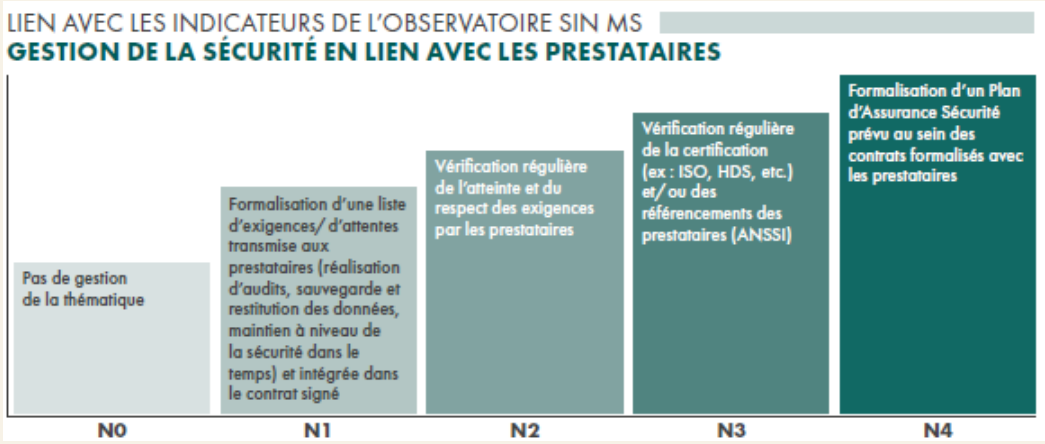
LE MÉDICO-SOCIAL ENGAGÉ POUR LA E-SANTÉ

Question n°13 - MAÎTRISEZ-VOUS LES RISQUES NUMÉRIQUES LIÉS À VOS RELATIONS AVEC DES TIERS ?

- Rédiger des contrats qui incluent des exigences précises pour lesquelles les tiers s'engagent
- Suivre et évaluer le respect des exigences de sécurité par les tiers

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.



A quoi ça sert ?

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.

LE MÉDICO-SOCIAL ENGAGÉ POUR LA E-SANTÉ

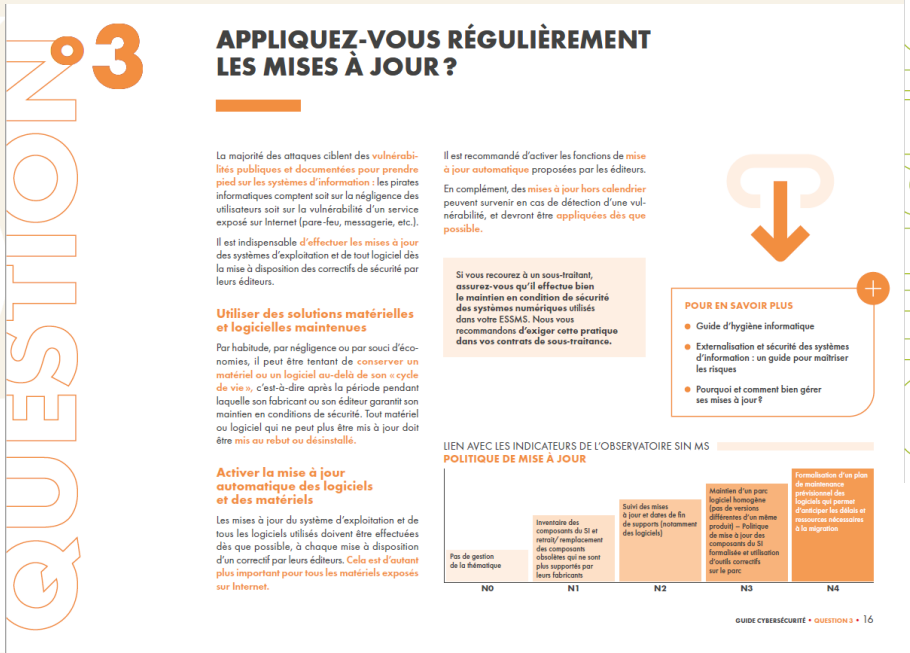
Avez-vous identifié la question « bonus » ?

LE MÉDICO-SOCIAL
ENGAGÉ
POUR LA E-SANTÉ

La cybersécurité pour les ESSMS en 13 questions

Une première version publiée dans le cadre de la journée du 13-14 octobre.

Le guide sortira officiellement prochainement avec les éditos des Ministres Jean-Christophe COMBE et François BRAUN, de la directrice générale de l'ANS Annie Prévot et de la directrice générale de la CNSA Virginie MAGNANT



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.

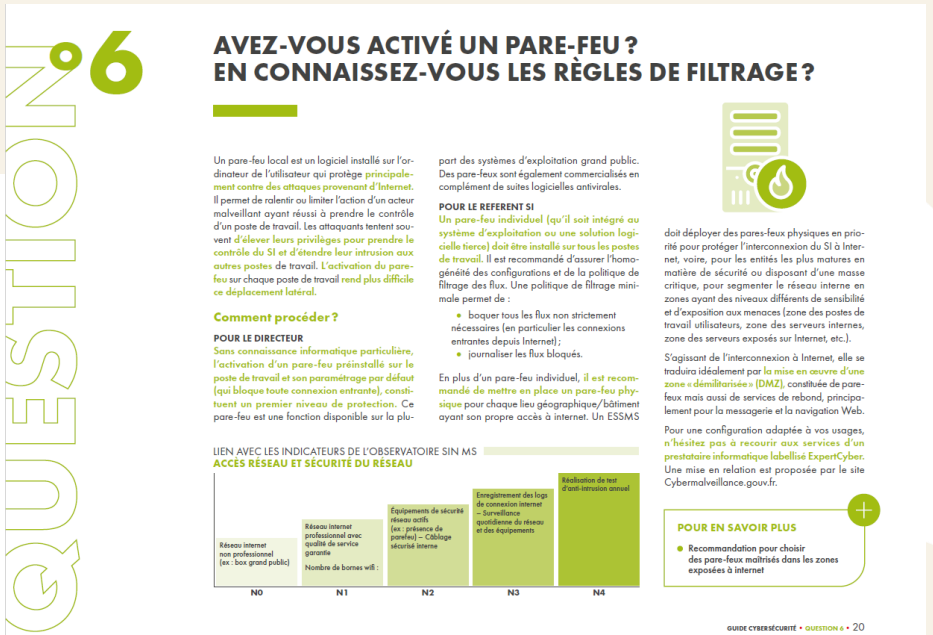
En complément, des mises à jour hors calendrier peuvent survenir en cas de détection d'une vulnérabilité, et devront être appliquées dès que possible.

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 n°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 :

- bloquer 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

LE MÉDICO-SOCIAL ENGAGÉ POUR LA E-SANTÉ

Merci pour votre attention

LE MÉDICO-SOCIAL
ENGAGÉ
POUR LA E-SANTÉ