Service de santé des armées

LA LETTRE TRIMESTRIELLE DU SSA SUR LA CYBERSÉCURITÉ ET LES CYBERMENACES

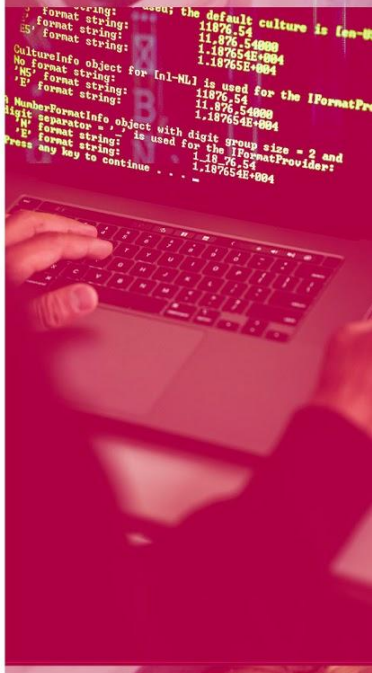
SENSIBILISATION

Pour votre sécurité…
faites vos mises à jour !

ACTUALITÉ DE LA CYBERSÉCURITÉ ET DE LA MENACE

FOCUS DU MOIS

La (cyber)sécurité des dispositifs médicaux : un enjeu de santé publique



SECOND TRIMESTRE 2021

SENSIBILISATION

Pour votre sécurité…faites vos mises à jour!

Les logiciels de nos appareils numériques (ordinateurs, tablettes et téléphones, équipements connectés, etc.) sont exposés à des **failles de sécurité**. Même si leur sécurité est soigneusement prise en compte à la conception, des failles de sécurité sont sans cesse recherchées, et régulièrement découvertes, par des **cybercriminels**.

Ces logiciels sont de natures diverses. Il peut s'agir des systèmes d'exploitation, comme Windows, MacOS, Android ou iOS ; des applications informatiques (apps)ı ; ou encore des pilotes, ces logiciels qui assurent la liaison entre le système d'exploitation et les périphériques.

Afin de prévenir et de corriger les failles de sécurité, les éditeurs et fabricants de logiciels proposent des **mises à jour**, à effectuer régulièrement. Pour un niveau de sécurité optimal, **les mises à jour des logiciels doivent être appliquées dès qu'elles sont rendues disponibles**. **Ces mises à jour, parfois longues (plusieurs minutes, voire plusieurs heures), sont souvent perçues comme une contrainte, mais constituent pourtant l'une des mesures les plus importantes de l'hygiène informatique**, comme l'expliquent ces vidéos: ⏯ et ⏯.

NB : en plus de corriger les failles de sécurité, les mises à jour servent également à supprimer les bugs et permettent d'accéder à de nouvelles fonctionnalités, parfois en améliorant l'ergonomie du logiciel concerné.

Puisque nous utilisons aujourd'hui de plus en plus d'appareils numériques, les failles de sécurité peuvent avoir des graves conséquences. Par exemple, une faille de sécurité découverte sur certains modèles de trottinettes électriques permettait de les déverrouiller ou encore d'agir sur l'accélération et le freinage. Une mise à jour a permis de corriger ces failles et d'éviter des accidents.

Il est facile d'en imaginer les déclinaisons dans le milieu médical : modification des paramètres d'un appareil d'examen radiologique ou d'un dispositif de suivi du rythme cardiaque d'un patient, par exemple. Il est donc indispensable de tenir à jour l'intégralité de ses appareils et de ses systèmes d'exploitation, dans la sphère tant personnelle que professionnelle.

"*Voilà ce qu'il se passe quand tu ne mets pas à jour Acrobat Reader*"

Le "jour zéro" (*zero-day*), qu'est ce que c'est?

Une vulnérabilité "jour zéro" (*zero-day*) désigne une faille de sécurité informatique qui n'est pas encore connue de l'éditeur du logiciel ou corrigée par lui. Ce type de faille peut être exploité par des cybercriminels pour lancer des attaques. On parle alors d'exploitation "jour zéro" (*zero-day exploit*).

Mises à jour : les bonnes pratiques à adopter

Effectuez toutes vos mises à jour, sans délai : nous utilisons un nombre grandissant d'appareils et de logiciels (ordinateurs, téléphones, logiciels de traitement de texte, objets connectés, etc.). Installer les mises à jour dès qu'elles sont disponibles permet d'empêcher que ces failles soient exploitées à des fins malveillantes, par exemple pour prendre le contrôle de votre environnement informatique, dérober des informations, rendre le système indisponible, modifier des données, lancer des attaques vers d'autres systèmes, envoyer des spams, etc.

Autant que possible, n'utilisez que les mises à jour proposées par les sites officiels: seuls les sites ou dispositifs officiels des éditeurs et fabricants garantissent que les mises à jour ne sont pas infectées par un virus. Méfiez-vous des autres sites et des mails de *phishing* qui vous conduiront vers de faux sites de mise à jour, au risque de piéger vos outils numériques au lieu d'en corriger les failles.

Activez les mises à jour automatiques : certains logiciels peuvent être configurés pour télécharger et installer automatiquement les mises à jour. Vérifiez toutefois de temps en temps que les mises à jour ont bien été effectuées automatiquement, en passant par le menu "Mises à jour" du logiciel concerné.

Planifiez vos mises à jour lors de périodes d'inactivité : même s'ils interrompent une activité personnelle ou professionnelle, et même si la mise à jour peut prendre plusieurs minutes, voire plusieurs heures, n'ignorez pas les messages indiquant la disponibilité d'une mise à jour. Afin d'éviter de toujours remettre les mises à jour à plus tard, profitez plutôt de périodes d'inactivité pour les effectuer (pause déjeuner, nuit...).

Désinstallez les logiciels que vous n'utilisez pas : il est probable que vous ne mettiez pas à jour les logiciels que vous n'utilisez jamais. Il est donc vivement recommandé de les désinstaller, afin d'éviter qu'ils servent de portes d'entrée aux cybercriminels.

Attention aux logiciels utilitaires ! De nombreux petits logiciels utilitaires (par exemple ceux servant à compresser des fichiers, nettoyer le disque dur, etc.) disponibles sur Internet ne sont jamais tenus à jour. Si vous en téléchargez pour un besoin ponctuel, supprimez-les dès que vous n'en avez plus besoin, quitte à les télécharger à nouveau ultérieurement s'il le faut.

ACTUALITÉ DE LA CYBERSÉCURITÉ ET DE LA MENACE

Les données personnelles et médicales de 500 000 personnes ont fuité sur Internet

Les données de 500 000 personnes piratées, les Armées touchées

Un piratage massif a provoqué la fuite des données de 500 000 personnes, provenant de 27 laboratoires et comprenant notamment des données médicales sensibles. Des informations de type adresse postale, téléphone, email, ou encore numéro de sécurité sociale, ont été repérées dans une base de données circulant librement sur un forum en ligne. Elles comprenaient parfois des indications sur le groupe sanguin, le médecin traitant ou la mutuelle, ou encore des commentaires sur l'état de santé, les traitements médicamenteux ou les pathologies des personnes concernées. Il s'agirait de données correspondant à des prélèvements effectués entre 2015 et 2020.

Les coordonnées et données médicales de près de 1 800 militaires auraient été repérées dans cette base de données, identifiables par leur affiliation à la Caisse nationale militaire de sécurité sociale (CNMSS).

Le numéro de sécurité sociale : une donnée critique

Les numéros de sécurité sociale piratés constituent des données particulièrement intéressantes pour qui voudrait en faire mauvais usage. Un cybercriminel avec un certain niveau d'expertise pourrait par exemple s'en servir via FranceConnect pour accéder aux différents comptes de la personne concernée.

Les rançongiciels menacent toujours le secteur de la santé

Les cyberattaques par rançongiciels contre des organisations de santé continuent. Le 31 mars, le groupe pharmaceutique français Pierre Fabre a été victime d'un rançongiciel ayant paralysé une partie de ses activités. Il s'agirait du rançongiciel REvil.

Les cybercriminels auraient d'abord demandé une rançon de 25 millions de dollars pour restituer les données chiffrées, avant de passer à 50 millions devant l'absence de réponse du groupe.

Courant avril, la Fondation santé des étudiants de France, à la tête de 13 cliniques réalisant des soins de psychiatrie ou de réadaptation pour des jeunes de 12 à 25 ans, a été victime d'un rançongiciel rendant inaccessibles la plupart des données des patients. La majorité des dossiers patients ont pu être récupérés grâce aux systèmes de sauvegarde.

L'hôpital de Saint-Gaudens (Haute-Garonne) a également été touché début avril par un rançongiciel, qui a, entre autres, privé le personnel de l'accès aux téléphones, aux messageries électroniques et aux dossiers des patients. Seule la téléphonie a pu être rapidement remise en service.

La cellule cybersécurité en santé de l'Agence du Numérique en Santé (ANS) devient le CERT Santé

La cellule d'Accompagnement Cybersécurité des Structures de Santé (ACSS) de l'ANS est devenue en avril 2021 le CERT Santé.

Un CERT (Computer Emergency Response Team) est un centre qui assure une veille sur les vulnérabilités logicielles et sur les modes opératoires des attaquants, fournit des recommandations pour parer ces menaces et apporte une assistance en cas d'attaque.

Le CERT Santé de l'ANS a pour mission de :

- Traiter les signalements d'incidents indésirables ;
- Apporter une assistance à la structure touchée ;
- Diffuser des alertes vers les autorités compétentes ;
- Mettre à disposition des structures de santé des recommandations et des bonnes pratiques ;
- Assister les structures dans l'identification des menaces ;
- Proposer des mesures de remédiation adaptées ;
- Si nécessaire, orienter les structures touchées vers un prestataire adapté ;
- Opérer une veille active des cybermenaces et en avertir les structures via le portail cyberveille santé.

Etat des lieux des incidents ayant touché les structures de santé en 2020

L'ANS a publié son rapport 2020 de l'Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé, présentant plusieurs informations clés :

- En 2020, 250 établissements ont déclaré 369 incidents de cybersécurité (-6% sur 2019) ;
- 60% des incidents déclarés sont d'origine malveillante (contre 43% en 2019) ;
- La majorité des signalement viennent des régions Ile-de-France et Auvergne-Rhône-Alpes (30% du total des signalements) ;
- Parmi les incidents ayant impacté des données (60% du total des incidents), 79% ont touché des données de santé à caractère personnel ;
- Parmi 34 mises en danger potentielles de patients, 2 sont avérées. Les incidents concernés sont principalement liés à la perte de liens téléphoniques, notamment pour les SAMU, et à l'indisponibilité des systèmes d'information.

L'ANS publie le référentiel "Force Probante" sur la conservation des données de santé

L'Agence du Numérique en Santé (ANS) a publié le 22 mars 2021 le référentiel "Force probante" relatif à la conservation sécurisée des documents de santé.

La "force probante" est définie comme "*le niveau de confiance que l'on peut accorder à un document ou une donnée. Dans le secteur du numérique en santé, la force probante des documents comportant des données de santé dématérialisées répond à un enjeu relatif au droit de la preuve mais avant de servir comme outil de preuve, elle est avant tout essentielle pour donner de la confiance dans la dématérialisation. Le degré de conviction que l'on peut accorder à un document dématérialisé varie en fonction des conditions de son élaboration et du maintien dans le temps de la réunion de ces conditions*".

Le référentiel "Force probante" est composé d'un document introductif et de 6 annexes :

- Annexe n°1 : Socle commun des principes techniques et organisationnels ;
- Annexe n°2 : Mécanismes de sécurité à mettre en œuvre dans le cadre de la numérisation ;
- Annexe n°3 : Mécanismes de sécurité à mettre en œuvre dans le cadre de la production de documents nativement numériques ;
- Annexe n°4 : Mécanismes de sécurité à adopter dans le cadre de la matérialisation des documents de santé ;
- Annexe n°5 : Gestion des métadonnées ;
- Annexe n°6 : Classification des documents de santé.

Plusieurs entités ont été impliquées dans la rédaction de ce référentiel, parmi lesquelles le ministère des Solidarités et de la Santé, l'Assurance maladie, la Haute autorité de santé (HAS), des Directions des systèmes d'information (DSI), des biologistes et des archivistes intervenant au sein de structures de santé.

Rappel : une ordonnance du 12 janvier 2017 encadre les modalités de destruction des dossiers médicaux une fois numérisés et les conditions permettant de garantir une valeur probante aux données et documents de santé numérisés.

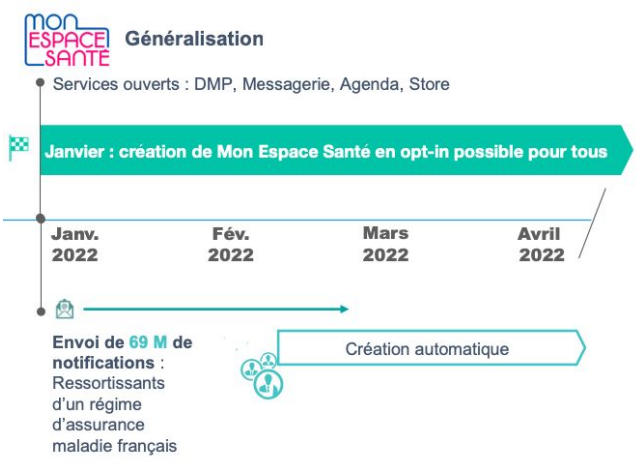
"Mon espace santé": le futur service public de gestion des données de santé

Le gouvernement français a présenté le futur service public "Mon espace santé", dont le lancement est prévu en janvier 2022 après une phase de test dans trois départements (Haute-Garonne, Loire-Atlantique et Somme) courant 2021. Concrètement, "Mon espace santé" sera un espace numérique individuel permettant aux Français de stocker leurs données de santé et de les partager si nécessaire avec des professionnels de santé. Les données stockées seront hébergées en France.

Le service "Mon espace santé", développé par Atos, Octo, Accenture et Maincare, intégrera 4 modules :

- Un dossier médical partagé (DMP), pour stocker des informations médicales (antécédents médicaux, traitements, résultats d'examens, comptes-rendus d'hospitalisation, etc.) ;
- Un agenda de santé, afin d'enregistrer ses rendez-vous médicaux et de recevoir des rappels pour les vaccins et les dépistages recommandés ;
- Une messagerie sécurisée pour les échanges entre patients et professionnels de santé ;
- Un catalogue d'applications dédiées à la santé et au bien-être.

"Mon espace santé" sera accessible sur *smartphone*, ordinateur ou tablette, via un site Internet (monespacesante.fr) et, plus tard, une application mobile dédiée.



Généralisation de "Mon espace santé" à partir de janvier 2022

Lancement d'un appel à manifestation d'intérêt pour des solutions innovantes de cybersécurité à l'hôpital

Dans le cadre du plan France Relance, un appel à manifestation d'intérêt a été lancé afin d'expérimenter des solutions innovantes "*pour répondre aux besoins de cybersécurité de trois types de structures : les collectivités territoriales, les établissements de santé et les infrastructures portuaires*".

Au moins trois projets de démonstrateurs seront retenus, puis un appel à projets sera lancé afin de soutenir le développement des solutions. L'Etat s'est engagé à cofinancer le développement de ces innovations.

Rappel : le gouvernement a annoncé en février 2021 que les 135 groupements hospitaliers de territoire (GHT) seront intégrés à la liste des opérateurs de services essentiels (OSE). Cela implique qu'ils devront donc respecter les règles de cybersécurité et les obligations fixées pour les OSE par la législation européenne et la réglementation nationale.

L'ANSSI propose des "parcours de cybersécurité" aux établissements de santé

Afin d'accompagner les établissement de santé dans l'amélioration du niveau de sécurité de leurs systèmes d'information (SI), l'Agence nationale de la sécurité des systèmes d'information (ANSSI) propose des "parcours de cybersécurité".

Les établissements doivent candidater afin de bénéficier d'un parcours adapté à leurs besoins et à leurs enjeux.

Quatre parcours sont proposés :

- Parcours fondation
- Parcours intermédiaire
- Parcours avancé
- Parcours renforcé.

Le système de santé irlandais paralysé par une cyberattaque

Le 14 mai 2021, le système informatique du Health Service Executive (HSE), le service public de santé irlandais, a été touché par une cyberattaque au rançongiciel Conti. Il pourrait s'agir d'une attaque "jour zéro" utilisant une version encore inconnue du rançongiciel. Les données chiffrées et volées contiendraient des dossiers médicaux de patients, mais également des documents sur la gestion de l'hôpital, comme des factures d'achat d'équipements ou des comptes-rendus de réunions.

➔ Le National Cyber Security Centre (NCSC) irlandais a publié un rapport détaillant de l'incident et présentant des détails techniques de l'attaque.

Pendant plus d'une semaine, le personnel de la plupart des hôpitaux irlandais ne pouvait plus se servir des ordinateurs des établissements. Un grand nombre de rendez-vous et des traitements ont dû être annulés. Les dossiers des patients, stockés électroniquement, n'étaient plus accessibles, forçant le personnel à recréer des dossiers "papier". Les services d'urgence et d'ambulance n'ont cependant pas été impactés et ont continué de fonctionner normalement. Les tests Covid-19 et la vaccination se sont poursuivis mais ont été considérablement ralentis.

Selon des sources journalistiques, la rançon demandée s'élèverait à £14 millions (€16 millions). La BBC a par ailleurs annoncé que deux semaines après la cyberattaque, les pirates responsables auraient donné au gouvernement irlandais un logiciel lui permettant de récupérer les données chiffrées sans demander de compensation, après que le gouvernement ait insisté sur le fait qu'il ne paierait pas la rançon. Le travail de réactivation du système est toutefois monumental. De plus, le groupe de pirates menacent toujours le HSE de publier ou de revendre les données volées si la rançon reste impayée. Les dossiers médicaux de 12 patients auraient déjà été publiés sur le *dark web*.

Quelques jours plus tard, le Department of Health du gouvernement irlandais a annoncé avoir été touché par une cyberattaque similaire. Les deux attaques ont été attribuées au groupe de cybercriminels russes Wizard Spider.

FOCUS

La (cyber)sécurité des dispositifs médicaux : un enjeu de santé publique

Des dispositifs médicaux de plus en plus connectés

Si ce n'était historiquement pas le cas, de plus en plus de dispositifs médicaux sont aujourd'hui **connectés**, soit directement, soit à distance à un **système d'information (SI) hospitalier** via des réseaux 4G/5G, Wi-Fi, *bluetooth* ou filaires, afin de permettre aux professionnels de santé de recueillir et de stocker les données collectées, et d'assurer la régulation d'un traitement à distance. En parallèle, les médias relaient de plus en plus d'affaires de piratage et de vols de données médicales dans les établissements de santé. Enfin, les cybermenaces qui pèsent actuellement sur les systèmes d'information et les dispositifs connectés, tout particulièrement dans le secteur de la santé, n'ont que rarement été prises en compte à la conception.

Le Règlement européen relatif aux dispositifs médicaux

Le Règlement européen 2017/745 relatif aux dispositifs médicaux, modifié en 2020, fixe l'ensemble des exigences applicables aux dispositifs médicaux, y compris de **cybersécurité**. Le texte prévoit notamment la sécurité des **logiciels** des dispositifs médicaux connectés dès leur **conception** (cybersécurité dite *by design*), ainsi que le **maintien en condition de sécurité** une fois ces logiciels mis en oeuvre, ce qui n'était jusqu'alors pas obligatoire. Le Règlement s'adresse ainsi tant aux fabricants de dispositifs médicaux connectés (leurs produits doivent être conformes au Règlement) qu'aux équipes de la Direction des systèmes d'Information (DSI) des établissements de santé (elles doivent veiller à acquérir uniquement des produits conformes et assurer le maintien en condition de sécurité des dispositifs).

Rappel: il s'agit d'un Règlement européen, c'est-à-dire applicable dans l'UE sans transposition dans le droit des pays et juridiquement au-dessus des dispositions nationales.

Le Règlement définit le terme **dispositif médical** comme une grande variété de produits utilisés à des fins de "*diagnostic, prévention, contrôle, prédiction, pronostic, traitement ou atténuation d'une maladie, d'une blessure ou d'un handicap ; investigation, remplacement ou modification d'une structure ou fonction anatomique ou d'un processus ou état physiologique ou pathologique ; soutien ou maintien en vie, etc.*" Il peut ainsi s'agir de simples bandages, de prothèses, mais également de **dispositifs connectés** destinés à collecter et suivre des données de santé (tension, rythme cardiaque, glycémie, etc.), ou à réguler un traitement à distance (pompe à insuline, par exemple).

La cybersécurité *by design* des dispositifs médicaux

Le Règlement européen relatif aux dispositifs médicaux prévoit l'intégration de mesures de cybersécurité dès la conception des équipements. Les fabricants doivent en effet mettre en place "*les mesures de sécurité informatique, y compris la protection contre l'accès non autorisé, qui sont nécessaires pour faire fonctionner le logiciel comme prévu*" (Annexe I, §17.4). Ils sont également tenus de respecter un certain nombre d'exigences, comme la mise en place d'un système de gestion des risques et d'un système de surveillance du dispositif après sa commercialisation. Ils doivent également informer immédiatement les autorités compétentes en cas de risque grave, ainsi que mettre en place des correctifs de sécurité en cas de failles de sécurité détectées (article 10).

Les "Règles pour les dispositifs connectés d'un Système d'Information de Santé"

Le guide "Règles pour les dispositifs connectés d'un Système d'Information de Santé", publié en 2013 parmi les documents de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), établit des règles de sécurité destinées aux fabricants de dispositifs médicaux connectés afin que ceux-ci soient conformes aux standards de sécurité du domaine de la santé. Parmi ces nombreuses règles, nous retiendrons les suivantes :

- Tous les dispositifs connectés et logiciels des ordinateurs utilisés dans les établissements de santé doivent pouvoir être régulièrement **mis à jour** de manière sécurisée ;
- Les dispositifs connectés doivent comporter une fonction d'**authentification** pour chaque utilisateur, grâce à la mise en place de comptes utilisateurs nominatifs et de mots de passe modifiables par les utilisateurs ;
- Les **mots de passe** par défaut doivent pouvoir être changés lors de la première connexion d'un utilisateur au dispositif ou au poste de travail, et être spécifiques à chaque utilisateur ;
- Les dispositifs médicaux connectés doivent embarquer un dispositif de **chiffrement des données** afin de garantir la confidentialité des données médicales personnelles collectées et stockées localement.

Quels incidents de cybersécurité est-il obligatoire de déclarer dans ce cadre?

En octobre 2017, le ministère des Solidarités et de la Santé a mis en place un dispositif de traitement des signalements des incidents de sécurité des systèmes d'information des structures de santé : la cellule d'Accompagnement Cybersécurité des Structures de Santé (ACSS) de l'Agence Numérique en Santé, devenue en 2021 le **CERT Santé**. Le CERT Santé assiste les structures de santé tant dans la prévention des attaques que dans la résolution des incidents dont elles seraient victimes.

Depuis la mise en place de ce dispositif en 2017, les établissements de santé, les centres de radiothérapie et les laboratoires de biologie médicale ont obligation de déclarer les **incidents graves ou significatifs** de sécurité de leurs systèmes d'information (article L. 1111-8-2 du code de la santé publique). En novembre 2020, il a été précisé que "*sous réserve du respect des règles relatives à la protection du secret de la défense nationale, le présent article est applicable au* ***service de santé des Armées*** *en ce qui concerne les incidents graves de sécurité des systèmes d'information intéressant les activités de prévention, de diagnostic ou de soins des* ***hôpitaux des Armées***". L'obligation a également été étendue aux établissements médico-sociaux.

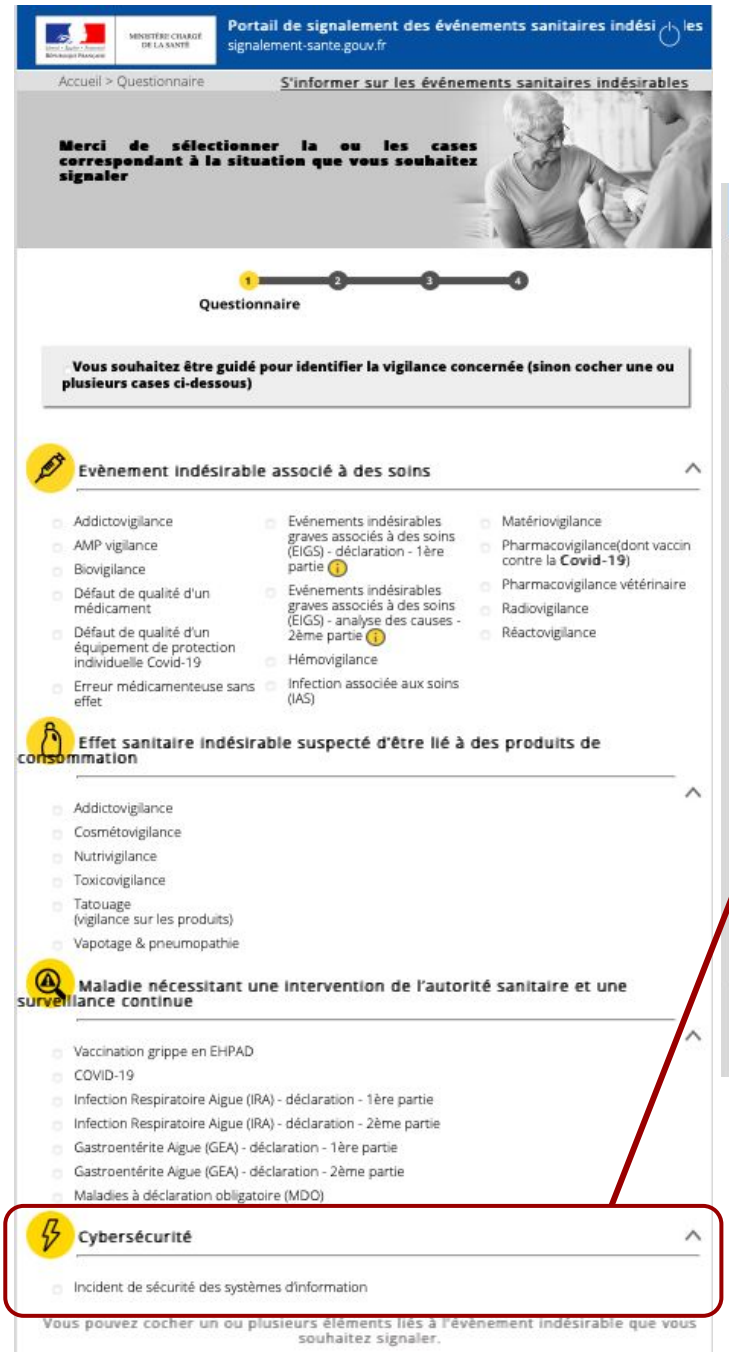
Les incidents **graves** de sécurité des systèmes d'information ont été définis par décret. Il s'agit d'"*événements générateurs d'une situation exceptionnelle au sein d'un établissement, organisme ou service, et notamment :*

- *Les incidents ayant des conséquences potentielles ou avérées sur la sécurité des soins ;*
- *Les incidents ayant des conséquences sur la confidentialité ou l'intégrité des données de santé ;*
- *Les incidents portant atteinte au fonctionnement normal de l'établissement, de l'organisme ou du service.*"

Parmi les incident graves, les incidents **significatifs** sont définis comme "*ayant un retentissement potentiel ou avéré sur l'organisation départementale, régionale ou nationale du système de santé*" et "*susceptibles de toucher d'autres établissements, organismes ou services*".

Comment signaler un incident de cybersécurité sur un système d'information de santé?

Le signalement se fait via le Portail de signalement des événements sanitaires indésirables*. L'encadré en bas de page présente la **procédure spécifique à appliquer au sein du SSA**. Les déclarations sont transmises à l'Agence du Numérique en Santé et à l'agence régionale de santé compétente. L'ANS analyse les déclarations et qualifie les incidents signalés, puis informe les autorités compétentes.



*Copies d'écran du Portail de signalement des événements sanitaires indésirables**

Au sein du Service, un compte rendu immédiat doit être transmis à la chaîne Cyber du SSA, au besoin par un FI@sh Event si l'événement le nécessite. La procédure ad hoc est détaillée dans l'instruction n°20/ARM/CAB/CM11/NP du 30 avril 2020 fixant la conduite à tenir par les autorités civiles et militaires en cas d'accidents ou d'incidents survenus au sein du ministère des Armées ou des établissements publics qui en dépendent. A l'issue, la déclaration auprès du CERT Santé doit être réalisée sur le Portail de signalement des événements sanitaires indésirables.

BIBLIOGRAPHIE

Sensibilisation

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour

https://www.codeur.com/blog/mettre-a-jour-application-mobile/

https://www.malekal.com/les-mises-a-jour-logiciels/

https://www.panoptinet.com/cybersecurite-pratique/importance-des-mises-a-jour-logicielles.html

https://www.nowteam.net/gestion-des-mises-a-jour-en-entreprise-les-bonnes-pratiques/

https://dai.ly/x7txg0d

https://dai.ly/x7n127n

https://www.youtube.com/watch?v=ZR3Gf8NKkc4

https://www.journaldunet.com/solutions/dsi/1496169-tout-ce-que-vous-devez-savoir-sur-zerologon/

https://blog.zimperium.com/new-advanced-android-malware-posing-as-system-update/

https://www.kaspersky.fr/resource-center/definitions/zero-day-exploit

Actualité

https://www.lefigaro.fr/flash-eco/une-fondation-a-la-tete-de-13-cliniques-victime-d-une-cyberattaque-20210420

https://www.lemondeinformatique.fr/actualites/lire-pierre-fabre-revil-a-la-manoeuvre-25-m$-de-rancon-demandes-82571.html

https://www.usine-digitale.fr/article/l-hopital-de-saint-gaudens-touche-par-un-ransomware-les-tests-covid-19-interrompus.N1081059

https://www.google.fr/amp/s/www.usine-digitale.fr/amp/article/victime-d-une-cyberattaque-la-production-du-groupe-pharmaceutique-pierre-fabre-est-a-l-arret.N1078119

https://www.solutions-numeriques.com/fuite-de-donnees-medicales-larmee-touchee-selon-le-site-intelligence-online/

https://www.ticsante.com/story.php?story=5628

https://esante.gouv.fr/force-probante-des-documents-de-sante

https://cyberguerre.numerama.com/11011-que-peuvent-faire-les-malfaiteurs-avec-votre-numero-de-securite-sociale.html

https://www.usine-digitale.fr/article/avec-mon-espace-sante-le-gouvernement-veut-faciliter-la-gestion-des-donnees-medicales-des-francais.N1088734

https://www.frenchweb.fr/a-quoi-va-ressembler-le-nouveau-service-public-mon-espace-sante/421130

https://esante.gouv.fr/mon-espace-sante

https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033860800/

https://www.lepoint.fr/high-tech-internet/fuite-de-donnees-medicales-l-armee-francaise-aurait-ete-touchee-egalement-04-03-2021-2416468_47.php

https://www.liberation.fr/checknews/les-informations-confidentielles-de-500-000-patients-francais-derobees-a-des-laboratoires-medicaux-et-diffusees-en-ligne-20210223_VO6W6J6IUVATZD4VOVNDLTDZBU/

https://www.cyberveille-sante.gouv.fr/sites/default/files/2021-04/ANS_ACSS_Rapport_Public_Observatoire_Incidents_ISSIS_2020.pdf

https://www.ticsante.com/story.php?story=5622

https://www.usine-digitale.fr/article/l-hopital-de-saint-gaudens-touche-par-un-ransomware-les-tests-covid-19-interrompus.N1081059

https://www.techopital.com/cybersecurite-a-l-hopital--lancement-d-un-appel-a-manifestation-d-interet-pour-experimenter-des-solutions-innovantes-NS_5571.html

https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/nis-un-dispositif-de-cybersecurite-pour-les-operateurs-de-service-essentiel/#a2

https://www.techopital.com/l-anssi-propose-des-parcours-de-cybersecurite-aux-etablissements-de-sante-NS_5563.html?search=cyber

https://www.ssi.gouv.fr/agence/cybersecurite/le-volet-cybersecurite-de-france-relance/securiser-le-socle-numerique-de-letat-des-collectivites-territoriales-et-des-organismes-au-service-des-citoyens/les-parcours-de-cybersecurite/

https://www.bbc.com/news/world-europe-57111615

https://www.bbc.com/news/world-europe-57197688

https://www.bbc.com/news/world-europe-57184977

https://abcnews.go.com/International/10-days-ransomware-attack-irish-health-system-struggling/story?id=77876092

https://www.bloomberg.com/news/articles/2021-05-16/irish-health-care-system-suffers-new-cyber-attack-rte-reports

https://www.insideprivacy.com/data-privacy/major-cyber-attack-on-irish-health-system-causes-commercial-concern/

https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf

https://news.sophos.com/fr-fr/2021/02/24/attaque-ransomware-conti-detaillee-jour-apres-jour/

Focus

https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A02017R0745-20200424

https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/choixSignalementPS

https://esante.gouv.fr/securite/cybersecurite

https://esante.gouv.fr/securite

https://esante.gouv.fr/sites/default/files/media_entity/documents/mss_ans_rapport_public_observatoire_signalements_issis_2020_v0.96_09042020_vf.pdf

https://esante.gouv.fr/securite/pgssi-s/espace-de-publication

https://esante-formation.fr/course/index.php?categoryid=6

https://esante.gouv.fr/sites/default/files/media_entity/documents/Guide_Pratique_Dispositif_Connecte.pdf

https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000036515017/2018-01-19

https://documents.lne.fr/fr/actualites/lettres-information/medical/0517/a2-cybersecurite.asp

https://www.revmed.ch/RMS/2016/RMS-N-535/Cybersecurite-des-dispositifs-medicaux-point-sur-la-menace-reelle-et-role-du-corps-medical

https://www.qualitiso.com/cybersecurite-des-dispositifs-medicaux/

https://www.legifrance.gouv.fr/jorf/id/JORFARTI000042532922

https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000033118341?init=true&page=1&query=D.+1111-16-2&searchField=ALL&tab_selection=all&anchor=LEGIARTI000033118811#LEGIARTI000033118811

Cette Lettre trimestrielle est réalisée par ceis avisa partners