FONDATIONS DES SYSTEMES D'INFORMATION DE SANTE ET REFERENTIELS SOCLES

2.3. Sécurité opérationnelle

DOCTRINE

Pour garantir la confiance dans la e-santé, la sécurité opérationnelle des systèmes numériques en santé doit être renforcée au travers :

- d'une extension à l'ensemble des acteurs de santé du dispositif de déclaration des incidents de sécurité, en particulier aux catégories de structures les plus vulnérables face à la menace cyber et pour une meilleure connaissance de l'exposition du secteur aux actes de cyber-malveillance ;
- d'une détection préventive des vulnérabilités des systèmes et en particulier en cas d'exposition sur Internet en vue d'améliorer la couverture des risques cyber.

❶ Extension du dispositif de déclaration des incidents de sécurité

La cellule Accompagnement Cybersécurité des Structures de Santé de l'ANS (cellule ACSS créée en 2017), sous pilotage du fonctionnaire de sécurité des systèmes d'information, apporte un appui aux établissements de santé, aux laboratoires de biologie médicale et aux centres de radiothérapie déclarant leurs incidents de sécurité sur le portail de signalement des évènements sanitaires indésirables.

Le dispositif vise à renforcer le suivi des incidents des structures concernées au sein du secteur santé, alerter et informer l'ensemble des acteurs de la sphère santé dans le cas d'une menace pouvant avoir un impact sur le secteur.

Le traitement des incidents remontés permet de proposer, sur la base de l'expertise de la cellule et de nombreux retours d'expérience, des actions concrètes adaptées au contexte de l'incident et à la structure pour stopper l'éventuelle progression de l'incident et protéger son système d'information.

Les principales recommandations prennent la forme de fiches réflexes par type de menaces (par exemple dans le cas d'un cryptovirus, d'une attaque de type Phishing, d'une intrusion web, etc.) portées à la connaissance des structures au travers du portail cyberveille-santé.

Les retours d'expérience permettent de faire la lumière sur le mode opératoire de certaines attaques et de présenter des mesures de remédiation à mettre en œuvre selon la nature de l'incident.

L'extension du dispositif à l'ensemble des structures de santé et du médico-social doit permettre d'accompagner l'ensemble des structures du secteur et en particulier d'apporter un appui aux structures les plus vulnérables afin d'améliorer leur résilience face à la menace cyber.

La mise en place d'un **observatoire des incidents** (dispositif national centralisant la remontée des incidents impactant l'ensemble du territoire) apporte une vision consolidée de la menace au niveau sectorielle. Il fournit des éléments de pilotage sectoriel de la sécurité, permet d'identifier les efforts à réaliser (nécessaires) en matière de sécurité opérationnelle (en fonction des incidents survenus). Il offre également l'opportunité de détecter les menaces sectorielles et de freiner leur exploitation généralisée en alertant le réseau des correspondants.

L'observatoire produit des analyses sectorielles de la sécurité, fondées sur le traitement des signalements d'incidents de sécurité complétés, le cas échéant, par des études et/ou veilles complémentaires. Il propose des axes d'amélioration de la sécurité opérationnelle fondés sur les retours d'expérience des incidents signalés ainsi que les statistiques consolidées d'évènements.

En complément, la cellule ACSS se prépare à rejoindre le groupe « InterCERT-FR » qui réunit de façon régulière un ensemble d'organismes ayant des activités d'IRT (Incident Response Team) sur le territoire français afin de gagner en visibilité, de bénéficier des retours d'expérience des membres du groupe et d'échanges bi ou multilatéraux.

❷ Mise en place d'un service national de cyber-surveillance en santé

Un service de **cyber-surveillance des systèmes d'information exposés** des structures de santé est mis en place.

Le service proposé doit **mesurer le degré d'exposition des interfaces** exposées d'un système au regard des vulnérabilités connues, de l'état de l'art, …

Le service de cyber-surveillance teste automatiquement les interfaces exposées sur internet ; il ne constitue pas un outil d'évaluation exhaustif de la sécurité d'un SI et ne permet pas au **responsable de traitement** de se soustraire à une **analyse de sécurité de l'ensemble de ses actifs numériques**. Le service pourrait toutefois être enrichi pour analyser le périmètre interne de l'établissement voire les équipements biomédicaux.

Pour ce faire, les fonctionnalités de la plateforme de cyber-surveillance sont de :

- cartographier et déterminer la surface d'attaque d'un système d'information ;
- détecter de manière pro-active les vulnérabilités qui affectent le système d'information d'une organisation ;
- détecter une éventuelle fuite de données (fuite de code-sources, fuite de données, fuite de données utilisateur, etc.) visant le système d'information.

Le rapport de cyber-surveillance fourni présente l'ensemble des vulnérabilités détectées par criticité ainsi qu'un plan d'actions de remédiation hiérarchisé.

Le service de cyber-surveillance **peut être mis en œuvre de façon récurrente** avec un suivi dans le temps des vulnérabilités afin de :

- tenir compte de l'apparition fréquente **de nouvelles failles** ;
- et mesurer les **efforts de correction** en restituant l'évolution de l'exposition à la menace cyber pour le périmètre considéré.

Un **observatoire des vulnérabilités** est constitué sur la base d'une consolidation des rapports de cyber-surveillance unitaires.

L'observatoire fournit une analyse de l'exposition sectorielle (benchmark), par typologie de vulnérabilités, par type de structures, …, et mesure son évolution dans le temps.

TRAJECTOIRE

❶ Extension du dispositif de déclaration des incidents de sécurité

Le dispositif de signalement des incidents de sécurité est étendu à l'ensemble des structures de santé et du secteur médico-social.

Les modalités d'accompagnement de l'ensemble des structures du secteur doivent être prévues en conséquence.

Les incidents remontés alimentent l'observatoire des incidents.

❷ Enrichissement de l'observatoire des incidents de sécurité

L'observatoire des incidents apporte une vision consolidée de la menace au niveau sectorielle.

Les services de l'observatoire sont enrichis avec :

- l'extension du périmètre des structures déclarant des incidents et la visibilité sectorielle associée ;
- le renforcement de la capacité d'alerte en cas d'attaque visant les acteurs de santé ;
- la capacité à diffuser des indicateurs de compromission permettant de faciliter la détection des actions malveillantes conjoncturelles par les structures de santé.

❸ Reconnaissance de la cellule ACSS au sein du groupe « Inter CERT »

En complément, la cellule ACSS se prépare à rejoindre le groupe « InterCERT-FR » qui réunit de façon régulière un ensemble d'organismes ayant des activités d'IRT (Incident Response Team) sur le territoire français afin de gagner en visibilité, de bénéficier des retours d'expérience des membres du groupe et d'échanges bi ou multi-latéraux.

❹ Poursuite de l'expérimentation de la cyber-surveillance

Le service de cyber-surveillance peut être proposé dans un premier temps aux structures victimes de cyber-malveillance et à un premier cercle de quelques CHU (Centre hospitalier universitaire).

En fonction des ressources allouées, une mise à disposition plus importante peut être envisagée pour l'ensemble des CHU, et dans un second temps pour les ES (Etablissement de santé) support de GHT (Groupement hospitalier de territoire).

❺ Industrialisation de la plateforme de cyber-surveillance

La plateforme de cyber-surveillance est aujourd'hui opérationnelle.

Des travaux de mise à jour doivent être réalisés pour tenir compte de l'évolution des vulnérabilités.

Par ailleurs, une deuxième phase d'industrialisation de la plateforme est souhaitable en fonction de la montée en charge.

❻ Création d'un observatoire des vulnérabilités

Un **observatoire des vulnérabilités** est constitué en complément de l'observatoire des incidents.

Pour une sélection d'un nombre restreint de structures, une vue sur l'évolution du niveau de sécurité dans le temps est restituée.

L'observatoire fournit une analyse de l'exposition sectorielle (benchmark), par typologie de vulnérabilités, par type de structures, …, et mesure son évolution dans le temps.

SYNTHESE DES ACTIONS CLES

Le tableau ci-après présente une vue synthétique des actions et les échéances associées.

Action	Jalon
Extension du dispositif de déclaration des incidents	2019
Enrichissement de l'observatoire des incidents	2020
Reconnaissance de la cellule ACSS au sein du groupe Inter CERT	2020
Poursuite de l'expérimentation de la cybersurveillance	2019
Industrialisation de la plateforme	S2 2019
Création d'un observation des vulnérabilités	S2 2019
Généralisation du service national de cybersurveillance en santé	A partir de 2020

POUR EN SAVOIR PLUS

- Accompagnement Cybersécurité des Structures de Santé :
  - https://esante.gouv.fr/securite/accompagnement-cybersecurite-des-structures-de-sante
- *Fiches réflexe par type de menaces accessible à travers le portail Cyberveille-Santé :*
  - https://www.cyberveille-sante.gouv.fr/
- Observatoire des signalements des incidents de sécurité des systèmes d'information pour le secteur santé :
  - https://esante.gouv.fr/media/2530