l'anap
l'expertise en partage
agence nationale de la performance sanitaire et médico-sociale

LA CYBERSÉCURITÉ EN ÉTABLISSEMENT DE SANTÉ

PLAN D'ATTAQUE CONTRE LES ATTAQUES

SOMMAIRE

Renforcez maintenant votre défense contre les cybermenaces

« Les secteurs sanitaires et médico-sociaux poursuivent leurs transformations numériques. Les usages des outils numériques sont inscrits dans la pratique quotidienne de tous les professionnels de santé. Cependant, avec des cyberattaques toujours plus nombreuses, il est indispensable à tous de comprendre et de se protéger pour ne pas mettre en péril la prise en charge du patient et impacter les professionnels. »

Stéphane Pardoux, directeur général de l'Anap

NOTE DE L'ANAP

Ces fiches pratiques reposent sur des échanges entre les experts numériques de l'Anap, des experts cybersécurité extérieurs au monde de la santé, des instances régulatrices et des établissements. Pour des raisons de confidentialité, les citations sont anonymes.

LE RISQUE CYBER EN CHIFFRES

Source : Observatoire des incidents de sécurité des systèmes d'information pour les secteurs santé et médico-social, rapport public 2022, ANS, CERT Santé

LE RISQUE CYBER AUGMENTE

+ 33

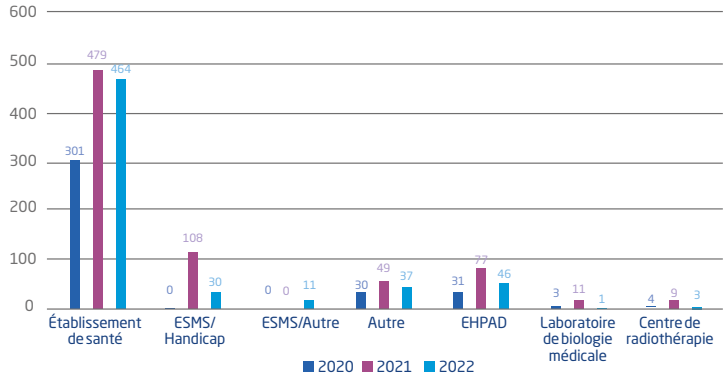
d'établissements ont déclaré au moins 1 incident en 2022

LE RISQUE CYBER TOUCHE MAJORITAIREMENT LE SECTEUR SANITAIRE

78 %

des cyberattaques ont eu lieu dans le secteur sanitaire en 2022

Répartition des cyberattaques par type de structure

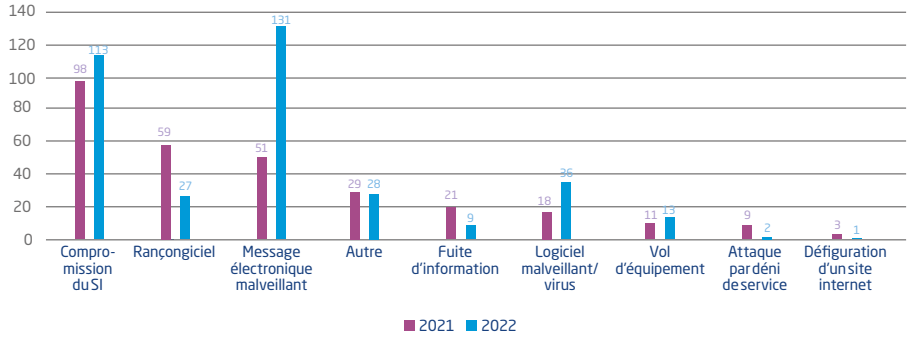


LA TECHNIQUE DE L'HAMEÇONNAGE ("PHISING")

1ER rang

des actes malveillants

Répartition des cyberattaques par type d'incident



L'ANALYSE DES RISQUES

L'analyse des risques permet de limiter les impacts des cyberattaques et de garantir la protection des informations médicales ainsi que des systèmes informatiques critiques. Elle repose sur cinq grandes étapes.

① Identification des actifs critiques essentiels au parcours de soins

L'identification précise des actifs critiques doit permettre de prioriser les efforts de sécurisation : d'abord les infrastructures physiques et logiques (serveurs, réseau, accès internet) ; puis les briques logicielles, à classer du plus au moins sensible (les dossiers médicaux numériques, les systèmes de gestion des patients, les équipements médicaux connectés au réseau, les systèmes de gestion des médicaments, etc.).

② Évaluation des vulnérabilités associées

Pour chacun des actifs critiques, il faut évaluer la vulnérabilité associée (infra, métier, équipements). Par exemple, certains logiciels de dossiers médicaux ou certains équipements biomédicaux sont plus vulnérables aux cyberattaques (par exemple, par obsolescence ou par absence de mises à jour).

③ Évaluation des menaces

Il s'agit d'évaluer la nature possible des attaques provenant d'acteurs internes ou externes et visant à voler des informations médicales, à perturber les services médicaux ou à compromettre la sécurité des patients.

④ Évaluation des risques

En considérant les actifs, les vulnérabilités et les expositions à la menace, la rédaction d'une synthèse qui hiérarchise les risques est nécessaire.

⑤ Planification de la réponse aux incidents

Étant donné la sensibilité des services de soins, il est crucial de mettre en place des plans détaillés de réponse aux incidents pour réagir rapidement en cas de compromission de la sécurité.

MUSCLEZ VOTRE GESTION DE CRISE

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) propose des kits pour s'entraîner à la gestion d'une cyberattaque. Les exercices permettent de tester et d'évaluer les capacités de la structure à répondre à une attaque informatique, de former et de sensibiliser les collaborateurs aux risques cybersécurité et d'identifier les failles de sécurité.

› https://cyber.gouv.fr/publications/organiser-un-exercice-de-gestion-de-crise-cyber

LA SEGMENTATION DES RÉSEAUX

Une meilleure fiabilisation technique globale du système d'information passe par la division du réseau.

La surface d'attaque est limitée tout comme la propagation des menaces au sein du SI. La division d'un réseau informatique en parties distinctes (ou sous-réseaux), chacune isolée des autres et avec des connectivités restreintes, permet la sécurité globale d'un établissement.

Chacune des parties peut avoir ses propres règles de contrôle d'accès et de flux non autorisés selon son niveau de criticité pour une meilleur isolation des ressources sensibles. L'allocation de ressources est alors plus efficace et la performance du système est améliorée en évitant la congestion du réseau.

« L'approche de la cybersécurité doit être globale et hiérarchisée, il ne sert à rien de fermer la porte d'entrée à double tour, si vous laissez les fenêtres de la maison grandes ouvertes ! »

Le directeur de la sécurité d'un groupe du CAC 40

PAR EXEMPLE

Imprimantes : l'angle mort de la cybersécurité

Les imprimantes sont des équipements peu protégés et faciles à pirater avec une clé USB ou des fichiers corrompus. Elles constituent une faille de sécurité. Pour cette raison, il est recommandé de les installer sur un sous-réseau séparé. Celui-ci sera protégé par pare-feu et n'acceptera que des protocoles entrants (envoi de fichier à imprimer) sans accès sortant.

L'ACTIVE DIRECTORY, LA GESTION DES DROITS ET DES IDENTITÉS

Pour renforcer la sécurité informatique de votre établissement, la gestion des droits et des identités doit s'appuyer sur l'Active Directory (AD). Il offre plusieurs avantages.

1. **Annuaire global**
   L'AD fournit un annuaire global qui permet aux utilisateurs de rechercher et d'accéder aux ressources réseau de manière efficace.
2. **Gestion des utilisateurs et des groupes**
   L'AD permet de créer, gérer et organiser des comptes utilisateurs et des groupes d'utilisateurs. Cela facilite l'attribution de droits d'accès et la gestion des autorisations, et harmonise les comportements autorisés des utilisateurs et des machines au sein du réseau.
3. **Authentification et autorisation**
   L'AD assure l'authentification des utilisateurs lorsqu'ils se connectent au réseau et gère les autorisations d'accès aux ressources en fonction de la configuration définie par les administrateurs.
4. **Gestion des ressources**
   L'AD offre un moyen centralisé de gérer les ordinateurs, les imprimantes, les serveurs et d'autres périphériques sur le réseau.

L'ACTIVE DIRECTORY, C'EST QUOI DÉJÀ ?

L'AD est un service de répertoire qui recense l'ensemble des personnes autorisées à accéder au système d'information. Il gère l'authentification (identifiant, mot de passe), les droits d'accès (réseau, logiciels) et la gestion des politiques (lecture/écriture, horaires d'accès, accès local/distant, *devices* autorisés, etc.).

LA GESTION DES HABILITATIONS ET DES MISES À JOUR

Combler les failles de sécurité se traite aussi en limitant les droits d'accès nécessaires à chaque utilisateur et en maintenant à jour les logiciels par l'application des correctifs publiés par les fournisseurs.

La gestion des habilitations

La gestion des habilitations repose sur une procédure partagée entre la direction informatique, la direction médicale, la direction des ressources humaines et la direction des soins (habilitations des intérimaires, des vacataires, etc.). Se protéger face à la menace cyber permet aussi de faire le lien entre les secteurs métiers et le secteur informatique.

La gestion des mises à jour

La conformité aux normes de sécurité ou aux réglementations exige de maintenir à jour les systèmes informatiques. Maintenir ses logiciels à jour réduit le risque d'exploitation de failles par des cybercriminels. Cette mesure est particulièrement critique pour les composants d'infrastructure : OS des serveurs, réseau, etc.

En corrigeant les bugs et en réduisant les risques de plantages ou de dysfonctionnements, la stabilité et la performance de l'organisation sont améliorées. Les logiciels et/ou équipements qui ne sont pas compatibles avec les dernières versions de serveur ou d'infrastructure doivent être désinstallés pour ne pas constituer une brèche d'entrée.

« Pour chaque nouvel arrivant, la DSI reçoit de la direction médicale ou de la DRH un formulaire définissant son rôle. Les droits d'accès sont générés en fonction du profil – infirmière, interne, PH – et du service d'affectation. Le cas échéant, des droits d'accès supplémentaires sont validés par les supérieurs hiérarchiques. Notre procédure d'habilitation prévoit également une fermeture automatique des comptes utilisateurs à la date prévisionnelle de fin de contrat et un lien avec le logiciel de paie pour contrôler les entrées et les sorties des utilisateurs. »

Le responsable SI d'un centre hospitalier

LA SENSIBILISATION AU PHISHING

Appelé également « hameçonnage », le phishing consiste à récupérer par duperie les données personnelles ou bancaires d'un collaborateur.

D'après le rapport de Cloudfare (2023), 90 % des cyberattaques qui aboutissent sont initiées par du phishing d'e-mails.

Pour éviter ces menaces, la mise en place d'antivirus à jour et une sensibilisation forte des salariés sont indispensables, en soulignant la nécessité de vigilance sur les liens extérieurs, les fautes d'orthographe dans les e-mails, les adresses e-mails des expéditeurs, etc. Ces campagnes peuvent être effectuées avec l'aide de logiciels spécialisés (Mailinblack, Avantdecliquer Knowbe4, Cofense, etc.).

PAR EXEMPLE

La « fraude au président »

La fraude au président consiste à se faire passer pour le dirigeant d'une organisation et à envoyer un nouveau RIB par e-mail auprès du service dédié au profit d'un compte bancaire tiers.

LA RÉPONSE AUX INCIDENTS

L'objectif de la réponse aux incidents est de limiter les dommages causés par une cyberattaque, de compliquer les chemins d'attaques, de restaurer les systèmes et de minimiser les interruptions des opérations.

N° 1 - La réactivité

La réactivité est essentielle pour isoler rapidement le système informatique d'Internet et fermer le plus de sous-réseaux possibles afin de limiter l'ampleur de l'attaque. Plus la réaction est rapide, plus l'impact sur la continuité des soins est limité. Le niveau ultime de réponse à incident est l'arrêt du système, générant un impact sur la capacité à assurer la continuité des soins. Les conditions pour prendre une telle décision doivent être définies dans le cadre de l'analyse des risques.

N° 2 - La connaissance du SI

La qualité de la réponse aux incidents dépend de la connaissance du SI. Il est donc indispensable d'avoir documenté et structuré la connaissance et la politique de sécurité informatique en interne ou avec l'aide d'un prestataire. Les établissements peuvent contractualiser avec un prestataire de réponse à incidents de sécurité (PRIS), habilité par l'ANSSI et soumis au secret défense.

N° 3 - La mise en place d'un centre opérationnel de sécurité (SOC)

La réponse aux incidents repose sur le centre opérationnel de sécurité, ou SOC, qui assure :

- une surveillance constante : contrôle en temps réel des activités du réseau, des journaux de sécurité, des systèmes et des applications pour détecter tout comportement suspect ou toute violation de sécurité ;
- une détection précoce des menaces par des outils spécialisés pour identifier les incidents de sécurité potentiels (tentatives d'intrusion, accès anormaux à des fichiers ou à des systèmes, logiciels malveillants ou anomalies dans le trafic réseau) ;
- une réponse rapide aux incidents : analyse de la situation, définition de la nature et de l'ampleur de la menace, mesures pour contenir, éliminer et récupérer l'incident.

Les SOC utilisent des technologies avancées telles que l'analyse comportementale, l'intelligence artificielle, les systèmes de détection d'intrusion (IDS) et les systèmes de prévention d'intrusion (IPS) pour éradiquer la menace rapidement.

La taille de la structure ne joue pas sur le dimensionnement d'un SOC : il faut organiser ses ressources en fonction des risques de l'établissement et du niveau d'acceptabilité du risque de la gouvernance.

LES INSTANCES RESPONSABLES

Les dirigeants doivent pleinement appréhender les répercussions potentielles d'une attaque cyber, notamment les conséquences d'un arrêt d'activité ou d'Internet. Leur implication active dans les décisions stratégiques relatives à la cybersécurité doit être au cœur de leur gouvernance.

La direction générale

Comme la sécurité incendie, la cybersécurité est une obligation de résultat, qui engage la responsabilité de la direction. Chaque directeur général, comme chaque président de CME, doit être formé aux scénarios possibles lors d'une cyberattaque. Ils doivent notamment veiller à ce que la prévention des menaces et les plans d'action de mise à niveau des SI soient priorisés dans les schémas directeurs informatiques.

Concernant la conduite à tenir en cas d'incident, elle doit être discutée en directoire, notamment pour définir à quel moment la direction du SI ou le SOC peut débrancher le système d'information. Cet arbitrage entre sécurité du système d'information et continuité de la prise en charge doit être à la main du directeur et du PCME.

Le délégué à la protection des données et le responsable de la sécurité des systèmes d'information

Les fonctions de DPO et de RSSI ne doivent ni être occupées par la même personne, ni être subordonnées à la DSI, cela pour préserver leur indépendance. Le DPO est rattaché à la direction qualité ou juridique, tandis que le RSSI dépend de la direction générale, de la direction qualité ou sécurité.

Tout en maintenant une collaboration étroite avec la DSI, le DPO et le RSSI renforcent les liens avec les équipes métiers et intègrent la cybersécurité dans la démarche qualité de l'établissement, au même titre que la sécurité des soins.

VERS UNE TERRITORIALISATION DE LA CYBERSÉCURITÉ

Bien que chaque établissement conserve sa responsabilité légale et son autorité en matière de cybersécurité, il est prévu que les systèmes d'information des GHT convergent progressivement. Cette convergence peut inclure la mutualisation des responsabilités du RSSI et du DPO au sein des GHT, ce qui présente plusieurs avantages : rendre les postes plus attractifs, permettre une réponse unifiée aux incidents au niveau du GHT, harmoniser les procédures en cas de dysfonctionnement et promouvoir l'adoption de bonnes pratiques de sécurité.

LES RELAIS DE COMMUNICATION

Chaque établissement doit trouver l'équilibre entre coercition et sécurité. Pour cela, le lien avec le équipes métiers est décisif. Comprendre les contraintes des professionnels tout en garantissant la sécurité cyber, tel est le défi des équipes dédiées.

L'ambassadeur cybersécurité

Relais du RSSI, l'ambassadeur est une personne qui ne porte aucune responsabilité en matière de sécurité informatique mais qui promeut les bonnes pratiques auprès de son équipe. Il est formé par le RSSI aux risques de cybersécurité et sensibilise ses collègues à être vigilants au quotidien. Il joue le rôle de formateur et de référent pour toutes les questions relatives aux risques cyber sur le terrain.

L'ambassadeur remonte au RSSI les contraintes du métier et les éventuels blocages de son équipe afin d'adapter les consignes en matière de cybersécurité. Il détecte les signaux de lassitude sur le terrain pour que les campagnes de communication et les formations internes soient ajustées.

« Grâce aux ambassadeurs, la cybersécurité est perçue comme un conseil, et non comme une contrainte. ».

Le RSSI d'un centre hospitalier

« Pour sensibiliser les collaborateurs aux menaces cyber, notre équipe informatique est allée à leur rencontre. Dès lors, toutes les bonnes pratiques ont été appliquées. ».

Le directeur cybersécurité d'une entreprise au CAC 40

BONNES PRATIQUES

RSSI, partez en campagne !

L'objectif du RSSI est de toucher chaque métier afin de diffuser les enjeux d'une bonne gestion cybersécurité et de donner ses instructions en cas de crise. Il doit utiliser tous les canaux de communication à sa disposition pour adresser ses cibles : messages intranet, e-mails, affiches, flyers, fonds d'écrans, etc. Parallèlement, le RSSI doit rester à l'écoute du terrain en créant notamment une adresse e-mail générique pour faire remonter les informations (e-mails suspects, alertes ou questions des collaborateurs).

FOCUS RÉGLEMENTAIRES ET PROGRAMMES NATIONAUX

Le réglement général sur la protection des données

Le RGPD (2018) est une législation européenne visant à renforcer et unifier la protection des données des citoyens au sein de l'UE. Il impose aux organisations de santé la transparence sur :

- l'**utilisation** des données personnelles et de santé (tout traitement doit nécessiter le recueil d'un consentement) ;
- l'**hébergement** des données dans des environnements à niveau élevé de sécurité (structures HDS) ;
- les **notices de violations** (en cas de risques sur les droits et libertés des personnes, l'autorité de contrôle compétente doit avoir été notifiée dans un délai de 72 h) ;
- les **transferts** de données entre établissements ou entre confrères (toute donnée personnelle de santé doit transiter via des messageries sécurisées, ou MSS).

L'obligation de déclarer les incidents de cybersécurité

Depuis 2022, les incidents graves de cybersécurité qui concernent la sécurité des soins, l'intégralité ou la confidentialité des données ou le fonctionnement normal d'un établissement doivent être signalés sans délai sur le portail du CERT Santé.

La directive NIS 2

Cette directive de l'Union européenne dont l'entrée en vigueur est prévue en octobre 2024 imposera notamment l'authentification forte, ou authentification à deux facteurs (A2F), pour l'accès aux données les plus sensibles comme le dossier patient informatisé ou aux logiciels cœur du système d'information hospitalier. Le professionnel devra fournir non pas une mais deux preuves d'identité :

1. une authentification via son mot de passe ou son code PIN
2. une confirmation via un élément extérieur (clé USB, jeton de sécurité, puce ou appareil mobile).

Le programme CaRE

Le programme CaRE (pour Cybersécurité accélération et Résilience des Établissements) vise à rendre les établissements plus résilients et mieux préparés aux cybermenaces en déclinant un plan d'action en quatre axes (gouvernance et résilience, ressources et mutualisation, sensibilisation, sécurité opérationnelle), pour la période de 2023 à 2027 avec un investissement de 750 M€.

LES OUTILS ET PUBLICATIONS POUR VOUS AIDER

- **Portail du CERT Santé**
  Portail de référence sur les menaces dans les établissements de santé et médico-sociaux, qui catalogue les retours d'expérience en matière de cyberattaques et propose des dossiers thématiques sur la cybersécurité.

- **Catalogue des offres cyber au sein des GRADeS**

- **Corpus documentaire PGSSI-S**
  Toutes les procédures et protocoles pour réaliser le PGSSI de son établissement.

- **Cybersécurité accélération et Résilience des Établissements**
  Pour en savoir plus sur le programme CaRE.

- **Partage de données de santé : pourquoi le RGPD n'est pas une contrainte ?**
  Une FAQ interactive de l'Anap qui répond à toutes les questions sur les données de santé et leur utilisation par les professionnels de santé.

- **Recommandations pour l'administration sécurisée des SI reposant sur AD**
  Guide pour l'administration sécurisée des SI reposant sur AD.

- **Guide d'hygiène informatique de l'ANSSI**

l'anap
agence nationale de
la performance sanitaire
et médico-sociale

L'Agence nationale de la performance sanitaire et médico-sociale est une agence publique de conseil et d'expertise qui agit avec et pour les professionnels des établissements sanitaires et médico-sociaux. Depuis 2009, elle a pour mission de soutenir, d'outiller et d'accompagner les établissements dans l'amélioration de leur performance sous toutes ses dimensions. Pour la mener à bien, l'Anap propose une offre d'accompagnement globale : diffusion de contenus opérationnels, organisation et animation de la mise en réseau et intervention sur le terrain.

Pour plus d'information :
www.anap.fr

Anap
23, Avenue d'Italie
75013 Paris
Tél. : 01 57 27 12 00

Retrouvez-nous sur

anap.fr