Conseil de
l'Union européenne

Bruxelles, le 16 janvier 2025
(OR. en)

5426/25

CYBER 21
SAN 15

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	15 janvier 2025
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	COM(2025) 10 final
Objet:	COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS Plan d'action européen sur la cybersécurité des hôpitaux et des prestataires de soins de santé

Les délégations trouveront ci-joint le document COM(2025) 10 final.

p.j.: COM(2025) 10 final

COMMISSION
EUROPÉENNE

Bruxelles, le 15.1.2025
COM(2025) 10 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

Plan d'action européen sur la cybersécurité des hôpitaux et des prestataires de soins de santé

1. Introduction

L'environnement de sécurité de l'Union européenne (UE) évolue rapidement, avec une montée en puissance des attaques hybrides et des cyberattaques qui visent à déstabiliser notre société en cherchant à créer des divisions et des perturbations, mais aussi à tirer des bénéfices de la cybercriminalité. Il est donc urgent que l'Europe renforce sa préparation et sa résilience face à cette nouvelle réalité, dans tous les secteurs et en accord avec son approche pangouvernementale englobant l'ensemble de la société, comme l'a demandé dans son rapport le conseiller spécial auprès de la présidente de la Commission européenne, Sauli Niinistö.

Le modèle social de l'Union repose sur des systèmes de soins de santé sûrs et résilients. Or, les hôpitaux et les systèmes de soins de santé sont exposés à des menaces croissantes, en particulier de la part de gangs de rançongiciels à la recherche de gains financiers, attirés par la valeur élevée des données des patients, et notamment des dossiers médicaux électroniques. Le secteur de la santé est en effet devenu le secteur le plus attaqué de l'UE au cours des quatre dernières années, y compris pendant la pandémie de COVID-19, au cours de laquelle on a observé une recrudescence des cyberattaques contre les infrastructures sanitaires. Les cyberattaques contre les hôpitaux et les prestataires de soins de santé sont directement préjudiciables aux personnes: elles retardent les actes médicaux, provoquent des engorgements dans les services d'urgence et, dans des cas extrêmes, peuvent même être à l'origine de décès.

Les enjeux sont d'autant plus importants que le secteur subit une transformation numérique fondamentale. La santé numérique, de même que l'utilisation et la réutilisation des données de santé, peuvent contribuer à la mise en place de modèles de soins mieux adaptés aux besoins et aux préférences des personnes et des patients, en prévenant l'apparition de maladies ou en permettant un traitement plus précoce. L'intégration d'outils et de solutions numériques aux processus cliniques ainsi que l'utilisation et la réutilisation des données de santé peuvent permettre de mieux éclairer les décisions cliniques, contribuer à l'automatisation dans le domaine de la santé et améliorer la rapidité et la qualité des soins prodigués aux patients. Les outils numériques, l'utilisation des données et les dispositifs médicaux — qui sont souvent connectés à l'internet et fonctionnent grâce à l'intelligence artificielle (IA) — sont également essentiels pour relever des défis tels que la pénurie de professionnels de santé.

Dans le même temps, les outils numériques sont autant de cibles potentielles supplémentaires pour les cybercriminels. En outre, certains acteurs étatiques n'hésitent pas à s'attaquer à des établissements de soins de santé, comme en témoigne la guerre d'agression menée actuellement par la Russie contre l'Ukraine. Le secteur est ainsi susceptible d'être ciblé par des cyberattaques dans le cadre de campagnes hybrides plus larges. Les cyberattaques mettent non seulement en danger la sécurité des patients, mais elles ébranlent également la confiance du public dans les infrastructures de santé et entraînent des coûts de rétablissement importants. Une infrastructure numérique résiliente et sécurisée est indispensable non seulement pour contrer les cyberattaques, mais aussi pour soutenir la mise en œuvre et le déploiement intégral de l'espace européen des données de santé (EHDS)[1].

[1] https://www.consilium.europa.eu/fr/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/

Il est donc temps d'améliorer et de renforcer la cybersécurité et la résilience des hôpitaux et des prestataires de soins de santé en Europe, comme l'a souligné la présidente von der Leyen dans ses orientations politiques pour la Commission 2024-2029[2]. Le présent plan d'action répond à l'urgence de la situation et aux menaces sans équivalent auxquelles le secteur est confronté. Il n'existe pas de solution miracle aux défis en matière de cybersécurité dans le domaine des soins de santé. Le plan d'action préconise plutôt le renforcement de la prévention, la préparation et une approche plus coordonnée de la solidarité, tout en mettant à profit l'expertise du secteur européen de la cybersécurité. Il reflète ainsi l'approche de l'Union en matière de sécurité, qui sera davantage développée et systématisée dans la prochaine stratégie de sécurité intérieure de l'UE. Il définit une réponse globale permettant de faire face à toutes les menaces pesant sur la sécurité intérieure et met l'accent sur la capacité à anticiper les menaces, à prévenir les dommages et à protéger les personnes, en adoptant une approche applicable à tous les niveaux et englobant l'ensemble de la société.

Le secteur de la santé compte un grand nombre d'entités et d'acteurs, notamment les hôpitaux, les cliniques, les établissements de soins, les centres de réadaptation et divers prestataires de soins de santé, aux côtés de l'industrie pharmaceutique, médicale et des biotechnologies, ainsi que des fabricants de dispositifs médicaux et des instituts de recherche en santé. Ce plan d'action met principalement l'accent sur la cybersécurité des hôpitaux et des prestataires de soins de santé, c'est-à-dire toute personne physique ou morale ou toute autre entité qui dispense légalement des soins de santé sur le territoire d'un État membre[3]. Les hôpitaux et les prestataires de soins de santé sont étroitement liés à d'autres entités du secteur de la santé et sont au plus proche des personnes. Dans le même temps, les mesures destinées à renforcer la cybersécurité des hôpitaux et des prestataires de soins de santé devraient également tendre à résoudre les risques qui pèsent sur la chaîne d'approvisionnement et l'écosystème au sens large, risques provenant par exemple des entités qui utilisent des données de santé à des fins de recherche et d'apprentissage automatique ou qui fabriquent des dispositifs médicaux, en particulier des dispositifs médicaux numériques connectés à l'internet ou à d'autres dispositifs («internet des objets»).

Si la protection des systèmes de santé relève principalement de la compétence nationale, la santé est également un secteur critique au titre de la directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (SRI 2)[4]. Les cybercriminels et les autres acteurs de la menace opèrent par-delà les frontières, et les défis en matière de cybersécurité auxquels font face les organismes de soins de santé sont semblables dans tous les États membres. La coopération au niveau européen est précieuse pour le partage et le développement des bonnes pratiques au niveau de l'Union et au niveau national. Par conséquent, le plan d'action propose une coordination et des mesures au niveau de l'UE, tout en invitant les États membres à prendre des dispositions efficaces en faveur des soins de santé et de l'écosystème de la santé au sens large.

---

[2] https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_fr

[3] Article 3, point g), de la directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers, http://data.europa.eu/eli/dir/2011/24/2025-01-12.

[4] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI 2), https://eur-lex.europa.eu/eli/dir/2022/2555.

Premièrement, le plan d'action met l'accent sur le renforcement des capacités du secteur en matière de **prévention** des incidents de cybersécurité, car il vaut toujours mieux prévenir que guérir. Deuxièmement, il décrit des actions destinées à améliorer le partage d'informations en matière de cybersécurité et la capacité à **détecter** les cybermenaces, ce qui permet une réaction plus rapide. Troisièmement, il prévoit des mesures permettant de mieux **réagir** aux incidents et de **se rétablir** après ceux-ci. Enfin, le plan d'action propose des moyens de **dissuader** les acteurs de la cybermenace de lancer des attaques contre les systèmes de santé en Europe.

Le plan d'action sera mis en œuvre conjointement avec les prestataires de soins de santé et l'écosystème de santé au sens large, les États membres et la communauté de la cybersécurité. Il est essentiel d'adopter une approche collaborative pour définir et préciser les actions les plus efficaces afin que celles-ci puissent bénéficier à tous les prestataires de soins de santé critiques en Europe. Par conséquent, une vaste consultation des parties prenantes, du secteur et des États membres sera lancée en parallèle de la présente communication. Étant donné que les cybermenaces sont interconnectées et ignorent les frontières, la coopération internationale joue un rôle essentiel pour la cybersécurité. Des cybermenaces comparables touchent également les pays concernés par l'élargissement et les pays du voisinage ainsi que d'autres pays partenaires stratégiques de l'Union, ce qui peut, au bout du compte, compromettre la sécurité des infrastructures critiques dans l'UE. Il sera donc important d'appliquer les enseignements tirés de la mise en œuvre du plan d'action à la coopération de l'UE avec les pays concernés par l'élargissement et avec les autres pays partenaires, en tenant compte des niveaux de menace auxquels chacun d'entre eux est exposé.

2. Les défis en matière de cybersécurité pour les hôpitaux et les prestataires de soins de santé

Les cybermenaces qui pèsent sur le secteur de la santé

Les cyberattaques se multiplient à l'échelle mondiale et dans l'UE, avec un panorama de la menace de plus en plus complexe et dynamique. Les progrès dans le domaine de l'IA permettent aux acteurs criminels et malveillants de disposer d'outils puissants augmentant la précision et l'impact de leurs actions, mais ils permettent aussi de repenser les solutions de cyberdéfense en rendant possible une réaction automatisée et en temps réel contre les attaques.

Les rançongiciels restent un défi majeur en matière de cybersécurité dans l'Union et dans le monde. Selon un rapport[5], leur coût annuel mondial est estimé à plus de 250 milliards d'EUR d'ici à 2031. Lorsque des criminels lancent des attaques par rançongiciel, ils chiffrent non seulement les données des victimes afin de leur réclamer une rançon, mais ils divulguent également des informations sensibles petit à petit pour exercer une pression supplémentaire. Les vulnérabilités des logiciels et du matériel

[5] Cybersecurity Ventures (1er juin 2024): «Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031». Disponible à l'adresse suivante: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

constituent un autre défi majeur: selon l'Agence de l'Union européenne pour la cybersécurité (ENISA)[6], le secteur des soins de santé est le secteur dans lequel le plus d'incidents de sécurité en lien avec ces vulnérabilités ont été déclarés[7]. Parmi les autres menaces croissantes figurent les attaques par déni de service distribué (DDoS), qui sont conçues pour saturer le trafic d'un système ciblé, le rendant inaccessible aux utilisateurs légitimes[8].

Dans le secteur de la santé, les cybermenaces suivent une évolution similaire, marquée par une forte présence des attaques par rançongiciel. Selon l'ENISA, les rançongiciels étaient responsables de 54 % des incidents de cybersécurité analysés dans le secteur de la santé entre 2021 et 2023. Dans 83 % des cas, les attaquants, attirés par la valeur élevée des données relatives aux soins de santé, obéissaient à des motivations financières, et dans 10 % des cas, ils étaient animés par des motivations d'ordre idéologique[9]. De même, la Commission a constaté, dans un rapport de 2024, que 71 % des attaques ayant eu des répercussions sur les soins aux patients, telles que des retards dans le traitement et le diagnostic ou un accès limité aux services d'urgence, étaient de type rançongiciel[10]. Les attaques de ce type peuvent avoir des effets particulièrement perturbateurs sur la fourniture de services de soins de santé, compromettant la sécurité des patients. En outre, les attaques par rançongiciel sont souvent associées à des violations de données des patients[11], qui comprennent généralement des données sensibles relatives à la santé, ce qui constitue une violation du droit fondamental des personnes à la protection de leurs données à caractère personnel.

Dans le même temps, compte tenu de la présence croissante du numérique dans les soins de santé, la surface d'attaque augmente. Selon le rapport 2024 sur l'état d'avancement de la décennie numérique, en moyenne 79 % des citoyens de l'UE peuvent accéder en ligne à leurs dossiers médicaux électroniques concernant les soins primaires[12]. Les dossiers médicaux électroniques, les systèmes d'information de santé, les systèmes de gestion des flux hospitaliers, les systèmes informatiques gérant les remboursements des traitements, les systèmes d'imagerie médicale et les dispositifs médicaux utilisés à des fins de diagnostic ou de suivi des patients sont autant d'exemples d'outils numériques qui peuvent jouer un rôle majeur dans le renforcement de l'efficacité et des performances du secteur de la santé, mais qui sont également des cibles potentielles de cyberattaques. Certaines activités de soins de santé telles

---

[6] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications (règlement sur la cybersécurité), https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.

[7] ENISA Threat Landscape: Health Sector (juillet 2023).

[8] ENISA Threat Landscape 2024.

[9] ENISA Threat Landscape: Health Sector (juillet 2023). Ce rapport se penche sur les prestataires de soins de santé, ainsi que sur d'autres types d'organisations, y compris les organismes menant des travaux de recherche en santé, les entités fabriquant des produits liés à la santé, les autorités sanitaires, les organismes d'assurance maladie, les établissements de soins résidentiels et les prestataires de services sociaux. Disponible à l'adresse suivante: https://www.enisa.europa.eu/publications/health-threat-landscape.

[10] Commission européenne, Centre commun de recherche, Reina, V. et Griesinger, C., *Cyber security in the health and medicine sector: a study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings*, Office des publications de l'Union européenne, 2024, https://data.europa.eu/doi/10.2760/693487.

[11] Selon le rapport de l'ENISA concernant le panorama des menaces dans le secteur de la santé, il a été confirmé que 43 % des incidents analysés liés à des rançongiciels impliquaient une violation ou un vol de données.

[12] Rapport 2024 sur l'état d'avancement de la décennie numérique.

que les soins intensifs et l'imagerie radiologique, ou certaines spécialités médicales telles que l'oncologie et la cardiologie, qui sont fortement tributaires de dispositifs numériques, sont particulièrement exposées à des risques de cyberattaques. En outre, les problèmes liés à la chaîne d'approvisionnement peuvent conduire à l'achat de dispositifs dont la cybersécurité est insuffisante, ce qui exacerbe les risques généraux existants.

Par exemple, pendant la pandémie de COVID-19, une grande partie du système de santé irlandais a été paralysée par une attaque par rançongiciel, ce qui a entraîné, dans 31 des 54 hôpitaux assurant des soins aigus, la suspension d'au moins une partie des services le matin de l'incident[13]. Les services de santé ont été obligés de revenir aux dossiers papier, ce qui a diminué l'efficacité des activités. L'attaque a été causée par un courriel d'hameçonnage contenant une pièce jointe malveillante[14]. L'incident a montré que les cyberattaques pouvaient se propager dans différents systèmes et qu'il était donc essentiel de protéger toute la surface d'attaque d'un organisme de soins de santé. Il en est également ressorti l'importance de maintenir une cyberhygiène et une culture de la cybersécurité de base dans l'ensemble des organisations.

La maturité des hôpitaux et des prestataires de soins de santé en matière de cybersécurité

Le paysage des soins de santé dans l'Union est très diversifié, la propriété, la structure et la taille des hôpitaux et autres prestataires de soins de santé variant énormément d'un État membre à un autre. La gouvernance des soins de santé peut reposer sur une approche centralisée au niveau national dans certains cas, tandis qu'elle s'opère au niveau régional et local dans d'autres; les prestataires de soins de santé peuvent être publics ou privés. En outre, il peut y avoir des différences au sein d'un même pays, par exemple lorsqu'il existe d'importantes disparités socio-économiques et territoriales entre les régions, ce qui complique la situation. Ce paysage complexe des soins de santé peut être mis à rude épreuve par des crises sanitaires majeures, causées par des maladies transmissibles, comme lors de la pandémie de COVID-19, mais aussi par d'autres risques sanitaires liés, par exemple, au changement climatique. Enfin, en ce qui concerne le niveau de transition numérique et d'adoption des technologies par les prestataires de soins de santé, la situation est très variable et très hétérogène. Par exemple, l'indisponibilité de services due à un incident de cybersécurité peut causer des dommages graves aux patients, même dans des établissements de soins de petite taille, notamment des cliniques ou des services d'aide médicale d'urgence qui fournissent un service essentiel à un nombre relativement faible d'utilisateurs.

Selon le rapport 2024 de l'ENISA sur l'état de la cybersécurité dans l'Union[15], le niveau de maturité du secteur de la santé de l'UE en matière de cybersécurité est modéré et varie fortement d'une entité du secteur des soins de santé à l'autre en Europe. On peut observer des lacunes dans des domaines essentiels tels que la disponibilité des ressources humaines, la connaissance qu'ont les organisations de leurs chaînes d'approvisionnement en technologies de l'information et de la communication (TIC) et

[13] Irish Health Service Executive (2021): «Conti cyber attack on the HSE: Independent Post Incident Review».
[14] Irish Health Service Executive: «Cyber-attack and HSE response». Disponible à l'adresse suivante: https://www2.hse.ie/services/cyber-attack/what-happened/.
[15] ENISA: «2024 Report on the State of Cybersecurity in the Union» (septembre 2024). Disponible à l'adresse suivante: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

l'installation de fonctions de sécurité à jour dans les produits. Le secteur peine à mettre en place une cyberhygiène de base et des mesures de sécurité fondamentales, comme en témoigne le fait que presque tous les organismes de santé interrogés éprouvent des difficultés lorsqu'ils doivent réaliser des évaluations des risques de cybersécurité, et que près de la moitié d'entre eux n'ont jamais effectué d'analyse des risques[16].

Un autre défi majeur pour la cybersécurité des hôpitaux est la confluence entre les technologies de l'information et les technologies opérationnelles, point de rencontre de priorités en matière de sécurité qui diffèrent du point de vue de la confidentialité, de la disponibilité et de la fiabilité, et où une violation dans un domaine peut affecter l'autre. Le rapport 2024 de l'ENISA sur l'état de la cybersécurité dans l'Union souligne en outre que le secteur de la santé ne parvient pas à garantir correctement la sécurité des produits et processus TIC auxquels il a recours, en raison de la grande variété d'entités, de dispositifs et de produits de santé.

Cette diversité, conjuguée aux niveaux variables de sensibilisation du personnel et de l'encadrement des hôpitaux à la cybersécurité, complique la tâche consistant à garantir la cybersécurité des systèmes de soins de santé. Par exemple, selon l'Eurobaromètre de 2024 sur les compétences en matière de cybersécurité, seules 25 % des entreprises interrogées dans les secteurs de la santé, de l'éducation et de l'aide sociale avaient proposé des formations ou des actions de sensibilisation à la cybersécurité au cours des 12 mois précédents[17]. Il faut prendre des mesures pour favoriser une culture de sensibilisation à la cybersécurité parmi les professionnels de santé de première ligne. Par exemple, les rotations de personnel, l'utilisation de postes de travail partagés, la mauvaise gestion de l'authentification et l'utilisation de supports amovibles sont des sources supplémentaires de vulnérabilités qui compromettent la cybersécurité des prestataires de soins de santé[18].

Les technologies de l'information et les technologies opérationnelles sont très souvent sous-traitées, au moins en partie. Selon l'Eurobaromètre de 2024, c'est dans les secteurs de la santé, de l'éducation et de l'aide sociale que la part des entreprises qui externalisent au moins certains aspects de leur cybersécurité est la plus élevée, 57 % des entreprises interrogées ayant déclaré avoir recours à la sous-traitance[19]. De même, on observe une forte tendance au passage à l'informatique en nuage, qui répond au besoin de stockage et de gestion modulables des données, d'efficacité au regard des coûts, d'amélioration de la collaboration et de soutien aux technologies avancées telles que l'IA et l'internet des objets médicaux. En 2022, 58 % des organismes de santé ont utilisé une plateforme de santé numérique en nuage[20]. Toutefois, si ce changement peut apporter des gains d'efficience substantiels, il engendre également des

[16] ENISA Threat Landscape: Health Sector (juillet 2023). Disponible à l'adresse suivante: https://www.enisa.europa.eu/publications/health-threat-landscape.
[17] Enquête Eurobaromètre Flash 547 sur les compétences en matière de cybersécurité (mai 2024). Disponible à l'adresse suivante: https://europa.eu/eurobarometer/surveys/detail/3176.
[18] PANACEA – People-centric cybersecurity in healthcare (2021): «White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres».
[19] Enquête Eurobaromètre Flash 547 sur les compétences en matière de cybersécurité (mai 2024). Disponible à l'adresse suivante: https://europa.eu/eurobarometer/surveys/detail/3176.
[20] ENISA: «NIS Investments Report 2022» (novembre 2022). Disponible à l'adresse suivante: https://www.enisa.europa.eu/publications/nis-investments-2022.

risques qui nécessitent que des décisions éclairées soient prises en matière de passation de marchés et de configuration sécurisée.

En arrière-plan de tous ces défis se pose la question du renforcement des capacités et du financement. Le financement de la cybersécurité dans le secteur de la santé a été limité et reste un défi universel dans toute l'UE[21]. En outre, ces problèmes de financement ont pour toile de fond le vieillissement de la population, qui risque de faire peser une pression budgétaire généralisée sur les systèmes de santé européens dans les prochaines décennies.

Le fait que des outils obsolètes et des systèmes hérités continuent d'être utilisés, que les ressources permettant de prévenir les incidents ou d'y réagir soient limitées, et que la maturité en matière de cybersécurité soit insuffisante peut souvent s'expliquer par un manque de financement. Les hôpitaux doivent constamment s'efforcer de trouver un équilibre entre la nécessité d'avoir une infrastructure numérique sécurisée et à jour et celle de réaliser d'autres investissements nécessaires pour améliorer les soins aux patients, tels que le recrutement de médecins et d'autres professionnels de santé, la mise en œuvre de nouvelles méthodes de diagnostic et de traitement et l'acquisition de matériel. Selon l'ENISA[22], le secteur de la santé n'arrive qu'à la 7e place parmi les 12 secteurs étudiés pour ce qui est de la part des dépenses consacrées à la sécurité de l'information par rapport au total des dépenses informatiques, sa médiane s'élevant à 8,3 %.

3. Le centre européen d'appui en matière de cybersécurité pour les hôpitaux et les prestataires de soins de santé

Le cadre de l'UE en matière de cybersécurité offre un large éventail d'outils qui devraient être exploités pour améliorer la sécurité et la résilience des hôpitaux et des prestataires de soins de santé. Pour répondre aux nombreux défis mis en évidence ci-dessus, il est indispensable d'élaborer, au niveau de l'UE, une approche stratégique unifiée qui réunisse les ressources, l'expertise et les outils nécessaires pour lutter efficacement contre les cybermenaces. Il est essentiel de disposer d'une vue d'ensemble complète et d'améliorer la planification et la coordination afin d'aider les prestataires de soins de santé dans toute l'UE à renforcer leurs moyens de défense. À cette fin, l'ENISA est la mieux placée pour mettre en place, en son sein, un **centre européen d'appui en matière de cybersécurité pour les hôpitaux et les prestataires de soins de santé**[23], dans le cadre de son mandat[24] visant à préserver et à soutenir les infrastructures critiques de l'UE.

---

[21] L'organisation et la prestation de services de santé et de soins médicaux relèvent de la compétence nationale en vertu de l'article 168 du traité sur le fonctionnement de l'Union européenne, et le financement des systèmes de soins de santé varie d'un État membre à l'autre.

[22] ENISA: «NIS Investments Report 2022» (novembre 2022). Disponible à l'adresse suivante: https://www.enisa.europa.eu/publications/nis-investments-2022.

[23] Aussi désigné par le terme «centre d'appui» dans le présent document.

[24] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

Le centre d'appui devrait progressivement **mettre au point un catalogue complet de services répondant aux besoins des hôpitaux et des prestataires de soins de santé**, présentant la gamme des services disponibles en matière de préparation, de prévention, de détection et de réaction. En collaboration avec les autorités des États membres et sur la base des enseignements tirés par les hôpitaux et les prestataires de soins de santé, le centre d'appui devrait créer un répertoire convivial et facile d'accès recensant tous les instruments disponibles aux niveaux européen, national et régional. Dans le cadre de ses activités, il devrait veiller à une bonne coordination avec les États membres et soutenir la hiérarchisation et la mise en œuvre des actions en fonction des besoins et en temps réel.

La Commission apportera une contribution importante à la constitution du catalogue de services du centre d'appui en proposant de lancer des projets pilotes dans l'ensemble de l'UE destinés à mettre au point de bonnes pratiques en matière de cyberhygiène et d'évaluation des risques pour la sécurité, ainsi qu'à répondre à la nécessité de surveiller la cybersécurité en continu, de disposer de renseignements sur les menaces et de réagir aux incidents à l'aide de solutions de cybersécurité de pointe. Les résultats de ces projets pilotes, qui seront financés par le programme pour une Europe numérique, mis en œuvre par le Centre de compétences européen en matière de cybersécurité (ECCC), serviront de base à d'autres actions au niveau de l'UE, notamment aux travaux du centre d'appui.

Figure 1: Concepts pour le catalogue de services du centre d'appui pour les hôpitaux et les prestataires de soins de santé

3.1. Prévention des incidents de cybersécurité

Mesures simples permettant de réduire la probabilité d'un cyberincident

Les mesures de cybersécurité de base, telles que la mise à jour des systèmes, la gestion des sauvegardes et l'application de l'authentification à plusieurs facteurs, peuvent, selon une estimation, protéger les organisations contre 98 % des attaques[25]. Bon nombre des mesures de cyberhygiène et de gestion des

[25] «Microsoft Digital Defense Report 2022». Disponible à l'adresse suivante: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

risques les plus efficaces sont assez simples à mettre en place et constituent des solutions faciles pour améliorer la cybersécurité. L'une des principales missions du centre d'appui devrait donc être d'**élaborer des conseils clairs et ciblés qui mettent en lumière les pratiques les plus importantes en matière de cybersécurité et aident les prestataires de soins de santé à les mettre en œuvre**. Ce soutien ne doit pas uniquement profiter aux grands hôpitaux, mais également, sous la forme de conseils personnalisés, à de petites entités à l'échelon local, telles que les cabinets de médecins généralistes et les cliniques spécialisées, qui n'ont souvent pas assez de ressources pour disposer d'équipes spécialisées dans la cybersécurité, mais qui sont pourtant tout aussi vulnérables aux attaques. En outre, il est nécessaire de tenir compte de l'importance régionale de certaines entités du secteur des soins de santé pour la fourniture de soins aux patients, par exemple dans les régions peu peuplées. Les instituts de recherche en santé qui manipulent de grandes quantités de données à caractère personnel sensibles pourraient également tirer profit de conseils sur les mesures de cybersécurité de base, qui contribueraient à accroître leur résilience.

Les organismes de soins de santé sont également soumis à une série d'obligations en matière de cybersécurité découlant de la législation de l'UE[26]. Si les obligations sont essentielles pour garantir un niveau de référence commun élevé en matière de cybersécurité et de sécurité des données, il est indispensable de veiller à ce qu'il ne soit pas inutilement difficile et laborieux de se repérer dans le paysage réglementaire. Le fait d'accorder une place importante au respect des règles ne devrait pas aller à l'encontre de l'objectif de promotion d'une solide culture de la cybersécurité. Un **outil de cartographie réglementaire facile d'accès pourrait contribuer à réduire au minimum la charge administrative pour les entités soumises à de multiples instruments réglementaires**. Parallèlement à l'élaboration de conseils et de boîtes à outils, le centre d'appui devrait travailler en étroite collaboration avec la Commission et les États membres afin de mettre au point et de diffuser cet outil dès que possible. Le centre d'appui jouerait donc un rôle important pour faciliter la compréhension et l'application des règles en matière de cybersécurité, par exemple en fournissant des orientations sur la mise en œuvre[27] et, le cas échéant, en promouvant les normes pertinentes.

[26] Notamment la directive SRI 2; le règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques (règlement sur la cyberrésilience), https://eur-lex.europa.eu/eli/reg/2024/2847/oj/fra; le règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux (règlement relatif aux dispositifs médicaux), https://eur-lex.europa.eu/eli/reg/2017/745/oj/fra; le règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro (règlement relatif aux dispositifs médicaux de diagnostic in vitro), https://eur-lex.europa.eu/eli/reg/2017/746/oj/fra; le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679; le règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle), https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32024R1689. Proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé, COM(2022) 197 final, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:52022PC0197. Les négociations ont abouti à un accord politique au printemps 2024 et, une fois finalisé, le texte devrait être publié au Journal officiel au printemps 2025.

[27] L'élaboration de lignes directrices sur l'interprétation du règlement général sur la protection des données (RGPD) relève de la responsabilité du comité européen de la protection des données. L'élaboration d'orientations par l'ENISA devrait respecter pleinement les prérogatives de ce dernier.

Les futurs **portefeuilles européens d'identité numérique** constituent un autre outil permettant de faciliter la mise en œuvre de bonnes pratiques de cyberhygiène. Il est essentiel de réduire le recours aux mécanismes d'identification à faible niveau de sécurité, tels que les mots de passe, afin d'atténuer les risques d'accès non autorisé aux données de santé. Il est primordial de passer à des solutions d'authentification sécurisées fondées sur une identification fiable. Le portefeuille européen d'identité numérique propose une approche harmonisée de l'identification électronique à l'échelle de l'Union pour les professionnels de santé, offrant une solution solide et unifiée qui sera disponible à la fin de l'année 2026. Tous les systèmes d'information sur la santé en ligne qui doivent disposer d'une authentification forte de l'utilisateur seront obligés d'accepter ce portefeuille à des fins d'identification à partir de la fin 2027[28].

Préparation et soutien ciblé

Les tests de préparation, qui impliquent des actions telles que les tests d'intrusion, sont essentiels à une cybersécurité efficace. La Commission a déjà accordé des fonds à l'ENISA pour des initiatives pilotes en matière de préparation, qui ont révélé que le secteur de la santé est l'un des domaines qui nécessite le plus de tests et d'évaluations complémentaires pour recenser les lacunes en matière de cybermaturité. Avec l'entrée en vigueur du règlement sur la cybersolidarité, ces efforts seront considérablement renforcés sous la houlette de l'ECCC. Pour répondre à ce besoin, la Commission proposera, en consultation avec le groupe de coopération SRI, EU-CyCLONe[29] et l'ENISA, de définir la santé comme un secteur qui peut bénéficier d'un soutien pour les **tests de préparation coordonnés** au titre du règlement sur la cybersolidarité. En outre, le centre d'appui devrait élaborer un **cadre sur mesure pour les évaluations de la maturité en matière de cybersécurité spécifiquement adapté au secteur des soins de santé**. Ces évaluations de la maturité fourniraient aux entités des données exploitables sur leurs vulnérabilités tout en leur permettant de démontrer leur état de préparation en matière de cybersécurité aux patients et aux parties prenantes, renforçant ainsi la confiance dans les services qu'elles proposent. Au niveau global, le centre d'appui devrait procéder à une **évaluation annuelle de la maturité en matière de cybersécurité dans le secteur de la santé**, qui permettrait d'obtenir une vue d'ensemble claire de la cybersécurité du secteur de la santé tant au niveau national qu'au niveau de l'UE.

Le secteur de la santé s'appuie largement sur des contractants externes pour les services de cybersécurité[30], ce qui souligne la nécessité d'un soutien ciblé pour renforcer les défenses. En s'appuyant sur des initiatives fructueuses telles que les chèques-innovation de l'UE, les **États membres devraient envisager des mesures ciblées telles que des chèques-cybersécurité pour les hôpitaux et prestataires de soins de santé de très petite taille, de petite taille et de taille moyenne**. Ces chèques fourniraient une aide financière pour la mise en place de mesures de cybersécurité spécifiques. L'ordre de priorité pour l'attribution des chèques devrait s'appuyer sur les résultats des tests de préparation et des évaluations de la maturité.

[28] Article 5 *septies*, paragraphes 1 et 2, du règlement (UE) nº 910/2014.
[29] Réseau européen d'organisations de liaison en cas de crises de cybersécurité.
[30] Voir le «NIS Investments Report 2023» (novembre 2023) de l'ENISA, qui met l'accent sur l'importance du soutien externe apporté aux audits et à la conformité en matière de cybersécurité. Disponible à l'adresse suivante: https://www.enisa.europa.eu/publications/nis-investments-2023.

Les connaissances et le contexte à l'échelle locale ont une importance essentielle pour le déploiement efficace d'un système de chèques ou d'autres programmes de soutien, en assurant la pertinence et l'accessibilité. Les fonds de l'Union, tels que le Fonds européen de développement régional, soutiennent déjà des initiatives dans le domaine de la cybersécurité et de la santé numérique, et pourraient donc contribuer à la mise au point de systèmes ciblés de chèques-cybersécurité destinés aux prestataires de soins de santé. Pour mener à bien cet effort, le centre d'appui collaborerait avec les États membres et les autorités régionales responsables des programmes en vue de soutenir l'élaboration de ces systèmes régionaux de chèques, en s'appuyant sur les enseignements tirés des projets existants à l'échelon national ainsi que des actions financées au titre du programme pour une Europe numérique pour faire en sorte que la mise en œuvre soit pratique et efficace.

En outre, les programmes Horizon contribuent grandement, depuis 2014, au financement d'un ensemble d'initiatives de recherche destinées à renforcer la résilience des établissements de soins de santé tels que les hôpitaux face aux cybermenaces et à atténuer les risques liés à l'utilisation abusive des technologies émergentes. Au nombre des résultats obtenus, on peut citer une série d'outils, de cadres et de systèmes spécialisés, tels que des outils d'évaluation des risques, des plateformes de partage de données respectueuses de la vie privée, des solutions cryptographiques, des programmes de formation visant à sensibiliser à la cybersécurité et des systèmes de détection des menaces en temps réel. On notera que ces solutions ont été rigoureusement validées au moyen de projets pilotes mis en œuvre en conditions réelles dans des environnements de soins de santé, garantissant qu'elles assurent une protection efficace contre les cybermenaces et qu'elles sont applicables dans la pratique.

Sécuriser les chaînes d'approvisionnement pour les soins de santé

Les organismes de soins de santé doivent relever un défi d'importance capitale, à savoir la gestion de chaînes d'approvisionnement en TIC complexes, couvrant des produits aussi divers que les dispositifs médicaux connectés, les systèmes de dossiers médicaux électroniques et le matériel de bureautique. Les hôpitaux et les prestataires de soins de santé ont besoin de systèmes et de services TIC fiables et sécurisés pour pouvoir fonctionner. Afin de contribuer à relever les défis en matière de cybersécurité dans le secteur de la santé, le groupe de coopération SRI devrait procéder à une **évaluation coordonnée des risques pour la sécurité, en évaluant les risques techniques et stratégiques associés aux chaînes d'approvisionnement en dispositifs médicaux et en proposant des mesures d'atténuation**[31]. Le cas échéant, le groupe de coopération SRI devrait collaborer avec le groupe de coordination en matière de dispositifs médicaux.

Le règlement sur la cyberrésilience est un nouveau cadre global qui fixe des exigences en matière de cybersécurité pour la planification, la conception, le développement, ainsi que le traitement, la correction et la notification des vulnérabilités activement exploitées concernant la quasi-totalité des produits matériels et logiciels, à tous les stades de la chaîne de valeur[32]. Les dispositifs médicaux sont un type de

[31] Conformément à l'article 22 de la directive SRI 2.

[32] Dans un premier temps, à partir du 1er août 2025, de vastes catégories d'équipements radioélectriques qui ne relèvent ni du champ d'application du règlement relatif aux dispositifs médicaux ni de celui du règlement relatif aux dispositifs

produit utilisé dans l'un des secteurs les plus sensibles de notre société. Les exigences en matière de cybersécurité applicables à ces produits découlent de deux actes législatifs existants, à savoir le règlement relatif aux dispositifs médicaux et le règlement relatif aux dispositifs médicaux de diagnostic in vitro[33]. Ces règlements font actuellement l'objet d'une évaluation destinée à examiner la possibilité de renforcer la cohérence et les synergies entre ces cadres législatifs, afin de parvenir à une simplification et au niveau le plus avancé possible en matière de cybersécurité.

En outre, les conclusions de l'évaluation des risques devraient aider les organismes de soins de santé à revoir les pratiques en matière de cybersécurité en usage dans leur chaîne d'approvisionnement, comme l'exige la directive SRI 2, et pourraient alimenter le processus d'élaboration de nouvelles **lignes directrices en matière de marchés publics**[34]**.** Établies par l'ENISA par l'intermédiaire de son centre d'appui, ces lignes directrices devraient refléter les tendances récentes, telles que la mise en nuage du stockage des données des patients, et notamment la nécessité de migrer les données de santé électroniques vers des environnements en nuage de manière sécurisée. En outre, les nouvelles lignes directrices devraient proposer aux organismes des outils pratiques tels que des fournisseurs de services de sécurité gérés, des rapports d'attestation ou des évaluations des risques par des tiers, qui leur permettraient d'assurer un suivi de leur chaîne d'approvisionnement.

En ce qui concerne l'informatique en nuage, il faut prendre des mesures supplémentaires pour relever le défi très singulier que représente la gestion de données sensibles en matière de soins de santé, et notamment le renforcement de la sécurité, le respect de la vie privée et les risques opérationnels. Afin de renforcer les garanties, les experts recommandent d'intégrer la «sécurité par défaut et dès la conception» dans les services en nuage. Cette approche donne la priorité à des infrastructures sécurisées, à la gestion proactive des vulnérabilités et, en ce qui concerne l'informatique en nuage, à une combinaison de solutions fournies tant par le secteur public que par le secteur privé. Pour garantir la robustesse des pratiques de sécurité, il est également essentiel d'assurer un suivi continu et de disposer d'attestations spécifiques aux fournisseurs, telles que les certifications des fournisseurs de solutions de sécurité et les audits de conformité avec les normes nationales et internationales.

En ce qui concerne les services tels que les infrastructures-services (IaaS), les plateformes-services (PaaS) et les logiciels-services (SaaS), la mise en œuvre de la sécurité incombe souvent au client. Cependant, de nombreux organismes de soins de santé ne disposent pas des ressources nécessaires pour satisfaire à ces exigences par leurs propres moyens. Pour remédier à cette situation, **il convient d'encourager les fournisseurs de services en nuage à faire de la mise en œuvre de mesures de sécurité de base une caractéristique standard**. Ces mesures permettraient de réduire le risque de mauvaises configurations, de maintenir une protection cohérente dans tous les environnements gérés par

médicaux de diagnostic in vitro devront être conformes aux exigences essentielles en matière de cybersécurité de la directive relative aux équipements radioélectriques lorsqu'ils sont mis sur le marché unique. Dans un second temps, à partir du 11 décembre 2027, le règlement sur la cyberrésilience entrera en vigueur.

[33] En décembre 2019, le groupe de coopération en matière de dispositifs médicaux a publié des orientations sur la cybersécurité des dispositifs médicaux, afin d'aider les fabricants à se conformer aux exigences de l'annexe I des deux règlements: https://ec.europa.eu/docsroom/documents/41863.

[34] Élaborées à partir des lignes directrices de l'ENISA de 2020 relatives aux marchés publics pour la cybersécurité dans les hôpitaux (février 2020). Disponible à l'adresse suivante: //www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

le client et de fournir davantage de garanties aux utilisateurs. Établir un niveau de sécurité de base par défaut permettrait de concilier la robustesse de la protection et les aspects pratiques, ce qui garantirait la facilité d'utilisation par un large éventail d'organismes de soins de santé. Cette tâche impliquerait une collaboration étroite entre les fournisseurs de services en nuage et le secteur des soins de santé, en tirant parti des meilleures pratiques en usage dans le secteur pour créer des solutions efficaces et évolutives.

Formation et développement des compétences

Disposer d'une main-d'œuvre dotée des compétences les plus demandées est important pour la croissance durable et la compétitivité à long terme en Europe, ainsi que pour des services de grande qualité, y compris en matière de soins de santé. La pénurie de professionnels qualifiés dans le domaine de la cybersécurité constitue un défi de taille dans toute l'Europe: selon les estimations, il manque 299 000 professionnels pour répondre aux besoins de main-d'œuvre dans l'UE[35]. Selon l'Eurobaromètre de 2024 sur les compétences en matière de cybersécurité[36], 81 % des entreprises estiment que les difficultés à recruter du personnel spécialisé dans la cybersécurité constituent un risque majeur de cyberattaques. Dans les secteurs de l'éducation, de la santé et de l'action sociale, 66 % des postes dans le domaine de la cybersécurité sont occupés par du personnel dont l'emploi précédent n'était pas lié à la cybersécurité, ce qui met en évidence le besoin urgent de miser sur la reconversion et le perfectionnement professionnels.

Pour relever ce défi, le centre d'appui devrait collaborer avec le futur consortium pour une infrastructure numérique européenne (EDIC)sur les compétences en matière de cybersécurité prévu dans la communication de la Commission sur l'académie des compétences en matière de cybersécurité[37]. Les travaux devraient faciliter les échanges entre les professionnels de la cybersécurité dans le secteur des soins de santé, tels que les directeurs de la sécurité de l'information (CISO). Au nombre des actions à envisager, on peut citer la création d'un **réseau européen des CISO dans le domaine de la santé**, avec, comme première étape, un groupe d'experts pour partager et développer les bonnes pratiques, les stratégies de rétention des talents et les solutions pour attirer les professionnels de la cybersécurité dans le secteur de la santé. En outre, sous l'égide de l'académie des compétences en matière de cybersécurité, il convient de mettre au point des ressources pour renforcer le personnel spécialisé dans la cybersécurité dans le secteur de la santé, avec le soutien des entreprises et du monde universitaire. À cet égard, les parties prenantes du secteur devraient être encouragées à s'engager en faveur de l'amélioration de la formation en matière de cybersécurité.

Les incidents de cybersécurité dans le domaine des soins de santé restent, en majeure partie, dus à des erreurs humaines, ce qui montre l'importance critique que revêtent la formation complète du personnel

[35] The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study | Plateforme pour les compétences et les emplois numériques.
[36] Enquête Eurobaromètre Flash 547 sur les compétences en matière de cybersécurité.
[37] Communication de la Commission au Parlement européen et au Conseil: Remédier à la pénurie de talents dans le secteur de la cybersécurité pour renforcer la compétitivité, la croissance et la résilience de l'UE («L'académie des compétences en matière de cybersécurité»), COM(2023) 207 final.

et la sensibilisation à la cybersécurité. Comme les professionnels de santé utilisent fréquemment des outils numériques, il est essentiel de les doter des connaissances nécessaires en matière de pratiques sûres. L'organisation de campagnes de formation et de sensibilisation ciblées peut réduire considérablement les risques. À cet effet, le centre d'appui devrait collaborer avec les professionnels et les prestataires de soins de santé, et coopérer avec les prestataires d'enseignement et de formation, les entreprises du secteur, l'EDIC sur les compétences en matière de cybersécurité ainsi que les autorités des États membres afin de créer et de diffuser des **modules et des cours de formation en ligne complets et faciles d'accès**.

L'intégration de modules sur les compétences numériques et la cybersécurité dans les programmes d'enseignement est essentielle pour créer une base solide en matière de cybersécurité dans le domaine des soins de santé. Ces modules devraient porter sur des problématiques sectorielles telles que la protection des données des patients et les vulnérabilités en matière de sécurité des dispositifs médicaux. Pour mettre au point ces ressources, il convient de tenir compte d'initiatives antérieures, telles que le projet BeWell financé dans le cadre du programme Erasmus +[38] et le projet PANACEA financé au titre d'Horizon 2020[39].

3.2. Capacités européennes de détection des cybermenaces visant le secteur de la santé

Il est essentiel de détecter efficacement les cybermenaces pour réagir rapidement aux incidents. Les acteurs de la menace peuvent utiliser des techniques pour rendre les intrusions difficiles à détecter, ce qui leur permet d'accéder de manière non autorisée à un système pendant de longues périodes[40]. Améliorer les capacités de détection des menaces peut donc contribuer à stopper net les cyberattaques. Par exemple, dans le cas de l'attaque par rançongiciel contre le prestataire finlandais de services de psychothérapie Vastaamo, dont l'auteur a exercé un chantage sur des patients auxquels il avait volé les dossiers médicaux confidentiels, l'intrusion initiale s'est produite en 2018, mais n'a été connue du prestataire qu'en 2020[41].

Pour améliorer la détection des menaces et la conscience situationnelle dans l'ensemble de l'UE, il est primordial de partager les informations et de collaborer de manière efficace. Les centres de réponse aux incidents de sécurité informatique (CSIRT) jouent un rôle crucial dans la mesure où ils reçoivent des signalements d'incidents, d'incidents évités et de menaces potentielles, et fournissent des conseils sur les mesures d'atténuation au niveau national. Toutefois, les **États membres sont vivement encouragés à transmettre également au centre d'appui de l'ENISA toutes les notifications d'incidents de cybersécurité soumises par les hôpitaux et les prestataires de soins de santé afin de développer une conscience situationnelle au niveau de l'UE.** Idéalement, cela devrait s'accompagner d'une

[38] BeWell – Blueprint alliance for a future health workforce strategy on digital and green skills (bewell-project.eu). Disponible à l'adresse suivante: https://bewell-project.eu/.
[39] PANACEA – Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for data and people. Disponible à l'adresse suivante: https://cordis.europa.eu/project/id/826293/fr.
[40] ENISA Health Threat Landscape 2023.
[41] Décision 1150/161/2021 du médiateur finlandais pour la protection des données.

caractérisation judicieuse des différentes dimensions pertinentes des incidents, y compris les vulnérabilités *root* connues, les effets sur les services de soins de santé et les événements préjudiciables pour les patients. En outre, les fabricants de dispositifs médicaux et de dispositifs de diagnostic in vitro sont engagés à signaler volontairement, par l'intermédiaire de la plateforme de signalement unique qui doit être mise en place et gérée par l'ENISA dans le cadre du règlement sur la cyberrésilience, les vulnérabilités activement exploitées ou les cyberincidents graves ayant une incidence sur la sécurité de ces dispositifs, ainsi que, le cas échéant, d'autres vulnérabilités, incidents, incidents évités ou cybermenaces susceptibles d'affecter le profil de risque de ces dispositifs.

Si les informations contenues dans les rapports ne sont plus sensibles, le centre d'appui pourrait établir, avec le soutien de l'ENISA, un catalogue européen des vulnérabilités exploitées connues (KEV) en ce qui concerne les dispositifs médicaux, les systèmes de dossiers médicaux électroniques et les fournisseurs d'équipements et de logiciels de TIC dans le domaine de la santé. Pour relever les défis importants liés à la détection des menaces, le centre d'appui devrait mettre en place un **service d'alerte précoce à l'échelle de l'UE pour le secteur de la santé, accessible sur abonnement et émettant des alertes en temps quasi réel**. Ce service s'appuierait sur les données traitées provenant des CSIRT, des entités et des fabricants du secteur des soins de santé, du renseignement en sources ouvertes (OSINT) et d'autres acteurs pertinents tels que les cyberpôles, les centres d'échange et d'analyse d'informations (ISAC) et les services répressifs. Une coopération plus étroite entre l'ENISA et l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) — par exemple en ce qui concerne les formes de cybercriminalité visant le secteur de la santé — permettrait de renforcer encore la conscience situationnelle.

Les ISAC constituent des ressources centrales pour le renseignement sur les cybermenaces, en favorisant l'échange bilatéral d'informations entre les secteurs public et privé et en favorisant l'instauration d'un climat de confiance. Le centre d'appui devrait renforcer le soutien à l'**ISAC européen dans le domaine de la santé** au moyen d'outils et d'échanges d'informations, ainsi que de rapports sectoriels sur la conscience situationnelle et en promouvant une communauté de confiance pour une collaboration tactique et stratégique. Les États membres devraient favoriser le développement d'ISAC nationaux dans le domaine de la santé[42]. Il convient également d'inciter les ISAC à réunir les prestataires de soins de santé et les fabricants afin de permettre une compréhension commune des cybermenaces, y compris dans la chaîne d'approvisionnement, et de faciliter un dialogue sur une conception sûre des produits qui tienne véritablement compte des réalités du déploiement sur le terrain.

[42] Par exemple, la Finlande dispose d'un ISAC national pour le secteur de la protection sociale et des soins de santé. Voir le centre national de cybersécurité finlandais: «ISAC information sharing groups». Disponible à l'adresse suivante: https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

3.3.Réaction rapide et rétablissement

Compte tenu de la grande sensibilité des données de santé des patients et des effets potentiellement dévastateurs des cyberattaques sur les services de soins de santé, il est essentiel, en cas d'incident de cybersécurité, de réagir rapidement et efficacement pour préserver la sécurité des patients. Lorsqu'un hôpital ou un prestataire de soins de santé subit une cyberattaque, il doit s'adresser en premier lieu au CSIRT national compétent[43]. Le CSIRT est chargé d'apporter un soutien en temps voulu, idéalement dans un délai de 24 heures, pour aider à gérer les incidents importants. Toutefois, si un incident dépasse la capacité du CSIRT, il faut pouvoir disposer d'un soutien de l'UE pour que la réaction soit rapide et efficace.

La réserve de cybersécurité de l'Union, créée en vertu du règlement sur la cybersolidarité, apporte une assistance en cas d'incident de cybersécurité important ou majeur ainsi qu'un soutien aux efforts de rétablissement initial, au moyen de services de réaction aux incidents assurés par des fournisseurs de services de sécurité gérés de confiance. Cette réserve est destinée à appuyer les efforts des CSIRT des États membres en leur permettant de demander une aide supplémentaire dans les cas qui concernent des secteurs critiques tels que celui de la santé. Pour améliorer ce système, la **Commission et l'ENISA devraient veiller à ce que la réserve soit dotée d'un service de réaction rapide spécifiquement consacré au secteur de la santé**. En complément d'autres cadres existants, ce service déploierait des experts pour gérer immédiatement les incidents de cybersécurité importants ou majeurs dans le domaine des soins de santé lorsque le soutien national est insuffisant.

Afin d'améliorer la réaction et le rétablissement, le centre d'appui, en collaboration avec le groupe de coopération SRI, le réseau des CSIRT et, le cas échéant, Europol, devrait élaborer des **manuels de réaction en cas d'incident de cybersécurité à l'intention du secteur des soins de santé**. Ces manuels aideraient les CSIRT et les organismes de soins de santé à réagir à des types particuliers de cybermenaces, y compris les rançongiciels. Compte tenu de l'importance que revêt une coopération efficace entre les CSIRT et les services répressifs pour réagir aux incidents de cybersécurité de nature criminelle et enquêter en la matière, les manuels devraient, entre autres aspects, fournir des orientations claires sur le signalement de ces incidents aux services répressifs. En outre, le centre d'appui pourrait **faciliter le déploiement à grande échelle d'exercices nationaux de cybersécurité, en s'appuyant sur les expériences tirées d'exercices tels que l'exercice CyberEurope 2022 organisé par l'ENISA, afin de tester les manuels et de renforcer les protocoles de réaction aux incidents**.

Il est nécessaire de collecter des données supplémentaires pour éclairer les politiques et évaluer l'efficacité des mesures prises contre les attaques par rançongiciel. À cet effet, les États membres devraient demander aux entités soumises à la directive SRI 2, y compris les organismes de soins de santé, de signaler tous les paiements qu'ils ont effectués ou ont l'intention d'effectuer en réponse à une demande de rançon, en plus des autres informations qu'ils fournissent lorsqu'ils signalent des incidents de cybersécurité importants. Ces signalements permettent d'enquêter efficacement sur les incidents liés

[43] L'article 23, paragraphe 1, de la directive SRI 2 impose aux entités essentielles et importantes de notifier les incidents importants au CSIRT dont elles relèvent ou, le cas échéant, à l'autorité compétente.

à des rançongiciels, et notamment de tracer les paiements sur les plateformes d'échange de cryptomonnaies afin d'en identifier les bénéficiaires.

La rapidité du rétablissement est un facteur essentiel pour maintenir la résilience et préserver la confiance du public, en particulier dans le domaine des soins de santé, où les temps d'arrêt peuvent perturber les soins aux patients. Pour que le rétablissement à la suite d'une attaque par rançongiciel soit efficace, les prestataires de soins de santé doivent disposer de sauvegardes sûres, actualisées et isolées, qui peuvent être rapidement restaurées. Dans son catalogue de services, le centre d'appui pourrait proposer un **service sur abonnement de rétablissement après une attaque par rançongiciel, afin d'aider les hôpitaux et les prestataires de soins de santé à élaborer à l'avance des plans de rétablissement**. L'ENISA et Europol devraient collaborer pour recenser les souches de rançongiciels les plus courantes ciblant les organismes de soins de santé et **étoffer le répertoire des outils de déchiffrement** disponibles dans le cadre du projet «No More Ransom»[44]. Ils devraient également se charger de la mise au point et de la promotion de conseils accessibles pour aider les prestataires de soins de santé à utiliser des outils de déchiffrement et éviter ainsi de payer une rançon.

L'**initiative internationale de lutte contre les rançongiciels**[45] constitue une enceinte très utile pour les échanges concernant des incidents spécifiques liés à des rançongiciels, ainsi que pour accroître les ressources des pays membres en ce qui concerne le renforcement de leurs cadres de cybersécurité et de leurs capacités d'enquête sur les acteurs du rançongiciel. La Commission, en collaboration avec la haute représentante, continuera à faire progresser la coopération dans le cadre de l'initiative de lutte contre les rançongiciels, y compris en matière de menaces liées aux rançongiciels visant le secteur de la santé. En outre, la Commission recherchera des modalités de coopération au sein du **groupe de travail du G7 sur la cybersécurité** afin de renforcer la cybersécurité dans le secteur de la santé. En particulier, ce groupe de travail pourrait examiner les possibilités de soutenir le secteur de la santé dans sa lutte contre les menaces telles que les rançongiciels, en s'appuyant sur des travaux tels que la déclaration commune du 8 novembre 2024 sur les attaques par rançongiciel contre les établissements de soins de santé, présentée dans le cadre du Conseil de sécurité de l'ONU[46].

4. Mesures au niveau national

La participation active et l'engagement des États membres détermineront la capacité du présent plan d'action à améliorer la cybersécurité dans le secteur de la santé. Pour mener à bien la mise en œuvre du plan d'action, les États membres pourraient désigner des **centres nationaux d'appui en matière de cybersécurité spécifiquement chargés des hôpitaux et des prestataires de soins de santé**. Ces centres, qui constitueraient les premiers points de contact pour le secteur de la santé au niveau national,

[44] https://www.nomoreransom.org/fr/index.html
[45] https://www.counter-ransomware.org/
[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/

collaboreraient étroitement avec le centre d'appui de l'ENISA. Lorsque cela est possible et pertinent, les États membres devraient désigner des organismes existants, tels que les CSIRT nationaux pour la santé ou les autorités compétentes, comme centres nationaux d'appui en matière de cybersécurité.

Les États membres sont aussi invités à élaborer des **plans d'action nationaux axés sur la cybersécurité dans le secteur des soins de santé**. Ces plans décriraient les risques spécifiques en matière de cybersécurité auxquels sont exposés les systèmes de soins de santé et les mesures prises au niveau national pour y remédier, tout en veillant à ce que les ressources et les pratiques au niveau européen soient utilisées efficacement. Le centre d'appui de l'ENISA peut aider à l'élaboration de ces plans, en tenant compte des plans nationaux existants et en coordonnant les efforts pour faire en sorte que les ressources et les stratégies des différents États membres se complètent mutuellement.

Les États membres doivent également s'attacher à faciliter le partage des ressources entre les prestataires de soins de santé, éventuellement en ayant recours à des **procédures conjointes de marchés publics ou à la mise en commun de ressources** au niveau national, régional, voire européen. Cette approche permettrait d'alléger la charge financière pesant sur les différentes entités tout en augmentant leur pouvoir de négociation avec les fournisseurs de services de cybersécurité.

Par exemple, le programme français CaRE[47] a introduit un certain nombre de mesures, aux niveaux national et régional, pour faire face aux défis en matière de ressources: un catalogue des offres cyber donne une vue d'ensemble des solutions de cybersécurité mises à la disposition des hôpitaux par l'intermédiaire de l'Agence nationale de la sécurité des systèmes d'information, de l'Agence du numérique en santé, des agences régionales de santé et des centrales d'achat nationales, ainsi que des solutions commerciales. Le programme prévoit en outre un financement supplémentaire destiné aux agences régionales afin qu'elles puissent mutualiser leurs ressources.

Les États membres devraient également s'attaquer à la problématique des niveaux insuffisants d'investissement dans la cybersécurité dans le secteur de la santé. Afin de garantir un financement adéquat, ils devraient fixer des **critères de référence non contraignants et assurer le suivi des objectifs de financement concernant spécifiquement la cybersécurité**, tout en veillant à ce que ces investissements ne soient pas réalisés au détriment des soins essentiels aux patients. Ces objectifs de financement devraient également servir à intégrer la dimension de la sécurité dans tous les investissements numériques réalisés dans le secteur. Les États membres peuvent échanger des bonnes pratiques et des conseils sur ces objectifs par l'intermédiaire de plateformes telles que le réseau «Santé en ligne»[48].

5. Coopération public-privé:

[47] Agence du numérique en santé: Cybersécurité accélération et Résilience des Établissements (CaRE). Disponible à l'adresse suivante: https://esante.gouv.fr/strategie-nationale/cybersecurite.

[48] Le réseau «Santé en ligne», créé sur la base de l'article 14 de la directive 2011/24/UE, est un réseau fonctionnant sur la base du volontariat qui relie les autorités nationales chargées de la santé en ligne désignées par les États membres.

La coopération public-privé et la consultation avec les prestataires de soins de santé, d'autres entités du secteur de la santé, ainsi que les acteurs concernés du secteur de la cybersécurité, sont essentielles à la bonne mise en œuvre du plan d'action. Afin de contribuer davantage aux travaux du centre d'appui, **la Commission, avec le soutien de l'ENISA, mettra en place un conseil consultatif conjoint en matière de cybersécurité dans le domaine de la santé** composé de représentants de haut niveau issus des secteurs des soins de santé et de la cybersécurité, qui pourra conseiller la Commission et le centre d'appui sur les actions efficaces et se pencher sur la poursuite du développement de partenariats public-privé dans ce domaine. Le conseil tirera parti des initiatives existantes en matière de partenariats public-privé, notamment l'ISAC européen dans le domaine de la santé.

En outre, la Commission **appellera** les entreprises, les fondations, les établissements d'enseignement et les parties prenantes dans le domaine de la cybersécurité à **s'engager à prendre des mesures pour relever les défis du secteur**. Ces engagements pourraient être inspirés de l'expérience de l'académie des compétences en matière de cybersécurité et concerner, par exemple, dans le cadre de cette académie, la fourniture de cours et de matériel de formation axés sur le secteur de la santé, à l'intention des professionnels de la cybersécurité[49]. Il pourrait aussi s'agir d'engagements portant sur des activités de sensibilisation ou consistant à fournir à des entités particulièrement vulnérables, à titre gratuit ou pour un prix réduit, des services de sécurité gérés leur permettant d'améliorer leur préparation et leur résilience en matière de cybersécurité. Par ailleurs, les engagements pourraient aussi concerner le partage des renseignements sur les cybermenaces avec le centre d'appui de l'ENISA. Ce dernier devrait conserver une vue d'ensemble des engagements pris dans le cadre de l'appel à l'action, afin de veiller à leur cohérence et à leur complémentarité.

6. Dissuader les acteurs de la cybermenace

Les politiques internes et externes de l'UE en matière de cybersécurité devraient avoir pour objectif de dissuader les acteurs de la cybermenace d'attaquer les systèmes de soins de santé européens. Les cyberattaques contre les organismes de soins de santé constituent une forme de cybermalveillance particulièrement inacceptable, compte tenu de la menace qu'elles peuvent représenter pour la sécurité des patients et la vie humaine. Par conséquent, il convient d'utiliser pleinement toutes les capacités de dissuasion de l'UE dans le domaine de la cybersécurité et du maintien de l'ordre pour mettre à mal le modèle économique global des acteurs de la menace ciblant le secteur de la santé et pour priver ces derniers de gains financiers facilement acquis. On pourrait, par exemple, appuyer les enquêtes transfrontières en améliorant le partage des indicateurs de compromission et d'autres données pertinentes, et se concentrer davantage sur les cibles de grand intérêt et les principaux moyens utilisés par les criminels tels que les hébergeurs dits «pare-balles» (*bulletproof hosting services*) ou les mixeurs de crypto-actifs.

La **boîte à outils cyberdiplomatique** constitue un cadre pour les mesures visant à prévenir, décourager et combattre les cyberattaques contre l'UE, les États membres et leurs partenaires. La haute représentante continuera d'utiliser le cadre existant de sanctions en matière de cybersécurité pour faire face aux menaces ciblant les systèmes de santé.

[49] Cyber Skills Academy: Get Involved | Plateforme pour les compétences et les emplois numériques.

Le fait d'obliger les acteurs criminels à répondre de leurs actes est un moyen de dissuasion important. Les États membres devraient donc veiller à ce que les services répressifs soient totalement intégrés à leurs plans d'action nationaux. En particulier, ils devraient tirer pleinement parti des dispositions de la directive relative aux attaques contre les systèmes d'information[50] et de la convention de Budapest sur la cybercriminalité du Conseil de l'Europe[51] afin de décourager les attaques, de traduire les criminels en justice et de démanteler les structures criminelles qui facilitent les attaques. La mise en œuvre réussie de ces outils devrait faire en sorte que les actions criminelles et malveillantes contre le secteur des soins de santé soient punies.

7. Mise en œuvre et suivi du plan d'action

Le présent plan d'action prévoit un certain nombre de tâches en vue de la création d'un centre d'appui au sein de l'ENISA. Cela permet d'assurer une mise en œuvre globale et cohérente du plan d'action tout en évitant la création de nouvelles entités susceptibles d'entraîner des doublons et des frais administratifs. La Commission compte faire en sorte que le centre d'appui dispose des ressources appropriées.

Une fois que le centre d'appui sera opérationnel, l'ENISA, en consultation avec la Commission, devrait tenir le conseil d'administration de l'ENISA ainsi que les réseaux pertinents des États membres, en particulier le groupe de coopération SRI, le réseau des CSIRT, le réseau «Santé en ligne» et, le cas échéant, le comité de l'espace européen des données de santé, régulièrement informés des travaux du centre. En outre, l'ENISA devrait échanger en permanence avec le conseil consultatif public-privé en matière de cybersécurité dans le domaine de la santé sur la mise en œuvre des actions prévues par le centre d'appui.

Les rapports réguliers de l'ENISA, tels que le rapport sur l'état de la cybersécurité dans l'Union, qui contient une évaluation agrégée du niveau de maturité des capacités de cybersécurité et des ressources en la matière dans l'ensemble de l'Union, y compris dans le secteur de la santé, devraient être utilisés pour publier des données pertinentes permettant d'appuyer le suivi du plan d'action. En outre, l'indice de cybersécurité de l'UE de l'ENISA[52] peut fournir des données quantitatives et qualitatives, qui constituent une base objective pour évaluer la criticité et la maturité du secteur de la santé.

8. Prochaines étapes

La présente communication a défini un programme ambitieux pour renforcer la cybersécurité dans le secteur de la santé de l'UE. Avec la proposition de création du centre d'appui en matière de cybersécurité

[50] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil: https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32013L0040.

[51] La Convention sur la cybercriminalité (convention de Budapest, STE nº 185) et ses protocoles: https://www.coe.int/fr/web/cybercrime/the-budapest-convention.

[52] ENISA: «EU Cybersecurity Index, Framework and Methodological Note» (2024). Disponible à l'adresse suivante: www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

pour les hôpitaux et les prestataires de soins de santé au sein de l'ENISA, le plan d'action présente une ébauche d'approche européenne commune cohérente pour relever le défi de la cybersécurité dans le secteur.

La présente communication devrait être considérée comme le début d'un processus destiné à améliorer la cybersécurité dans le secteur de la santé. Par conséquent, l'adoption du plan d'action s'accompagnera du lancement de consultations approfondies avec les parties prenantes et de la poursuite des échanges avec les États membres et les réseaux concernés afin de recueillir des informations. La Commission s'appuiera sur les résultats de ces consultations pour formuler, au cours du quatrième trimestre de 2025, des recommandations afin d'affiner davantage le plan d'action.

La Commission invite les États membres et toutes les parties prenantes à collaborer pour concrétiser l'ambition du plan d'action.

Annexe — Vue d'ensemble des actions proposées

La Commission:

Centre d'appui en matière de cybersécurité pour les hôpitaux et les prestataires de soins de santé au sein de l'ENISA	
Veiller à la mise à disposition de ressources appropriées pour le centre d'appui en matière de cybersécurité Collaborer avec l'ECCC pour lancer des projets pilotes visant à mettre au point des bonnes pratiques en matière de cyberhygiène et d'évaluation des risques pour la sécurité, et à répondre à la nécessité d'un suivi permanent de la situation dans les domaines de la cybersécurité, du renseignement sur les menaces et de la réaction aux incidents à l'aide de solutions de pointe, en vue de l'élaboration du catalogue des services du centre européen d'appui en matière de cybersécurité	2025
Prévention des incidents de cybersécurité	
En consultation avec le groupe de coopération SRI, EU-CyCLONe et l'ENISA, étudier la possibilité de faire figurer le secteur de la santé au nombre des secteurs pouvant bénéficier d'un soutien en vue de tests de préparation coordonnés au titre du règlement sur la cybersolidarité	T1 2025
Réaction rapide et rétablissement	
En collaboration avec l'ENISA, veiller à ce que la réserve de cybersécurité de l'UE soit dotée d'un service de réaction rapide spécifiquement consacré au secteur de la santé	T4 2025
Coopération public-privé	
Avec le soutien de l'ENISA, mettre en place un conseil consultatif en matière de cybersécurité dans le domaine de la santé	T1 2025
Appeler les entreprises, les fondations, les établissements d'enseignement et les parties prenantes dans le domaine de la cybersécurité à s'engager à prendre des mesures pour relever les défis dans le secteur de la santé	T2 2025

Dissuader les acteurs de la cybermenace	
En collaboration avec la haute représentante, étudier l'utilisation des mesures de la boîte à outils cyberdiplomatique visant à prévenir, décourager et combattre les activités malveillantes ciblant les systèmes de santé et à y réagir	2025
Faire progresser la coopération internationale dans la lutte contre les acteurs du rançongiciel, notamment dans le cadre de l'initiative internationale de lutte contre les rançongiciels, en collaboration avec la haute représentante	2025-2026
Rechercher des modalités de coopération au sein du groupe de travail du G7 sur la cybersécurité afin de renforcer la cybersécurité dans le secteur de la santé	2025-2026
Prochaines étapes	
Lancer des consultations approfondies avec les parties prenantes	T1 2025
Adopter des recommandations en vue d'affiner davantage le plan d'action	T4 2025

L'ENISA:

Centre européen d'appui en matière de cybersécurité pour les hôpitaux et les prestataires de soins de santé	
Lancer les préparatifs en vue de la création d'un centre européen d'appui en matière de cybersécurité pour les hôpitaux et les prestataires de soins de santé	T2 2025
Mettre au point un catalogue complet de services à fournir par le centre d'appui en matière de cybersécurité	À partir du T4 2025
Prévention des incidents de cybersécurité	
Publier des conseils qui mettent en lumière les pratiques les plus importantes en matière de cybersécurité et aident les prestataires de soins de santé à les mettre en œuvre	T3 2025

Mettre au point, en étroite collaboration avec la Commission et les États membres, un outil de cartographie réglementaire	T1 2025
Élaborer un cadre pour les évaluations de la maturité en matière de cybersécurité spécifiquement adapté au secteur des soins de santé	T3 2025
Procéder à une évaluation annuelle de la maturité en matière de cybersécurité dans le secteur de la santé	2025-2026
Collaborer avec les États membres et les autorités régionales responsables des programmes pour créer des programmes types de chèques-cybersécurité	2025-2026
Élaborer de nouvelles lignes directrices en matière de marchés publics pour la cybersécurité des hôpitaux et des prestataires de soins de santé	T3 2025
Créer un réseau européen des CISO dans le domaine de la santé	T1 2026
Concevoir et promouvoir des modules et des cours de formation pour les professionnels de santé	T1 2026
Capacités européennes de détection des cybermenaces visant le secteur de la santé	
Créer un catalogue européen des vulnérabilités exploitées connues (KEV) en ce qui concerne les dispositifs médicaux, les systèmes de dossiers médicaux électroniques et les fournisseurs d'équipements et de logiciels de TIC dans le domaine de la santé	T4 2025
Mettre en place un service d'alerte précoce à l'échelle de l'UE pour le secteur de la santé, accessible sur abonnement	À partir de 2026
Soutenir l'ISAC européen dans le domaine de la santé au moyen d'outils et d'échanges d'informations	2025-2026
Réaction rapide et rétablissement	
En collaboration avec la Commission, veiller à ce que la réserve de cybersécurité de l'UE soit dotée d'un service de réaction rapide spécifiquement consacré au secteur de la santé	T4 2025
En collaboration avec le réseau des CSIRT, élaborer des manuels de réaction en cas d'incident de	T3 2025

cybersécurité à l'intention du secteur des soins de santé	
Faciliter le déploiement à grande échelle d'exercices nationaux de cybersécurité afin de tester les manuels et de renforcer les protocoles de réaction aux incidents	À partir du T4 2025
Fournir un service sur abonnement de rétablissement après une attaque par rançongiciel	À partir de 2026
En collaboration avec Europol, recenser les souches de rançongiciels les plus courantes ciblant les organismes de soins de santé et élargir le répertoire des outils de déchiffrement disponibles dans le cadre du projet «No More Ransom»	T4 2025
Mettre au point, en collaboration avec Europol, des conseils accessibles pour aider les prestataires de soins de santé à éviter de payer des rançons	T3 2025
Mesures au niveau national	
Aider les États membres à élaborer des plans d'action nationaux	2025
Coordonner les efforts pour faire en sorte que les ressources et les stratégies des différents États membres se complètent mutuellement	2025-2026
Mise en œuvre et suivi du plan d'action	
En consultation avec la Commission, tenir les réseaux concernés des États membres régulièrement informés des travaux du centre d'appui en matière de cybersécurité	2025-2026
Échanger en permanence avec le conseil consultatif en matière de cybersécurité dans le domaine de la santé	2025-2026

Les États membres:

Capacités européennes de détection des cybermenaces visant le secteur de la santé	
Transmettre au centre européen d'appui en matière de cybersécurité les notifications d'incidents soumises par les hôpitaux et les prestataires de soins de santé dans le cadre de la directive SRI 2	À partir du T4 2025

Encourager le développement d'ISAC nationaux dans le domaine de la santé	2025-2026
Prévention des incidents de cybersécurité	
Au sein du groupe de coopération SRI, procéder à une évaluation coordonnée des risques pour la sécurité, en évaluant les risques techniques et stratégiques associés aux chaînes d'approvisionnement en dispositifs médicaux	T4 2025
Réaction rapide et rétablissement	
Déploiement d'exercices nationaux de cybersécurité afin de tester les manuels et de renforcer les protocoles de réaction aux incidents	À partir de 2026
Mesures au niveau national	
Désigner des centres nationaux d'appui en matière de cybersécurité pour les hôpitaux et les prestataires de soins de santé	T2 2025
Élaborer des plans d'action nationaux axés sur la cybersécurité dans le secteur des soins de santé	T4 2025
Faciliter le partage des ressources entre les prestataires de soins de santé	2025-2026
Fixer des critères de référence non contraignants et assurer le suivi des objectifs de financement concernant spécifiquement la cybersécurité	T4 2025
Demander aux organismes de soins de santé et autres entités soumises à la directive SRI 2 de signaler les paiements qu'ils ont l'intention d'effectuer en réponse à une demande de rançon	T4 2025