Nos vies en péril: pirater la santé, c'est attaquer les personnes.

Mars 2021

Résumé

Sur Internet et en dehors, **attaquer les services de santé**, **c'est attaquer les individus**. **Ces services étant essentiels et vitaux**, **ils doivent être protégés de toute action malveillante**, **sauvegardés pour et par tous, dans des conditions garantissant aux citoyens le respect de la sécurité**, **la dignité et l'équité dans le monde numérique**. **Ces conditions ont un nom** : **la paix dans le cyberespace**.

Depuis novembre 2020, le nombre de cyberattaques au niveau mondial contre la santé a augmenté de 45%, contre une moyenne de 22% dans d'autres secteurs[1]. Rien qu'en novembre 2020, les organisations de santé de toutes les régions du monde ont connu une hausse significative du nombre d'attaques, notamment en Europe centrale, en Asie de l'Est et en Amérique latine, où elles ont été multipliées par deux[2].

Ce rapport constitue la pierre angulaire de notre programme Cyber 4 Healthcare, lancé en 2020 pour assister les professionnels de santé, analyser les cyberattaques et améliorer les politiques visant à protéger le secteur médical et les populations dont il prend soin. Nos objectifs consistent à réduire le nombre et la force des cyberattaques, responsabiliser les acteurs et permettre aux victimes de s'exprimer et d'obtenir un droit à réparation.

Tout en consolidant les informations qui démontrent la complexité, l'ampleur et la violence des menaces, **ce rapport met l'accent pour la première fois sur les conséquences des attaques sur les individus et la société**. Sur la base des témoignages des victimes, des données analytiques, des initiatives bénévoles, des cadres juridiques légaux et de la recherche universitaire, il couvre un large spectre d'analyse : les innovations relatives aux modes opératoires, la diversité des criminels et leurs motivations, la difficile mise en œuvre des normes et lois nationales et internationales et le manque de ressources malgré les différentes initiatives d'assistance existantes. Des demandes de rançons aux campagnes de désinformations liées à la COVID-19, notre étude souligne à quel point la responsabilisation fait partie de la solution car bon nombre d'incidents ne sont pas déclarés et les auteurs des attaques, rarement identifiés, échappent aux sanctions.

[1] Check Software (2021) 'Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again', Check Point Software, 5 janvier. Disponible sur : https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/ (Consulté le 12 janvier 2021).

[2] idem.

Recommandations

Sur Internet et en dehors, **attaquer les services de santé**, **c'est attaquer les individus**. Tout au long de ce rapport, nous voulons montrer que, bien que les professionnels de la santé et les patients soient confrontés à une menace évolutive et d'ampleur, **une action collective est possible**. Le rapport met en avant la responsabilité des États car il leur revient de montrer la voie à suivre pour que les attaques diminuent à l'échelle mondiale et que les criminels soient sanctionnés.

Ces recommandations sont adressées aux gouvernements, aux entreprises, au secteur médical, aux universités et à la société civile dans le but de réduire durablement les cybermenaces et les attaques contre la santé. Elles visent à :

1 **Détailler les attaques et analyser leur impact humain et sociétal** ;

2 **Améliorer la solidité et la résilience des services de santé en** :

- 2.1 Fortifiant leur cybersécurité,
- 2.2 Augmentant leurs ressources et en perfectionnant les compétences,
- 2.3 Améliorant leur préparation aux attaques.

3 **Rendre opérationnels les instruments techniques et juridiques pour protéger la santé en** :

- 3.1 Renforçant l'écosystème juridique et normatif,
- 3.2 Améliorant le partage et la remontée d'informations.

4 **Rendre justiciables les criminels**.

Le CyberPeace Institute s'engage à soutenir ces recommandations à travers :

- **La surveillance**, **l'étude et la diffusion des informations relatives aux attaques contre la santé**, **de même que le partage des sanctions appliquées en cas d'infractions aux lois et aux normes** ;
- **Le recensement des témoignages des victimes** ;
- **L'accompagnement et le développement des initiatives d'assistance**.

Il analysera également avec ses partenaires les risques et les vulnérabilités, de manière à définir et évaluer précisément les lacunes en termes d'effectifs, de finance, de technique et de couverture d'assurance nécessaires à la sécurisation des infrastructures du secteur médical. De plus, grâce à l'application d'un cadre de responsabilisation, le CyberPeace Institute surveillera le respect des règles dans le cyberespace afin de réduire la menace sur la santé.

Notre institut militera à l'international et engagera toutes les parties prenantes autour d'un objectif simple : permettre à chaque professionnel de santé de travailler, et à chaque patient et individu de bénéficier de soins, sans crainte ni préjudice, en périodes de conflit comme en temps de paix.

Pourquoi le secteur médical est-il attaqué ?

Les attaques financières et politiques contre le système de santé exploitent ses faiblesses en matière de cybersécurité et profitent de la fragilité de son infrastructure numérique.

La santé a toujours été la cible d'attaques mais la pandémie de COVID-19 les a encore exacerbées, exposant le secteur à une convergence des menaces qui peut être liée à trois facteurs-clés :

- **Le secteur a la responsabilité du fonctionnement de services d'importance vitale**, ce qui en fait une cible de choix pour des attaques d'extorsion numérique et une cible lucrative pour les attaques de ransomwares. Être garant des vies humaines rend le secteur médical particulièrement vulnérable.
- **Les établissements de santé sont dépositaires de données précieuses**. Les dossiers médicaux sont extrêmement rentables sur le marché noir, vendus jusqu'à 250 $ l'unité.
- **Le positionnement stratégique** de la recherche médicale pendant la pandémie l'a placée au centre des rivalités existant entre États. Certains ont ainsi cherché à saboter les réponses à la crise sanitaire apportée par leurs rivaux, en visant les établissements de santé et la confiance que la société leur porte.

Ces menaces sont facilitées par **la fragilité de l'infrastructure numérique des établissements de santé** et de leur **manque d'investissements caractérisé en termes de cybersécurité**. En outre, du fait de la numérisation rapide de ses données, la santé se trouve exposée à toujours plus d'attaques. Et si certaines structures ont su s'adapter grâce à des protections efficaces, elles restent minoritaires. L'essentiel du secteur souffre d'un manque de moyens financiers et humains pour sécuriser une infrastructure complexe et obsolète et restera une cible de choix si ces lacunes ne sont pas comblées.

Quel est le véritable impact des attaques contre le secteur médical ?

Les attaques contre la santé causent un préjudice direct aux personnes et représentent une menace pour la santé, à l'échelle mondiale.

Tout concourt à menacer le secteur de la santé et les vies humaines sur le plan mondial : la convergence des attaques sur les infrastructures et à l'encontre des actions mises en place pour lutter contre la pandémie, ainsi que la perte de confiance de la société dans le bon fonctionnement des centres de soins. Les acteurs de la santé (hôpitaux et centres de soins, industries pharmaceutiques et ministères de la santé) dont les données et les infrastructures ont été fragilisées, sont le plus souvent les cibles des attaques. Mais ce sont les professionnels de santé, les patients et la société dans son ensemble qui en souffrent à long terme. Bien que ce phénomène soit encore peu étudié, les travaux menés montrent que les conséquences sont préoccupantes et doivent être traitées urgemment.

Les attaques contre les hôpitaux et les centres de soins ont un **impact sur la santé physique des individus**. Les demandes de rançons retardent les chirurgies, renvoient vers d'autres établissements les ambulances et alourdissent le fonctionnement quotidien des services. À long terme, de telles attaques peuvent avoir un effet durable sur la capacité d'un hôpital à offrir un service de qualité, comme en témoigne une étude qui a observé un taux de mortalité plus élevé dans les hôpitaux qui avaient connu une cyberattaque au cours des trois dernières années[3]. Dans ces temps de pandémie, le dysfonctionnement des services médicaux peut également avoir une influence néfaste pour le patient, voire sur la propagation du virus.

L'impact psychologique des attaques est beaucoup moins visible, mais provoque des souffrances tout aussi importantes. Au cours d'une cyberattaque, les soignants ressentent des niveaux accrus de stress tandis qu'au cours d'une demande de rançon, d'autres sentiments prévalent, tels que la peur, la perte de contrôle, la coercition et l'impuissance. Après l'attaque, la confiance dans le système de santé se détériore et les patients se sentent violés et trahis lorsque les cybercriminels usurpent leurs identités. Plus largement, les attaques qui ont un impact sur la chaîne d'approvisionnement du soin amenuisent la confiance portée dans les infrastructures techniques du monde médical.

Si les conséquences sur les individus diffèrent d'un cas à l'autre, **l'impact sociétal** des cyberattaques sur la santé demeure quant à lui sensiblement le même. En effet, le piratage de données médicales confidentielles, le dysfonctionnement des services ainsi que les campagnes de désinformation liées à la COVID-19 favorisent toujours un **climat de peur, de confusion et de méfiance**. Dans cette spirale infernale, le secteur médical perd en réactivité et les patients se détournent des meilleurs traitements possibles.

L'impact économique des cyberattaques sur la santé se répercute sur plusieurs années, ce qui rend les coûts difficilement mesurables. Après l'attaque, la structure met du temps à retrouver un fonctionnement normal et cette phase nécessite un apport de trésorerie pour restaurer et améliorer ses infrastructures numériques, régler les amendes dues aux non-conformités, reformer ses équipes et retrouver son ancienne réputation. A ces coûts s'ajoute parfois le paiement d'une rançon, mais ce dernier est fortement déconseillé car les criminels sont incités à recommencer et les résultats escomptés ne sont pas garantis.

[3] Choi, S. J., Johnson, M. E. and Lehmann, C. U. (2019) 'Data breach remediation efforts and their implications for hospital quality', Health Services Research, 54(5), pp. 971–980. doi: 10.1111/1475-6773.13203.

Comment se déroulent et évoluent les attaques contre la santé ?

Les attaques se multiplient tandis que l'arsenal d'armes utilisées pour attaquer la santé évolue.

À la suite de l'augmentation constante des cybermenaces au cours des dernières années, le monde a connu une accélération et une évolution de trois types d'attaques principales pendant la pandémie de COVID-19 :

Les attaques qui viennent déstabiliser le secteur médical ont touché tous les pays et continuent d'évoluer au travers de nouveaux modes opératoires. Parmi elles, les ransomwares constituent une menace particulière vis-à-vis des soins à caractère vital. Ces demandes de rançon ont fortement évolué en 2020, leurs auteurs adoptant des tactiques de double extorsion qui recouvrent encryptage et menace de fuite des données. Leur force est de créer un risque immédiat pour la santé des patients et d'avoir un impact durable sur l'organisation des soins. Dans le même temps, la coopération s'est accrue entre les cybercriminels, qui ont cherché à maximiser leur efficacité et leurs profits. La survenue d'attaques venant perturber les services médicaux correspond à une tendance qui va s'accroître sous la forme d'autres actions, comme les attaques par déni de service, de même que la monétisation des données volées (extorsion de fichiers, vente de dossiers médicaux…).

Les piratages de données médicales ont considérablement augmenté au cours de la pandémie, les États-Unis ayant notamment enregistré une hausse de 39 % entre 2019 et 2020[4]. Le télétravail et les téléconsultations ont fortement contribué à exposer le système de santé aux menaces et la pandémie a exacerbé la valeur financière et stratégique des données liées à la COVID-19. Par conséquent, la santé a été ciblée à la fois par les cybercriminels pour gagner de l'argent, mais aussi par les acteurs étatiques qui ont cherché à obtenir un avantage stratégique dans la recherche sur les vaccins et dans les actions de lutte contre la pandémie.

Les campagnes de désinformation, qui ont ciblé directement et indirectement la santé, ont été à l'origine d'une véritable « Infodémie » concernant la COVID-19. Certains acteurs étatiques ont volé, manipulé et diffusé des informations provenant d'organisations luttant contre la pandémie ou de laboratoires de recherche sur les vaccins. En introduisant des informations authentiques dans leur récit fictif, ils donnent de la crédibilité à l'ensemble pour mieux désinformer. En découle une perte de confiance de la société dans les structures attaquées, qui peut nuire à la réponse apportée à la crise sanitaire.

[4] U.S. DoHHS (sans date) Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, U.S. Department of Health & Human Services - Office for Civil Rights. Disponible sur : https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (Consulté le 17 février 2021).

Qui sont les principaux auteurs ?

Les attaques contre la santé sont des crimes peu risqués et très lucratifs. En toute impunité, les criminels et les Etats unissent leurs forces pour servir leurs intérêts mercantiles ou politiques.

Les cybercriminels et les acteurs étatiques représentent les deux principaux auteurs d'attaques contre le monde médical. Néanmoins, la limite devient de plus en plus floue depuis quelques années entre les différents protagonistes avec l'émergence d'acteurs étatiques sponsorisés par les États et d'autres agissant au nom des gouvernements ; cela complique encore l'identification des auteurs. **Les cybercriminels** représentent une forte menace pour la santé. Principalement motivés par l'argent, ils n'ont pas hésité à demander des rançons aux hôpitaux alors qu'ils s'étaient engagés à ne pas le faire. De leur côté, certains **acteurs étatiques** bien renseignés ont profité de la COVID-19 pour influer sur l'équilibre géopolitique mondial, en commettant des attaques visant à voler, corrompre ou détruire des informations : depuis mars 2020, des cybers espions ciblent les laboratoires de recherche sur les vaccins et les centres de dépistage pour donner un avantage concurrentiel aux États qui les emploient.

Les acteurs malveillants agissent presque en toute impunité. Le taux de poursuite est extrêmement faible car les attaques sont sous-déclarées, la police et la justice manquent de moyens et les auteurs sont rarement identifiés. Les possibilités offertes sur le plan juridique, telles que la coopération sur des enquêtes, et sur le plan légal, telles que les sanctions, sont rarement utilisées en cas d'attaques. Pour des raisons d'ordre géopolitique, les sanctions sont en outre complexes à mettre en œuvre en cas d'attaques directes ou indirectes des États.

Quels sont les dispositifs disponibles pour protéger la santé contre les cyberattaques ?

Les États ne se prévalent pas de toutes les normes et lois pour protéger la santé.

Durant la pandémie de COVID-19, les attaques contre la santé n'ont cessé d'augmenter, parallèlement à l'urgence de la crise sanitaire et de ses conséquences désastreuses sur l'exercice des droits fondamentaux. Et même si les sanctions existent, la réticence est de mise pour les appliquer, ce qui laisse le secteur encore plus vulnérable. De nombreux dispositifs, issus du droit national, du droit international et des normes volontairement non-contraignantes des nations, existent pour obliger les criminels à rendre des comptes et pour mieux protéger les services d'importance vitale ainsi que les données numériques. Malheureusement, **ces possibilités d'action sont entravées**. Dans le cadre des processus mandatés par l'ONU (GEG de l'ONU et GTCNL de l'ONU) et des initiatives multipartites (comme l'Appel de Paris), les gouvernements n'ont pas unanimement déclaré que les établissements médicaux devaient impérativement être protégés contre les cyberattaques. De surcroît, il n'existe pas d'accords internationaux pour appliquer les principes du droit international, et les normes non-contraignantes fixées par les nations ne sont pas appliquées de manière cohérente.

Ces contraintes empêchent les États de lutter contre l'impunité dans le cyberespace et sont renforcées par le manque de capacité des organismes nationaux en charge de l'application des lois et de la justice à agir en cas d'attaque extraterritoriale. De tels déficits accentuent le besoin de responsabilisation et d'application de la loi dans le monde numérique.

Les industriels peuvent appliquer davantage les normes multipartites pour protéger les soins de santé.

Les normes multipartites, comme celles proposées dans l'Appel de Paris, l'Accord sur les technologies de cybersécurité et la Charte de confiance, offrent des renseignements importants et utiles sur la façon dont les industriels peuvent mieux protéger la santé. La mise en œuvre de mesures de sécurité dès la conception des produits, le signalement des vulnérabilités, en particulier dans les services d'importance vitale, et l'amélioration de la protection des utilisateurs grâce à des actions concrètes, représentent une opportunité pour répondre à certaines des menaces urgentes visant le secteur médical. La standardisation de ces normes, au moyen de cadres contraignants, contribuerait considérablement à assurer une protection adéquate aux utilisateurs, aux sous-traitants et aux fournisseurs d'équipements médicaux.

Un cadre solide pourrait-il responsabiliser les comportements dans le cyberespace ?

Il n'existe pas aujourd'hui de mécanisme indépendant pour surveiller la bonne marche du cyberespace.

Le CyberPeace Institute a clairement identifié la nécessité de **combler le manque de responsabilité des acteurs** comme un prérequis à la paix numérique et à la protection des communautés vulnérables, notamment dans le contexte de l'absence actuelle de déclaration systématique des incidents et du manque de transparence sur la façon dont les acteurs malveillants violent les lois, les normes et les principes.

Pour combler ce déficit de responsabilité, la qualification des actes ne suffit pas. Il faut aussi assigner un rôle précis à toutes les parties prenantes, tout en définissant les lois et principes applicables pour veiller au respect de la sécurité, de la dignité humaine et de l'équité. Le cadre de responsabilisation du CyberPeace Institute propose un modèle dans lequel les attentes et les engagements des acteurs du cyberespace sont cartographiés en fonction du degré de contrainte et des risques encourus en cas de manquement.

Dans la mesure où les éditeurs de logiciels, l'industrie, les établissements de santé et les praticiens sont impliqués dans la sécurisation du système, c'est aux États de les accompagner en agissant à tous les niveaux (technique, éthique, judiciaire et normatif). A eux de mettre en place puis de faire respecter les obligations grâce à la réglementation et l'application de la loi. Pour le bien de la santé, les États ont le pouvoir unique, et sans doute la responsabilité, de montrer le chemin pour atteindre la paix dans le monde numérique. Un cadre de responsabilisation solide et contraignant pourrait ouvrir la voie à cela.

Comment les différents acteurs unissent-ils leurs forces pour soutenir la santé ?

Les aides déployées manquent de soutien et de visibilité.

Tout comme les criminels ont uni leurs forces pour attaquer la santé, de nombreuses coalitions se sont formées pour la protéger en fournissant une aide rapide et gratuite. Il existe plusieurs types d'initiatives :

- **celles qui touchent à la solidité et à la résilience** pour aider les établissements de santé à se prémunir et à se défendre contre les attaques grâce à une meilleure prise de conscience, au partage d'informations et à la mise en place d'outils et services adaptés ;
- **celles qui touchent à l'aide technique** pour assurer la cybersécurité et apporter une expertise en temps de crise, enquêter sur la menace et sécuriser les infrastructures ;
- **celles qui touchent à l'assistance aux victimes**, pour leur fournir une aide sur le plan pratique et psychologique.

La société civile, les gouvernements, les entreprises privées, les universités, les organisations internationales, ainsi que les professionnels de la cybersécurité du monde entier, ont mené des actions ciblées et adaptées tandis que divers réseaux (public-privé, privé-privé, bénévoles) se sont développés. Malheureusement, ces initiatives ont souvent manqué de visibilité et sont restées ponctuelles. En revanche, elles prouvent que de nombreux acteurs sont disposés à protéger la santé et qu'**une action collective est possible**.

Conclusion

Notre rapport constitue une première étape d'identification et d'évaluation des problèmes systémiques de cybersécurité auxquels sont confrontés le monde de la santé et le cyberespace en général. Il pointe du doigt une lacune dans l'accessibilité et la disponibilité des données concernant les attaques du secteur médical, leur ampleur et leur véritable impact. Il n'existe pas aujourd'hui de normes mondiales pour déclarer ces attaques, collecter les données et les partager. De même, et sans doute par conséquent, il existe peu de recherches sur leurs conséquences à court et long termes sur la société, notamment sur les soins prodigués aux patients. Mais **il ne peut pas y avoir de réponse sans connaissance** et les recommandations que nous proposons visent à combler ce manque. Le CyberPeace Institute s'engage par ailleurs à susciter des réponses collectives aux défis numériques de notre époque.

Les victimes d'attaques sont multiples à travers le monde et les cybercriminels, quelles que soient leurs motivations, mettent des vies en péril en perturbant la bonne marche des établissements de santé. Pour en finir avec la mise en danger de la vie d'autrui, il faut responsabiliser toutes les parties prenantes qui agissent dans le cyberespace. Grâce à une réponse collective et coordonnée, la confiance et la sécurité prévaudront sur la peur et le préjudice.