PRÉSENTATION

Défis et complexité de la cybersécurité dans les soins de santé en contexte de transformation

Les quatre principaux enjeux de la cybersécurité dans le domaine de la santé.

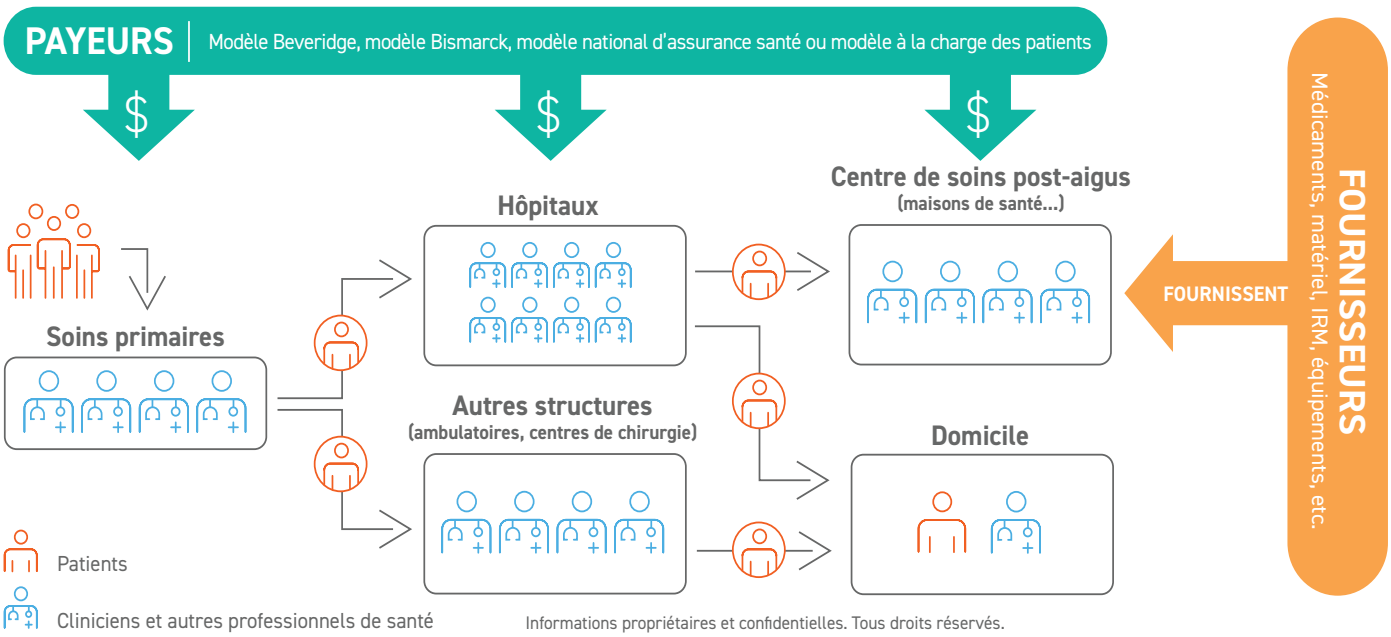
Résumé

Depuis le début de la pandémie de COVID-19, les organismes de soins de santé ont fait évoluer et étendu leur empreinte technologique. Une réponse au développement rapide de la télémédecine, au déferlement de professionnels de santé à distance, au passage à une gestion des données et à une activité basée sur le cloud, ainsi qu'à la prolifération des dispositifs connectés de télésurveillance des patients. Cette évolution, si elle a permis aux professionnels de fournir de n'importe où des soins de qualité en personne, de manière virtuelle ou à domicile, a également créé – ou exacerbé – un certain nombre de défis en matière de cybersécurité. Cette présentation se penche sur les défis et la complexité de la cybersécurité propres au secteur de la santé dans son ensemble suite à ces transformations.

Introduction

Les enjeux sont élevés dans le domaine de la santé. Les nouvelles technologies et applications médicales influencent le bien-être et la sécurité des patients tout au long des soins.

L'effet domino de cyberattaques abouties sur les infrastructures sanitaires vitales et sur les dossiers médicaux électroniques peut avoir de terribles répercussions sur les soins aux patients :



- Des patients ne reçoivent pas les soins nécessaires parce que les prestataires sont déconnectés suite à une attaque de ransomware ou DDoS.
- Des chirurgiens repoussent des opérations vitales parce que les informations nécessaires pour les effectuer deviennent inaccessibles.
- Des défaillances dans les procédures de diagnostic et les tests de laboratoire retardent les traitements médicaux.
- Une indisponibilité des urgences force les ambulances à dévier vers des établissements beaucoup plus éloignés, entraînant une aggravation de l'état de santé qui peut avoir une issue irréversible.

Les PHI ont plus de valeur sur le Dark Web

Les hôpitaux et autres établissements de santé sont parmi les cibles les plus recherchées de cyberattaques, qu'elles se produisent en interne ou de l'extérieur, car les informations de santé protégées (PHI) sont très demandées sur le Dark Web. Elles se vendent donc souvent plus cher que d'autres informations d'identification personnelle (PII).

Les numéros de cartes de crédit, par exemple, sont désactivés et remplacés dès la détection de transactions douteuses, d'où une valeur moindre sur le marché. Les dossiers médicaux, en revanche, sont plus intéressants parce qu'immuables et difficiles à modifier ou à effacer. Les cybercriminels en retirent donc des bénéfices durables. Les patients, eux, souffrent financièrement et psychologiquement et il faut du temps pour réparer les dommages d'activités frauduleuses. Il peut s'agir de la prescription d'ordonnances, de l'obtention de traitements, du remboursement de faux frais médicaux, ou de l'obtention de prêts personnels ou de cartes de crédit avec des dossiers de santé volés.

Les ransomwares sèment toujours le trouble

Les agresseurs trouvent encore des moyens d'exploiter des faiblesses que les centres des opérations de sécurité (SOC) sanitaires n'ont pas traitées ou décelées (parce que les méthodes de piratage évoluées ont toujours une longueur d'avance sur les investissements dans le renforcement des contrôles de sécurité). Par exemple, les cybercriminels sont activement à l'affût des vulnérabilités sans correctif, comme Log4j, premier vecteur de lancement d'une attaque de ransomware. Aussi les ransomwares sont-ils considérés comme la plus grande menace dans le secteur de la santé.

Cette tendance se poursuivra probablement en 2022, sachant que 42 %[1] des organismes de soins de santé ont subi des attaques de ransomwares au cours des deux dernières années. À cela s'ajoute qu'environ 36 %[2] de ces incidents se sont produits via des tiers, comme c'est le cas des attaques hautement médiatisées sur la chaîne logistique contre des logiciels de gestion d'infrastructure critique vulnérables.

Les vulnérabilités de serveurs réseau, cause de la plupart des incidents

2021 fut une année noire en termes de fuites de données pour le secteur, leur nombre atteignant des records et révélant de nombreux dossiers PHI. À titre d'exemple, l'Office américain des droits civils du Département des services sociaux et de santé indique que plus de 700 (Figure 1) des entités couvertes ont subi une infraction, entraînant le vol, la perte ou la publication de plus de 42 millions de dossiers PHI individuels (Figure 2). Les incidents[3] signalés récemment montrent que les brèches et les vulnérabilités ont d'ores et déjà pris un cours inquiétant en 2022 (Figure 3).

Figure 1
Fuites de 500 dossiers de données médicales ou plus

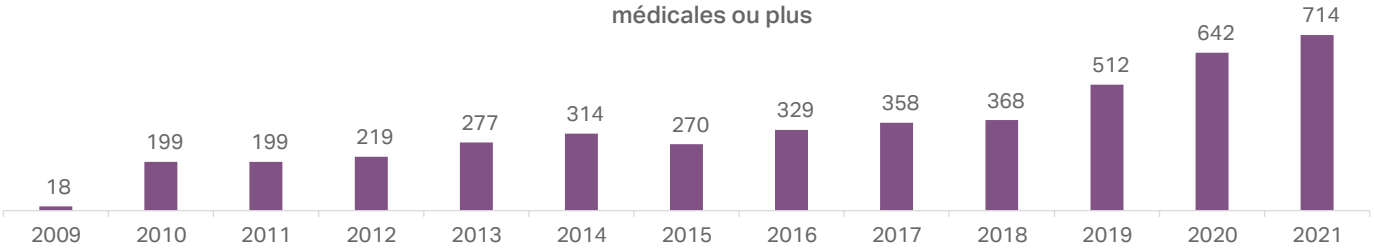
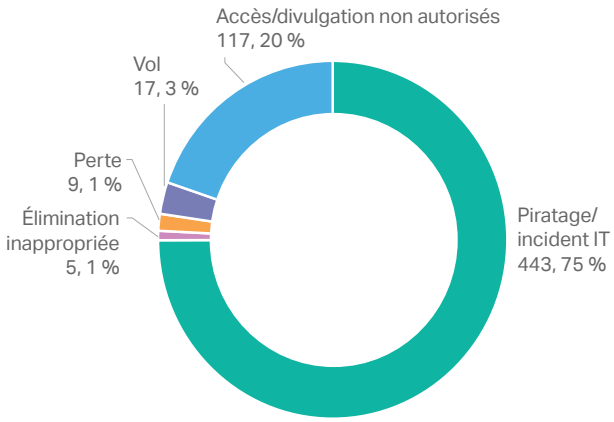


Figure 2

Office américain des droits civils du département des services sociaux et de santé, fuites de données signalées en 2021
Total : 5



Office américain des droits civils du département des services sociaux et de santé, sujets atteints en 2021

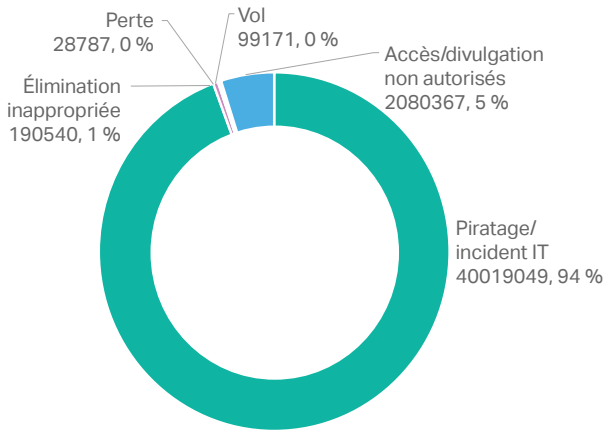
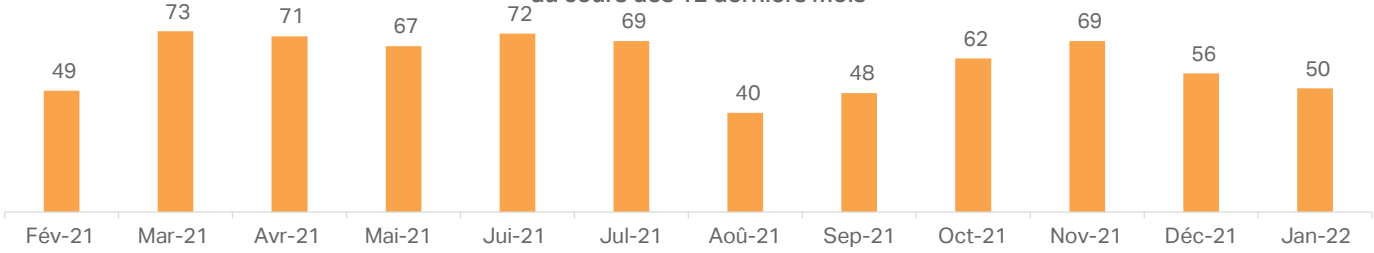


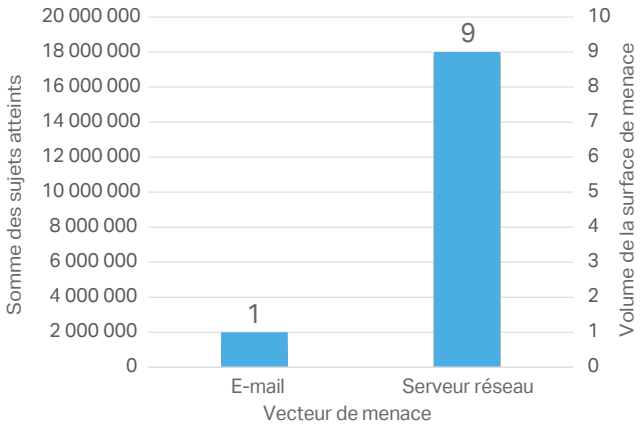
Figure 3
Fuites de données de santé aux États-Unis au cours des 12 derniers mois



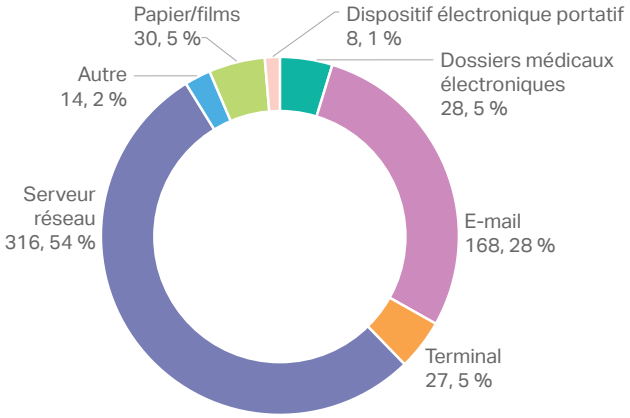
Les dix principales fuites de données de santé signalées en 2021 ont toutes été attribuées à un piratage abouti, la gravité étant mesurée par le nombre de sujets atteints. 90 % de ces fuites se sont produites sur les serveurs réseau des prestataires (Figure 4). Serveurs réseau et messages électroniques réunis totalisent 80 % des vecteurs d'attaque, impactant les traitements aigus, avec les graves conséquences que cela peut avoir.

Figure 4

Top dix des fuites de données de santé signalées aux États-Unis en 2021



Office américain des droits civils du département des services sociaux et de santé, surface d'attaque en 2021



Quatre risques de cybersécurité critiques pour la santé

Malgré les nombreux avantages des technologies, l'adoption de nouveaux dispositifs médicaux et les interconnexions entre différents systèmes de santé sont sources de risques multiples. Les organismes de soins de santé doivent faire face à quatre grands problèmes de cybersécurité propres au secteur :

1. Maintenir l'infrastructure vitale couverte et toujours disponible
2. Protéger la vie privée des patients contre les risques venant de l'intérieur
3. Préserver l'intégrité des données de santé
4. Prévenir les fuites de données provenant de ransomwares et attaques de phishing

Dans un contexte d'expansion des infrastructures vitales, il est impensable de négliger les investissements dans la sécurité. Toute lacune de cybersécurité, par exemple dans la gestion des patchs, la gestion de la configuration, des contrôles d'accès appropriés, le chiffrement des données et la sécurité des portails de patients mine la mission des établissements de santé, à savoir fournir des soins de qualité en temps utile, tout en protégeant la vie privée des patients. Tout échec de la protection des PHI selon les lois de protection des données et directives en vigueur peut avoir des conséquences graves pour les prestataires : fuite de données, interruption des soins, mauvais résultats thérapeutiques, perturbations au niveau de la facturation, perte financière, coûts de réparation, frais juridiques et de règlement, lourdes amendes, érosion de la confiance, réputation entachée, etc.

Conclusion

La pandémie perdurant, la situation des organismes de soins de santé reste tendue. Ils sont toujours en sous-effectifs et dépassés par la transformation technologique et numérique qu'ils doivent opérer pour mieux servir leurs patients. La pile de solutions de cybersécurité SonicWall pour le domaine de la santé est conçue pour faciliter cette transition et renforcer la sécurité des infrastructures de santé, afin d'assurer des soins plus efficaces, plus résilients et plus sécurisés. Cette pile de sécurité intégrée, à la gestion centralisée, englobe périphérie, centre de données, accès, sans-fil, messagerie et terminaux, permettant aux organismes de soins de santé d'accompagner efficacement les patients jusqu'au bout de leurs soins.

Lisez notre livre blanc « Une cybersécurité sans limites pour un secteur de la santé plus sûr » et apprenez comment les solutions de sécurité SonicWall pour la santé garantissent la disponibilité des infrastructures vitales, l'intégrité des dossiers médicaux électroniques et la confidentialité des informations personnelles sur la santé.

1 Source : « The Impact of Ransomware on Healthcare During COVID-19 and Beyond » par le Ponemon Institute.
2 Source : « The Impact of Ransomware on Healthcare During COVID-19 and Beyond » par le Ponemon Institute.
3 Source : HIPAA Journal « January 2022 Healthcare Data Breach Report », https://www.hipaajournal.com/january-2022-healthcare-data-breach-report/

À propos de SonicWall

SonicWall offre une solution de cybersécurité sans limites pour l'ère de l'hyper-distribution dans une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. SonicWall comble le fossé commercial en matière de cybersécurité pour les hôpitaux, les cliniques et les prestataires du monde entier en connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies. Pour plus d'informations, rendez-vous sur https://www.sonicwall.com/fr-fr/solutions/industry/healthcare/.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour de plus amples informations.
www.sonicwall.com

SONICWALL

ExecBrief-HealthcareCybersecurity-A4-JK-6455