Sécurisation des établissements de santé avec Proofpoint

Protection des personnes, des processus et des données des patients

Les cyberattaques ciblant le secteur de la santé ne cessent d'augmenter. Les données extrêmement sensibles des patients peuvent avoir une valeur monétaire élevée, ce qui fait des établissements de santé une cible privilégiée des cybercriminels. La pandémie de COVID-19 a rendu ce secteur encore plus vulnérable. Les médecins et le personnel non médical prodiguent désormais des soins aux patients à distance, ce qui accroît leur exposition aux cybermenaces. Proofpoint peut vous aider. Nos solutions de cybersécurité et de conformité protègent votre établissement, votre personnel et vos patients.

La télésanté et le télétravail sont des outils puissants permettant au personnel soignant de prodiguer des soins aux patients en toute facilité. Mais ces nouveaux modes de travail à distance ouvrent la voie à des cybermenaces qui pourraient mettre en péril les données médicales, perturber les soins prodigués aux patients ou fragiliser leur sécurité.

Les établissements de santé considèrent désormais la cybersécurité comme un objectif prioritaire. Mais, à l'instar de nombreuses entreprises des secteurs les plus divers, ils ont investi dans des outils de sécurité traditionnels qui protègent le périmètre réseau. Or ces outils sont incapables de détecter, et encore moins de bloquer, les menaces avancées qui mettent en péril les données de santé.

Par ailleurs, les menaces évoluent. À mesure que le secteur de la santé s'étend au-delà du périmètre réseau, les cybercriminels suivent le mouvement. De plus, les menaces ne se contentent pas de se déplacer : elles changent de forme et de cibles. Chaque personne au sein de votre établissement de santé représente un niveau de sécurité ou un risque de conformité différent, en fonction des données auxquelles elle a accès et de la façon dont elle utilise les technologies pour exercer son métier.

Les infirmiers ont davantage accès aux données des patients, ce qui en fait une cible de choix. Les médecins-chercheurs ont quant à eux accès à des éléments de propriété intellectuelle de valeur, ce qui accroît considérablement leur niveau de vulnérabilité. Le personnel hospitalier en poste au sein de la chaîne logistique interagit régulièrement avec différents systèmes tiers, ce qui augmente son exposition aux menaces. Les menaces telles que le phishing d'identifiants de connexion permettent non seulement aux cybercriminels de prendre le contrôle d'un compte de messagerie, mais aussi d'accéder à une profusion de données stockées dans le cloud, hors de portée des outils de sécurité traditionnels. Les soignants, les patients, les médecins et autres membres du personnel sont exposés à ce nouveau type d'attaques centrées sur les personnes.

Nous ne devons toutefois pas oublier que les établissements de santé demeurent des cibles de choix pour les ransomwares et autres attaques basées sur des malwares. Ces attaques, bien que moins nombreuses, sont désormais plus ciblées. Plus que jamais, les établissements doivent lutter contre ce type de menace en adoptant une approche qui allie technologies et formations.

Défis de cybersécurité dans le secteur de la santé

Dans leur quête d'approches innovantes pour prodiguer des soins tout en assurant leur protection, celle des médecins et celle des patients, les établissements de santé sont confrontés à de nouveaux défis. Les problèmes que attendent les responsables informatiques et de sécurité du secteur de la santé en 2021 et au cours des années à venir sont désormais bien plus complexes. De ce fait, il est plus difficile pour les établissements de santé de maintenir un environnement sécurisé pour la télésanté.

Adoption de nouveaux modèles de soins sécurisés

Le recours à la santé mobile, à la télémédecine et à l'Internet des objets a élargi la surface d'attaque. Les consommateurs utilisent un large éventail d'applications de santé mobile, de dispositifs médicaux portables et de technologies médicales à domicile. Les médecins apportent leurs terminaux personnels au travail et leurs appareils professionnels chez eux. En outre, les technologies émergentes et les frontières floues entre les paramètres cliniques et domestiques augmentent la complexité. Elles contribuent à la transition vers une infrastructure informatique décentralisée et sans périmètre, bien plus difficile à protéger.

Stockage et protection des données

Protéger la relation médecin-patient est primordial. Si les données ne sont pas stockées de façon sécurisée par les tiers ou ne sont pas chiffrées avant d'être envoyées, les informations des patients risquent d'être exposées. Alors que tous les établissements de santé déclarent collecter, stocker et partager des données sensibles, seuls 38 % d'entre eux les chiffrent[1].

Sécurité du cloud

Les établissements de santé ont conscience des nombreux avantages qu'offre le cloud, notamment l'utilisation d'applications normalisées, la mise en place de modèles de facturation à l'utilisation et la réduction des dépenses en capital. Compte tenu des risques encourus, ils ont tardé à adopter les services cloud, mais rattrapent maintenant leur retard. Face aux avantages évidents des offres cloud, les responsables de la sécurité du secteur de la santé cherchent des solutions permettant d'assurer la conformité et de préserver la confidentialité et l'intégrité des transactions, et pouvant être adaptées pour protéger les applications cloud de leurs associés et de leurs partenaires au sein de la chaîne logistique.

Parallèlement, de nombreux établissements de santé continuent à utiliser des systèmes d'ancienne génération en raison de la nature propriétaire de certains composants, ce qui les empêche de migrer vers des services cloud. Cette situation introduit des risques supplémentaires, car les cybercriminels exploitent de nouvelles vulnérabilités pour propager des malwares, notamment des ransomwares, qui peuvent mettre les établissements hors ligne.

Sécurité de la chaîne logistique

Les prestataires de santé font appel à un large éventail de fournisseurs externes, de partenaires et d'associés pour assurer leurs activités. Ces relations interdépendantes forment un écosystème tiers complexe et vulnérable au vol et aux cybermenaces émergentes. Elles constituent de nouveaux points d'entrée que les cybercriminels peuvent exploiter pour compromettre la chaîne logistique hospitalière. Plus que jamais, la sécurité d'un établissement de santé se mesure au maillon le plus faible de la chaîne. Lorsqu'un maillon faible de la chaîne logistique d'un hôpital est compromis, puis utilisé pour extraire des données sensibles, les conséquences peuvent être dramatiques.

Évolution du paysage des cybermenaces dans le secteur de la santé

La croissance du marché des informations médicales fait des établissements de santé une cible attrayante. Vous devez adopter une approche défensive et supposer que le secteur est ciblé par des menaces telles que le piratage et les attaques menées par des États. Les virus et les malwares simples ne sont plus qu'un vestige d'une époque révolue. Les cyberattaques les plus dévastatrices sont centrées sur les personnes et menées par des pirates ayant repéré des points d'entrée stratégiques au fil du temps, qui, ensemble, peuvent provoquer des dégâts considérables. Selon un rapport, ce sont les établissements de santé qui mettent le plus de temps à détecter une compromission de données, avec une moyenne de 329 jours[2].

1 « 2019 Thales Data Threat Report »
(Rapport 2019 de Thales sur les menaces ciblant les données)

2 Ponemon Institute, « 2020 Cost of a Data Breach Report »
(Rapport 2020 sur le coût des compromissions de données) d'IBM Security

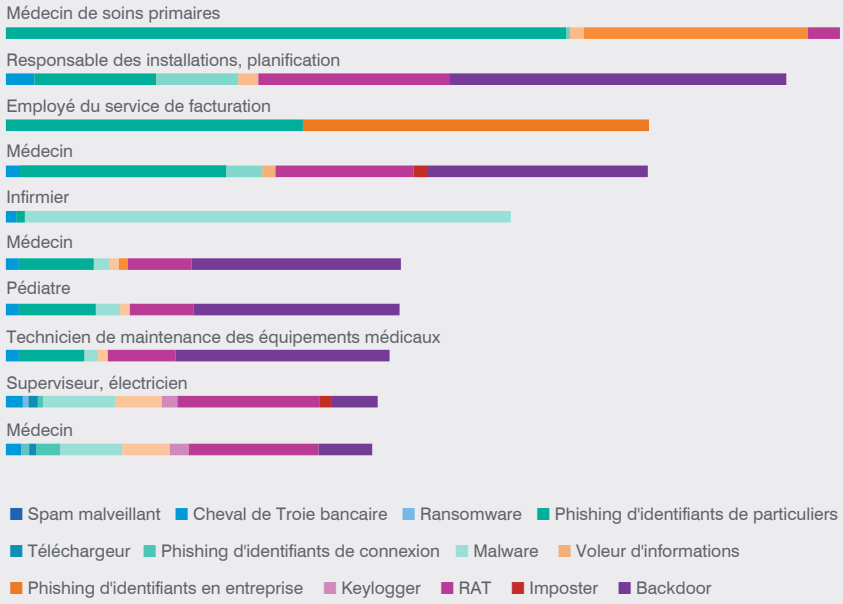

Figure 1. Répartition des VAP au sein d'un prestigieux hôpital pour enfants

Adoption d'une approche centrée sur les personnes

Les cyberattaques d'aujourd'hui ciblent les personnes, pas les technologies. C'est pourquoi les établissements de santé doivent adopter une approche centrée sur les personnes de la protection de leurs collaborateurs médicaux et non médicaux, ainsi que des données sensibles qu'ils utilisent et partagent. La mission des établissements de santé consiste à prodiguer des soins optimaux aux patients, souvent dans des délais courts, ce qui ne leur laisse pas le temps de réfléchir à la légitimité de chaque email. C'est l'une des raisons pour lesquelles le secteur demeure une proie facile pour les cybercriminels. Qui plus est, les gains potentiels en cas de succès de l'attaque sont élevés.

Les établissements de santé sont également tenus de respecter les exigences strictes du règlement général sur la protection des données (RGPD) de l'Union européenne, en particulier dans la mesure où ils traitent et stockent des données génétiques, biométriques et médicales (toutes les catégories de données considérées comme sensibles), pour lesquelles des niveaux de contrôle supérieurs doivent être appliqués. Les établissements doivent mettre en œuvre des contrôles de sécurité appropriés pour protéger ces données, non seulement pour éviter tout risque d'amende, mais aussi pour préserver la vie privée des patients.

Notre rapport 2020 sur le paysage des menaces dans le secteur de la santé s'intéresse à ce que nous appelons les VAP (Very Attacked People™, ou personnes très attaquées) de ce secteur. Nous employons ce terme pour désigner les utilisateurs les plus ciblés par les cybermenaces au sein d'une entreprise. La figure 1 propose un exemple concret.

Hôpital pour enfants

Dans cet exemple, les médecins occupent le poste le plus attaqué. Les problèmes de confidentialité sont d'autant plus importants que les enfants sont une cible de choix pour l'usurpation d'identité. Le dossier médical d'un mineur se vend à prix d'or sur le Dark Web ou le marché clandestin. La plupart des enfants n'ont pas d'antécédents bancaires et n'auront pas encore introduit de demande de prêt ou de carte de crédit au moment de la compromission. Il n'a pas échappé aux cybercriminels que la plupart des gens ne vérifient pas si leurs données sont exploitées à des fins frauduleuses. Par ailleurs, le nombre de portes dérobées (backdoor) est plus élevé dans les départements de gestion des installations, où les contrôles de sécurité sont souvent moins pointus.

Ces environnements emploient généralement des ressources permissives, telles que des terminaux IoT et des systèmes de filtration d'air. Ils font souvent office de vecteurs d'attaque pour infiltrer le réseau d'entreprise.

Scénarios d'utilisation dans le secteur de la santé

Sécurité distribuée

La santé englobe un large éventail d'établissements et d'environnements informatiques qui partagent des informations entre les patients et les médecins pour migrer vers un modèle de soins connectés ou centrés sur les patients. Les emails sont une méthode prisée pour distribuer des informations confidentielles, et une grande majorité des compromissions de données de grande envergure ciblant les établissements de santé commencent par des attaques de phishing ciblées.

Proofpoint propose des solutions adaptées au secteur de la santé afin de protéger les utilisateurs dans le contexte actuel :

- **Proofpoint Email Protection** est une solution performante de protection de la messagerie permettant de bloquer les malwares et autres menaces.
- **Proofpoint Data Loss Prevention (DLP)** limite le risque de fuites de données via la messagerie et vous met à l'abri de la fraude par email.
- **Proofpoint Targeted Attack Protection (TAP)** intègre des fonctionnalités de sandboxing permettant de détecter et de bloquer les menaces avancées.
- **Proofpoint Threat Response** permet aux établissements d'intervenir rapidement afin de neutraliser les menaces et de supprimer les emails malveillants.
- Le programme **Proofpoint Security Awareness Training** propose des formations permettant aux collaborateurs d'apprendre à identifier les attaques d'ingénierie sociale ciblant le secteur de la santé, notamment les techniques de phishing sophistiquées.

Protection contre les attaques d'imposteurs

Les emails d'imposteurs sont des messages frauduleux conçus pour se faire passer pour une personne que le destinataire connaît ou en qui il peut avoir confiance. Ces attaques peuvent être difficiles à détecter, car elles n'exploitent pas de vulnérabilités techniques. Elles ciblent des postes spécifiques, dont les activités sont propices à la monétisation, telles que les pharmaciens, les médecins-chercheurs, les employés de la chaîne logistique et le personnel hospitalier de base.

Proofpoint offre une solution de bout en bout, intégrée et centrée sur les personnes qui bloque la fraude par email sous toutes ses formes, quelle que soit la tactique employée ou la personne ciblée :

- La solution de **sécurité avancée de la messagerie** de Proofpoint bloque le phishing et les emails d'imposteurs qui utilisent des noms de domaine similaires et usurpés. Elle s'appuie sur un système d'apprentissage automatique avancé et plusieurs moteurs de détection pour identifier ces attaques ciblées et les bloquer avant qu'elles n'atteignent la boîte de réception des utilisateurs.
- Le protocole **DMARC (Domain-based Message Authentication Reporting and Conformance)** est déployé pour faciliter l'authentification des emails. Il bloque les emails usurpés avant que les collaborateurs, le personnel médical et les associés soient victimes d'une escroquerie.

Sécurisation de Microsoft 365 et d'autres environnements cloud

Une solution CASB (Cloud Access Security Broker) constitue un élément essentiel de toute architecture de sécurité cloud. De plus en plus d'établissements de santé migrent leurs données et applications vers le cloud et accèdent à des données sensibles toujours plus nombreuses via une connexion Internet. Ils ont besoin d'une visibilité sur les activités dans le cloud à l'échelle de l'écosystème de santé et de la chaîne logistique.

Proofpoint CASB aide les établissements à analyser et à neutraliser rapidement les violations potentielles des règles de messagerie dans le cloud afin d'assurer la continuité des soins. Il réduit les risques de cyberattaque ou de compromission de données. Il s'appuie sur le flux d'emails d'une entreprise pour identifier les données confidentielles au sein des services d'hébergement de fichiers dans le cloud, notamment Microsoft 365, Dropbox, Box et Salesforce.

Sécurisation de la collaboration dans le domaine des soins

Pour prodiguer des soins optimaux, le personnel soignant a besoin de pouvoir collaborer et communiquer efficacement. À cette fin, il dispose de solutions mobiles qui mettent en relation médecins et patients. Mais celles-ci sont conçues pour être fonctionnelles et pratiques plutôt que sécurisées. De plus, elles sont souvent utilisées en dehors du réseau d'entreprise protégé.

Les médecins peuvent accéder aux applications médicales à partir de leurs terminaux personnels. De même, ils peuvent utiliser leurs comptes de messagerie personnels sur les appareils fournis par l'établissement. **Proofpoint Browser Isolation** maintient les contenus dangereux et les activités personnelles des utilisateurs à l'écart de votre environnement.

Pour cela, il isole le webmail et les URL figurant dans les emails au sein d'un conteneur protégé. Les utilisateurs peuvent accéder librement et en toute confidentialité à leurs comptes personnels via leur navigateur Web habituel. Toutefois, les actions et les contenus potentiellement dangereux sont désactivés afin de préserver la sécurité de votre environnement.

Protection contre les menaces internes

Un utilisateur interne exfiltrant des données de patients dans le cabinet d'un médecin ou dans un hôpital est une scène digne d'une série TV. Pourtant, les menaces internes sont bien réelles. En réalité, près de la moitié des compromissions dans le secteur de la santé impliquent un utilisateur interne[3].

Voici trois des menaces internes les plus courantes au sein des établissements de santé :

1. Vol ou utilisation abusive de données médicales protégées
2. Vol ou utilisation abusive de dossiers médicaux électroniques
3. Fraude financière et aux assurances

Proofpoint Insider Threat Management (ITM) assure une protection contre les fuites de données, les actes malveillants et les atteintes à la marque dus à la malveillance, à la négligence ou au manque de connaissances des utilisateurs internes. Notre solution ITM met en corrélation les activités et les mouvements de données, de façon à permettre aux équipes de sécurité d'identifier les risques liés aux utilisateurs, de détecter et de contrer les compromissions de données induites par des utilisateurs internes, ainsi que d'accélérer la réponse aux incidents de sécurité.

3 Verizon, « 2020 Data Breach Investigations Report » (Rapport d'enquête 2020 sur les compromissions de données)

Protection des données médicales personnelles : sécurisation des données des patients

Dans le secteur de la santé, la messagerie électronique constitue le premier vecteur de menaces. Il est donc essentiel de disposer d'une solution de prévention des fuites de données (DLP) adaptée pour garantir que les informations sensibles et critiques sont classées et consultées par les personnes autorisées.

Grâce à la solution **DLP centrée sur les personnes de Proofpoint**, les établissements de santé peuvent identifier et neutraliser rapidement les risques liés à la malveillance, à la négligence ou à la compromission des utilisateurs. La plate-forme unifiée de Proofpoint permet aux clients de définir les données de valeur et de tirer parti de ces définitions dans tout l'environnement, puis de protéger la confidentialité de chaque email grâce à **Proofpoint Email Encryption**. Les utilisateurs peuvent activer automatiquement le chiffrement des messages en ajoutant un mot clé de leur choix à la ligne d'objet, ou déclencher le chiffrement au niveau du message en fonction de règles DLP.

Le gestionnaire d'incidents unifié de Proofpoint permet non seulement de visualiser les infractions aux règles DLP au niveau de la messagerie électronique, du cloud et des endpoints à partir d'un emplacement centralisé, mais aussi de bénéficier d'informations approfondies sur le contexte et les menaces en combinant ces données.

Gestion des normes de conformité réglementaire et réduction de la complexité

De nombreux établissements réglementés éprouvent des difficultés à :

- identifier les canaux de communication utilisés ;
- s'assurer que le contenu que ces communications génèrent est capturé et archivé en toute sécurité ;
- rechercher et récupérer le contenu pour les audits rapidement et à moindre coût ;
- surveiller et superviser les collaborateurs qui utilisent ces canaux.

La solution d'**archivage et de conformité de Proofpoint** offre une conformité tout-en-un centrée sur les personnes.

Vous bénéficiez des avantages suivants :

- Vous êtes couvert dès le moment où le contenu est distribué, et jusqu'à son indexation, son archivage et sa récupération.
- Vos politiques réglementaires sont appliquées automatiquement, notamment les réglementations locales en matière de santé et les règles liées au RGPD.
- Vous avez l'assurance que vos efforts d'interaction numérique sont conformes aux règles de communication et de conservation.
- Vous pouvez superviser, corriger (réviser ou supprimer) et archiver du contenu facilement, rapidement et à moindre coût.

Conclusion

Proofpoint offre aux établissements de santé visibilité et protection pour leur principal risque de cybersécurité : leurs collaborateurs. Nous proposons la cybersécurité la plus efficace pour protéger les professionnels de la santé, qu'ils soient ciblés via la messagerie électronique, le Web, les réseaux sociaux ou les applications cloud. Nous aidons les établissements de santé à bloquer les menaces avant qu'elles n'atteignent le personnel médical et de support, à sécuriser les données et à protéger les patients des cyberattaques. Des établissements de santé de toutes tailles font confiance à Proofpoint pour prévenir, détecter et neutraliser les menaces critiques avant qu'elles ne provoquent le moindre dégât.

EN SAVOIR PLUS

Pour découvrir comment nous pouvons vous aider à adopter une approche centrée sur les personnes de la protection de vos données, de vos opérations et de vos soins, consultez la page **proofpoint.com/us/solutions/healthcare-information-security**.