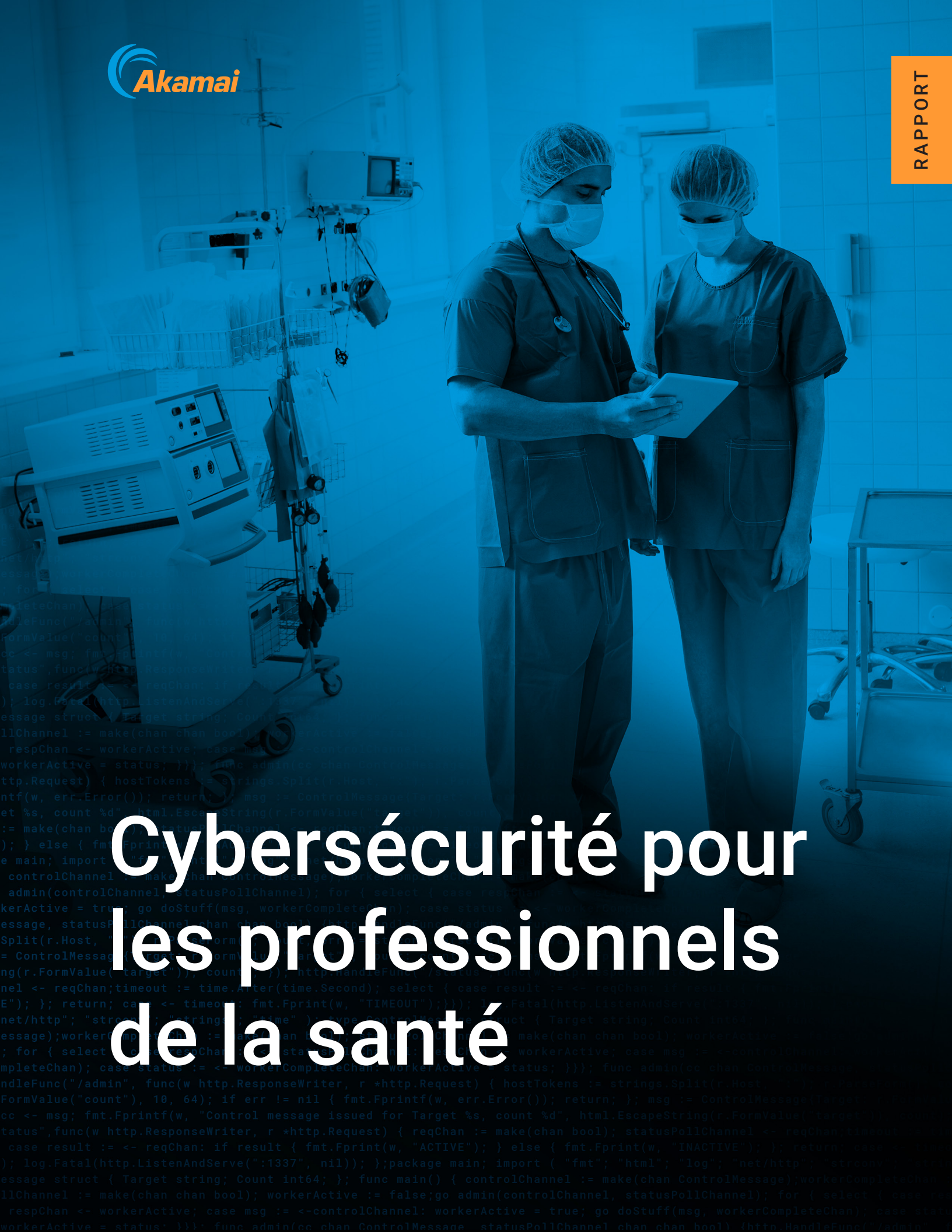


RAPPORT

Cybersécurité pour les professionnels de la santé

Introduction

Pour être compétitifs sur un marché en constante évolution, les professionnels de la santé adoptent de nouveaux terminaux et de nouvelles applications afin d'offrir des soins et des expériences de qualité aux patients. Chaque nouvel ajout apporte ses propres avantages aux patients et ses propres risques de sécurité pour l'organisation.

Cet environnement informatique complexe, associé à la valeur élevée des informations médicales protégées (PHI), crée une opportunité irrésistible pour les cybercriminels, qui s'attaquent sans relâche aux systèmes. Selon un rapport du Département américain de la santé et des services sociaux et une étude d'IBM, le secteur de la santé a enregistré une augmentation de 50 % des cyberattaques depuis le début de la pandémie. De plus, ces attaques ont été les plus coûteuses, avec un coût moyen de 7,13 millions de dollars par incident. Ce rapport d'IBM souligne que les attaques par ransomware constituent la menace la plus courante. Les cybercriminels profitent en effet de la nécessité de restaurer rapidement les systèmes hospitaliers et de santé, le vol de données et l'accès aux serveurs venant ensuite. Les professionnels de la santé, en particulier, sont des cibles de choix pour les attaques par ransomware, car les dossiers de santé électroniques (DSE) peuvent se vendre pour 1 000 dollars pièce sur le Dark Web, alors que les informations de cartes de crédit se vendent à environ 110 dollars et les numéros de sécurité sociale à seulement 1 dollar pièce.

Face au nombre croissant de menaces qui pèsent sur leurs systèmes, de nombreuses organisations ne sont pas suffisamment préparées à gérer ce risque. Pire, certaines ont déjà été infiltrées sans le savoir. Les acteurs malveillants sont peut-être déjà en train d'exfiltrer des données ou d'attendre le bon moment pour frapper.

Il est temps de déterminer clairement la surface d'attaque de votre organisation en dressant la liste des terminaux et en analysant la manière dont ils se connectent à votre infrastructure. Avec une meilleure connaissance des points de vulnérabilité, la mise en place d'un plan d'atténuation solide permettra de prévenir ou de minimiser l'impact potentiel des cyberattaques.

Comment faire face aux plus grands risques de cybersécurité pour votre organisation

Menace n° 1 : les attaques par hameçonnage

L'hameçonnage est l'un des vecteurs de cyberattaque les plus courants, tous secteurs confondus. Selon le Health Sector Cybersecurity Coordination Center, l'année 2021 a été marquée par une augmentation significative des attaques par hameçonnage dans le secteur de la santé. Tout au long de l'année 2020, Akamai a vu les criminels exploiter la COVID-19 et la promesse d'une aide financière, ainsi que le stress lié aux difficultés financières, pour cibler des personnes dans le monde entier via des attaques par hameçonnage.

L'hameçonnage vise à acquérir des données sensibles à l'aide de pages Web ou d'e-mails frauduleux. En cas de succès, il incite l'utilisateur à saisir par inadvertance ses identifiants de connexion, ce qui permet aux malfaiteurs d'accéder au réseau.

C'est ce qui est arrivé aux personnes qui ont déposé une demande d'assurance-chômage à New York. Selon un rapport sur les attaques par hameçonnage de Steve Ragan, ancien rédacteur en chef de CSO Online et désormais chercheur en sécurité chez Akamai, plusieurs kits d'hameçonnage ont ciblé les programmes d'assistance chômage relative à la pandémie (PUA) au début de 2021. Ces programmes ont été conçus pour aider les personnes dans le besoin pendant les confinements liés à la COVID-19 et ont fourni des services essentiels à des millions d'Américains.

Dans un reportage diffusé sur CBS News dans tout le pays, M. Ragan a évoqué un kit d'hameçonnage ciblant les chômeurs de New York et la manière dont les criminels collectaient et vendaient les informations personnelles compromises dans le cadre de cette escroquerie. Depuis la diffusion de ce reportage, il a découvert des escroqueries à l'assistance chômage relative à la pandémie (PUA) ciblant des personnes dans le Wisconsin, l'Indiana, la Pennsylvanie et le Massachusetts.

Comment arrêter et atténuer les attaques par hameçonnage

En fonction des paramètres d'autorisation et des mesures de sécurité en place, l'accès à un seul compte d'utilisateur peut potentiellement permettre aux criminels d'accéder librement à des parties critiques de votre réseau, voire même d'étendre leur emprise après avoir infiltré le réseau de votre organisation.

La microsegmentation limite l'accès des acteurs malveillants à la seule partie de votre réseau à laquelle ils ont initialement accès, ce qui empêche tout déplacement latéral et les rend incapables d'infliger des dommages supplémentaires dans d'autres zones. Elle limite l'impact d'une compromission en empêchant les criminels d'utiliser n'importe quel point d'entrée pour accéder à l'ensemble du réseau de votre organisation.

Outre la microsegmentation, l'authentification multifactoreille (MFA) est l'une des meilleures manières de se protéger contre les attaques par hameçonnage. Elle fournit une couche supplémentaire de protection en exigeant une vérification supplémentaire de l'identité avant d'autoriser l'accès à un compte, empêchant ainsi l'exploitation d'informations d'identification compromises.

La MFA, en particulier une solution approuvée par FIDO2, garantit une protection contre les dernières attaques et exige des utilisateurs qu'ils saisissent un code unique transmis via un SMS ou une application d'authentification sur le terminal mobile de l'utilisateur. Cette étape de connexion supplémentaire permet de déjouer les attaques par hameçonnage, même lorsque les criminels disposent d'identifiants de connexion valides.

Il est essentiel de former votre personnel aux tactiques d'ingénierie sociale telles que l'hameçonnage. En réalité, l'hameçonnage est l'un des problèmes pour lesquels il n'existe pas de solution miracle, en raison de son grand nombre de variables. Il est difficile de prédire les prochaines actions des criminels. L'être humain étant la clé de l'hameçonnage, il reste le maillon faible de la chaîne.

Il est donc essentiel de simplifier la sécurité. Akamai propose une solution MFA anti-hameçonnage simple pour vous protéger contre les cybercriminels les plus rusés.

Menace n° 2 : anciens logiciels non pris en charge

Les logiciels obsolètes constituent un autre problème de vulnérabilité important. Chaque nouvelle mise à jour de sécurité (correctif) qui n'est pas immédiatement installée crée des portes ouvertes sur votre réseau. C'est particulièrement vrai pour les terminaux anciens qui ne sont plus pris en charge et ne reçoivent plus de mises à jour.

Les logiciels non pris en charge peuvent présenter des vulnérabilités Zero Day que les entreprises hésitent à corriger elles-mêmes. La création d'un correctif personnalisé peut parfois annuler la garantie d'un terminal et entraîner des réparations coûteuses en cas de problème.

Bien que les terminaux médicaux aient un long cycle de vie, s'ils n'exécutent pas la dernière version du système d'exploitation ou utilisent un système d'exploitation non pris en charge, les pirates peuvent exploiter leurs vulnérabilités pour voler des données, infiltrer le réseau d'un hôpital et perturber les soins. Selon Fortune, jusqu'à 83 % des terminaux d'imagerie médicale connectés à Internet, des mammographes aux terminaux IRM, sont vulnérables.

Plus un terminal est ancien (notamment si son cycle de maintenance est dépassé), plus les criminels sont susceptibles de connaître les points faibles qui leur permettront d'accéder au réseau de votre organisation par l'intermédiaire d'un terminal tiers.

Par exemple, Windows 95 ne reçoit plus de mises à jour depuis des années, et pourtant de nombreux terminaux IRM (entre autres) utilisent encore ce système d'exploitation, car il a été le dernier à permettre l'écriture directe. Les développeurs internes peuvent corriger une vulnérabilité, mais leur correctif risque d'annuler la garantie du terminal. La seule option sûre consiste à remplacer entièrement le terminal d'IRM, mais de nombreux établissements ne peuvent assumer ce coût.

Les administrateurs réseau tentent d'exclure du réseau les systèmes non pris en charge, mais cela n'est pas toujours possible, surtout lorsque les terminaux sont nécessaires aux soins des patients et doivent fournir rapidement des données aux médecins. L'isolement échoue également lorsque la carte des terminaux connectés au réseau est incomplète, ce qui crée des portes dérobées. Il est difficile de protéger ce qui n'est pas visible.

Comment protéger les terminaux vulnérables non pris en charge

Pour empêcher ces terminaux d'accéder au réseau de votre entreprise, il est essentiel d'adopter une architecture ZTNA (Zero Trust Network Access). ZTNA est un cadre qui traite chaque requête entrante comme une menace potentielle jusqu'à ce que sa sécurité soit prouvée, ce qui permet d'arrêter les attaquants avant qu'ils n'accèdent au terminal, même si votre logiciel n'est plus à jour.

Le passage à l'architecture ZTNA marque un changement fondamental par rapport à l'approche de type « château fort » des années passées, au profit d'un modèle Zero Trust (« Vérifier, puis faire confiance »). Bien qu'une approche Zero Trust ne protège pas à 100 % contre les cyberattaques, elle limite les dommages potentiels. C'est HealthITSecurity qui le dit le mieux : « Si un acteur malveillant parvient à obtenir des informations d'identification et à manipuler un terminal, il est peu probable qu'il aille beaucoup plus loin en présence d'une architecture Zero Trust ».

Akamai propose un plan efficace pour aider les professionnels à adopter une architecture Zero Trust, sans subir de temps d'arrêt ni compromettre la flexibilité des flux de travail actuels. Découvrez l'architecture ZTNA avec ce guide de référence.

Menace n° 3 : professionnels travaillant à domicile et BYOD

Au XXIe siècle, la continuité des soins est décentralisée. Les patients reçoivent des soins confortablement installés chez eux. Les professionnels prodiguent des soins via leur terminal mobile plutôt qu'en personne. Cependant, cette accessibilité accrue se traduit par une augmentation spectaculaire des risques de cybersécurité pour les professionnels, car les membres du personnel alternent entre l'accès au réseau sur site et à domicile, et se connectent à l'aide de terminaux non gérés.

Bien que les membres de votre équipe aient pu se connecter occasionnellement à votre système depuis leur domicile avant la pandémie, le nombre de terminaux personnels accédant au réseau de votre organisation a inévitablement augmenté au cours de cette période. Si ces ordinateurs portables, tablettes ou smartphones étaient infectés par des logiciels malveillants, ils pourraient devenir la porte d'entrée d'une attaque par ransomware.

Par exemple, si un membre de votre équipe est victime d'une attaque par hameçonnage en saisissant accidentellement ses identifiants de connexion sur une fausse page Web, les acteurs malveillants auront le même accès que l'utilisateur, ce qui leur permettra potentiellement de chiffrer des fichiers, de bloquer votre équipe et de paralyser votre établissement en exigeant une forte rançon pour décrypter les fichiers.

Comment protéger la bordure de votre réseau

En surveillant de près les personnes qui accèdent au réseau de votre organisation (emplacement de connexion, adresse IP, terminal utilisé, etc.), vous pouvez minimiser la probabilité qu'une telle situation se produise et arrêter une attaque avant qu'elle n'ait lieu.

Si votre équipe utilise des terminaux personnels ou travaille à domicile, posez-vous les questions suivantes :

- Avons-nous mis en place une approche ZTNA (Zero Trust Network Access) pour optimiser la surveillance des requêtes entrantes et arrêter une attaque avant qu'elle ne se produise ?
- Avons-nous mis en place une microsegmentation pour limiter l'accès et empêcher les mouvements latéraux si un criminel s'introduit dans le réseau de l'organisation ?
- Utilisons-nous un framework SASE (Secure Access Service Edge) pour protéger notre réseau tout en minimisant la latence et en proposant une expérience rapide et agréable pour l'utilisateur ?
- Notre équipe utilise-t-elle des codes d'accès, des mots de passe forts et uniques, ainsi qu'une authentification multifactorielle (MFA) pour chaque terminal et chaque connexion de compte ?

Akamai facilite la gestion de l'accès au réseau grâce à ses solutions de sécurité pour le personnel à distance.

Menace n° 4 : mauvaise cartographie des flux de données

Avec un pied sur site et l'autre dans le cloud, il est quasiment impossible de déterminer où se trouvent vos données et la manière dont elles circulent. Il y a plusieurs raisons à cela.

Tout d'abord, le volume. Il peut être difficile de suivre le nombre de terminaux et d'applications ajoutés et retirés de votre réseau tous les jours, voire toutes les heures, car les prestataires, les sous-traitants et les consultants semblent tous utiliser des terminaux, des solutions et des outils différents.

Ensuite, votre système de suivi du matériel et des logiciels est peut-être devenu obsolète et n'est plus précis ou fiable en raison de la rotation des membres de l'équipe, des changements de processus ou de priorités divergentes.

Quelle que soit la raison, il est important de visualiser votre réseau et vos terminaux connectés, car on ne peut pas protéger ce que l'on ne voit pas.

Comment cartographier le flux de vos terminaux connectés

Il est crucial de disposer d'un outil de visualisation capable de créer une feuille de route des terminaux connectés. D'autant plus qu'un article de 2019 du HIPAA Journal indique que 82 % des organismes de santé ont subi une cyberattaque sur leurs terminaux connectés au cours des 12 mois précédents.

Pour cartographier vos terminaux connectés, la première étape consiste à choisir une solution qui suit les flux de données sur votre réseau et indique leur provenance et leur destination, y compris les terminaux qui ne sont pas connectés au réseau. Vous disposez ainsi d'un schéma du réseau en temps réel indiquant où circulent les informations, ce qui vous permet de détecter les terminaux malveillants susceptibles de se trouver sur votre réseau. En plaçant des anneaux de microsegmentation définis par logiciel autour des systèmes centraux, des actifs et des données (comme les informations médicales protégées), votre organisation peut limiter les mouvements latéraux des attaquants au sein du réseau. Obtenez la visibilité dont vous avez besoin grâce aux outils de microsegmentation d'Akamai.

Menace n° 5 : gestion de la complexité des réseaux, des applications et des systèmes

Savez-vous quelles applications et quels logiciels peuvent lire vos données ? Certaines applications logicielles, comme les plateformes multimédias, indiquent clairement leur caractère invasif dans leur déclaration de confidentialité ou leurs conditions d'utilisation. D'autres, comme les fournisseurs de messagerie électronique, sont plus discrets, mais présentent néanmoins un risque important (par exemple, l'accès aux photos d'un terminal lorsque les photos contiennent des informations médicales protégées).

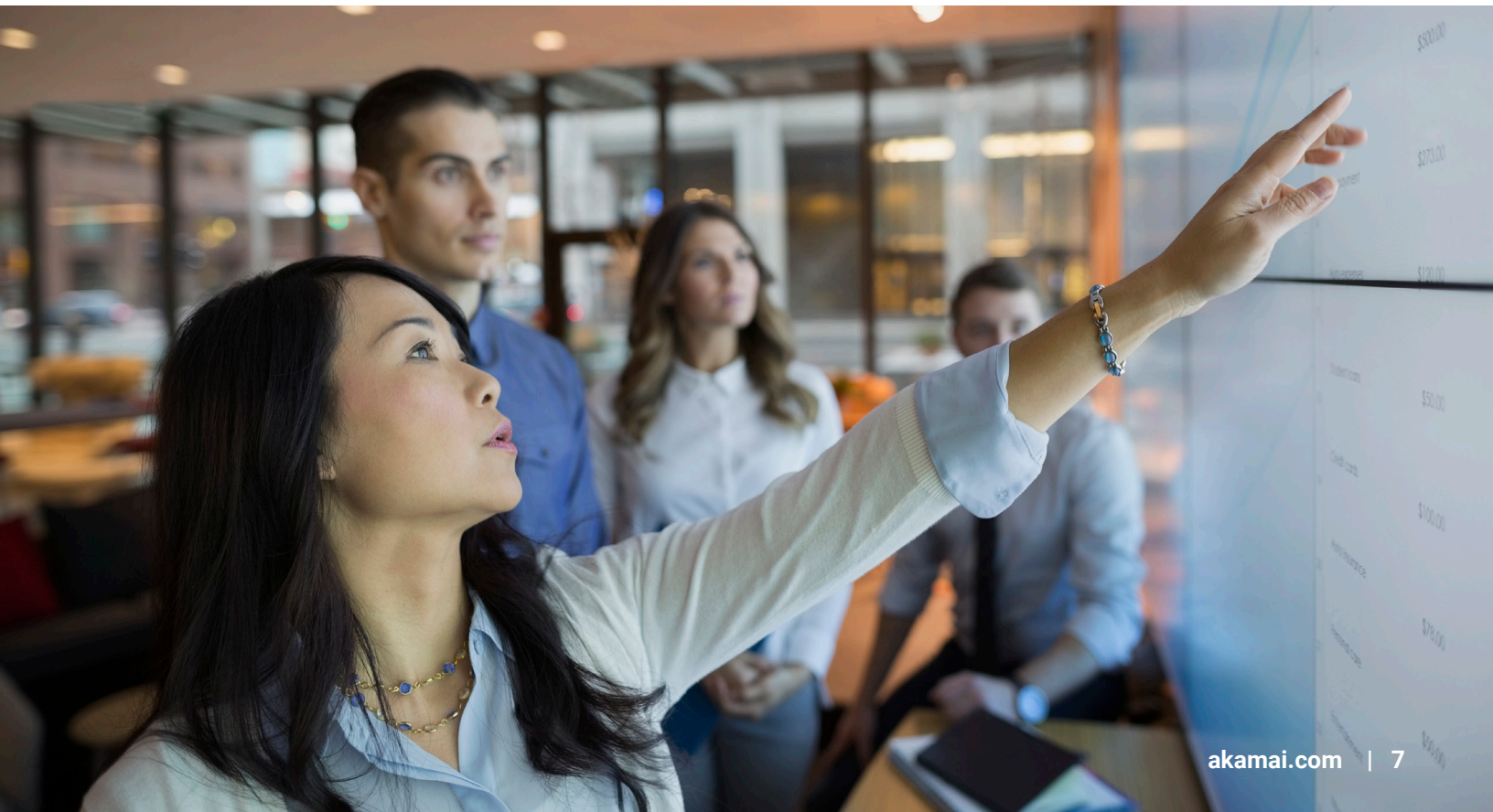
Les applications peuvent également être autorisées à visualiser les éléments copiés dans le presse-papiers, y compris les identifiants ou les mots de passe des patients. Si des informations sur un patient sont stockées sur un terminal, il y a un risque qu'un tiers (ou un acteur malveillant) y accède (et les enregistre).

Sensibilisez votre équipe, surveillez l'ensemble de votre réseau, protégez votre périphérie

Vous devez impérativement informer tous les membres de votre organisation des risques liés à l'utilisation de terminaux personnels et des mesures à prendre pour protéger les informations confidentielles des patients.

Vous devez également tenir compte de la vision qu'a votre organisation de votre surface d'attaque et des vecteurs potentiels. Votre équipe de sécurité surveille-t-elle l'ensemble du réseau à travers plusieurs fournisseurs de services cloud et centres de données sur site ? Ou est-elle divisée en plusieurs groupes qui se concentrent sur différents aspects de l'infrastructure de votre organisation ? Il est indispensable d'avoir une vue d'ensemble du réseau de votre organisation et de son activité, en particulier lors d'une attaque.

Comme pour la menace n° 4, les meilleures solutions pour protéger la bordure de votre réseau sont l'architecture Zero Trust combinée à la microsegmentation et à la MFA pour les connexions aux comptes. Le recours à un fournisseur unique pour protéger tous les systèmes dans le cloud ou sur site, indépendamment de leur propriétaire, vous permettra de protéger votre réseau sans entraver l'expérience de l'utilisateur.



Quel est le coût de l'inaction ?

Les coûts peuvent prendre de nombreuses formes. La plus évidente est d'ordre financier : selon le rapport d'IBM sur le coût d'une violation de données en 2021, le coût total d'une seule violation de données s'élevait en moyenne à 9,23 millions de dollars pour les entreprises du secteur de la santé américaines. D'autres coûts sont plus qualitatifs, comme la sécurité et la confiance des patients, qui peuvent avoir un impact égal, voire supérieur, sur les organismes de santé.

Réduction de la sécurité des patients

La sécurité des patients est un objectif essentiel de la cybersécurité. Lorsque les systèmes informatiques sont contraints de s'arrêter à la suite d'une attaque, les soins aux patients sont perturbés. Les traitements et les rendez-vous sont reportés et peuvent avoir des conséquences néfastes sur la santé des patients. Un procès récent a marqué la toute première allégation de décès d'un patient découlant directement d'une attaque par ransomware.

Par ailleurs, les terminaux médicaux connectés utilisés pour la surveillance à distance des patients (ex. : rythme cardiaque ou glycémie) font planer une menace plus directe sur les soins. Par exemple, la perturbation des relevés de tension artérielle d'un patient pourrait empêcher la détection et le traitement de maladies graves, ce qui pourrait entraîner un « événement sentinelle ».

Perte de confiance des patients

L'incapacité à fournir des soins fiables et à protéger les informations des patients entraîne une perte de confiance de ces derniers. Plus de 90 % des patients se disent prêts à changer de professionnel de santé si leurs informations privées étaient compromises par une violation de données. Le chiffre réel pourrait être inférieur le moment venu, mais faites le calcul : Si la moitié seulement de ces patients, ou un dixième d'entre eux, quittaient l'établissement, quel serait l'impact sur votre patientèle ? Et pendant combien de temps subiriez-vous des pertes continues tout en acquérant progressivement de nouveaux patients ?

Perte de revenus

À 38 %, la perte d'activité est le facteur de coût le plus important d'une violation de données. Lorsque les systèmes de base des prestataires tombent en panne (comme les DSE, les serveurs de messagerie, etc.), les nouvelles activités s'interrompent brutalement. Cela signifie qu'il n'y a pas de rendez-vous, pas de visites, pas de rencontres et pas de revenus (sans parler de l'impact sur les soins prodigués aux patients).

Scripps Health, une clinique basée à San Diego, a subi une cyberattaque majeure en mai 2020 qui a entraîné une perte de revenus de 91,6 millions de dollars, principalement en raison de la réduction du volume des soins d'urgence et des opérations non urgentes.

Même si certaines parties du réseau du système de santé sont encore opérationnelles, vous ne pouvez pas être certain que tout est sûr tant que vous n'avez pas localisé le vecteur, corrigé la vulnérabilité et terminé l'enquête.

Augmentation des frais généraux

Le recrutement, l'embauche et la fidélisation d'ingénieurs en cybersécurité tant convoités coûtent cher, mais les coûts réels vont bien au-delà. La gestion d'une équipe de cybersécurité en interne peut entraîner une couverture insuffisante et des coûts importants.

D'une manière générale, plus il faut de temps à votre organisation pour identifier et exfiltrer un acteur malveillant de votre réseau, plus les coûts sont élevés. Un rapport du Ponemon Institute indique que la détection d'une cyberattaque dans les 200 premiers jours permet à une entreprise d'économiser plus de 1,26 million de dollars. Malheureusement, selon ce même rapport, il faut en moyenne 287 jours pour identifier et contenir une attaque. *287 jours !* Cela signifie que les acteurs malveillants infiltrent souvent l'infrastructure du réseau pendant plus de neuf mois, préparant et planifiant leur attaque afin d'infliger un maximum de dommages à la réputation et au chiffre d'affaires de votre hôpital.

Il est essentiel de quantifier le temps dont votre équipe de sécurité a besoin pour identifier une attaque et prendre des mesures pour la contrer. Le regroupement des fournisseurs de solutions de sécurité avec ceux qui proposent des services gérés et une assistance technique en cas de pic d'activité peut vous permettre de réaliser d'importantes économies.

Amendes réglementaires

Si vous gérez une grande quantité d'informations personnelles précieuses, une violation de données peut entraîner de lourdes amendes de la part des organismes de réglementation. Au 30 novembre 2021, le Bureau des droits civils du Département de la santé et des services sociaux avait négocié ou imposé des amendes à 106 entités couvertes par la loi HIPAA pour un montant total de plus de 131 millions de dollars. Cela représente une moyenne de plus d'1,2 million de dollars par amende (en plus des coûts supplémentaires mentionnés ici).

Comment préparer au mieux votre organisme de soins à une cyberattaque

Les cybermenaces actuelles obligent les organismes de santé à disposer d'une sécurité de pointe. Vos patients et votre entreprise en dépendent. Le coût de l'inaction est trop élevé.

Les contraintes financières, les priorités divergentes ou l'incertitude à l'égard des risques peuvent vous inciter à prendre des risques inconsidérés. Votre politique en matière de sécurité doit être exhaustive, stratégique, rigoureuse et souple.

Un écosystème correctement protégé aujourd'hui ne le sera pas nécessairement demain. Les menaces évoluent rapidement. Il suffit parfois d'un jour (ou moins) pour que les acteurs malveillants exploitent une nouvelle vulnérabilité.

Les professionnels qui cherchent à réduire cette exposition et à appliquer les conseils de sauvegarde décrits dans l'avis fédéral (enregistrer trois copies dans au moins deux formats différents, dont une hors ligne) optent de plus en plus pour une approche hybride. Le stockage des données sur site leur permet de mieux contrôler la sécurité, mais cette approche peut s'avérer coûteuse et difficile à étendre à la vitesse nécessaire, en particulier avec l'explosion actuelle des données de santé et la transformation digitale des soins, toutes deux stimulées par la pandémie. Le stockage des données dans le cloud public est plus rentable, mais les organisations risquent des pannes et un manque de transparence sur la façon dont les données sont protégées.

Une approche hybride permet de conserver les données sensibles dans les locaux, tandis que les données moins sensibles sont stockées dans le cloud. Même cette approche n'est pas parfaite, car la sécurité doit être mise en place pour protéger le transfert des données entre les deux types de stockage et garantir que l'accès est limité aux personnes autorisées à effectuer les transferts et à consulter les données. Le respect des sept exigences clés pour la mise en œuvre d'une architecture ZTNA permet aux organisations de protéger leurs données, en accordant aux utilisateurs l'accès aux seules applications dont ils ont besoin dans le cadre de leur fonction, avec une sécurité supplémentaire offerte par la MFA.

Akamai est là pour vous aider à vous préparer à l'éventualité d'une attaque. Travaillons ensemble pour construire une vision cohérente de votre réseau afin de repérer rapidement une attaque et d'atténuer efficacement les dommages. Notre mission consiste à protéger les réseaux contre les attaques par déni de service distribué et les ransomwares, afin d'offrir des expériences Web fluides et sécurisées (y compris les applications et les API).

Nous renforçons la bordure de votre réseau afin de limiter les risques d'intrusion et de réduire le rayon d'action en cas d'attaque. Et ceci, tout en conservant la flexibilité de l'accès des utilisateurs, afin que votre organisation puisse se concentrer sur sa mission première : fournir des soins optimaux dans un contexte d'exigences opérationnelles et de soins en constante évolution.

Il n'a jamais été aussi important de protéger les informations de vos patients contre les attaques de plus en plus sophistiquées des cybercriminels et l'expansion de la surface d'attaque dans le cloud. Les entreprises et les organismes gouvernementaux centrés sur le patient font confiance à la plateforme en bordure de l'Internet d'Akamai pour rapprocher leurs expériences digitales des patients et éloigner les menaces.

Faites confiance à Akamai, le partenaire qui fera de la cybersécurité un atout concurrentiel pour votre organisation.

Contactez-nous pour en savoir plus ou appelez-nous au +1-877-425-2624.