ManageEngine

Cybersécurité dans le domaine de la Santé : 10 manières de contrecarrer les cyberattaques et les violations de données dans le Secteur Médical

Table des matières

01 Les difficultés du secteur médical:
Cette situation passera aussi

02 Principaux problèmes informatiques rencontrés par le secteur médical

03 Analyser et tirer les leçons des exploits récents dans le secteur de la santé

04 10 manières de contrecarrer les cyberattaques et les violations de données dans le Secteur Médical

05 Feuille de route pour l'IT/OT du secteur médical

06 A propos de ManageEngine UEM

Les difficultés du secteur médical: Cette situation passera aussi

Du coronavirus au changement climatique, il est presque impossible de trouver des solutions aux menaces systémiques auxquelles l'homme est confronté à l'échelle mondiale sans l'aide de la médecine moderne. Alors que nous réalisons des percées majeures en quelques mois plutôt qu'en quelques années, nous nous rendons compte que les difficultés opérationnelles du secteur de la santé ne cessent également d'évoluer. De l'adoption de la cybersécurité et de la transformation numérique à la redéfinition de la santé publique et de la prestation des soins de santé, nous devons nous demander si le secteur de la santé dispose des ressources nécessaires pour une évolution durable qui pourrait améliorer considérablement nos vies.

Dans cet e-book, nous nous concentrerons principalement sur les difficultés liées aux technologies de l'information et aux technologies d'exploitation dans le secteur médical, les cousins IT (Information Technology) et OT (Operational Technology). L'informatique fait référence à la technologie des ordinateurs, y compris le matériel et les logiciels, et se concentre principalement sur les données. La technologie d'exploitation, en revanche, concerne les processus et les périphériques qui, dans un environnement médical, comprennent souvent des équipements anciens et disparates. Nous analyserons l'état actuel des technologies de l'information dans le secteur de la santé et examinerons les moyens de minimiser les risques de cybermenaces dans le but de fournir des services de santé fiables et sécurisés.

Principaux problèmes informatiques rencontrés par le secteur médical

Quels sont les problèmes auxquels est confronté un administrateur informatique dans le secteur médical ?

01
Incidents de sécurité

02
Fuites de données mettant en danger la vie privée des patients et des données professionnelles sensibles

03
Manque de visibilité du réseau

04
Adaptation à la transformation numérique

05
Adoption des nouvelles technologies

06
Gestion de la conformité

01 Réduire les incidents de sécurité

Les incidents de sécurité dans le secteur médical vont des attaques par ransomware qui paralysent les systèmes informatiques des hôpitaux à la compromission de la vie privée des patients, par exemple par une violation des informations personnelles identifiables.

Au-delà de ces nuisances opérationnelles, l'évolution des méthodes de cyberattaques ces derniers temps a eu de graves répercussions.

Le premier décès recensé dû à une cyberattaque s'est produit en septembre 2020, lorsqu'un hôpital allemand, victime d'une attaque par ransomware, n'a pas pu accueillir une patiente de 78 ans souffrant d'un anévrisme. La raison : une défaillance des systèmes numériques chargés de coordonner les équipes médicales et les lits d'hôpital. Le temps qu'elle puisse être admise dans un autre hôpital, il était trop tard.

02 Lutter contre les fuites de données

Dans les secteurs de la santé et pharmaceutique, deux groupes spécifiques sont principalement visés par les pirates informatiques. Le premier est celui des clients, c'est-à-dire des patients, et le second celui des fournisseurs ou des entreprises du secteur de la santé. Ces deux groupes possèdent leur propre lot de données et de ressources sensibles susceptibles d'être consultées et manipulées. Une part importante des données est également stockée et gérée par plusieurs fournisseurs qui traitent les données pour le compte de l'hôpital. Avec autant de variables, et des données stockées et traitées par de multiples entités, il devient difficile de les cartographier et de les sécuriser.

03 Manque de visibilité du réseau IT/OT de l'hôpital

Outre les équipements informatiques, tels que les ordinateurs, les ordinateurs portables et les périphériques mobiles, le réseau de l'hôpital se compose également de systèmes et de périphériques OT, tels que les systèmes HVAC (chauffage, ventilation, climatisation d'air), les systèmes de surveillance des patients, les équipements utilisés dans les unités de soins intensifs, etc. L'utilisation de périphériques intelligents et de périphériques IoT a également connu un pic, car de plus en plus de périphériques sont intégrés et connectés les uns aux autres.

Avec autant de types de périphériques différents sur le réseau, un administrateur informatique peut ne pas avoir une compréhension complète et les outils nécessaires pour s'enoccuper, ce qui entraîne des zones d'ombre. Ces zones d'ombre du réseau sont essentiellement des zones négligées, mais qui jouent un rôle majeur dans les systèmes informatiques et technologiques des hôpitaux. Les choses peuvent empirer lors d'une fusion ou d'une acquisition, car les entreprises ont du mal à bien comprendre le comportement du réseau, des données et des applications. Ce faisant, les zones d'ombre se multiplient.

04 Adaptation à la transformation numérique et à l'innovation radicale

Si le secteur médical est fortement axé sur l'innovation, il a aussi la mauvaise réputation d'être le secteur le plus vulnérable aux cyberattaques. Le coût moyen d'une fuite de données dans le secteur de la santé s'élève à 9,23 millions de dollars, soit près du double de celui du secteur financier, qui occupe la deuxième place en termes de coûts des fuites de données.
Le coût moyen d'une fuite de données dans le secteur de la santé s'élève à 9,23 millions de dollars, soit près du double de celui du secteur financier, qui occupe la deuxième place en termes de coûts des fuites de données.

Alors que les hôpitaux et les équipes médicales tentent d'adopter de nouvelles technologies permettant de sauver des vies et des pratiques innovantes, ils risquent également de laisser leurs infrastructures critiques sans surveillance aux mains des intrus et des acteurs de la menace. Le Third-Party Breach Report a révélé que le secteur de la santé était la victime la plus ciblée des cyberattaques en 2021, avec 33 %, le secteur gouvernemental arrivant loin derrière avec moins de la moitié de ce chiffre. Mais l'investissement pour s'adapter aux nouvelles technologies peut être un énorme facteur limitant pour les entreprises qui cherchent à adopter la transformation numérique.

05 Conformité et organismes de réglementation

La plupart des entreprises du secteur de la santé considèrent les réglementations, comme l'HIPAA, comme des obstacles. En réalité, ces réglementations sont plutôt des anges gardiens qui aident les entreprises à gérer les ePHI (informations électroniques sur la santé des patients) de manière sûre et sécurisée, loin des regards indiscrets des cybercriminels. Bien que l'application des stratégies rigoureuses des organismes de réglementation puisse constituer un obstacle, le résultat en vaut la peine.

Analyser et tirer les leçons des exploits récents dans le secteur de la santé

Un écosystème de santé typique est composé de multiples systèmes IT et OT allant des ordinateurs et serveurs aux périphériques de niche tels que les moniteurs de lit et les ventilateurs. Alors que les hôpitaux modernisent leurs infrastructures et leurs services publics avec des périphériques innovants et des solutions IoT intelligentes, ils risquent également d'exposer ces équipements à divers attaquants et acteurs de la menace. Selon le 2021 Cost of a Data Breach Report compilé par le Poneman Institute, les organisme de santé ont connu le coût moyen le plus élevé d'une fuite de données pour la 11e année consécutive, et une augmentation de près de 30 % par rapport à l'année précédente.

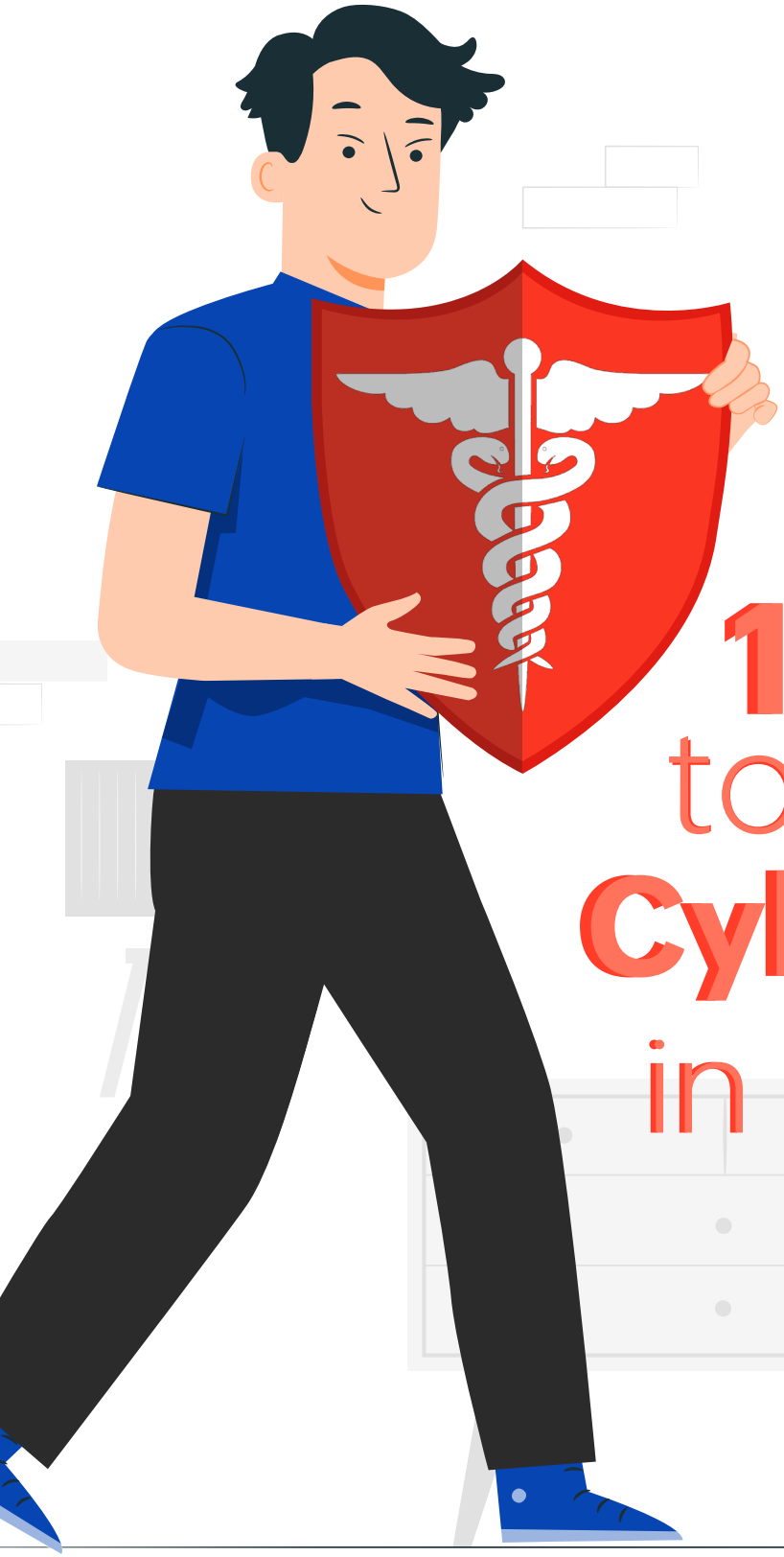
Coût moyen d'une fuite de données de santé : 9,23 millions de dollars en 2021. Une augmentation de 29.5% depuis 2020 (qui était de 7,13 millions de dollars)

Le secteur de la santé est le plus exposée aux cyberattaques, suivi des services financiers.

Selon des chiffres tirés du rapport **Breach of Unsecured Protected Health Information report** du United States Health and Human Services Office, rien qu'en janvier 2022, plus de 2,3 millions de patients ont été touchés par des fuites de données. Après avoir fait le bilan et compris la nature des cyberattaques qui se produisent dans le secteur de la santé, on peut attribuer ces brèches à certaines sources communes :

- Email professionnel compromis
- Accès non autorisé
- Vol de données
- Ransomware
- Un serveur de réseau piraté
- Serveur/base de données non sécurisé

Au lieu de plonger dans le quoi et le comment de chaque cyberattaque ci-dessus, ce qui peut être fait par une simple recherche Google (ou en consultant cet article), essayons de réduire le risque que représentent ces vecteurs et de protéger votre informatique contre les cyberattaques.



10 Ways to Minimize Cyberattacks in Healthcare

01 Activer le Zero Trust

Le Zero Trust est un modèle de défense du réseau déployé pour restreindre l'accès au réseau et aux applications. Il s'agit d'un modèle de réseau fondé sur le principe selon lequel il ne faut faire confiance à personne. Le Zero Trust Network Access (ZTNA) considère chaque périphérique du réseau comme hostile jusqu'à ce qu'il soit prouvé qu'il est digne de confiance, ce qui est contraire à l'approche traditionnelle du réseau qui considère qu'un périphérique est digne de confiance dès qu'il franchit la couche de sécurité.

L'approche ZTNA qui consiste à ne faire confiance à aucun utilisateur ou entité par défaut, peut être appliquée aux services VPN et proxy, ainsi qu'à d'autres services qui reposent sur la confiance entre le client et le serveur.

02 Appliquer le MFA

L'authentification multi-facteurs (MFA) est un moyen d'ajouter une couche de sécurité supplémentaire pour vérifier l'identité d'une personne pendant le processus de connexion. Lorsque l'authentification multi-facteurs est activée, les utilisateurs doivent s'authentifier de deux façons ou plus pour accéder aux informations de leur entreprise. Ainsi, même si le mot de passe d'un employé est compromis, son autre authentification empêchera les acteurs de la menace de se connecter.

Ces facteurs d'authentification supplémentaires sont généralement un mot de passe unique basé sur le temps (OTP), un scan biométrique ou un code provenant d'une application d'authentification. Le MFA présente de nombreux avantages et constitue sans doute le mécanisme de cyberdéfense le plus facile à mettre en place pour les entreprises.

03 Réduire la surface d'attaque

La surface d'attaque est l'ensemble des équipements physiques et numériques de votre réseau par lesquels un utilisateur non autorisé peut y accéder et extraire des données privées. Parmi les exemples courants de votre surface d'attaque figurent les ordinateurs, les switchs, les applications, le code, les ports, les serveurs et les sites web. Vous pouvez gérer et sécuriser votre surface d'attaque en cartographiant vos ressources sur le cloud et sur site, en identifiant les vulnérabilités ou faiblesses potentielles, en vérifiant les rôles des utilisateurs et les niveaux de privilèges.

Alors que le secteur médical devient de plus en plus intelligent et que des solutions innovantes nous mènent vers de nouvelles avancées, l'expansion de l'empreinte numérique des entreprises ne doit pas être un motif d'inquiétude. Il est préférable de surveiller et de sécuriser votre surface d'attaque existante plutôt que d'essayer de la réduire. En bref, l'adoption des nouvelles technologies ne doit pas être entravée par la menace de cyberattaques potentielles.

04 Déploiement de correctifs et mises à jour automatiques des OS et des applications

L'application des derniers correctifs et la mise à jour des logiciels et des applications en temps et heure restent des éléments essentiels de tout plan de prévention des cyberattaques. Les responsables informatiques ne peuvent se permettre de minimiser l'importance de l'application de correctifs et de la mise à jour de leurs logiciels.

Le timing étant essentiel pour l'application des correctifs et des mises à jour logicielles, il est important d'automatiser ces processus pour limiter l'exposition de votre IT médical aux vulnérabilités. Les systèmes non patchés restent une cible majeure des cyberattaques, c'est pourquoi l'**automatisation des mises à jour logicielles** et l'installation en temps et en heure des correctifs dès qu'ils sont publiés sont la meilleure chose à faire.

05 Assurer un contrôle efficace des périphériques et des applications

Les hackers qui utilisent un périphérique de stockage pour pirater les systèmes hospitaliers ne sont pas seulement une scène palpitante d'un film de science-fiction. Les acteurs de la menace peuvent brancher des périphériques sur vos ports USB et exécuter un script qui peut rendre les installations de santé inutilisables.

Une manière de limiter ce problème est de bloquer l'utilisation de périphériques de stockage externes. Pour ce faire, vous pouvez utiliser une **solution de contrôle des périphériques** qui vous permet de garder un œil sur les périphériques et les ports. Vous pouvez également contrôler les périphériques branchés et analyser le comportement des utilisateurs dans l'ensemble de votre établissement afin de prévenir les menaces internes.

En plus de surveiller les actions potentiellement nuisibles entourant le matériel, vous pouvez également renforcer les actions de sécurité des terminaux d'entreprise en accordant des privilèges d'accès uniquement à un groupe particulier ou **restreignant l'utilisation d'applications ou de logiciels non autorisés** sur les machines de l'entreprise.

06 Appliquer le contrôle d'accès

Du chirurgien en chef à l'infirmière débutante, tout le personnel hospitalier a besoin d'un accès rapide et facile aux données pour assurer une bonne prise en charge du patient. Un contrôle d'accès adapté permet de s'assurer que chaque utilisateur dispose du niveau d'accès approprié, ce qui réduit la nécessité de fournir un accès administrateur à tout le monde, tout le temps.

Si le personnel de santé a besoin d'accéder à des ressources nécessitant un privilège d'administrateur, vous pouvez élever temporairement leurs privilèges afin qu'ils puissent accomplir leur travail efficacement. Le contrôle d'accès permet de sécuriser vos données, d'assurer la traçabilité des accès des utilisateurs et de garantir la conformité aux réglementations informatiques.

07 Corriger les vulnérabilités

Les déploiements de correctifs traditionnels ne prennent en compte que les vulnérabilités connues qui sont documentées par les fournisseurs. Les autres vulnérabilités inconnues ne sont pas documentées et passent généralement inaperçues avant de faire des ravages. Les **solutions de gestion des vulnérabilités** assurent une visibilité continue, détectent les faiblesses, évaluent les risques et corrigent les menaces. Ainsi, vous pouvez auditer et maintenir vos systèmes en accord avec les critères de conformité et rester à jour avec des informations détaillées sur les mesures correctives.

08 Mettre en place plusieurs couches de sécurité.

Le périmètre de sécurité de votre entreprise doit comporter plusieurs couches de sécurité afin d'offrir plus de profondeur. En fonction des besoins, vous pouvez mettre en place plusieurs couches de sécurité avec différents niveaux de protection, par exemple :

- → Des Firewalls
- → Un systèmes de détection et de prévention des intrusions, comme un antivirus et un logiciel anti-malware.
- → Un systèmes de surveillance des réseaux
- → Une authentification sécurisée

09 Mettre en œuvre le chiffrement et les sauvegardes de données

Le chiffrement rend les informations sensibles de votre organisation, comme les informations hospitalières et les dossiers des patients, illisibles pour toute personne qui ne devrait pas y avoir accès, comme les utilisateurs non autorisés ou les pirates. C'est particulièrement utile en cas d'attaque par ransomware. Même si vos données sont compromises, les acteurs de la menace ne seront pas en mesure d'en divulguer le contenu, mettant ainsi votre organisation hors de danger.

Le chiffrement est incomplet sans des sauvegardes de données appropriées. Il est essentiel de sauvegarder les informations importantes et sensibles de l'entreprise. En procédant ainsi, vous pourrez assurer une transition sans difficulté en cas de violation des données. Disposer d'un plan de sauvegarde et de récupération des données est également un processus vital.

Il s'agit de répertorier les éléments qui doivent être sauvegardés hors ligne dans des périphériques de stockage, ou dans un stockage en cloud sécurisé, comme les fichiers et dossiers de données, les images de systèmes d'exploitation, les bases de données clients, les images de machines, les systèmes d'exploitation et les fichiers de registre. Les besoins de chaque service, de la biochimie au service de radiologie, doivent être pris en compte. De nombreux fournisseurs proposent des solutions de sauvegarde et de récupération des données conformes à la loi HIPAA qui rationalisent ce processus et garantissent des interruptions minimales.

10 Assurer la gestion et la protection des terminaux

Les terminaux peuvent être des ordinateurs de bureau, des téléphones mobiles, des tablettes, des routeurs et d'autres périphériques, et ils peuvent accéder à un réseau aussi bien sur site qu'à distance. La protection des terminaux est un terme large qui comprend de multiples facettes telles que la gestion des vulnérabilités, la sécurité des navigateurs et le contrôle des applications.

ManageEngine Endpoint Central est une solution de protection des terminaux qui les protège de plusieurs façons, de la sécurisation des navigateurs des utilisateurs finaux au contrôle de vos périphériques et applications externes.
Vous pouvez utiliser la suite complète des fonctionnalités de sécurité avec un seul add-on de sécurité. En plus, Endpoint Central peut gérer et surveiller de manière centralisée tous vos périphériques sur plusieurs plateformes réparties sur un réseau distribué. Un réseau bien sécurisé est un réseau bien géré.

Feuille de route pour l'**IT/OT du secteur médical**

01
Gagner en visibilité

- Déterminer la surface d'attaque en cartographiant les ressources.
- Identifier les zones d'ombre du réseau.
- Effectuer des contrôles de conformité
- Lancer une analyse des insuffisances et des contrôles de santé
- Analyser les besoins

02
Renforcer votre périmètre de sécurité

- Utiliser des firewalls
- Activer le Zero Trust
- Installer des systèmes de détection d'intrusion
- Déployer des systèmes de prévention des menaces
- Exploiter l'authentification sécurisée en utilisant le MFA
- Instaurer une gestion des mots de passe
- Utiliser des VPN

03
Surveiller en permanence

- Déployer des outils de sécurité des terminaux
- Mettre en œuvre des stratégies de prévention des pertes de données
- Adopter un contrôle des périphériques et des applications
- Appliquer l'accès privilégié
- Utiliser un scanner de vulnérabilité

04
Assurer une disponibilité maximale des services de santé

- Assurer la disponibilité des services de santé essentiels
- Faire des sauvegardes de données
- Chiffrer les informations
- Trouver un équilibre entre cyber-résilience et productivité
- Utiliser la protection des terminaux

05
Valider et faire évoluer

- Tester en permanence la sécurité du réseau
- Qualifier et vérifier les mises à niveau des périphériques et les déploiements de technologies
- Chiffrer les informations
- Mettre en place un environnement de test pour vérifier les dernières mises à jour et correctifs logiciels

À propos de ManageEngine

Unified Endpoint Management and Security

ManageEngine UEMS développe des outils de gestion et de sécurité des terminaux pour les équipes qui visent à adopter le changement et à innover en toute confiance. Notre solution de gestion unifiée des terminaux (**UEM**) automatise les tâches, fournit des informations et constitue un moyen fiable d'assurer la gestion et la sécurité de votre personnel. Depuis un tableau de bord unique, vous êtes en mesure de sécuriser votre entreprise en minimisant les risques sans affecter votre agilité. Travaillez plus intelligemment, restez informé et accélérez vos opérations sans rencontrer d'obstacles.

Obtenez ManageEngine UEM pour votre IT >>>

PG Software EUROPE

Retrouvez-nous sur Gartner peerinsights™ Capterra G2

sales@manageengine.fr | 0 805 296 540 Service & appel gratuits