PHILIPS

mShield

Document de présentation technique

mShield de Philips pour les réseaux d'hôpital

Sécuriser les instruments médicaux

Résumé

La prolifération des instruments médicaux connectés au réseau qui utilisent des systèmes d'exploitation intégrés prêts à l'emploi et l'augmentation des cyberattaques visant les établissements de santé rendent les hôpitaux de plus en plus vulnérables aux attaques malveillantes. Pour se protéger contre de telles attaques, les hôpitaux ont besoin d'une approche de sécurité multicouche dotée de nombreuses barrières pour empêcher les intrusions, notamment des correctifs, des solutions antiprogramme malveillant et des coupe-feu. mShield de Philips est un coupe-feu développé pour les systèmes d'imagerie qui offre une couche de sécurité supplémentaire sans limiter les fonctionnalités de l'instrument. Il protège les instruments médicaux afin que les patients puissent continuer à passer leurs examens, même s'il y a une activité malveillante sur le réseau.

Introduction

La numérisation dans les milieux hospitaliers continue d'évoluer pour offrir de meilleurs soins de santé aux patients et un flux de travail amélioré aux opérateurs. Les données personnelles, sensibles et confidentielles sont transmises dans l'hôpital par les systèmes de radiologie et inversement. Sécuriser ces renseignements et les protéger contre les attaques informatiques malveillantes est aussi essentielle que difficile.

Utilisez mShield pour

- Empêcher la reproduction de programmes malveillants sur le réseau
- Garantir la disponibilité de l'équipement
- Fournir une couche de sécurité supplémentaire

Protégez votre instrument médical avec mShield de Philips

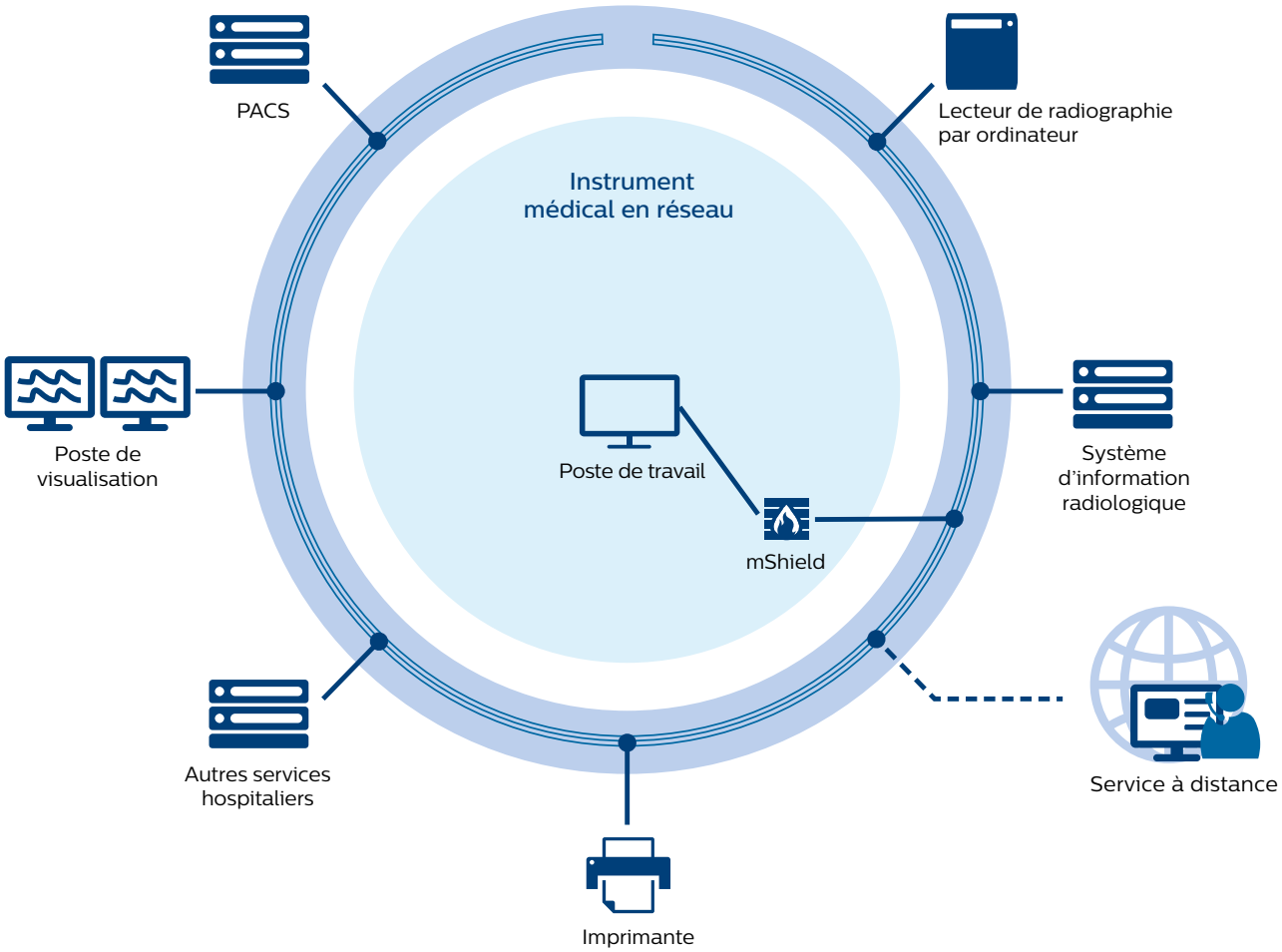
Contrer les risques : recommandations et défis

Un concept de sécurité multicouche aide les hôpitaux à se défendre contre de nombreuses menaces pesant sur leurs données et leurs systèmes. Il est recommandé d'inclure ce qui suit :

- Des correctifs de sécurité essentiels du système d'exploitation et des solutions antiprogramme malveillant courants pour se protéger contre les cyberattaques et les virus pendant toute la durée de vie du système

Bien que cette liste soit similaire – sinon identique – aux recommandations pour d'autres industries, les instruments médicaux ont des conditions particulières qui rendent particulièrement importante une mise en œuvre efficace de la sécurité à plusieurs niveaux.

- Un renforcement au niveau de l'application et des contrôles d'accès pour atténuer les risques en autorisant uniquement les données autorisées et reconnues sur le système
- Des coupe-feu matériels n'autorisant que le trafic autorisé



Correctifs logiciels
Les correctifs logiciels éliminent les vulnérabilités détectées après l'installation du logiciel. Des mises à jour régulières aident les établissements de santé à éviter les vulnérabilités logicielles qui pourraient faciliter les cyberattaques dans les systèmes et endommager les systèmes et les données.

Solutions antiprogramme malveillant
Les solutions antiprogramme malveillant sont une protection importante qui devrait faire partie de tout concept de sécurité des terminaux. Une solution anti-programme malveillant courante est un antivirus. Pour être efficaces, les antivirus doivent disposer de fichiers de définitions de virus à jour contenant les nouveaux virus et le dernier moteur d'analyse. Si les instruments médicaux sont hors réseau, même pour une courte période, ils peuvent manquer une mise à jour importante.

Une deuxième solution antiprogramme malveillant est la mise en liste blanche des applications, qui empêche tous les logiciels qui ne figurent pas sur une liste blanche d'être exécutés sur le système. La liste blanche des applications « fige » efficacement le logiciel système dans un état connu. Étant donné qu'elle évite les modifications non autorisées même par des programmes malveillants qui ne sont pas encore connus (attaques du jour zéro), la liste blanche des applications ne nécessite pas de mises à jour régulières pour être efficace.

Coupe-feu matériels
Les coupe-feu matériels constituent une troisième arme dans la lutte contre les attaques. Un coupe-feu classique est conçu pour établir une barrière entre les réseaux interne et externe et utilise des règles de sécurité pour déterminer si le trafic des réseaux est sûr. Il peut également séparer le réseau interne en sous-réseaux et appliquer entre eux des règles liées au filtre de coupe-feu. Cette approche peut isoler les nœuds importants présents sur le réseau jusqu'à ce que la menace soit neutralisée.

mShield : un coupe-feu spécialisé pour les instruments médicaux de Philips
Les conditions particulières des instruments médicaux font en sorte que même avec une sécurité exceptionnelle des terminaux, les systèmes d'imagerie sont vulnérables. Pour renforcer les efforts de sécurité des hôpitaux tout en protégeant la fonction de soins de santé essentielle des instruments médicaux de Philips, Philips a développé mShield, un coupe-feu spécialisé qui bloque efficacement les menaces pesant sur les systèmes d'imagerie, en les protégeant sans limiter leur utilisation.

mShield comprend à la fois du matériel et des logiciels et est basé sur le système d'exploitation axé sur la sécurité OpenBSD[1]. Il assure l'isolement et la protection du réseau, en réduisant l'exposition de la connectivité (« surface d'attaque ») entre l'équipement médical et le réseau de l'hôpital. Chaque instrument médical doit être doté de son propre dispositif mShield, bien qu'il soit possible d'utiliser un seul mShield sur plusieurs instruments connectés.

Étant donné que mShield est si spécifique, il peut utiliser des règles strictes pour évaluer la validité du trafic et limiter le trafic uniquement à des instruments autorisés et à des services précis. Par exemple, l'équipement radiologique utilise généralement DICOM comme protocole de communication principal et seulement certains autres protocoles connexes. Avec une politique de refus par défaut et quelques exceptions liées au coupe-feu, mShield peut efficacement dissocier la modalité du réseau et masquer la structure de la modalité, tout en maintenant la connectivité pour les applications médicales ou le service à distance.

mShield peut empêcher la reproduction de programmes malveillants sur le réseau, garantir la disponibilité de l'équipement, fournir une couche de sécurité supplémentaire et offrir une protection si le système d'exploitation intégré de l'instrument médical n'est plus pris en charge par le fabricant du système d'exploitation.

Empêche la reproduction de programmes malveillants sur le réseau
mShield bloque pratiquement tous les chemins de reproduction sur réseau classiques pour les virus et les vers, évitant ainsi les infections. Cette approche permet d'éviter le plus gros problème lié aux antivirus, qui dépendent de mises à jour régulières et en temps opportun et qui peuvent réagir seulement lorsque le virus commence à interagir avec le système.

S'il est vrai que la sécurité de l'équipement médical pourrait encore être compromise par un protocole réseau accepté par mShield, le risque d'infection est faible. En effet, les milieux hospitaliers sont différents les uns des autres à bien des égards, et les réseaux médicaux sont souvent intensivement personnalisés de telle sorte qu'il est difficile pour les programmes malveillants de réussir des attaques de masse partout. De plus, mShield établit et applique des relations de confiance entre des nœuds précis au sein d'un réseau d'hôpital, réduisant ainsi le risque de propagation massive de programmes malveillants.

L'infection est également possible par des chemins qui contournent mShield, tels que les supports amovibles. Le risque dépend de la fréquence d'utilisation, des mesures de sécurité mises en place sur l'équipement médical et de la politique de sécurité de l'hôpital. Cependant, si l'équipement médical est infecté par l'intermédiaire de ce chemin d'accès, mShield empêche le virus de se reproduire sur d'autres machines du réseau, car il inspecte les paquets entrants et sortants.

Garantit la disponibilité de l'équipement médical
mShield sert de point d'entrée unique pour toute communication réseau provenant de l'équipement médical protégé ou transmise vers celui-ci. Ainsi, mShield absorbe l'impact de l'attaque à la place de l'équipement médical, et même si mShield plante en raison de l'attaque, l'équipement continue de fonctionner.

Cela rend de nombreux types d'attaques – tout comme les anomalies de réseau accidentelles qui pourraient affecter l'appareil – impossibles ou beaucoup plus difficiles à réaliser. L'instrument médical fonctionnera comme s'il était déconnecté du réseau et se reconnectera pour transférer des images ou d'autres données une fois que le réseau sera disponible.

Fournit une couche de sécurité supplémentaire
mShield sert à maintenir en permanence un niveau élevé de sécurité continue du réseau en bloquant l'exploitation à distance basée sur le réseau. Par le passé, mShield a réussi à bloquer des programmes malveillants comme le ver informatique SASSER ou le rançongiciel WannaCry.

Offre une sécurité pour les logiciels tiers non pris en charge
Les logiciels abandonnés et non pris en charge posent également des problèmes aux hôpitaux. Philips prend en charge ses équipements pendant au moins 10 ans après l'arrêt de la production, mais les fournisseurs de logiciels tiers interrompent généralement la prise en charge de leurs logiciels, y compris la fourniture de correctifs de sécurité, beaucoup plus tôt, ce qui entraîne des lacunes en matière de prise en charge. La mise à niveau vers le système d'exploitation le plus récent garantit une prise en charge continue, y compris la réception de correctifs de sécurité. Cependant, lorsque des restrictions financières ou techniques rendent cela impossible, mShield ajoute une couche de protection.

« Ce que nous avons actuellement… est un écosystème de soins de santé encore très fragile, c'est ainsi que je le décrirais. Et nous devons améliorer nos systèmes afin qu'on puisse y appliquer des correctifs et les mettre à jour et afin qu'ils puissent supporter une exploitation, une attaque ou une brèche tout en fonctionnant en toute sécurité et correctement, et afin que l'hôpital lui-même et les fabricants et, encore une fois, le secteur dans son ensemble, soient résilients pour pouvoir y résister et assurer la continuité des soins[2]. »

- Susanne Schwartz, M.D., directrice par intérim, Office of Strategic Partnerships and Technology Innovation, Center for Devices and Radiological Health de la FDA.

Addenda

Fonctionnement de mShield : description technique, installation et configuration

Le dispositif mShield de Philips comprend le filtrage de la couche 2, y compris le filtre ARP (protocole de résolution d'adresse), ainsi que le filtrage de la couche 3 (inspection dynamique de paquets ou SPI) en combinaison avec un mode furtif (également appelé mode pont). Comme l'a expliqué un expert, « Un coupe-feu est une porte que tout le monde sait vouloir franchir. Un pont de filtrage de paquets ressemble plus à un agent secret qui fait sortir les méchants de l'ombre et que personne ne peut attaquer. Les ponts de filtrage de paquets OpenBSD peuvent considérablement augmenter la sécurité de toute architecture de réseau.[3] » Les règles de filtrage sont personnalisées en fonction des exigences de communication des produits médicaux de Philips. La conception de mShield est conforme aux recommandations de consortiums industriels internationaux, tels que NEMA, COCIR et JIRA. Ils recommandent le coupe-feu comme étant un « outil flexible et efficace » faisant partie d'une stratégie globale de sauvegarde de l'intégrité des données des systèmes d'information médicaux[4].
En tant qu'outil conçu sur mesure pour protéger les systèmes au niveau de l'instrument, mShield présente de nombreux avantages par rapport aux mesures de sécurité étendues. Il offre une solution de sécurité comparable aux produits logiciels de coupe-feu hôte, mais présente des avantages en matière de flexibilité, de service et de sécurité.

Agit comme un commutateur Ethernet

En règle générale, les coupe-feu sont dotés de deux interfaces ou plus, chaque interface étant configurée pour un sous-réseau précis. Le coupe-feu effectue ensuite le routage entre ces sous-réseaux en plus de l'inspection et du filtrage des paquets. Chaque ordinateur d'un sous-réseau doit connaître le coupe-feu (routeur) par son adresse IP (et son adresse MAC [contrôle d'accès au support]*) afin d'envoyer tous les paquets destinés à un autre sous-réseau.
* Le format de l'adresse MAC est aa:bb:cc:dd:ee:ff (chaque partie séparée par un deux-points est une valeur hexadécimale comprise entre 00 et ff). L'adresse MAC est un identifiant unique pour une carte d'interface réseau.

Contrairement à ces coupe-feu courants, mShield n'est pas un routeur, mais agit plutôt comme un commutateur Ethernet, en ce sens qu'il ne divise pas le réseau en sous-réseaux. Cela offre un avantage en matière de service et d'administration dans de nombreux cas, y compris les cas de mise à niveau, dans lesquels il élimine le besoin de reconfigurer les instruments médicaux protégés, ainsi que la nécessité pour un administrateur de TI local d'attribuer un sous-réseau dédié à l'instrument médical.

Invisible

mShield n'est pas directement visible sur le réseau, ni par son adresse IP ni par son adresse MAC. Cette fonction réduit la surface d'attaque de mShield, ce qui permet une longue durée de fonctionnement sans maintenance.

Robuste

Le système d'exploitation de mShield – OpenBSD – est connu pour être l'un des systèmes d'exploitation de réseau les plus sécurisés. Implanté dans mShield, ce système d'exploitation général est réduit en taille et en fonction pour ne contenir que le minimum nécessaire. Par exemple, il ne dispose que du minimum de pilotes de noyau et d'outils système nécessaires et il n'autorise pas les connexions d'utilisateur interactives par défaut. De plus, mShield fonctionne entièrement à partir de la mémoire (disque RAM). À l'exception de la configuration et des mises à jour logicielles, il n'y a pas d'accès en écriture au disque flash intégré, ce qui améliore considérablement le temps de disponibilité et la robustesse. Cette architecture permet à mShield de survivre à une panne de courant ou à une mise hors tension manuelle à tout moment sans violer l'intégrité de son logiciel interne. Ainsi, mShield démarre toujours de manière fiable dans un état sain et fonctionnel.

Traitement du trafic réseau

Le filtrage des paquets du réseau fonctionne à différents niveaux de la pile de protocoles TCP-IP. Par défaut, mShield bloque tous les paquets qui ne sont pas emballés conformément aux protocoles IPv4 ou ARP. Les adresses IP de tous les hôtes protégés sont stockées dans la configuration mShield. Cela facilite le filtrage basé sur les adresses IP. De plus, un filtre ARP spécialement conçu empêche l'usurpation ARP (intentionnelle ou accidentelle, p. ex., au moyen d'une adresse IP dupliquée) des adresses configurées.

La communication TCP ne passe qu'avec un ensemble valide de drapeaux TCP. Tous les paquets mal formés sont abandonnés, quelle que soit leur origine (p. ex., les paquets dont le drapeau SYN et le drapeau FIN sont actifs en même temps). Les paquets UDP et ICMP sont également filtrés par état.

Lorsque cela a du sens, le nombre de nœuds sources amorçant une communication (TCP, UDP ou ICMP) est limité et suivi. Une limite de débit de paquet maximale est appliquée pour empêcher les conditions de déni de service d'affecter l'instrument médical protégé. En d'autres termes, si une modalité est protégée par mShield, le pire des cas lors d'une condition de déni de service est la perte de la connectivité du réseau, car mShield lui-même devient saturé. Par contre, la modalité reste disponible pour les flux de travail cliniques locaux, de sorte que les patients pourront quand même passer leurs examens. Le transfert de données se produit lorsque le réseau et le système sont sécurisés.

Matériel
Le matériel mShield a été choisi en gardant à l'esprit la sécurité et la continuité des activités et il est conforme à toutes les réglementations nationales nécessaires, telles que CE, UL et CSA. Aucun périphérique de stockage mécanique prédisposé aux défaillances n'a été intégré, ce qui garantit une longue durée de vie du matériel. Il n'a pas non plus de fonctionnalités matérielles supplémentaires, comme un clavier ou une vidéo. Le matériel de haute qualité est certifié pour des températures de fonctionnement étendues pouvant atteindre 55 °C. Le matériel mShield convient à la mise à niveau d'équipements médicaux plus anciens ainsi qu'à l'intégration à de nouveaux équipements médicaux.

Installation et configuration
Pour installer et configurer correctement mShield, le technicien doit connaître la configuration réseau de l'instrument médical, tous ses composants et les hôtes pairs avec lesquels l'instrument médical communique. L'utilisation de modèles prédéfinis (par système) facilite la configuration adéquate de mShield, et tout changement des paramètres réseau peut être facilement effectué tout en préservant l'interopérabilité du réseau.

Les techniciens utilisent un outil de service Philips compatible qui contient tous les renseignements nécessaires (y compris l'information sur les versions) pour configurer mShield, faciliter les mises à niveau, rechercher les défauts et extraire les fichiers journaux.

Les mises à jour logicielles peuvent être effectuées localement au moyen des outils de service ou indirectement par l'intermédiaire d'une connexion à distance à l'instrument médical protégé, en fonction de la capacité de l'instrument à prendre en charge la distribution à distance de logiciels et des capacités du marché.

L'équipe de recherche et développement de Philips surveille activement les bogues potentiels et émergents relatifs aux noyaux et aux applications et utilise un système de qualité de renommée mondiale pour évaluer et déployer rapidement les correctifs, s'il y a lieu.

Éléments de configuration
Au moment de la configuration, la tâche principale des techniciens locaux consiste à identifier tous les instruments connectés en fonction de leur type et de leurs paramètres réseau, comme l'adresse IP. Ils doivent également repérer et configurer les relations de communication entre les hôtes sur le réseau en fonction de la situation individuelle sur place, par exemple en ce qui concerne ce qui suit :
- Protocole NTP (synchronisation d'horloges)
- Journal d'exploitation (journalisation centrale / piste de vérification)
- Systèmes PACS et SIR, imprimantes, lecteurs PCR et autres périphériques basés sur DICOM ou « DICOM sécurisé »
- Service à distance de Philips

Journalisation
Le journal d'exploitation, intégrée à mShield, écrit tous les fichiers journaux dans la mémoire (RAM). Les fichiers journaux peuvent être exportés avant une perte d'alimentation ou redémarrés pour éviter toute perte. mShield contient des fichiers journaux non permanents afin que le système puisse être éteint à tout moment sans violer l'intégrité du disque flash intégré.

Références

1 Voir le site http://openbsd.org/ ainsi que la licence BSD respective accessible à http://openbsd.org/policy.html
2 « Medical Device Security: The FDA's View. », Careers Info Security, 9 juillet 2019, https://www.careersinfosecurity.com/medical-device-security-fdas-view-a-12748, consulté le 5 novembre 2019.
3 Source : George Rosamond, « Building a more secure network » : http://www.sans.org/rr/whitepapers/modeling/1415.php
4 Source : « Defending Medical Information Systems Against Malicious Software », décembre 2003, par NEMA (National Electrical Manufacturers Association-USA), COCIR (European Coordination Committee of the Radiological Electrometrical Industry) et JIRA (Japan Industries Association of Radiological Systems) : www.nema.org/prod/med/upload/medical-defending.pdf

4522 991 57051 * FÉV. 2020

Pour communiquer avec nous
Veuillez visiter le site www.philips.com
healthcare@philips.com