PHILIPS

Sécurité des données

RM

Dans quelle mesure protégez-vous efficacement votre équipement d'imagerie contre les brèches de données de patients?

Comme toute industrie qui repose sur des réseaux informatiques de plus en plus connectés, l'industrie mondiale des soins de santé doit composer avec un nombre croissant de brèches de sécurité.

L'impact de l'attaque contre le National Health Service du Royaume-Uni au moyen du rançongiciel WannaCry est considérablement plus important que prévu

Selon le rapport du National Audit Office (NAO) sur l'attaque du rançongiciel WannaCry, qui exploitait une faille dans le protocole SMB de Microsoft Windows, fonctionnalité qui était présente dans tous les systèmes d'exploitation Windows de la version XP à la version Server 2008 R2, et qui a infecté les services dans l'ensemble du National Health Service (NHS) du Royaume-Uni, les conséquences de cette attaque sont considérablement plus graves que les rapports précédents portaient à croire[1].

L'attaque du rançongiciel a causé une perturbation généralisée des systèmes informatiques mondiaux en mai 2017. Selon le rapport publié par le NAO, WannaCry a touché au moins 81 des 236 fiducies en Angleterre, directement ou indirectement.

Trente-sept fiducies, dont vingt-sept étaient des fiducies de soins de courte durée, ont perdu l'accès à leurs appareils après avoir subi une attaque du rançongiciel WannaCry, ce qui a entraîné l'annulation de milliers de rendez-vous et d'interventions chirurgicales pour les patients.

En plus d'empêcher l'accès aux ordinateurs, la cyberattaque a également verrouillé d'importants équipements médicaux tels que des appareils d'IRM et des systèmes d'analyse d'échantillons de sang et de tissus.

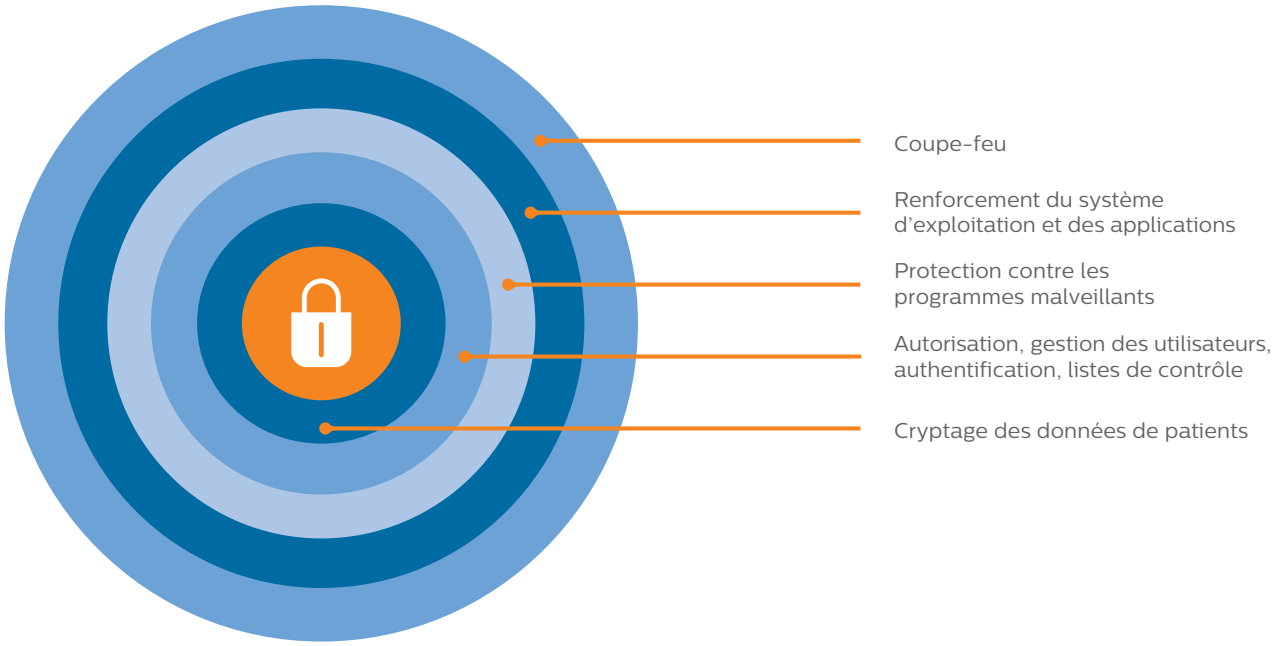
Le rapport du NAO a conclu que le NHS aurait pu empêcher la cyberattaque WannaCry s'il avait appliqué les pratiques de base en matière de sécurité informatique, y compris la migration des systèmes informatiques vers des versions logicielles plus récentes.

Le défi pour les appareils d'imagerie

Les appareils d'imagerie ne sont pas à l'abri de ces types de cyberattaques. La plupart ont été conçus en mettant l'accent sur l'utilité clinique, sans tenir compte du risque d'exploitation à des fins illégales de leurs ordinateurs connectés à un réseau. Cela rend les instruments médicaux vulnérables, et les assaillants peuvent utiliser ces appareils fermés comme points de pivot dans le système de santé. Une stratégie de sécurité cohérente de défense en profondeur peut aider les professionnels de la santé à éviter les brèches de sécurité dans le futur.

Stratégie de sécurité de défense en profondeur

Une stratégie de sécurité de défense en profondeur, fondée sur le fait qu'un système de défense à plusieurs couches est plus difficile à pénétrer qu'une seule barrière, constitue la base des meilleures pratiques en matière de sécurité des instruments médicaux. Les couches peuvent comprendre des politiques et procédures de sécurité, des contrôles d'accès, des mesures techniques, des formations et des évaluations des risques.



Chacune de ces couches défensives joue un rôle important en vous aidant à faire obstacle aux pirates, à contrer les programmes malveillants et à empêcher les accès non autorisés à vos systèmes et appareils d'imagerie.

« Les meilleures pratiques courantes doivent toujours être appliquées lors de mises à jour logicielles et lorsque des courriels suspects contiennent des liens et des pièces jointes, et ce, comme première ligne de défense contre tout rançongiciel ou autre programme malveillant. Une formation continue devrait également être offerte fréquemment à tous les niveaux du personnel afin de promouvoir la sensibilisation et la conformité à ces meilleures pratiques. »

source : ECRI
https://www.ecri.org/components/HDJournal/Pages/Ransomware-Attacks-How-to-Protect-Your-Systems.aspx

Assurer la sécurité des systèmes d'imagerie à résonance magnétique (RM) version 5 de Philips

Philips a appliqué le principe de la stratégie de défense en profondeur à ses systèmes de RM version 5 en mettant en œuvre une stratégie de sécurité comprenant de multiples couches :

- Coupe-feu
- Renforcement du système d'exploitation et des applications
- Protection contre les programmes malveillants
- Autorisation, gestion des utilisateurs et authentification
- Listes de contrôle
- Cryptage des données de patients

Protection d'un coupe-feu contre les attaques sur le réseau

Des politiques de coupe-feu strictes qui bloquent tous les ports superflus aident à empêcher la communication avec des ordinateurs non autorisés, limitant le profil d'attaque qu'un pirate informatique pourrait essayer d'exploiter.

Renforcement du système d'exploitation pour limiter la surface d'attaque

Semblable en principe à un coupe-feu, le renforcement du système d'exploitation comprend l'identification de tous les services et fonctions superflus inclus dans le système d'exploitation et la désactivation de ceux qui ne sont pas requis par les systèmes de RM version 5. Le renforcement du système d'exploitation réduit la surface d'attaque en éliminant les services qui peuvent devenir vulnérables au fil du temps. Les systèmes de RM de Philips respectent les lignes directrices fournies par le Center of Internet Security (CIS) comme principes de base du renforcement du système d'exploitation.

L'utilisation d'une liste blanche contre les programmes malveillants offre une protection contre les menaces inconnues

Pour atténuer le risque de menaces inconnues, Philips a mis en place des politiques qui autorisent uniquement les codes validés à s'exécuter sur le système. Cette solution, appelée « liste blanche », aide à protéger les systèmes de RM contre les programmes malveillants.

Un antiprogramme malveillant ordinaire offre une protection supplémentaire contre les menaces connues

Pour atténuer le risque d'infections pendant les activités de maintenance, Philips a aussi mis en œuvre un antiprogramme malveillant courant qui protège vos systèmes de RM contre les programmes malveillants pendant la réalisation de ces activités. Pour maintenir l'antiprogramme malveillant à jour, Philips maintient les signatures antiprogramme malveillant au moyen d'un service en ligne dans le cadre d'un contrat de service pour la RM de Philips.

Autorisation pour protéger vos actifs

Pour mieux gérer l'accès aux données sur votre système de RM version 5 de Philips, les utilisateurs ont un accès établi en fonction des besoins :

- **Un utilisateur clinique** peut effectuer des examens et accéder à tous les examens précédents qui sont stockés sur le système. Il doit se connecter au système avant de pouvoir accéder aux données. Une fois leur compte configuré, les utilisateurs cliniques peuvent installer les mises à jour publiées.
- **Les administrateurs d'hôpital** peuvent effectuer des tâches administratives simples, verrouiller/déverrouiller des comptes cliniques et créer de nouveaux comptes pour les utilisateurs cliniques. Les administrateurs peuvent installer les mises à jour publiées, mais n'ont pas accès aux données de patients.
- **Les techniciens** peuvent effectuer des tâches de maintenance du système et les activités d'installation initiale et de dépannage.

Gestion des utilisateurs pour améliorer le contrôle des accès et les pistes de vérification

Avec les systèmes de RM version 5, vous avez la possibilité de créer plusieurs comptes d'utilisateurs cliniques et plusieurs comptes d'administrateurs d'hôpital. Avec les deux systèmes, les administrateurs d'hôpital ont la possibilité de préciser des politiques relatives aux mots de passe conformément aux exigences et aux politiques locales en matière de sécurité des données.

Les systèmes de RM version 5 peuvent s'interfacer avec votre environnement LDAP pour authentifier les utilisateurs et les groupes à l'aide de vos comptes réseau standards (p. ex., Active Directory). Les techniciens peuvent accéder au système à l'aide d'une authentification à 2 facteurs. Les clés électroniques peuvent être activées et/ou révoquées par Philips.

Les listes de contrôle fournissent des données pour l'analyse

Philips a amélioré les capacités des systèmes de RM version 5 en matière de listes de contrôle. Les utilisateurs peuvent configurer le système pour qu'il envoie des listes de contrôle à un serveur de journal d'exploitation local à des fins de conservation, d'accessibilité et d'analyse approfondie. Pour faciliter l'analyse médico-légale, les utilisateurs peuvent assurer la cohérence des horodatages en synchronisant l'heure des systèmes de RM avec l'heure du serveur de votre réseau.

Cryptage des données inactives et en transit pour protéger les données des patients

Toutes les données de patients stockées sur le disque dur des systèmes de RM version 5 de Philips peuvent être cryptées en fonction des exigences particulières de votre établissement. De plus, vous pouvez choisir DICOM avec protocole TLS pour l'authentification des nœuds sans cryptage, DICOM utilisant le cryptage par protocole TLS ou une combinaison des deux pour crypter les données de patients en transit. (Remarque : Cela nécessite une fonctionnalité correspondante sur votre système d'archivage et de transmission d'images.)

Protection d'un coupe-feu contre les attaques sur le réseau

- Politique en matière de coupe-feu bloquant tous les ports superflus
- Renforcement du système d'exploitation Microsoft Windows 7 (remarque : la prochaine version logicielle pour les systèmes de RM de Philips sera fondée sur Microsoft Windows 10)
  - Paramètres du système d'exploitation utilisant les jalons du Center for Internet Security (CIS) comme référence
  - Désactivation par défaut des services superflus
  - Désactivation de la fonction d'auto-exécution des supports amovibles et accès configurable
- Sécurité relative à l'exportation vers un support
  - Possibilité de désactiver la fonction d'exportation des données de patients vers un support amovible (configurable)
  - Possibilité de crypter les données sur supports amovibles
- Protection contre les programmes malveillants au moyen de la solution d'antiprogramme malveillant de McAfee associée à des politiques de liste blanche
- Politique en matière de gestion des utilisateurs
  - Gestion des utilisateurs au moyen de comptes locaux
  - Prise en charge de multiples comptes d'utilisateurs distincts
  - Prise en charge de multiples comptes d'administrateurs distincts
  - Protocole LDAP de gestion des utilisateurs
  - Prise en charge de l'authentification Active Directory au moyen du protocole LDAP (le système sera intégré au domaine)
  - Prise en charge de comptes individuels ou de groupes Active Directory pour les utilisateurs et les administrateurs

- Politiques en matière de mots de passe configurables
  - Capacité de préciser les politiques en matière de mots de passe pour les comptes locaux et LDAP
  - Historique des mots de passe (de 0 à 24)
  - Longueur minimale du mot de passe (de 0 à 14)
  - Longueur maximale du mot de passe (14 [authentification locale], 63 [LDAP])
  - Durée de vie minimale du mot de passe (de 0 à 998 jours)
  - Durée de vie maximale du mot de passe (de 1 à 999 jours)
  - Mot de passe complexe requis (oui/non)
  - Politiques en matière de blocage de compte
  - Seuil de blocage (de 0 à 999 tentatives)
  - Durée du blocage (de 1 à 99 999 minutes)
  - Remise à zéro du compteur lié au blocage (de 1 à 99 999 minutes)
- Écran de veille avec protection par mot de passe – verrouillage de l'écran après la période d'inactivité définie. L'écran de veille ne sera pas activé pendant l'acquisition (activé/désactivé, de 1 à 999 minutes, protégé par mot de passe oui/non)
- Cryptage des données de patients
  - Cryptage au moyen de la fonctionnalité Bitlocker en AES 128 bits (peut être activé lors de l'installation)
  - DICOM (DICOM sécurisé, géré au moyen de certificats)
- Exportation des listes de contrôle
  - Possibilité d'exporter les listes de contrôle en utilisant la fonction de journal d'exploitation

Philips reconnaît l'importance de sécuriser vos instruments médicaux et de protéger les données de vos patients. Ensemble, nous pouvons maintenir un environnement sécurisé en restant vigilants et en définissant le paysage des cybermenaces en constante évolution. Nous nous engageons à répondre aux besoins et aux exigences de nos clients.

Pour illustrer la posture de sécurité du système de RM Ingenia de Philips, ce système a reçu une autorisation de fonctionnement (ATO) de la DHA (Defense Health Agency) des États-Unis en fonction des exigences relatives à la conformité et des évaluations des risques requises par le processus du cadre de gestion du risque. L'approche fondée sur les risques a été élaborée par le NIST (National Institute for Standards and Technology) pour créer une méthode de sécurité stricte comprenant une surveillance continue de tous les contrôles d'assurance de l'information.

[1] D'après Digitalhealth, le 27 octobre 2017 (www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested)

[2] D'après BankInfo Security (www.bankinfosecurity.com/wannacry-healthcare-reax-a-9921)

www.philips.com

4522 991 34081 * FÉVR. 2018