La cybersécurité pour la surveillance des patients

Cadre de sécurité relatif aux moniteurs pour les patients, aux centres de contrôle et aux passerelles

Document destiné aux professionnels de santé.

NIHON KOHDEN

LA CYBERSÉCURITÉ – UN ENJEU MONDIAL

Le domaine de la sécurité opérationnelle ne se limite plus aux systèmes informatiques administratifs. Il englobe désormais les infrastructures critiques. Les réseaux qui intègrent des dispositifs médicaux sont exposés à des risques nettement plus élevés en cas de dysfonctionnement que les environnements informatiques classiques. Les systèmes de surveillance des patients sont tout particulièrement exposés à ce type de vulnérabilité. En cas de défaillance totale de ces systèmes ou d'atteinte à leur intégrité, ils pourraient ne pas détecter à temps des états pathologiques susceptibles de mettre en péril la vie des patients.

Nihon Kohden adopte une approche globale visant à protéger les patients et à garantir la fiabilité de la surveillance des personnes hospitalisées. Cet engagement ne se limite pas seulement à la sécurité des appareils, mais s'étend à l'ensemble du spectre du réseau et des communications avec les systèmes hospitaliers.

Notre approche de la surveillance de la sécurité des réseaux se compose de plusieurs éléments distincts : la sécurité des appareils, la sécurité des réseaux et la sécurité des connexions aux réseaux hospitaliers. Cette synergie constitue la base de la prévention des menaces et des dysfonctionnements dans le domaine des technologies de l'information.

En tant que fabricant de dispositifs médicaux, Nihon Kohden surveille attentivement le marché pour détecter les nouvelles vulnérabilités des systèmes utilisés. Des mesures sont prises rapidement afin de garantir la sécurité opérationnelle des dispositifs et, par conséquent, la sécurité des patients. En réponse aux menaces existantes, un groupe de travail dédié à la cybersécurité a été créé en vue d'évaluer les demandes, de formuler des mesures et de concevoir des méthodes visant à renforcer la sécurité de nos solutions médicales.

LA CONCEPTION AU SERVICE DE LA SÉCURITÉ

Responsabilités partagées du fournisseur et de l'utilisateur

La cybersécurité des dispositifs médicaux est une responsabilité commune des fabricants et des opérateurs. Pour Nihon Kohden, en tant que fabricant, cette responsabilité implique non seulement de sécuriser les dispositifs médicaux eux-mêmes, mais aussi de déterminer des caractéristiques techniques appropriées pour le déploiement de ces dispositifs dans l'environnement opérationnel et réseau.

Les opérateurs, en vertu de leur responsabilité première concernant ces environnements, doivent agir dans le respect de la sécurité et se conformer aux recommandations du fabricant. Le rôle de Nihon Kohden est d'aider les opérateurs à déployer des produits et des services spécifiques, garantissant ainsi un niveau élevé de sécurité opérationnelle.

La sécurité des appareils est assurée par des tâches définies par le fabricant qui correspondent à l'utilisation prévue de ces appareils, ainsi que par des instructions relatives à une intégration sécurisée au sein d'un réseau médical. Les prestataires de soins doivent intégrer des mesures de cybersécurité lors de la mise en œuvre du système afin de créer un environnement protégé (conformément à la norme IEC 80001).

Pendant la phase de conception, Nihon Kohden intègre des processus qui tiennent compte des vecteurs d'attaque potentiels. Lorsque de nouvelles menaces apparaissent, des contre-mesures appropriées sont rapidement mises en œuvre afin de protéger les appareils. La surveillance proactive du réseau permet de détecter les attaques potentielles, ce qui permet d'adopter des mesures de protection avant que les acteurs de la menace ne puissent porter atteinte à l'intégrité du système.

Sécurité du réseau

Les vecteurs de menace couramment exploités tels que le phishing, les pages web malveillantes et les fenêtres contextuelles ne sont pas pertinents ici, car le système reste déconnecté d'internet et du réseau hospitalier. En l'absence de connexion aux serveurs de commande et de contrôle, il n'y a aucun risque que des données soient exfiltrées et qu'il soit porté atteinte à leur intégrité.

Le réseau de surveillance, y compris les moniteurs individuels, les stations centrales pour le personnel infirmier et les solutions de passerelle, fonctionne au sein d'un réseau physiquement isolé, comme précisé par le fabricant. Cet isolement offre l'avantage d'une séparation complète du réseau hospitalier, atténuant toute interférence potentielle même si l'infrastructure réseau de l'hôpital subit des perturbations telles que des défaillances de composants de gestion ou des pertes de configuration.

La transmission de données en temps réel caractérise le réseau de surveillance. Tout problème de communication entre les moniteurs de surveillance et les centres de contrôle déclenche des alertes d'erreur de communication.

Nihon Kohden utilise des logiciels avancés pour surveiller le trafic du réseau, détecter les activités anormales à un stade précoce et mettre en œuvre des mesures de protection. Par conséquent, les outils de surveillance et de contrôle du réseau sont intégrés de manière transparente dans la solution de soins du réseau.

Si le réseau de surveillance doit utiliser des composants actifs exploités par des établissements de santé (tels que des commutateurs), le client doit procéder à une évaluation des risques. Cette évaluation porte sur tous les facteurs influençant la communication entre les moniteurs de surveillance et les centres de contrôle. Il est impératif d'empêcher à tout prix que le trafic de données soit mixte, même en cas de défaillance des composants de commande du commutateur.

Sécurité des transmissions et protection des données

Afin d'empêcher les appareils non autorisés d'accéder au réseau, le filtrage des adresses MAC est utilisé au niveau des composants à la périphérie du réseau, ce qui renforce la sécurité des points d'accès.

Seuls les appareils approuvés ont accès à la zone de surveillance des patients. Tous les autres dispositifs sont bloqués efficacement. En outre, Nihon Kohden garantit la confidentialité des données en les chiffrant entre les moniteurs de surveillance et les centres de contrôle.

Pour les appareils de télémétrie ou les moniteurs pour le transport qui fonctionnent au sein du réseau local sans fil du client (une action planifiée nécessitant une passerelle de télémétrie), la connexion entre les appareils et les points d'accès doit être sécurisée à l'aide de la norme WPA2 ou ultérieure. Ces appareils prennent en charge diverses méthodes de sécurité standard, notamment la norme WPA2 (PSK, Enterprise, 802.1x).

Transition vers le réseau des établissements de santé – Échange de données

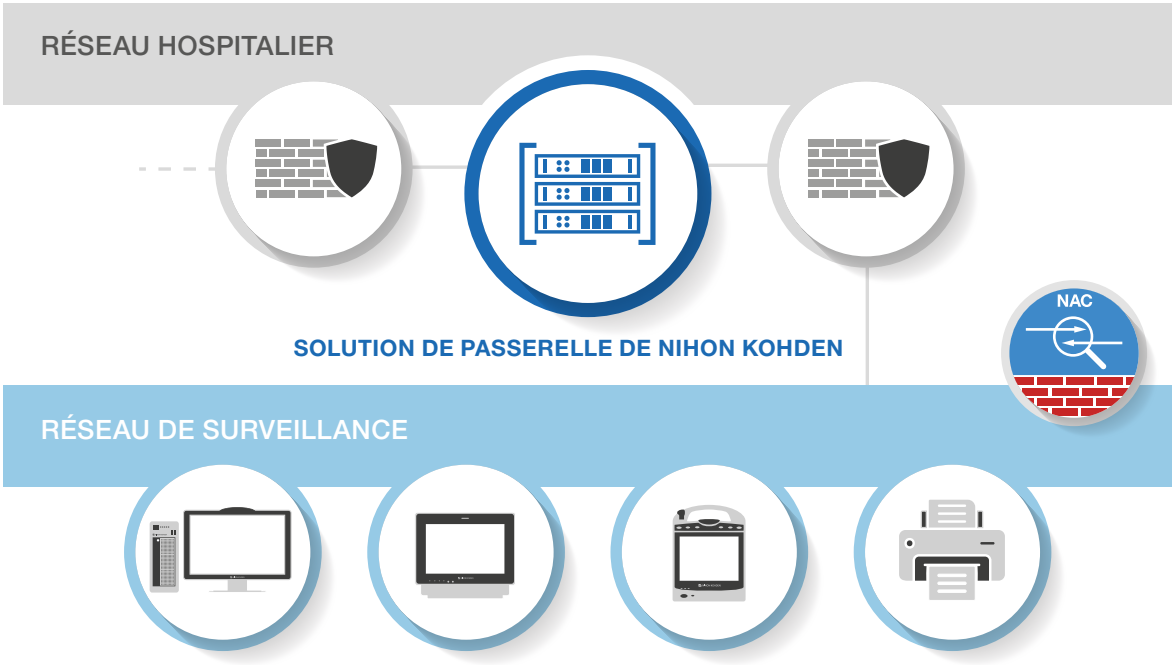
Nihon Kohden a pour rôle de soutenir les opérateurs au moyen de produits et de services dédiés visant à optimiser la sécurité opérationnelle.

Il est essentiel de disposer d'une passerelle afin de permettre l'échange de données entre le réseau de surveillance et les systèmes des centres hospitaliers ou des établissements de santé. Une telle passerelle comporte deux interfaces, ce qui permet de préserver l'isolement physique du réseau de surveillance.
Elle récupère, traite et échange les données entre le réseau de surveillance et le réseau du centre hospitalier ou de l'établissement de santé. Les centres de données centralisés améliorent la disponibilité des services et contribuent à la cybersécurité grâce à l'isolation des systèmes et au contrôle des accès. Nihon Kohden facilite l'installation des passerelles dans les centres de données, en prenant en charge toutes les solutions de virtualisation disponibles sur le marché.

Les serveurs fonctionnent sur les plateformes Microsoft Windows modernes. Les applications et les extensions sont exclusivement installées en tant que services, ce qui réduit au minimum la nécessité d'ouvrir des sessions sur les serveurs, qui sont réservées à des fins de maintenance. Le système est compatible avec les logiciels antivirus courants et, si nécessaire, le pare-feu interne peut être activé, s'il ne l'est pas déjà au niveau du réseau.

Nihon Kohden fournit sur son site web, des informations actualisées sur les mises à jour de Windows et la validation des correctifs. L'installation en temps voulu des correctifs approuvés garantit que le système est protégé et fonctionne de manière sûre.

Recommandation concernant la sécuritédu réseau



Afin de garantir l'intégrité et la sécurité des données au sein du réseau de surveillance, il est impératif d'isoler le trafic de manière stricte. Nihon Kohden conseille un isolement physique entre le réseau de surveillance et le trafic des clients. L'utilisation d'infrastructures réseau distinctes offre une meilleure protection contre les attaques provenant du réseau client.

Afin d'assurer une protection complète du réseau contre le réseau client, il est recommandé de mettre en place des zones protégées par pare-feu, avec une protection au niveau des ports pour chaque carte réseau et chaque direction de la passerelle.

Sécurité des appareils

Tous les moniteurs de surveillance fixes et les appareils de télémétrie sont dotés de systèmes d'exploitation renforcés, distincts des plateformes Windows ou Linux.

Les services à distance sont réduits au minimum et excluent les interventions critiques. Nihon Kohden privilégie la sécurité des patients en adoptant une approche prudente. La probabilité d'attaques externes ou d'atteinte à l'intégrité des données en extrayant des informations est faible, étant donné que le protocole de préparation des données n'est pas public.

Un chiffrement performant des données et des mesures de protection de l'intégrité des appareils de bout en bout empêchent l'accès aux données et l'infiltration de données de tiers.

Les centres de surveillance sont protégés contre les modifications logicielles non autorisées grâce à l'établissement d'une liste blanche et au confinement du système de démarrage dans une zone protégée. Le système de démarrage est externalisé dans une zone sécurisée, ce qui empêche l'exécution de logiciels malveillants après le redémarrage du centre de contrôle.

Improving Healthcare with Advanced Technology

Depuis sa fondation en 1951, Nihon Kohden a pour mission d'améliorer la qualité de la vie au moyen de technologies d'avant-garde. Nous développons des solutions dans des domaines essentiels tels que les diagnostiques, les soins intensifs, les informations cliniques et les diagnostiques in vitro ; nous sommes à vos côtés pour confronter les défis de la santé d'aujourd'hui et de demain.

N'hésitez pas à visiter notre site **www.nihonkohden.com**

NIHON KOHDEN FRANCE SARL
Centre d' Affaires, La Boursidière,
Bâtiment C – RDC, 92357 Le Plessis-Robinson, France
Téléphone: +33 1 49080550, Fax: +33 1 49089332
Internet : https://eu.nihonkohden.com, E-mail : info@nkfrance.fr
SIRET 479 402 935 00023 (RCS Créteil B)

NIHON KOHDEN EUROPE GmbH
Raiffeisenstrasse 10, 61191 Rosbach, Allemagne
Téléphone: +49 6003 827 0, Fax: +49 6003 827 599
Internet : https://eu.nihonkohden.com, E-mail : info@nke.de

NIHON KOHDEN CORPORATION
1-31-4 Nishiochiai, Shinjuku-ku, Tokyo 161-8560, Japon
Téléphone : +81 (3) 59 96-80 36, Fax : +81 (3) 59 96-81 00
Internet : www.nihonkohden.com

Date dernière modification : Novembre 2023
Fabricant : Nihon Kohden Corporation Japon
Bon usage : vous référer à la notice d'utilisation

NIHON KOHDEN

E/BR-CYSEC-FR01