Cybersicherheit bei der Patientenüberwachung

Sicherheitsrahmen für Patientenmonitore, Kontrollzentren und Gateways

NIHON KOHDEN

CYBERSICHERHEIT – EINE GLOBALE HERAUSFORDERUNG

Der Bereich Betriebssicherheit ist nicht mehr nur auf administrative IT-Systeme beschränkt, sondern umfasst nun auch kritische Infrastrukturen. Netzwerke, zu denen medizinische Geräte gehören, sind im Störungsfall mit deutlich höheren Risiken behaftet als herkömmliche IT-Umgebungen. Patientenüberwachungssysteme bilden in diesem Zusammenhang eine besonders ausgeprägte Schwachstelle. Wenn diese Systeme beeinträchtigt werden oder komplett ausfallen, werden lebensbedrohliche Zustände bei Patienten unter Umständen nicht rechtzeitig erkannt.

Nihon Kohden setzt auf einen umfassenden Ansatz zum Schützen der Patienten und Sichern der Zuverlässigkeit bei der Patientenüberwachung. Das Engagement geht über die reine Gerätesicherheit hinaus – einbezogen ist das gesamte Spektrum der Vernetzung und Kommunikation mit Krankenhaussystemen.

Unser Ansatz zur Sicherheit von Monitoring-Netzwerken berücksichtigt mehrere unterschiedliche Elemente – Gerätesicherheit und Netzwerksicherheit ebenso wie die Sicherheit der Verbindungen zu Krankenhausnetzwerken. Die Synergie dieser Kombination bildet die Grundlage für die Abwehr von Bedrohungen und Fehlfunktionen im IT-Bereich.

Als Hersteller medizinischer Geräte behält Nihon Kohden das Marktumfeld aufmerksam im Blick, um neue Schwachstellen bei den verwendeten Systemen zu erkennen. Für die Betriebssicherheit der Geräte und damit auch die Sicherheit der Patienten werden im Fall der Fälle unverzüglich Maßnahmen ergriffen. Als Reaktion auf die aktuelle Bedrohungslage wurde eine spezielle Taskforce für Cybersicherheit eingerichtet, um Anfragen auszuwerten, Maßnahmen zusammenzustellen und Methoden zum Steigern der Sicherheit unserer medizinischen Lösungen auszuarbeiten.

SICHERHEIT VON GRUND AUF

Gemeinsame Verantwortung von Anbieter und Nutzer

Die Cybersicherheit von medizinischen Geräten liegt in der gemeinsamen Verantwortung von Herstellern und Anwendern. Für Nihon Kohden als Hersteller umfasst diese Verantwortung nicht nur die Sicherung der medizinischen Geräte selbst, sondern auch die Festlegung geeigneter Spezifikationen für den Einsatz dieser Geräte in der vorgesehenen Betriebs- und Netzwerkumgebung.

Anwender müssen aufgrund ihrer vorrangigen Verantwortung für diese Umgebungen sicherheitsbewusst handeln und sich an die Empfehlungen der Hersteller halten. Die Aufgabe von Nihon Kohden besteht darin, Anwender beim Einsatz von zweckgerechten Produkten und Dienstleistungen zu unterstützen, um damit für ein hohes Maß an Betriebssicherheit zu sorgen.

Gerätesicherheit wird erreicht durch vom Hersteller vorgegebene Maßnahmen, die auf den Verwendungszweck des jeweiligen Geräts abgestimmt sind. Hinzu kommen Anleitungen für die sichere Integration in ein medizinisches Netzwerk. Gesundheitsdienstleister müssen (gemäß IEC 80001) bei der Systemimplementierung Maßnahmen für Cybersicherheit integrieren, um eine geschützte Umgebung zu schaffen.

Nihon Kohden bindet Prozesse zur Berücksichtigung möglicher Angriffsvektoren schon in der Entwurfsphase ein. Wenn neue Bedrohungen aufkommen, werden schnell geeignete Gegenmaßnahmen eingeleitet, um die Geräte zu schützen. Durch proaktive Überwachung des Netzwerksystems werden potenzielle Angriffe erkannt, sodass Schutzaktionen zum Einsatz kommen, bevor Bedrohungsakteure das System gefährden können.

Netzwerksicherheit

Gängige Bedrohungsvektoren wie Phishing, schädliche Webseiten und Pop-ups sind hier irrelevant, da das System vom Internet und vom Krankenhausnetzwerk getrennt bleibt. Das Risiko einer Datenexfiltration und -kompromittierung ist nicht gegeben, da keine Verbindung zu Befehls- und Kontrollservern besteht.

Das Monitoring-Netzwerk – einschließlich von Bettseitmonitoren, zentralen Pflegestationen und Gateway-Lösungen – wird der Spezifikation des Herstellers entsprechend innerhalb eines physisch isolierten Netzwerks betrieben. Vorteil dabei ist die vollständige Abtrennung vom Krankenhausnetzwerk, wodurch potenzielle Gefahren selbst dann abgewehrt werden, wenn es bei der Infrastruktur des Krankenhausnetzwerks zu Störungen etwa durch den Ausfall von Managementkomponenten oder den Verlust der Konfiguration kommt.

Das Überwachungsnetzwerk zeichnet sich durch Datenübertragung in Echtzeit aus. Jegliche Kommunikationsprobleme zwischen Überwachungsmonitoren und Überwachungszentren lösen entsprechende Fehleralarme aus.

Nihon Kohden nutzt fortschrittliche Software zur Überwachung des Netzwerk-Traffics. Ungewöhnliche Aktivitäten werden damit frühzeitig erkannt, um dann entsprechende Schutzmaßnahmen einzuleiten. Tools zur Netzwerküberwachung und -steuerung sind insofern nahtlos in die Netzwerklösung integriert.

Wenn für das Monitoring-Netzwerk klinikeigene aktive Komponenten (beispielsweise Switches) genutzt werden sollen, muss der Kunde eine Risikobewertung durchführen. In diese umfassende Bewertung fließen alle Faktoren ein, die sich auf die Kommunikation zwischen Überwachungsmonitoren und Kontrollzentren auswirken. Eine Vermischung des Datenverkehrs muss unbedingt vermieden werden, auch wenn Fehler in den Steuerungskomponenten des Switches auftreten.

Übertragungssicherheit und Datensicherung

Um zu verhindern, dass nicht autorisierte Geräte auf das Netzwerk zugreifen, wird bei den Komponenten am Netzwerkrand MAC-Adressfilterung eingesetzt. Dadurch steigt die Endpunktsicherheit.

Nur zugelassene Geräte erhalten Zugang zum Patientenüberwachungsbereich – alle anderen Geräte werden effektiv blockiert. Zudem sichert Nihon Kohden die Vertraulichkeit der Daten durch Verschlüsselung zwischen Patientenüberwachungsmonitoren und Kontrollzentren.

Bei Telemetriegeräten oder Transportmonitoren, die (per geplanter Aktion mit erforderlichem Telemetrie-Gateway) im WLAN des Kunden betrieben werden, muss die Verbindung zwischen Endgeräten und Access Points mindestens mit WPA2 abgesichert werden. Diese Endgeräte unterstützen verschiedene Sicherheitsstandards wie WPA2 (PSK, Enterprise, 802.1x).

Datenaustausch beim Übergang zum Krankenhausnetzwerk

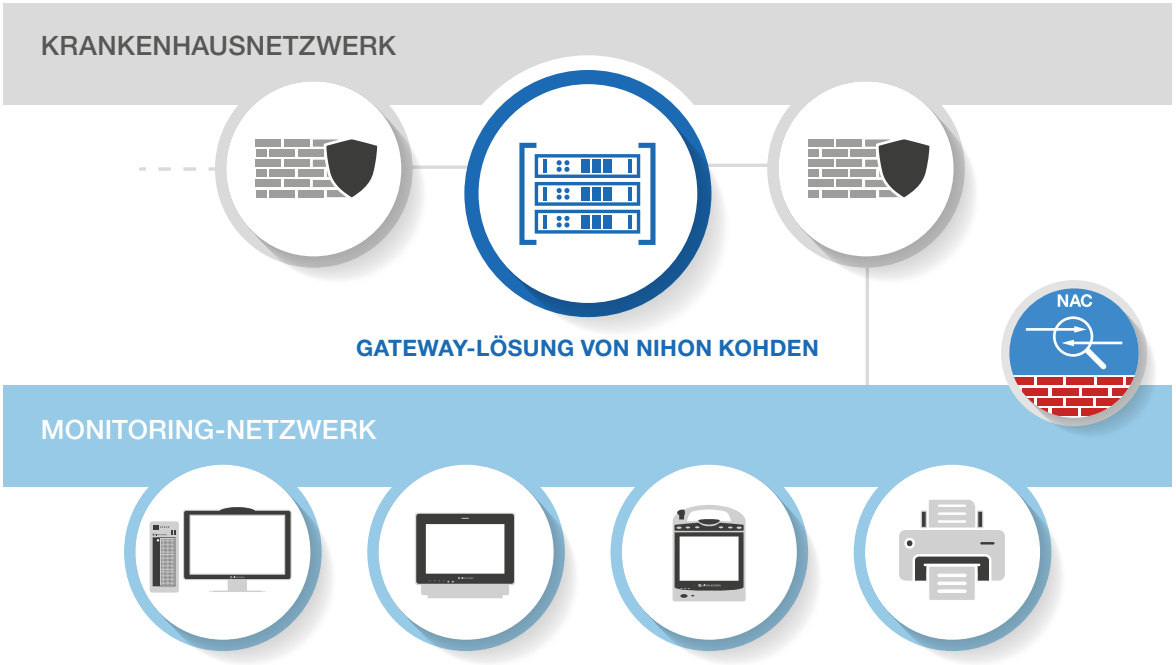
Nihon Kohden hat in diesem Zusammenhang schwerpunktmäßig die Aufgabe, Anwender durch spezielle Produkte und Dienstleistungen zu unterstützen, damit eine hohe Betriebssicherheit aufrechterhalten bleibt.

Um den Datenaustausch zwischen Monitoring-Netzwerk und Krankenhaussystemen zu ermöglichen, ist ein Gateway erforderlich. Dieses mit zwei Schnittstellen ausgestattete Gateway sorgt für die physische Abtrennung des Monitoring-Netzwerks. Das Gateway ruft Daten ab, verarbeitet sie und übernimmt den Datenaustausch zwischen dem Monitoring-Netzwerk und dem Krankenhausnetzwerk. Zentralisierte Rechenzentren verbessern die Serviceverfügbarkeit und tragen durch getrennte Systeme und kontrollierten Zugang zur Cybersicherheit bei. Nihon Kohden ermöglicht die Installation von Gateways in Rechenzentren und unterstützt alle auf dem Markt erhältlichen Virtualisierungslösungen.

Die Server werden auf modernen Microsoft-Windows-Plattformen ausgeführt. Applikationen und Erweiterungen werden ausschließlich als Services installiert. Die Notwendigkeit von Serveranmeldungen, die für Servicezwecke reserviert sind, beschränkt sich dadurch auf ein Minimum. Das System unterstützt gängige Antivirenscanner, und bei Bedarf kann die interne Firewall aktiviert werden, sofern die Aktivierung nicht bereits auf Netzwerkebene erfolgt ist.

Auf der Website von Nihon Kohden sind aktuelle Informationen zu Windows-Updates und zur Patch-Validierung abrufbar. Durch rechtzeitige Installation der genehmigten Patches kann für den sicheren und geschützten Betrieb des Systems gesorgt werden.

Empfehlung zur Netzwerksicherheit



Für die Datenintegrität und -sicherheit innerhalb des Monitoring-Netzwerks ist eine strikte Trennung des Datenverkehrs unerlässlich. Nihon Kohden empfiehlt eine physische Trennung zwischen dem Monitoring-Netzwerk und dem Kundendatenverkehr. Eine geteilte Netzwerkinfrastruktur bietet besseren Schutz vor Angriffen, die ihren Ursprung im Kundennetzwerk haben.

Für umfassenden Schutz des Monitoring-Netzwerks gegenüber dem Kundennetzwerk empfiehlt es sich, Firewall-Zonen mit Sicherheit auf Port-Ebene für jede Netzwerkkarte und Gateway-Richtung anzulegen.

Gerätesicherheit

Alle stationären Überwachungsmonitore und Telemetriegeräte verfügen über gehärtete Betriebssysteme, die sich von Windows- oder Linux-Plattformen unterscheiden.

Remote-Services werden auf ein Mindestmaß reduziert und schließen kritische Eingriffe aus. Nihon Kohden räumt der Patientensicherheit durch umsichtiges Vorgehen Priorität ein. Die Wahrscheinlichkeit für externe Angriffe oder Datenkompromittierung durch Informationsextraktion ist gering, da das Datenaufbereitungsprotokoll nicht öffentlich ist.

Durch robuste Datenverschlüsselung und Endpunkt-zu-Endpunkt-Schutz der Geräteintegrität werden Datenzugriffe und das Eindringen fremder Daten verhindert.

Überwachungszentren sind durch Whitelisting und die Eingrenzung von Startsystemen innerhalb eines geschützten Bereichs vor unbefugten Software-Modifikationen geschützt. Das Startsystem wird in einen sicheren Bereich ausgelagert, um die Ausführung von Malware nach dem Neustart des Kontrollzentrums zu verhindern.

Improving Healthcare with Advanced Technology

Seit der Gründung im Jahr 1951 hat es sich Nihon Kohden zur Aufgabe gemacht, die Lebensqualität durch fortschrittliche Technologien zu verbessern. Wir bieten Lösungen für Diagnose, Intensivmedizin, klinische Informationen und In-vitro-Diagnostik – und wir arbeiten mit Ihnen zusammen, um den Herausforderungen des Gesundheitswesens von heute und morgen gerecht zu werden.

Für mehr Informationen besuchen Sie uns bitte auf **www.nihonkohden.com**

NIHON KOHDEN DEUTSCHLAND GmbH
Raiffeisenstrasse 10, 61191 Rosbach, Deutschland
Telefon: +49 6003 827 0, Fax: +49 6003 827 599
Internet: https://eu.nihonkohden.com, E-mail: bestellung@nke.de

NIHON KOHDEN EUROPE GmbH
Raiffeisenstrasse 10, 61191 Rosbach, Deutschland
Telefon: +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, Japan
Telefon: +81 (3) 59 96-80 36, Fax: +81 (3) 59 96-81 00
Internet: www.nihonkohden.com

NIHON KOHDEN

E/BR-CYSEC-DE01