

IEC 80001 – Übersicht

DEUTSCH

Allgemeine Informationen

Die folgenden Informationen sind für den Risikomanager des medizinischen IT-Netzwerks innerhalb der verantwortlichen Organisation bestimmt (um Aufgaben gemäß IEC 80001-1:2010 und IEC 60601-1:2005+AMD1:2012 durchzuführen).

Diese Informationen gelten für folgende Brainlab-Produkte:

| | Produkte |
|----------------------------|--|
| Plattformen | <ul style="list-style-type: none"> • Buzz • Buzz Navigation CM • Cirq Robotisches Ausrichtungsmodul • Curve Navigation 17700 • Curve Ceiling-Mounted • Curve-Navigationsstation • Digital Lightbox • Digitaler OP-Computer für Barco-Integration • Kick EM-Navigationsstation • Kick-Navigationsstation • iPlan Net (3.6, 3.7) • Origin Server (3.x) • Kolibri-Navigationsstation 2.x • VectorVision Compact • VectorVision Sky • VectorVision² |
| RT-Patientenpositionierung | <ul style="list-style-type: none"> • ExacTrac |
| Software | <ul style="list-style-type: none"> • Alle Brainlab-Elements • Jegliche Brainlab-Navigationssoftware • DICOM Viewer für Touchscreen-PC • iPlan 3.0 (Cranial/ENT/CMF/Stereotaxy/Flow/Spine/View) • iPlan RT (4.1, 4.5) • Qentry |

PEMS zur Integration in IT-Netzwerke

Wenn ein Brainlab-Produkt in ein IT-Netzwerk mit anderen Geräten eingebunden wird, könnten unbekannte Risiken für Patienten, Bediener oder Dritte entstehen.

Die verantwortliche Organisation sollte diese Risiken bestimmen, analysieren, bewerten und kontrollieren. Spätere Änderungen am IT-Netzwerk könnten zu neuen Risiken führen und daher zusätzliche Analysen erfordern. Änderungen am IT-Netzwerk schließen Folgendes ein:

- Änderungen an der IT-Netzwerkkonfiguration
- Anschließen zusätzlicher Elemente an das IT-Netzwerk
- Entfernen von Elementen aus dem IT-Netzwerk
- Updates/Upgrades von Geräten, die mit dem IT-Netzwerk verbunden sind

Gültige Gruppenrichtlinieneinstellungen

Um die korrekte Funktion des Systems zu gewährleisten, ändern Sie die folgenden Gruppenrichtlinieneinstellungen für Windows 10 nicht, wenn das System in ein Krankenhausnetzwerk integriert ist (z. B. durch einen Domänen-Controller).

Dies gilt für die Einstellungen unter folgendem Pfad:

Computer/Policies/Administrative Templates (Computer/Richtlinien/Administrative Vorlagen):

- Control Panel/Personalization (Systemsteuerung/Personalisierung)
- Control Panel/User Accounts (Systemsteuerung/Benutzerkonten)
- System/Device Installation (System/Geräteinstallation)
- System/Logon (System/Anmeldung)
- System/Internet Communication Management (System/Internetkommunikationsverwaltung)
- System/Power Management (System/Energieverwaltung)
- System/Shutdown (System/Herunterfahren)
- Windows Components/AutoPlay Policies (Windows-Komponenten/Richtlinien für die automatische Wiedergabe)
- Windows Components/Desktop Window Manager (Windows-Komponenten/Desktopfenster-Manager)
- Windows Components/Event Log Service (Windows-Komponenten/Ereignisprotokollendienst)
- Windows Components/Internet Explorer/Security Features/Add-on Management (Windows-Komponenten/Internet Explorer/Sicherheitsfunktionen/Add-On-Verwaltung)
- Windows Components/Windows Defender/Exclusions (Windows-Komponenten/Windows Defender/Ausschlüsse)
- Windows Components/Windows Update (Windows-Komponenten/Windows Update)

Technische Spezifikationen der Netzwerkverbindung

Brainlab-Plattformen verfügen über folgende IT-Netzwerkverbindungen:

| | Alle Plattformen | Manche Plattformen |
|--------------------|---|---|
| Netzzugangsschicht | ≥ 1 Ethernet-Port, kompatibel mit 100/1000BASE-T-Netzwerken | <ul style="list-style-type: none"> • Ethernet-Ports, kompatibel mit 1000BASE-T-Netzwerken • WLAN kompatibel mit IEEE 802.11b/g/n/ac |
| Internetschicht | IPv4-Konnektivität | IPv6-Konnektivität |

HINWEIS: Genauere Informationen zur Kompatibilität erhalten Sie in den entsprechenden Benutzerhandbüchern.

Produktkonfigurationen

Produkte, die von einem Brainlab-Kundendienstmitarbeiter installiert und konfiguriert werden, sind mit dem Microsoft Baseline Security Analyzer (MSBA) für IT-Sicherheit konform (wenn dies technisch durchführbar und sinnvoll ist).

Beachten Sie, dass sich nachfolgende Modifikationen auf die Sicherheit und Leistung des Produkts auswirken können.

Erforderliche IT-Netzwerkkonfigurationen

Firewalls müssen entsprechend der in diesem Dokument aufgelisteten IT-Netzwerkspezifikationen konfiguriert werden.

Brainlab hält Netzwerke, die nicht vor unberechtigtem Zugriff geschützt sind, für fehleranfällig.

Risiken durch IT-Netzwerkfehler

Bei der zeitkritischen OP-Planung führen Netzwerkfehler zu keinen Gefahrensituationen.

Wenn die IT-Netzwerkverbindung ausfällt, kann die Behandlung jedoch möglicherweise nicht fortgesetzt bzw. muss wiederholt werden. Wird ExacTrac während dieses Netzwerkausfalls verwendet, kann dies zu einer unnötigen KV-Bildgebung am Patienten führen.

Wenn darüber hinaus der intraoperative DICOM Push (von der Modalität oder dem C-Bogen) an das Brainlab-Produkt fehlschlägt, kann das Brainlab-Produkt nicht mehr für die Patientenbehandlung verwendet werden.

Technische Anleitungen und Handbücher

Die folgenden Dokumente sind auf Anfrage für Ihre Produktplattform erhältlich:

- DICOM-Konformitätserklärungen: (<https://www.brainlab.com/dicom>)
- FDA- und CE-Erklärungen
- IT-Netzwerkplanung
- Navigationssoftware-Benutzerhandbuch
- System- und Technisches Benutzerhandbuch
- Klinisches Benutzerhandbuch
- Technisches Spezifikationsblatt

Produktrückrufe

Bei auftretenden Mängeln informiert Brainlab seine Kunden umgehend.

Benachrichtigungen zur Cyber-Sicherheit

Wenn Cyber-Sicherheitslücken identifiziert werden, informiert Brainlab alle Kunden und stellt entsprechend Software-Updates zur Verfügung.

IEC 80001 – Übersicht

Vorgesehener Informationsfluss und IT-Netzwerkspezifikationen

| BETROFFENE PRODUKTE | ZWECK DER VERBINDUNG ZUM IT-NETZWERK | IT-NETZWERKANFORDERUNGEN | | SICHERHEITSSPEZIFIKATIONEN | | | | |
|---|--|---------------------------------------|---|---|--|--|--|-----------|
| | | VERFÜGBARE BANDBREITE | ZUSÄTZLICHE ANFORDERUNGEN | PROTOKOLL | PORT | | | |
| Alle Produkte | Laden von medizinischen Bilddaten | ≥ 100 Mbit/s (empfohlen: 1 Gbit/s) | Speicherplatz: ≥ 250 GB (empfohlen: SSD) | DICOM | • 104/TCP (geschlossen für externe Verbindungen) • 11112/TCP | | Eingehend & Ausgehend | |
| | Speichern medizinischer Bilddaten | | | CIFS | 445/TCP | | | |
| | Fernzugriff auf HTML5-Applikationen | ≥ 10 Mbit/s | Latenz < 100 ms | • HTTP • HTTPS | • 44388/TCP/UDP • 55581/TCP/UDP | | Eingehend | |
| | Remote-Support | ≥ 2 Mbit/s | • Internetzugriff • Latenz < 100 ms | iHelp® (Axeda) | 443/TCP | Authentifizierungsserver | support.brainlab.com | Ausgehend |
| | | | | | | Europa | gas-de2.axeda.com gas-de3.axeda.com gas.ie1.axeda.com gas.ie2.axeda.com | |
| Nord- und Südamerika | | | | | | ghsom1.axeda.com gas-bo3.axeda.com gas-bo7.axeda.com ghsj1.axeda.com ghsj2.axeda.com | | |
| Asien/Pazifik | | | | | | ghjap1.axeda.com ghjap2.axeda.com gas-aus2.axeda.com gas-aus3.axeda.com gas-cne4.axeda.com gas-cne6.axeda.com | | |
| | | | | | Vereinigtes Königreich | ghuk2.axeda.com ghuk3.axeda.com | | |
| | | | | | USA | servicesus1.quentry.com v01-us1.quentry.com v02-us1.quentry.com | | |
| | | | | | EU | serviceseu1.quentry.com v01-eu1.quentry.com v02-eu1.quentry.com | | |
| Plattformen | Quentry-Cloud-Zugriff | ≥ 2 Mbit/s (empfohlen: 10 Mbit/s) | – | Quentry | | | | |
| | Buzz-Fernbedienung | ≥ 15 Mbit/s | WLAN-Verbindung | Brainlab-Fernsteuerung | 55578/TCP | | Eingehend | |
| | Kommunikation mit Cirq Robotischem Ausrichtungsmodule via Medineering-Positionierarm | ≥ 1 Mbit/s | Latenz < 100 ms | • HTTP • HTTPS | • 80 TCP • 443 TCP | | Ausgehend | |
| | Herstellen von Datenverbindungen | – | – | mDNS/DNS-SD | 5353/UDP (Multicast 224.0.0.251) | | | |
| | Verbindung zu Bildgebungsmodalitäten | ≥ 1 Mbit/s | Verbindungen innerhalb derselben Broadcast-Domäne für minimale Latenz | BK Medical OEM-Schnittstelle | 7915/TCP | | Eingehend & Ausgehend | |
| | | | | Brainlab C-Bogen | • 44445/TCP/UDP • 55555/TCP/UDP • 56666/TCP/UDP | | | |
| | Übertragung von Navigationsinformationen | | | NTP | 123/UDP | | Ausgehend | |
| | Session-Sharing | ≥ 1 Gbit/s | | • Brainlab flex • Backbone | • 57575/TCP • 57574/TCP • 50001/TCP • 57581/TCP • 50002/UDP • 57578/TCP/UDP | | Eingehend | |
| | Video-Aufnahmen, -Streaming, -Konferenzen | ≥ 40 Mbit/s | – | • HTTP • HTTPS • SDP • RTP | • 80/TCP • 443/TCP • 3396/TCP • 57581/TCP • 55588/TCP • 55500/UDP | | | |
| | Remote-Desktop-Verbindungen (nur verfügbar mit Origin Server) | ≥ 1,5 Mbit/s | Latenz < 100 ms | • RDP • HTTPS | • 3389 (konfigurierbar)/TCP • 443/TCP • 8080/TCP | | | |
| • Plattformen • RT-Patientenpositionierung | Benutzerauthentifizierung | – | Microsoft Active Directory® | • LDAP • LDAP SSL • LDAP GC • LDAP GC SSL • Kerberos • DNS • Microsoft-DS • Kerberos • Kerberos Passwort ändern | • 389/TCP/UDP • 636/TCP/UDP • 3268/TCP • 3269/TCP • 88/TCP • 53/TCP/UDP • 445/TCP/UDP • 464/TCP | | Ausgehend | |
| | Windows®-Domänen-Integration | | | • Microsoft-DS • Kerberos • LDAP • DNS | • 445/TCP/UDP • 389/UDP • 53/TCP/UDP • 88/TCP/UDP | | | |
| RT-Patientenpositionierung | Anschluss an Drittsysteme | ≥ 1 Mbit/s | – | VNC | 5900/TCP | | Eingehend | |
| | Anschluss an Linearbeschleuniger | – | • Latenz < 100 ms • Voll geschwichtetes Netzwerk | Varian ADI | 56050/TCP | | Eingehend & Ausgehend | |
| | | | | Elekta | • 135/TCP • 1801/TCP • 2101/TCP | | | |
| | Konfiguration von Firewalls | – | Drittsysteme | Varian | 56050/TCP | | | |
| Elekta (z. B. NSS) | | | | 9090/TCP | | | | |