Smith & Nephew, Inc.
2905 Northwest Blvd, Suite 40
Plymouth, MN 55441
USA

T +1 763 452 4950
F +1 763 452 4980
www.smith-nephew.com

Operationssystem RI.HIP NAVIGATION auf CORI◊

AKTUALISIEREN DES BETRIEBSSYSTEMS UND DER SICHERHEITSSOFTWARE

Allgemeine Informationen

Um den vorgesehenen Betrieb Ihres Operationssystems RI.HIP NAVIGATION auf CORI von Smith+Nephew dauerhaft sicherzustellen, empfiehlt Smith+Nephew die Einhaltung dieser Leitlinien für das Aktualisieren von Microsoft Windows und Antivirensoftware. Diese Leitlinien werden über diese Website fortlaufend aktualisiert. Bitte stellen Sie sicher, dass Sie mit dem IT-Sicherheitsteam Ihrer Einrichtung in Bezug auf die Verwendung von RI.HIP NAVIGATION und diese Leitlinien Rücksprache halten.

Windows-Updates

RI.HIP NAVIGATION wird standardmäßig über die Einstellungen der lokalen „Group Policy“ (Gruppenrichtlinie) konfiguriert. Wenn Ihre Einrichtung die Einstellungen für die Windows „Group Policy“ (Gruppenrichtlinie) auf Servern verwendet, auf denen die RI.HIP NAVIGATION-Software installiert ist, darf die Konfiguration nicht geändert werden.

Nur Microsoft-Sicherheitsupdates installieren. Es sind sowohl **monatliche Rollups** als auch **reine Sicherheitsupdates** erlaubt. Keine Service Packs und optionalen Updates installieren. Gemäß den Vorschriften für Medizinprodukte müssen Service Packs vom Medizinproduktehersteller geprüft und freigegeben werden. Wenn RI.HIP NAVIGATION zur Krankenhaus-Domain hinzugefügt wird, werden die Leitlinien in diesem Dokument empfohlen.

Auch wenn **Microsoft-Sicherheitsupdates** unverzüglich nach der Freigabe von Microsoft installiert werden können, empfiehlt Smith+Nephew die Installation erst nach fünf Werktagen vorzunehmen. Dieses Dokument wird innerhalb dieser fünf Tage gegebenenfalls aktualisiert, nachdem Smith+Nephew die Sicherheitsupdates beurteilt hat.

Nachfolgend sind die Informationen bezüglich folgender computergestützter Richtlinieneinstellungen aufgeführt:

Ab Windows 10:

- Die Funktion „**Empfohlene Updates über automatische Updates aktivieren**“ deaktivieren.
- Die Funktion „**Automatische Updates sofort installieren**“ deaktivieren.
- Die Funktion „**Keinen automatischen Neustart**“ für geplante Installationen automatischer Updates durchführen, wenn Benutzer angemeldet sind“ aktivieren.
- Die Funktion „**Automatische Updates konfigurieren**“ auf „**Deaktiviert**“ einstellen.

Während der Patientenbehandlung dürfen keine Updates installiert werden.

Die folgenden Sicherheitsupdates dürfen nicht installiert werden:

- **KB2823324**: Sicherheitsrisiken beim Kernelmodustreiber könnten die Erhöhung von Berechtigungen erlauben (2829996): MS13-036
- **KB2984615**: Sicherheitsrisiken beim Kernelmodustreiber könnten die Erhöhung von Berechtigungen erlauben (2984615) MS14-045
- **KB4577051**: 2020-09 Monatliches Sicherheitsqualitäts-Rollup für Windows Embedded Standard 7 für x64-basierte Systeme

Treiberupdates

Aktualisieren Sie keine Treiber in RI.HIP NAVIGATION.

Verwenden Sie weder die manuelle Einrichtung noch Windows-Updates, um Treiber in RI.HIP NAVIGATION zu aktualisieren. Diese Richtlinie wird durch die Einstellungen der „Group Policy“ (Gruppenrichtlinie) gewährleistet, die nicht geändert werden sollten.

Für Windows 10:

- Die Option „**Suchreihenfolge für Quellspeicherorte für Gerätetreiber festlegen**“ auf „**Aktiviert**“ einstellen und das Kontrollkästchen „**Nicht nach Windows-Updates suchen**“ markieren.
- Im Editor für die lokale „Group Policy“ (Gruppenrichtlinie) die Option „**Keine Treiber in Windows-Updates einschließen**“ auf „**Aktiviert**“ einstellen.

Anwendbare Einstellungen der „Group Policy“ (Gruppenrichtlinie)

Wenn Ihre Einrichtung die Einstellungen für die Windows „Group Policy“ (Gruppenrichtlinie) auf Servern verwendet, auf denen Software von Smith+Nephew installiert ist, darf die Konfiguration der folgenden Richtlinien nicht geändert werden:

- Computer ConfigurationPoliciesAdministrative TemplatesWindows ComponentsRemote Desktop Services*
- Computer ConfigurationPoliciesAdministrative TemplatesWindows ComponentsWindows PowerShell*
- Computer ConfigurationPoliciesWindows SettingsSecurity SettingsSoftware Restriction Policies*
- User ConfigurationPoliciesAdministrative TemplatesWindows ComponentsRemote Desktop Services*
- User ConfigurationPoliciesAdministrative TemplatesWindows ComponentsWindows PowerShell*
- User ConfigurationPoliciesWindows SettingsSecurity SettingsSoftware Restriction Policies*

Antivirensoftware

Smith+Nephew empfiehlt, das System mit aktueller Antivirensoftware zu schützen. Die Systemleistung muss nach der ersten Installation der Antivirensoftware durch einen Smith+Nephew Mitarbeiter verifiziert werden. Beachten Sie, dass sich bestimmte Einstellungen von Software zum Schutz vor Schadsoftware (z. B. Virenscanner) negativ auf die Systemleistung auswirken können. Wenn beispielsweise Echtzeit-Scans durchgeführt werden und jeder Dateizugriff überwacht wird, könnte der Zugriff auf Patientendaten eingeschränkt werden. Für beste Ergebnisse:

- Sämtliche zusätzliche Antivirensoftwarefunktionen (z. B. Browser- oder E-Mail-Scanner, zusätzliche Firewall) deaktivieren.
- Pop-up-Meldungen der Antivirensoftware deaktivieren.

Die Antivirensoftware so konfigurieren (z. B. durch Hinzufügen zum Ordner „Ausnahmen“), dass folgende Verzeichnisse nicht gescannt oder geändert werden:

- C:\Brainlab, D:\Brainlab und F:\Brainlab usw.
- C:\PatientData, D:\PatientData und F:\PatientData usw.

Software von Drittherstellern

Bis auf Antiviren- und Microsoft-Sicherheitsupdates darf ohne die Genehmigung von Smith+Nephew keine Software von Drittherstellern installiert werden. Wenn Software von Drittherstellern installiert wird, kann die Sicherheit und Effektivität des Medizinprodukts nicht länger gewährleistet werden und es verfallen möglicherweise jegliche Garantien.

Bewährte Praktiken

Um beste Ergebnisse zu erzielen, empfiehlt Smith+Nephew folgende Maßnahmen:

- Vor der Nutzung von Produkten oder Medien Sicherheitsscans von Speichergeräten und -medien (z. B. CD-ROM, DVD-ROM, USB HDD und USB-Flash-Speicherlaufwerke) zur Erkennung und Entfernung jeglicher Schadsoftware durchführen.
- Die Option „**System Restore**“ (Systemwiederherstellung) für das Laufwerk **C:** aktivieren, um das System gegebenenfalls in einem vorherigen Zustand wiederherstellen zu können.
- Das Herunterladen und die Installation von Windows- und Antiviren-Updates für den Zeitpunkt der Systemabschaltung planen. Achten Sie besonders auf Server und virtuelle Maschinen und stellen Sie sicher, dass die Systeme anschließend vollständig neu gestartet werden.
- Wenn kein Scan bei Zugriff/in Echtzeit aktiviert ist, einen Scan bei Bedarf/geplanten Scan bei Systemabschaltung festlegen.

Weitere Informationen

Diese Richtlinie ersetzt jegliche vorherige und gegenwärtige Produktdokumentation. Für weitere Informationen wenden Sie sich an den Kundendienst von Smith+Nephew.

- +1 833 766 2846 (Telefon)
- ri.support@smith-nephew.com