Dräger Schweiz AG, CH-3097 Liebefeld

Betroffene Kunden werden direkt angeschrieben

An die Kunden und Anwender der Dräger-Beatmungsgeräte
Infinity Acute Care System – Workstation Critical Care (Evita V500),
Infinity Acute Care System – Workstation Neonatal Care (Babylog VN500)
und Evita V300

Datum
04.02.2022

Unser Zeichen
PR114992

Tel.
+41 58 748 74 74

Fax
+41 58 748 74 01

E-Mail
quality.ch@draeger.com

Wichtiger Sicherheitshinweis!

Massnahme zur Steigerung der Cybersicherheit

Die folgenden Produkte sind betroffen:
Infinity Acute Care System – Workstation Critical Care (Evita V500) mit SW 2.60 und älter
Infinity Acute Care System – Workstation Neonatal Care (Babylog VN500) mit SW 2.60 und älter
Evita V300 mit SW 2.60 und älter

Sehr geehrte Damen und Herren

Medizinprodukte werden zunehmend in Netzwerkumgebungen betrieben. Der Austausch von Informationen zwischen Medizinprodukten, Krankenhausnetzwerken und dem Internet ermöglichen Lösungen, welche die Behandlung von Patienten durch Gesundheitsdienstleister und das Gesundheitswesen verbessern können. Gleichzeitig steigt durch den Betrieb in Netzwerkumgebungen jedoch das Risiko potenzieller Bedrohungen der Cybersicherheit. Eine Cyberattacke könnte sich auf die Sicherheit und Wirksamkeit von Medizinprodukten auswirken.

Die Beatmungsgeräte der Produktfamilien Evita V500/V300 und Babylog VN500 sind weltweit seit 2007 in vielen Ländern im Einsatz. Die Beatmungsgeräte sind sehr zuverlässig, weisen eine hohe Akzeptanz auf und verfügen über eine Gesamtbetriebszeit von mehr als 124.000 Jahren. Bis heute hat Dräger nicht ein einziger Bericht oder Nachweis eines Cyberangriffs erreicht. Nur eine Handvoll Kunden betreibt die Beatmungsgeräte in einer Netzwerkumgebung, die einen Informationsaustausch zwischen den Beatmungsgeräten und dem Dräger Service Connect Gateway ermöglicht. Die meisten Geräte werden über eine serielle Medibus/Medibus-X-Schnittstelle angeschlossen, welche nicht anfällig für Cyberattacken ist.

Theoretisch können auch Geräte, die nicht an ein Netzwerk angeschlossen sind, potenziellen Bedrohungen der Cybersicherheit ausgesetzt sein. Ein solcher Angriff würde allerdings direkten physischen Zugriff auf das Gerät erfordern. Jemand müsste sich unbefugt Zutritt zu einer Intensivstation verschaffen, jedes einzelne Beatmungsgerät manipulieren und damit möglicherweise die Beatmungstherapie beeinträchtigen.
Betreiber sollten deshalb generell und kontinuierlich die Zugangsbeschränkungen zu ihrer Arbeitsumgebung bewerten.

In den zuvor genannten Beatmungsgeräten kommen besonders abgesicherte Betriebssysteme zum Einsatz. Eines der verwendeten Betriebssysteme kann jedoch nicht mehr aktualisiert werden, sodass seine Sicherheitslücken nicht mehr behoben werden können. Daher sind sie nicht in dem Masse auf potenzielle Bedrohungen der Cybersicherheit vorbereitet wie neuere Geräte. Dies umfasst auch solche Bedrohungen mit physischem Zugriff. Daher gibt Dräger die folgenden Empfehlungen:

- Befolgen Sie die Hinweise in der Gebrauchsanweisung:
  - Beschränken oder kontrollieren Sie den physischen Zugriff auf die zuvor genannten Beatmungsgeräte.
  - Schliessen Sie keine nicht zugelassenen Geräte an die USB-, LAN- und DVI-Schnittstellen an.
  - Achten Sie auf Benachrichtigungen, Alarme und Warnmeldungen.
- Verschliessen Sie nach Möglichkeit alle nicht verwendeten USB-, LAN- und DVI-Schnittstellen oder decken Sie diese ab.

Sollten Sie sich dazu entscheiden, alle nicht verwendeten Schnittstellen zu verschliessen/abzudecken, stellt Dräger auf Wunsch kostenlos Material und Werkzeuge zum Abdecken oder Verschliessen dieser Datenschnittstellen der Beatmungsgeräte zur Verfügung. Setzen Sie sich bei Bedarf mit Ihrer Dräger-Organisation vor Ort in Verbindung. Zur bestimmungsgemässen und zugelassenen Verwendung der Schnittstellen können die USB-Schlösser und Schnittstellenabdeckungen mit den entsprechenden Schlüsseln oder Werkzeugen wieder entfernt werden.

Die von den betroffenen Geräten verwendeten Kommunikationsprotokolle Medibus und MedibusX sind nicht betroffen, da es sich um nicht netzwerkfähige, serielle Point-to-Point-Kommunikationsprotokolle handelt. Sie können daher ohne Sicherheitsbedenken verwendet werden. Sollten Sie die zuvor genannten Geräte in einem Remote-Service-Netzwerk betreiben, wenden Sie sich bitte an Ihre Dräger-Organisation vor Ort.

Bitte stellen Sie sicher, dass alle Anwender der o. g. Produkte und sonstige betroffene Personen in Ihrer Einrichtung von diesem wichtigen Sicherheitshinweis in Kenntnis gesetzt werden. Wenn Sie das Produkt Dritten zur Verfügung gestellt haben, leiten Sie diese Information bitte weiter.

Die zuständigen Behörden wurden hierüber informiert.

Wir entschuldigen uns für etwaige Unannehmlichkeiten, halten dies jedoch für eine unerlässliche Präventivmassnahme zur Steigerung der Patientensicherheit. Wir bedanken uns für Ihre kontinuierliche Unterstützung.

Freundliche Grüsse
Dräger Schweiz AG

Jürg Kaltenrieder
Head of Services, Qualiy & RA

Désirée Flükiger
Assistant of Service, Quality & RA

Beilage: Empfangsbestätigung

Rückantwort!

Betrifft:	Wichtiger Sicherheitshinweis - Maßnahme zur Steigerung der Cybersicherheit
Betroffene Produkte:	Infinity Acute Care System – Workstation Critical Care (Evita V500), Infinity Acute Care System – Workstation Neonatal Care (Babylog VN500) und Evita V300
Kunde Name/Adresse:	…….
	…….
	…….

Hiermit bestätigen wir den Erhalt des wichtigen Sicherheitshinweises. Es wurden alle Anwender über den Inhalt des Hinweises in Kenntnis gesetzt.

Ausgefüllt durch:

Name in Druckbuchstaben: _____

Unterschrift/Datum: _____

Bitte senden Sie uns kostenlos Material und Werkzeuge zum Abdecken oder Verschliessen dieser Datenschnittstellen an

…… Geräten zu (Bitte Anzahl Geräte eintragen)

Bitte senden Sie die Empfangsbestätigung an unten stehende Adresse oder senden Sie uns eine kurze Rückantwort an quality.ch@draeger.com.

Dräger Schweiz AG
Qualitätsmanagement
Waldeggstrasse 30
3097 Liebefeld
Fax: 058 748 74 01
E-Mail: quality.ch@draeger.com