

Target CI Version 1.6

LEITFADEN ZUR CYBERSICHERHEIT

Deutsch

Stand: Juli 2026



Inhalt

1. EINLEITUNG	3
1.1 ABKÜRZUNGEN UND BEGRIFFSBESTIMMUNGEN:	3
2. WEITERE INFORMATIONSQUELLEN.....	4
2.1 KUNDENSERVICE	4
2.2 AB PRO PORTAL	4
2.3 ERWEITERTE INSTALLATIONSANLEITUNG	4
2.4 TARGET CI FIREWALLKONFIGURATION.....	4
2.5 MDS2.....	4
2.6 GEBRAUCHSANWEISUNG	5
2.7 HIMSA.....	5
3. NETZWERK- UND KONTEXTDIAGRAMME	6
3.1 BEREITSTELLUNGSMODELL 1: STANDALONE.....	6
3.2 BEREITSTELLUNGSMODELL 2: NOAH DISTRIBUTED	7
3.3 BEREITSTELLUNGSARTEFAKTE	8
3.4 SYSTEMVERBINDUNGEN	9
4. SYSTEMANFORDERUNGEN	11
5. CYBERSICHERHEIT IM PRODUKTLEBENSZYKLUS	12
5.1 EINSATZ.....	12
5.2 INSTALLATION	12
5.3 KONFIGURATION UND BETRIEB	13
5.4 DEMONTAGE UND AUSSERBETRIEBNAHME	14
6. SICHERHEITSKONTROLLEN.....	16
6.1 ZUGANGSKONTROLLEN.....	16
6.2 AUDITPROTOKOLLIERUNG UND KONTROLLEN ZUR RECHENSCHAFTSPFLICHT	17
6.3 FERNZUGRIFF	17
7. DATENSCHUTZ.....	18
7.1 Advanced Bionics DATENSCHUTZRICHTLINIE	18
7.2 US-BUNDESSTANDARDS FÜR DIE INFORMATIONSVERRARBEITUNG (FIPS) ...	18
7.3 VOM PRODUKT VERARBEITETE PESONENBEZOGENE IDENTIFIZIERBARE INFORMATIONEN (PERSONALLY IDENTIFIABLE INFORMATION, PII) UND GESCHÜTZTE GESUNDHEITSINFORMATIONEN (PROTECTED HEALTH INFORMATION, PHI).....	18
7.4 SICHERHEIT BEI DER ÜBERTRAGUNG	19
7.5 SICHERHEIT IM RUHEZUSTAND	20

8. SOFTWARE-INTEGRITÄT	24
8.1 ÜBERPRÜFEN DER HERUNTERGELADENEN INSTALLATIONSMEDIEN	24
8.2 MANUELLES ÜBERPRÜFEN DER ANPASSSOFTWARE VOR DER INSTALLATION.....	24
8.3 AUTOMATISCHES ÜBERPRÜFEN DER INTEGRITÄT DER INSTALLIERTEN ANPASSSOFTWARE.....	26
8.4 MANUELLES ÜBERPRÜFEN DER INTEGRITÄT DER INSTALLIERTEN ANPASSSOFTWARE.....	26
9. SOFTWARE-PATCHES UND UPDATES	28
10. DATENVERWALTUNG.....	28
10.1 DATENBANKEN	28
10.2 DATENMIGRATION.....	29
10.3 HÖRSYSTEMKONFIGURATIONEN.....	29
10.4 DATENENTSORGUNG	29
11. SICHERHEITSUMGEBUNG – GEMEINSAME VERANTWORTUNG	30
12. HERSTELLUNG, SOFTWARE-ENTWICKLUNG UND SICHERHEITSMANAGEMENT	32
13. SOFTWAREKOMPONENTEN UND STÜCKLISTE.....	34
14. REFERENZEN	56

1. EINLEITUNG

Das vorliegende Dokument enthält technische Sicherheits- und Datenschutzinformationen zum Softwaresystem Target CI v1.6 (Version 1.6) von Advanced Bionics, im Folgenden „Anpasssoftware“ genannt. Die Anpasssoftware ist für die Verwendung durch qualifizierte Audiologen und Hörakustiker zum Konfigurieren (d. h. Anpassen) von Hörsystemen für Patienten konzipiert, die Cochlea-Implantate von Advanced Bionics tragen.

Das vorliegende Dokument widmet sich schwerpunktmäßig Aspekten der Cybersicherheit und des Datenschutzes, soweit sie für die Verwendung der Anpasssoftware relevant sind. Dies umfasst eine Bewertung der Sicherheits- und Datenschutzkontrollen, die derzeit in die Software integriert sind, sowie solcher, die voraussichtlich in der IT-Umgebung eingesetzt und konfiguriert werden, in der das Produkt für den vorgesehenen Zweck genutzt wird.

Das vorliegende Dokument enthält keine technischen Sicherheits- und Datenschutzinformationen zu Folgendem:

- Frühere Versionen der AB Anpasssoftware
- Andere AB Software als Target CI v1.6
- AB Websites
- AB App-Anwendungen
- AB Hörsysteme

1.1 ABKÜRZUNGEN UND BEGRIFFSBESTIMMUNGEN:

Abkürzung	Begriff
FSW	Fitting Software (Anpasssoftware)
SaMD	Software as a Medical Device (Software als Medizinprodukt)
Noah	Ein Patientenmanagementsystem des Drittanbieters HIMSA, das zur Speicherung und Verwaltung von Patienten- und Anpassdaten verwendet wird
TeamViewer	Ein plattformübergreifendes Tool für Fernzugriff und Desktop-Freigabe
SOUP	Software of Unknown Provenance (Software unbekannter Herkunft)
HCP	Hearing Care Professional (Audiologe oder Hörakustiker)
SaMD	Software as a Medical Device (Software als Medizinprodukt)
AB	Advanced Bionics
Sonova	Advanced Bionics ist eine hundertprozentige Tochtergesellschaft von Sonova und fungiert als integraler Bestandteil der Sonova-Gruppe.
IFU	Instructions For Use (Gebrauchsanweisung)
PHI	Protected Health Information (geschützte Gesundheitsinformationen)
PII	Personally Identifiable Information (personenbezogene identifizierbare Informationen)
SBOM	Software Bill of Materials (Software-Stückliste)

2. WEITERE INFORMATIONQUELLEN

2.1 KUNDENSERVICE

Für Kunden in den USA und Kanada bietet Advanced Bionics eine gebührenfreie Technik-Hotline an (877 271 6727). Unter dieser Hotline sind von Montag bis Freitag von 5:00 bis 17:00 Uhr (Pacific Time) kompetente und professionelle Servicemitarbeitende erreichbar.

Außerhalb der USA und Kanada erhalten Sie technische Unterstützung in Ihrer jeweiligen Region. Sollten Sie Fragen zur Anpasssoftware oder zur Hardware oder andere Anliegen in Zusammenhang mit der Programmierung haben, kontaktieren Sie bitte Ihre AB Vertretung vor Ort.

2.2 AB PRO PORTAL

Die Anpasssoftware und die dazugehörige Dokumentation können heruntergeladen werden unter <https://www.abproportal.com> oder aus dem Sonova Web Client. Hierfür ist ein Konto-Login erforderlich. Diese Ressource ist möglicherweise nicht in allen Märkten verfügbar. Wenden Sie sich für weitere Informationen an Ihren Vertreter von AB.

2.3 ERWEITERTE INSTALLATIONSANLEITUNG

Die erweiterte Installationsanleitung für Target CI v1.6 ist auf Anfrage erhältlich. Die Anleitung enthält technische Informationen zum Installationsprogramm für die Anpasssoftware, einschließlich Befehlszeilenoptionen für unbeaufsichtigte und automatisierte Installationen.

2.4 TARGET CI FIREWALLKONFIGURATION

Das Dokument zur Firewallkonfiguration ist auf Anfrage erhältlich. Dieses Dokument enthält IT-spezifische Anleitungen, um sicherzustellen, dass Target CI 1.6 hinter einer Unternehmens-Firewall funktioniert. Es beschreibt detailliert den erforderlichen HTTP/HTTPS-Zugriff sowie die wichtigsten Hostnamen. Es behandelt die WebRTC-Konnektivität über Twilio und Xirsys, erläutert die TURN- und Peer-Relay-Ports und weist darauf hin, dass viele IP-Adressen dynamisch sind, weshalb nach Möglichkeit hostnamenbasierte Regeln verwendet werden sollten.

2.5 MDS2

MDS2 (Manufacturer Disclosure Statement for Medical Device Security) ist ein branchenübliches Standardformblatt, das Informationen zu Sicherheits- und Datenschutzfragen bezüglich der Anpasssoftware von AB enthält. Das Formblatt ist auf Anfrage erhältlich.

2.6 GEBRAUCHSANWEISUNG

Die Gebrauchsanweisung wird mit dem Softwareinstallationsmedium ausgeliefert. Für einige Märkte steht die elektronische Gebrauchsanweisung unter www.advancedbionics.com/ifu zum Download bereit.

Die folgenden Abschnitte der Gebrauchsanweisung können für IT-Fachleute relevant sein:

- Produktbeschreibung
- Mindestanforderungen an das System und Leistungsmerkmale
- Richtlinien für IT-Sicherheit
- Gebrauchsanleitung
- Entsorgung und gefährliche Materialien
- Technischer Dienst

2.7 HIMSA

Hearing Instrument Manufacturer's Software Association (HIMSA) ist ein Drittanbieter von Software, der Noah System 4 herstellt. Dies ist eine für die Hörsystembranche entwickelte Software, die Audiologen und Hörakustikern ein herstellerunabhängiges System zur Durchführung kundenbezogener Aufgaben bereitstellt.

Die Anpassungssoftware kann optional so konfiguriert werden, dass sie zur Datenspeicherung statt einer lokalen Datenbank Noah System 4 verwendet.

Auf der Sicherheitswebseite von HIMSA finden Sie Antworten auf häufige Fragen zur IT-Sicherheit von Noah System 4.

<https://www.himsa.com/support/noah-enterprise-support/security-questionnaire-support/>

<https://www.himsa.com/support/noah-enterprise-support/security-considerations/>

Weitere Sicherheitsinformationen finden Sie im Abschnitt „Sicherheit“ des HIMSA Trainingscenters:

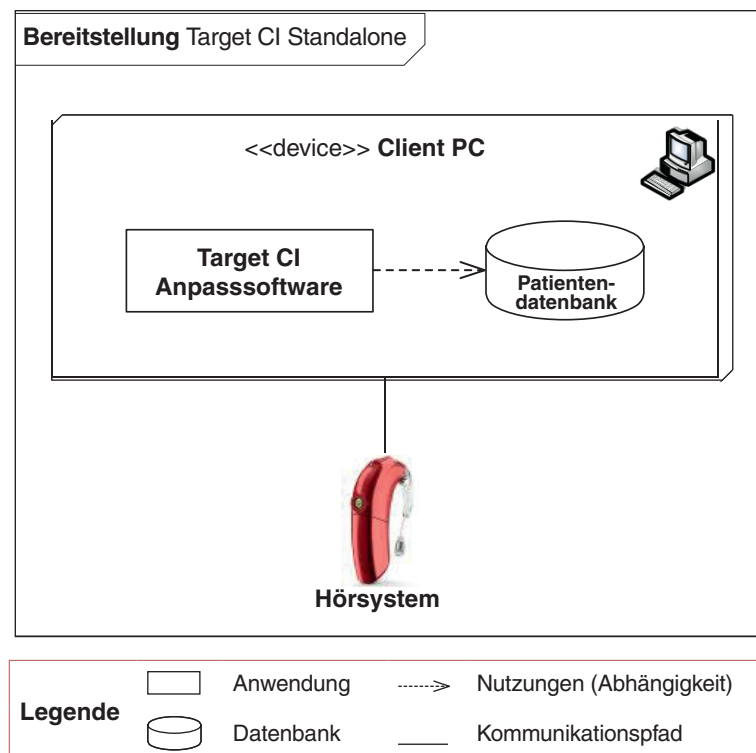
<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/>

3. NETZWERK- UND KONTEXTDIAGRAMME

Für die Anpasssoftware, bei der es sich um eine Client-Anwendung (SaMD) handelt, die auf einem handelsüblichen Microsoft Windows-PC installiert wird, werden zwei Bereitstellungsmodelle unterstützt. Die Software beinhaltet weder die Hardware noch das Betriebssystem.

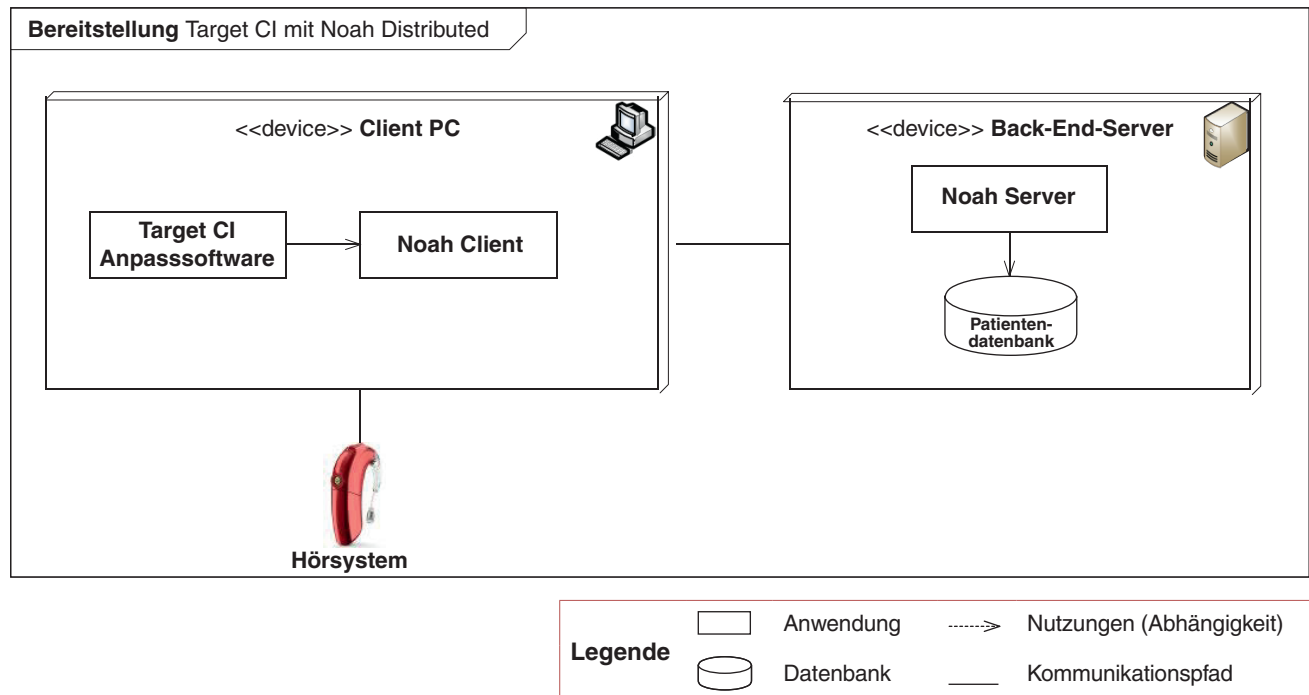
3.1 BEREITSTELLUNGSMODELL 1: STANDALONE

Beim Standalone-Bereitstellungsmodell wird die Anpasssoftware auf einem Client-PC bereitgestellt. Die Patientendatenbank wird auf demselben PC gespeichert und zusammen mit der Anpasssoftware installiert.



3.2 BEREITSTELLUNGSMODELL 2: NOAH DISTRIBUTED

Im Bereitstellungsmodell Noah Distributed wird die Anpasssoftware auf einem oder mehreren Client-PCs bereitgestellt, auf denen Noah installiert ist. Noah ist der Name des Patientenverwaltungssystems eines Drittanbieters. Dieses wird auf einem internen Server bereitgestellt, auf den die Client-PCs zugreifen können. Die Patientendatenbank wird auf dem Noah Server gespeichert und über das Netzwerk von einem oder mehreren Client-PCs abgerufen.

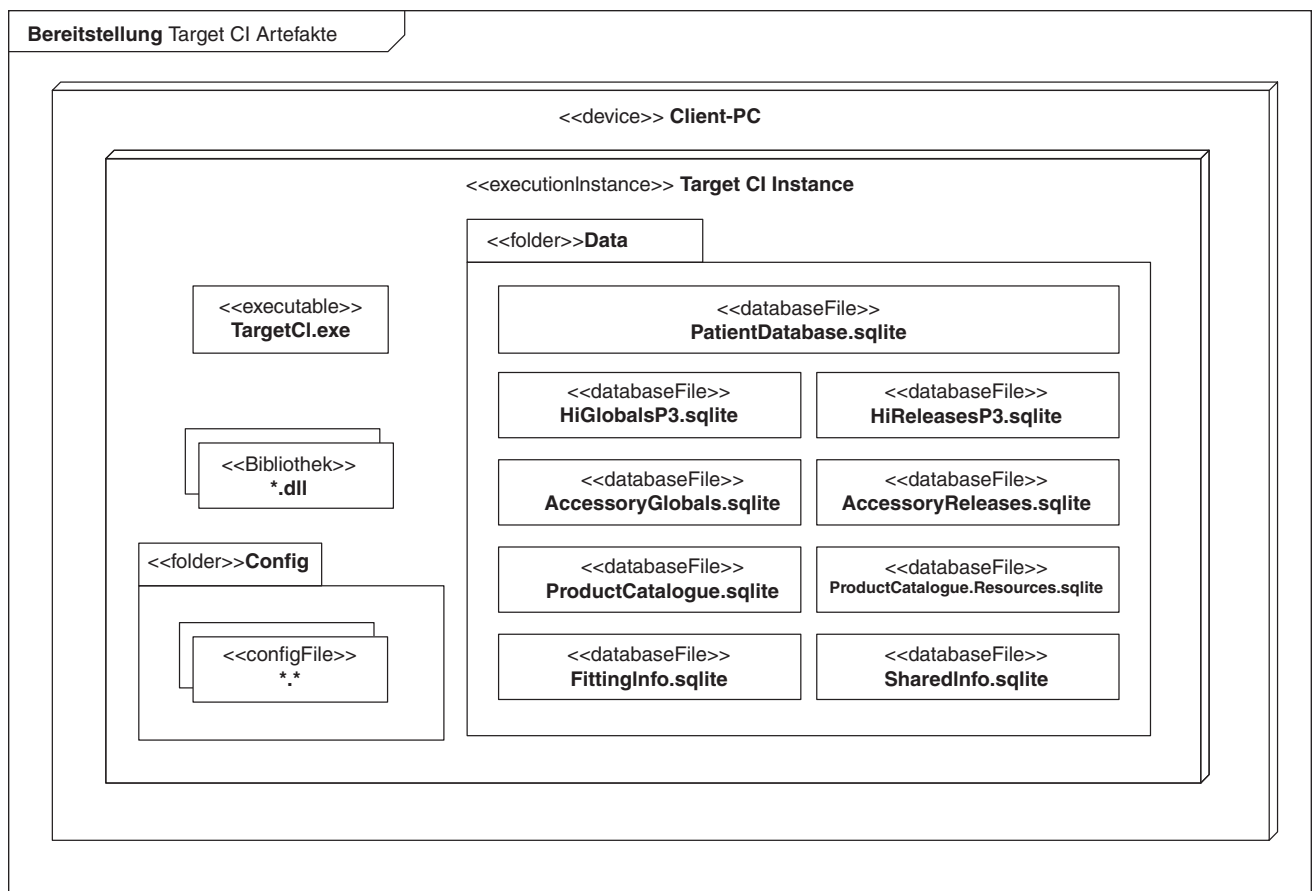


3.3 BEREITSTELLUNGSARTEFAKTE

Die Anpasssoftware wird mit einer ausführbaren Datei und einer Reihe zugehöriger Dateien installiert, darunter DLL-Komponenten, Konfigurationsdateien und SQLite-Datenbankdateien. Die Konfigurationsdateien werden im Ordner „%ProgramData%\Advanced Bionics\Target CI\Target CI\Config“ installiert, die Datenbankdateien im Ordner „%ProgramData%\Advanced Bionics\Target CI\Target CI\Data“. Der Ordner „Data“ enthält eine einzelne Transaktionsdatenbankdatei und mehrere Infodatenbankdateien.

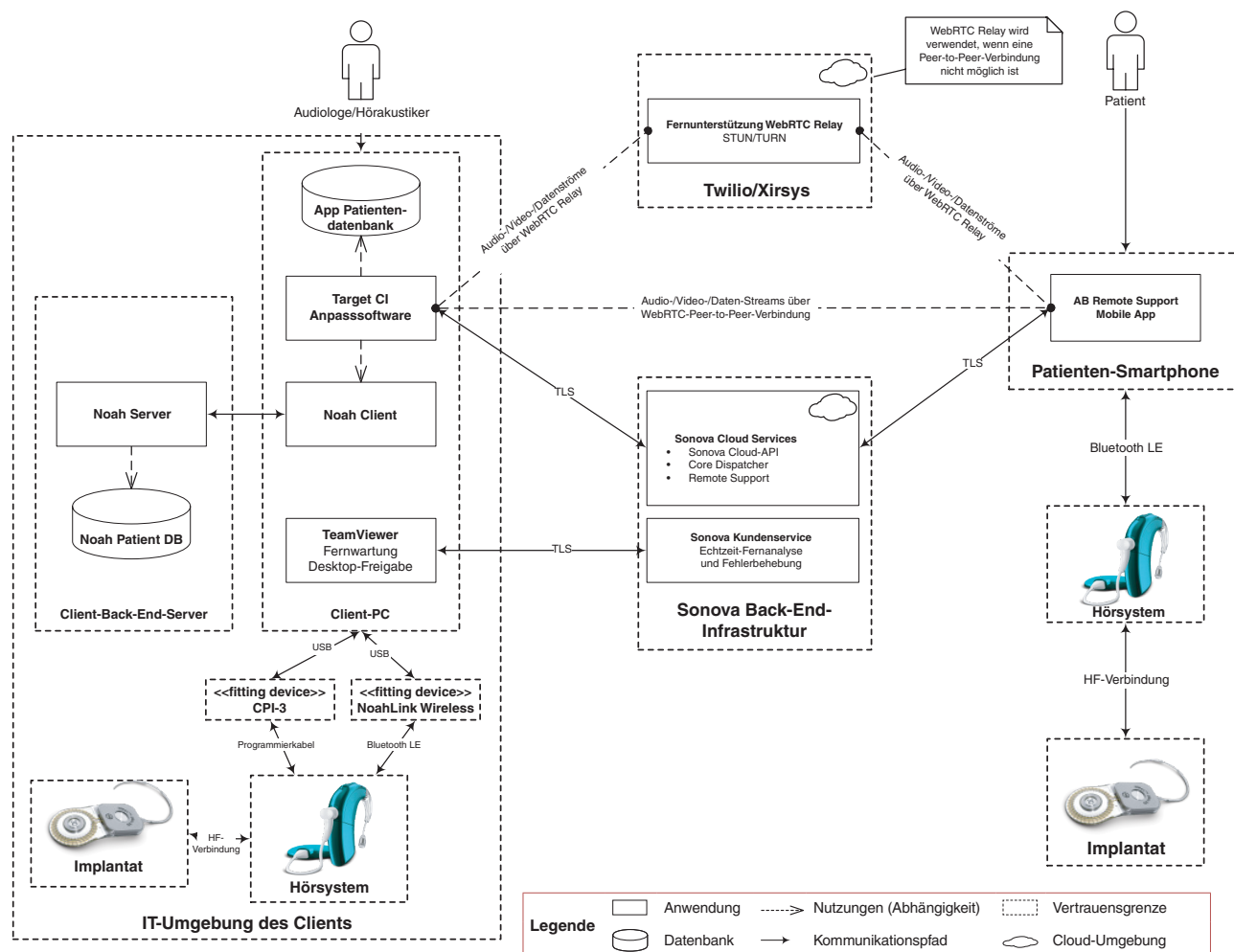
Die Transaktionsdatenbank „PatientDatabase.sqlite“ speichert demografische Daten und Anpassdaten des Patienten und wird nur installiert, wenn die Anpasssoftware im Standalone-Modus bereitgestellt wird.

Wenn die Anpasssoftware als Noah Modul bereitgestellt wird, stellt das Noah System der Anpasssoftware die erforderlichen Dienste zur dauerhaften Speicherung der Patientendaten bereit. Die verbleibenden SQLite-Dateien sind wesentlicher Bestandteil der Anpasssoftware und bei allen Bereitstellungsmodellen erforderlich.



3.4 SYSTEMVERBINDUNGEN

Das Diagramm und die Tabelle unten veranschaulichen die primären Systemverbindungen. Normalerweise wird nur ein Teil der angegebenen Verbindungen genutzt.



Quelle/Ziel	Service	Protokoll	Port	Beschreibung
Hörsystem	Hörsystemkommunikation	Kabelverbindung/ Bluetooth® Low Energy	k. A.	Dient zur Kommunikation mit Hörsystemen zur Steuerung und Konfiguration sowie zum Auslesen von Status und Daten
Noah	Noah 4 ModuleAPI	.NET Remoting	k. A.	Primäre Schnittstelle für das Modul, das für den Zugriff auf die Noah Software verwendet wird (nur beim Bereitstellungsmodell Noah Distributed)

Quelle/Ziel	Service	Protokoll	Port	Beschreibung
Sonova Cloud Services	Sonova Cloud-API, Core Dispatcher, Remote Support	SOAP, REST	443	Sonova-Dienste, die in einem Microsoft Azure Data Center gehostet werden, werden zu folgenden Zwecken verwendet: • Abrufen der Client-Konfigurationsdaten der Anpasssoftware aus dem Sonova Back-End-Speicher • Übertragungsprotokollierung und Analysedaten • Einrichten der Echtzeit-Fernanpassung
Twilio/Xirsys, AB Remote Support und AB Remote Support + Mobile Apps	Remote Support	WebRTC	Siehe Konfigurationsdokument zur Target CI Firewall	Wird von der Remote Support-Funktion genutzt, um WebRTC-Signalisierung und Echtzeit-Fernanpassungen durchzuführen
AB Kundenservice	Desktop-Freigabe	Proprietäres TeamViewer-Protokoll	5938, 443, 80 Siehe TeamViewer-Ports	Wird verwendet, um Echtzeit-Fernanalysen und Fehlerbehebungen durchzuführen, welche die Installation der Anpasssoftware beeinträchtigen. Weitere Informationen finden Sie im Abschnitt 6.3 FERNZUGRIFF .

4. SYSTEMANFORDERUNGEN

Betriebssystem	Windows 10, 11, Pro/Enterprise
.NET Framework	Version 4.8
CPU	Intel® Core™ i5 oder gleichwertig mit gleicher oder besserer Leistung
RAM	4 GB min.
Freier Festplattenspeicher	3 GB min.
Displaymindestanforderungen	• Auflösung 1280 × 1024 Bildpunkte (maximale Skalierung 125 %) • 24-Bit-Farben
Gerätetreiber	• NoahLink Wireless-Treiber (bei Verwendung einer über USB verbundenen NoahLink Wireless-Programmierschnittstelle eines Drittanbieters ist die neueste Version erforderlich, die bei HIMSA bezogen werden kann) • CPI-3-Treiber (erforderlich bei Verwendung einer über USB verbundenen CPI-3-Programmierschnittstelle)
Datenbank	SQLite oder Noah System 4 (Version 4.16 oder höher)
Internetverbindung	Für Fernunterstützung und Analyseprotokollierung ist eine Internetverbindung erforderlich (vgl. Abschnitt 3.4 „Systemverbindungen“); bei Verwendung eines vernetzten Noah System 4 wird ein Intranet benötigt.
Netzwerkports	Informationen hierzu finden Sie in Abschnitt 3.4 „Systemverbindungen“. In Abschnitt 2 „Weitere Informationsquellen – HIMSA“ finden Sie zudem weitere Informationen zu den von Noah System 4 verwendeten Ports.

5. CYBERSICHERHEIT IM PRODUKTLEBENSZYKLUS

5.1 EINSATZ

Genehmigte Bereitstellungsmethoden:

1. Download über den Sonova Web Client (SFTP) unter <https://webclient.sonova.com> oder über das AB Pro Portal unter <https://www.abproportal.com>
2. Installation von einem offiziellen Advanced Bionics USB-Stick.

Überprüfen Sie vor der Installation die digitale Signatur des Installationsprogramms und scannen Sie die Datei mit aktueller Antivirensoftware. Anweisungen zur Integritätsprüfung finden Sie in Abschnitt 8. Wenden Sie während der Bereitstellung die üblichen IT-Sicherheitsmaßnahmen im Gesundheitswesen an, einschließlich Endgeräteschutz und Netzwerkeinschränkungen.

Bei Verwendung eines USB-Sticks:

- Verwenden Sie ausschließlich offiziell von Advanced Bionics bereitgestellte USB-Sticks.
- Bewahren Sie den USB-Stick physisch sicher auf und verändern Sie dessen Inhalt nicht.
- Überprüfen Sie den USB-Stick und die Installationsumgebung mit aktueller Antivirensoftware und einer Whitelist für Anwendungen.
- Advanced Bionics übernimmt keine Verantwortung für unbefugt gespeicherte Daten auf USB-Sticks, die das Installationspaket enthalten.

5.2 INSTALLATION

Für die Installation der Anpasssoftware ist ein Administratorkonto erforderlich. Nach Abschluss der Installation kann die Software ohne Administratorrechte oder erhöhte Berechtigungen ausgeführt werden.

Informationen zur Verifizierung der Software-Integrität vor der Installation finden Sie in Abschnitt 8 „Software-Integrität“.

Vor der Installation wird Systemadministratoren empfohlen, Folgendes sicherzustellen:

- Die zu installierende Version der Anpasssoftware ist die neueste Version.
- Das zugrunde liegende Betriebssystem ist auf dem neuesten Stand.
- Integrität und Authentizität der Daten des Anpasssoftware-Installationsprogramms werden überprüft. Informationen zur Validierung der Software-Integrität vor der Installation finden Sie in Abschnitt 8.

Zum Installieren der Anpasssoftware sind zwei Installationsprogramme verfügbar:

- Standardinstallationsprogramm
- IT Professional-Installationsprogramm

Das IT Professional-Installationsprogramm ist eine einzelne MSI-Datei und schließt erforderliche Komponenten aus, ist ansonsten jedoch mit dem Standardinstallationsprogramm identisch.

Zu den erforderlichen Komponenten gehören Microsoft .NET Framework v4.8 und die Microsoft Visual C++ Redistributable-Pakete.

Beide Installationsprogramme unterstützen erweiterte Installationsszenarien, einschließlich der unbeaufsichtigten Installation.

Das IT Professional-Installationsprogramm sollte nur verwendet werden, falls in Ihrem Unternehmen die Installation und Verwaltung der erforderlichen Komponenten durch das Unternehmen selbst vorgeschrieben ist und daher nicht durch das Installationsprogramm der Anpasssoftware durchgeführt werden kann. In allen anderen Fällen sollte das Standardinstallationsprogramm verwendet werden.

Das IT Professional-Installationsprogramm kann über einen Vertreter von AB bezogen werden. Das IT Professional-Installationsprogramm kann nicht zum Reparieren, Neuinstallieren oder Deinstallieren von Installationen mit dem Standardinstallationsprogramm verwendet werden. Ebenso kann das Standardinstallationsprogramm nicht zum Reparieren, Neuinstallieren oder Deinstallieren von Installationen mit dem IT Professional-Installationsprogramm verwendet werden.

Befolgen Sie für erweiterte Installationsszenarien die Anweisungen in der Erweiterten Installationsanleitung für die Anpasssoftware (siehe Abschnitt 2.3). Für Standardinstallationsszenarien lesen Sie bitte Abschnitt 2.5 dieses Dokuments, der einen Link zur Gebrauchsanweisung der Anpasssoftware enthält.

5.3 KONFIGURATION UND BETRIEB

Die Anpasssoftware unterstützt eine Reihe von Datenschutz- und Sicherheitsmaßnahmen sowie -funktionen. Einige Datenschutz- und Sicherheitsfunktionen der Anpasssoftware sind standardmäßig aktiviert, andere lassen sich bei der Installation konfigurieren und hängen vom gewählten Bereitstellungsmodell ab, wieder andere können während des normalen Betriebs über die Benutzeroberfläche der Anwendung konfiguriert werden.

Siehe:

- Abschnitt 6 für eine Liste der Sicherheitsmaßnahmen, die den Schutz des Anwendungssystems der Anpasssoftware verbessern
- Abschnitt 7 für eine Liste der Sicherheitsmaßnahmen, die den Schutz der von der Anpasssoftware verarbeiteten Daten verbessern

Zusätzliche Datenschutz- und Sicherheitsmaßnahmen (die von der Anpasssoftware auf Anwendungsebene nicht unterstützt werden) sollten von den Benutzern (z. B. Audiologen oder Hörakustikern, Systemadministratoren, IT-Mitarbeitenden) auf Betriebssystemebene und/oder auf Ebene der IT-Infrastruktur aktiviert und konfiguriert werden. Eine detaillierte Liste mit Empfehlungen zu bewährten Vorgehensweisen und Sicherheitsmaßnahmen für die Anpassungsumgebung, in der die Anpasssoftware eingesetzt wird, finden Sie in Abschnitt 11 dieses Dokuments.

Firewall

Die Anpasssoftware ist nicht mit einer internen Firewall ausgestattet.

Falls eine externe Firewall aktiviert ist (z. B. auf Betriebssystemebene), muss deren Konfiguration möglicherweise angepasst werden, um den erforderlichen ein- und ausgehenden Datenverkehr zuzulassen (z. B. WebRTC-Audio-/Video-/Datenströme während einer Remote Support-Sitzung). Weitere Informationen finden Sie im Dokument zur Firewall-Konfiguration der Anpasssoftware, das eine Liste der von der Anpasssoftware verwendeten Netzwerkadressen und Ports enthält.

Proxy-Einstellungen

Die Anpasssoftware ist mit einem lokalen Proxy ausgestattet. Über die Benutzeroberfläche der Anpasssoftware können die Einstellungen des Proxys geändert werden:

- Kein Proxy
- Proxy-Einstellungen automatisch erkennen
- Manuelle Proxy-Konfiguration. Wenn diese Option ausgewählt ist, können die folgenden Einstellungen konfiguriert werden:
 - Adresse
 - Port
 - Proxy-Authentifizierung aktivieren/deaktivieren (Benutzername, Passwort, Domäne)

5.4 DEMONTAGE UND AUSSERBETRIEBNAHME

Detaillierte Anweisungen zur Deinstallation der Software finden Sie in der Gebrauchsanweisung der Anpasssoftware.

Das Deinstallationsprogramm entfernt nicht die in der folgenden Tabelle aufgeführten Datenkategorien. Sofern in der Spalte „Hinweise“ der Tabelle nicht anders angegeben, müssen diese Daten von Systemadministratoren manuell aus den Systemen entfernt werden, z. B. durch manuelles Löschen der Dateien oder durch Löschen der für die Datenspeicherung verwendeten Systemfestplatte.

Datenkategorie	Standard-Speicherort	Anmerkungen
Anwendungsdaten	C:\ProgramData\ Advanced Bionics\ Target CI\Target CI	Umfasst die folgenden Datentypen: • Analysedaten • Konfigurationsdaten • Anwendungsprotokolle • Temporäre Dateien

Datenkategorie	Standard-Speicherort	Anmerkungen
Personenbezogene Daten	C:\ProgramData\ Advanced Bionics\ Target CI\Target CI\Data	Patientendatenbank (gilt nur für das Standalone-Bereitstellungsmodell)
Fernzugriffstool	C:\Program Files (x86)\Common Files\ Advanced Bionics\ TeamViewer	Wird zur Echtzeitanalyse und Fehlerbehebung bei Problemen mit der Anpasssoftware verwendet, einschließlich solcher, die während der Installation und Deinstallation auftreten. Weitere Informationen finden Sie in Abschnitt 6.3.

Wenn Sie die entsprechende Software von dem Computer/Laptop deinstallieren, der stillgelegt oder entsorgt werden soll, stellen Sie sicher, dass alle sensiblen Daten (z. B. PHI, PII) gelöscht werden.

Für Noah Installationen finden Sie detaillierte Anweisungen zur Datenlöschung unter:

<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/>

Sorgen Sie für den Schutz externer Medien mit aus der Anpasssoftware exportierten Daten, insbesondere Berichten und Protokollen. Wenn Daten nicht mehr benötigt werden, sollten sie und/oder die betreffenden Medien sicher gelöscht werden.

Zum sicheren Entfernen von auf Wechselmedien gespeicherten Daten sollten gemäß geltenden Vorschriften und Richtlinien für den Umgang mit Patienteninformationen/ personenbezogenen identifizierbaren Informationen (PII)/geschützten Gesundheitsinformationen (protected health information, PHI) zugelassene Verfahren und Tools genutzt werden.

6. SICHERHEITSKONTROLLEN

Bei der Anpasssoftware handelt es sich um eine Client-Anwendung, die auf einem handelsüblichen Microsoft Windows-PC installiert wird. Die Anpasssoftware kann als eigenständige Anwendung („Standalone“) oder als Noah Modul installiert werden.

6.1 ZUGANGSKONTROLLEN

Die Anpasssoftware schränkt den Zugriff auf ihre Funktionen nicht anhand von Anmeldeanforderungen und Rollen einzelner Benutzer ein. Rollenbasierte Zugriffskontrollen werden nicht unterstützt.

Lokaler Benutzerzugriff

Wenn die Anpasssoftware als eigenständige Anwendung installiert wird, stützt sie sich auf die Zugriffskontrollmechanismen des Host-Betriebssystems. Das IT-Personal des Kunden kann das Host-Betriebssystem so konfigurieren, dass es die Benutzerauthentifizierung verwaltet und Zugriffsrechte oder -privilegien zuweist. Jedem Benutzer wird dringend empfohlen, sich mit einem eindeutigen, individuellen Konto anzumelden.

Weitere kompensierende Kontrollmaßnahmen sind in Abschnitt 11 dieses Dokuments sowie im Abschnitt „Richtlinien für IT-Sicherheit“ der Gebrauchsanweisung beschrieben.

Wenn die Anpasssoftware als Noah Modul installiert ist, erfolgt die Zugriffskontrolle über Noah System 4.

Einzelheiten zu den von Noah System 4 implementierten Zugriffskontrollfunktionen finden Sie in der Dokumentation unter www.HIMSA.com.

Servicezugriff

Servicetechniker vor Ort können auf die Montage-Software zugreifen, wobei die vom IT-Personal des Kunden konfigurierten Zugriffskontrollen zur Authentifizierung berücksichtigt werden.

Supporttechniker von AB können über die von der Montage-Software unterstützte Desktop-Sharing-Funktion auf die Montage-Software zugreifen. Ausführliche Informationen zu den für diese Funktion aktivierten Sicherheitskontrollen finden Sie in Abschnitt 6.3.

6.2 AUDITPROTOKOLLIERUNG UND KONTROLLEN ZUR RECHENSCHAFTSPFLICHT

Die Anpasssoftware erstellt keine zusätzlichen Protokolle oder Berichte, die über die vom zugrunde liegenden Betriebssystem bereitgestellten hinausgehen.

Standalone-Bereitstellungsmodell

Wenn die Anpasssoftware als Standalone-Anwendung installiert wird, nutzt sie die Auditmechanismen des Host-Betriebssystems. Die Anpasssoftware selbst verfügt über keine solche integrierte Funktion. Das Host-Betriebssystem kann vom IT-Personal des Kunden so konfiguriert werden, dass bestimmte Ereignisse wie das Starten bzw. Ausführen der Anpasssoftware protokolliert werden. Es wird empfohlen, dass sich jeder Benutzer mit einem benutzerspezifischen Konto beim Host-Betriebssystem anmeldet, um Audits zu erleichtern.

Bereitstellungsmodell Noah Distributed

Wenn die Anpasssoftware als Noah Modul installiert ist, wird die Auditprotokollierung vom Noah System (Noah Activity Log) übernommen. Einzelheiten zu den in Noah System 4 verfügbaren Auditkontrollen finden Sie in der Dokumentation unter www.himsa.com.

6.3 FERNZUGRIFF

Die Funktion zur Desktop-Freigabe ermöglicht eine Echtzeit-Fernanalyse sowie die Fehlerbehebung bei Problemen mit der Anpasssoftware-Installation. Diese Funktion beruht auf dem Drittanbietertool TeamViewer QuickSupport (das standardmäßig zusammen mit der Anpasssoftware bereitgestellt wird) und ermöglicht es Kundendienstmitarbeitern von AB, eine Fernverbindung mit dem Computer des Audiologen oder Hörakustikers herzustellen und dessen Desktop uneingeschränkt (auch mit Zugriff auf das zugrunde liegende Betriebs- und Dateisystem) zu steuern.

Zum Einrichten einer Desktop-Freigabebesitzung ist die Interaktion des Audiologen bzw. Hörakustikers erforderlich. Der Audiologe bzw. Hörakustiker muss zunächst das QuickSupport-Tool von TeamViewer ausführen (z. B. durch Aufruf über die Target CI-Anpasssoftware) und seine TeamViewer-ID-Zugangsdaten über einen separaten Kommunikationskanal (z. B. telefonisch) an das AB Supportteam übermitteln.

Der Name des Supportmitarbeitenden von AB sowie seine TeamViewer-ID werden bei jeder aktiven Desktop-Freigabebesitzung standardmäßig auf dem Computermonitor des Audiologen bzw. Hörakustikers angezeigt.

Der gesamte bei einer Desktop-Freigabebesitzung ausgetauschte Netzwerkverkehr wird mithilfe kryptografischer Protokolle und Algorithmen gesichert, die nach heutigen Maßstäben als sicher gelten (Austausch öffentlicher und privater Schlüssel nach RSA-Verfahren, AES-256-Bit-Sitzungsverschlüsselung).

Das Fernzugriffstool kann manuell entfernt werden, ohne dass sonstige Funktionen der Target Anpasssoftware beeinträchtigt werden. Das Installationsprogramm für die Target Anpasssoftware unterstützt einen Installationsparameter für die Kommandozeile. Auf diese Weise soll eine Installation der Target Anpasssoftware über die Kommandozeile ohne Einbeziehung des Fernzugriffstools ermöglicht werden.

7. DATENSCHUTZ

7.1 Advanced Bionics DATENSCHUTZRICHTLINIE

Die Datenschutzrichtlinie, die beschreibt, wie Advanced Bionics personenbezogene Daten erhebt, überträgt, speichert und nutzt, kann hier heruntergeladen werden: AdvancedBionics.com/privacy.

Weder hostet, speichert oder sichert Advanced Bionics Daten, die in der Anpasssoftware oder den Noah Datenbanken gespeichert sind, noch hat Advanced Bionics Zugriff auf diese Daten, sofern diese nicht ausdrücklich an Advanced Bionics gesendet werden.

7.2 US-BUNDESSTANDARDS FÜR DIE INFORMATIONSVERARBEITUNG (FIPS)

Target CI v1.6 entspricht den Verschlüsselungsstandards nach FIPS 140-2.

7.3 VOM PRODUKT VERARBEITETE PERSONENBEZOGENE IDENTIFIZIERBARE INFORMATIONEN (PERSONALLY IDENTIFIABLE INFORMATION, PII) UND GESCHÜTZTE GESUNDHEITSINFORMATIONEN (PROTECTED HEALTH INFORMATION, PHI)

Die Anpasssoftware verarbeitet personenbezogene Daten und Gesundheitsdaten von Patienten.

Die Patientendaten werden entweder manuell vom Benutzer der Anpasssoftware eingegeben oder von der Anwendung über einen oder mehrere ihrer Datenflüsse empfangen.

In den Hauptdatenflüssen der Anpasssoftware werden folgende Arten von Informationen verarbeitet:

	Sonova Cloud Services (Core Dispatcher, Remote Support)	Hör-system	Mobile Apps	Patienten-datenbank (lokal/ Noah)	Fernzu-griff
Name				X	X(2)
Adresse				X	X(2)
Geburtsdatum	X(1)		X	X	X(2)
Telefonnummer				X	X(2)
E-Mail-Adresse				X	X(2)
Krankenakten-nummern				X	X(2)
Produktkennung und Seriennummern	X(1)	X	X	X	X(2)
IP-Adresse	X(1)				
Audiogramm, RECD, REUG	X(1)	X	X	X	X(2)
Anpassdaten		X	X	X	X(2)
Hörsystem-Nutzungsdaten	X(1)	X	X	X	
Nutzungsdaten der Anpasssoftware	X(1)				

(1) Pseudonymisierte Daten vor der Speicherung im Sonova Datalake.

(2) Während einer Echtzeit-Desktop-Sharing-Sitzung erhalten die Kundenservicetechniker von AB die volle Kontrolle über den Desktop des Audiologen oder Hörakustikers, einschließlich des Zugriffs auf das zugrunde liegende Betriebs- und Dateisystem sowie auf die darin gespeicherten Daten. Weitere Informationen finden Sie in Abschnitt 6.3.

Für detailliertere Informationen zur Datenerfassung und -verarbeitung wenden Sie sich bitte an Ihren lokalen Supportmitarbeitenden.

7.4 SICHERHEIT BEI DER ÜBERTRAGUNG

Kommunikationssicherheit ist bei allen eingehenden und ausgehenden Netzwerk-kommunikationen der Anpasssoftware gewährleistet und aktiviert. Mit Ausnahme der Remote Support-Funktion (die das WebRTC-Protokoll verwendet) und der Bluetooth-Kommunikation mit Hörsystemen und Zubehör sind alle Verbindungen durch das TLS-Protokoll (Transport Layer Security) geschützt, das Vertraulichkeit, Integrität und Authentizität gewährleistet.



TLS

Die TLS-Konfiguration entspricht geltenden Best Practices und Sicherheitsempfehlungen, die in BCP 195 („Recommendations for Secure Use of TLS and DTLS [8]“) dokumentiert sind, darunter:

- Keine Unterstützung für SSL- und TLS-Versionen vor 1.2
- Keine Unterstützung für Cipher Suites, die kryptografische Algorithmen verwenden, die weniger als 128-Bit-Sicherheit bieten
- Unterstützung in BCP 195 empfohlener TLS-Erweiterungen
- Keine Unterstützung von in BCP 195 als unsicher eingestuften Erweiterungen

DTLS

Verschlüsselung ist eine obligatorische Funktion von WebRTC und wird für alle über WebRTC gesendeten Medien-Streams erzwungen. Das verwendete Verschlüsselungsprotokoll hängt vom Kanaltyp ab. Daten-Streams werden mit DTLS 1.2 verschlüsselt, Medien-Streams hingegen mit dem Secure Real-time Transport Protocol (SRTP), da es eine im Vergleich zu DTLS schlankere Option ist.

Ausführlichere Informationen zur Sicherheitskonfiguration von Remote Support WebRTC finden Sie unter folgendem Link:

<https://developer.liveswitch.io/liveswitch-server/server/security.html>

BLE

Die drahtlose Bluetooth Low Energy-Kommunikation mit Hörsystemen und Zubehör ist standardmäßig verschlüsselt und ihre Integrität geschützt (außer bei Anwendungsfällen zur Identifizierung und Erkennung). Darüber hinaus ist die Dauer des Bluetooth-Kopplungsmodus beim Hörsystem zeitlich begrenzt. Eine ausführlichere Beschreibung der Sicherheit des Bluetooth-Kommunikationskanals finden Sie in der Dokumentation zum Hörsystem.

7.5 SICHERHEIT IM RUHEZUSTAND

Anwendungsdaten

Die Anwendungsdaten befinden sich auf demselben Rechner im Standardverzeichnis:
C:\ProgramData\Advanced Bionics\Target CI\Target CI

Die Zugriffsrechte werden vom übergeordneten Ordner übernommen und sind auf Benutzer beschränkt, die während der Installation der Software am lokalen System angemeldet waren (integrierte INTERAKTIVE Benutzergruppe¹).

Autorisierte Benutzer haben Lese- und Schreibzugriff auf das Verzeichnis.

¹ <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-special-identities-groups#interactive>

Um das Risiko eines unbefugten Zugriffs auf die Anwendungsdaten über das Netzwerk zu verringern, stellen Sie bitte sicher, dass keiner der Ordner oder Dateien, welche die Daten enthalten, im Netzwerk freigegeben ist. Die Standardpfade der Anwendungsdaten sind in Abschnitt 5.4 aufgeführt.

Patientendatenbank bei Standalone-Bereitstellung

Wenn die Anpasssoftware als eigenständige Anwendung installiert ist, befindet sich die Patientendatenbank auf demselben Rechner, und die Patientendatensätze werden im Ruhezustand nicht verschlüsselt. Personenbezogene Daten werden von der Anwendung nicht über das Netzwerk übertragen.

Jeder Benutzer, der sich am Rechner mit der installierten Anpasssoftware anmelden kann, hat vollen Zugriff auf alle Anwendungsdaten, einschließlich der Patientendatenbank. Hinweise zu empfohlenen Datenschutzmaßnahmen finden Sie im Abschnitt Datenschutz.

In einigen Rechtsordnungen können Vorschriften die Verschlüsselung aller Patientendaten vorschreiben, um eine mögliche Haftung im Falle von Datenverlust oder -diebstahl zu vermeiden. Aktivieren Sie BitLocker oder eine gleichwertige vollständige Festplattenverschlüsselung (auf Betriebssystemebene oder hardwarebasiert), um die Daten vor unbefugtem Zugriff oder Kopieren im Ruhezustand zu schützen.

BitLocker ist eine in Windows integrierte Funktion, die das gesamte Laufwerk verschlüsselt und für den Zugriff eine Authentifizierung verlangt. Ziehen Sie vor der Aktivierung von BitLocker immer die offiziellen Empfehlungen von Microsoft und die IT-Sicherheitsrichtlinien Ihres Unternehmens zurate.

So aktivieren Sie BitLocker

Zum Verwalten von BitLocker sind Administratorrechte erforderlich.

1. Nach „BitLocker verwalten“ suchen
Öffnen Sie das Startmenü, geben Sie „BitLocker verwalten“ ein und wählen Sie den entsprechenden Eintrag in den Suchergebnissen aus.
2. Systemlaufwerk auswählen
Wählen Sie das Laufwerk aus, auf dem Windows installiert ist, um die Verschlüsselungseinstellungen zu konfigurieren.
3. Entsperrmethode wählen
Wählen Sie eine der folgenden Optionen:
 - Nur TPM
 - TPM + PIN
 - TPM + USB-Schlüssel

Befolgen Sie beim Auswählen der Entsperrmethode die von Microsoft empfohlenen Best Practices sowie die IT-Sicherheitsrichtlinien Ihres Unternehmens.

4. Wiederherstellungsschlüssel sichern

Erstellen Sie eine Sicherungskopie des Wiederherstellungsschlüssels mithilfe sicherer, unternehmensweit zugelassener Methoden. Zu den empfohlenen Optionen gehören:

- Speichern in Microsoft Entra ID (vormals Azure AD) oder Active Directory für Geräte, die einer Domäne beigetreten sind
- Speichern an einem sicheren, zugriffskontrollierten Netzwerkspeicherort mit Verschlüsselung und Prüfprotokollierung
- Nutzen einer von Ihrer Organisation genehmigten verwalteten Lösung zum Hinterlegen von Schlüsseln

Speichern Sie den Schlüssel nicht auf lokalen Laufwerken oder USB-Sticks und drucken Sie ihn nicht aus, sofern dies nicht ausdrücklich durch eine Richtlinie erlaubt ist. Wiederherstellungsschlüssel müssen mit der gleichen Sorgfalt wie andere vertrauliche Zugangsdaten geschützt und bei Offenlegung sofort ausgetauscht werden.

5. Verschlüsselung starten

Wählen Sie aus:

- „Gesamtes Laufwerk“: empfohlen für die meisten Unternehmensszenarien. Verschlüsselt alle Sektoren, einschließlich ungenutztem Speicherplatz, um Datenremanenz zu verhindern.

Patientendatenbank – Noah Distributed-Bereitstellungsmodul

Wenn die Anpasssoftware als Noah Modul installiert wird, werden personenbezogene Daten in der von Noah gehosteten Patientendatenbank gespeichert. Die von Noah gehostete Patientendatenbank kann sich auf einem anderen Computer befinden. Personenbezogene Daten und andere Patientendaten werden von der Noah Software verwaltet, und die Verschlüsselung der ruhenden Patientendaten wird durch das Noah System sichergestellt. Die Anpasssoftware kann personenbezogene Daten über eine kabelgebundene oder kabellose Netzwerkverbindung senden/empfangen, wenn der Netzwerkzugriff für eine Noah Datenbank konfiguriert ist.

In der vernetzten Noah Datenbank gespeicherte personenbezogene Daten sind für andere Benutzer auf anderen PCs zugänglich, die über Berechtigungen für diese vernetzte Datenbank verfügen. Die Noah Datenbank kann auch ohne Netzwerkzugriff konfiguriert und dann auf demselben PC wie die Anpasssoftware installiert werden.

Noah verhindert, dass die Anpasssoftware auf die Datenbank mit den Patientendaten zugreift. Wenn ein Benutzer im Noah Client einen Patienten in der Anpasssoftware öffnet, kann die Anpasssoftware nur den aktuell geöffneten Patientendatensatz lesen und bearbeiten, hat jedoch keinen Zugriff auf andere Patientendatensätze in der Noah Datenbank.

Weitere Informationen zu den von Noah System verwendeten Verschlüsselungsstandards finden Sie unter dem folgenden Link:

<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/patient-database-encryption/>

RMA-Exportdateien

Die Anpasssoftware ermöglicht den Export von Kundendaten in eine Datei. Die RMA-Datei kann an Advanced Bionics gesendet werden, um RMA- oder damit verbundene Supportprobleme zu lösen.

Die RMA-Datei ist asymmetrisch RSA-verschlüsselt und verwendet eine Schlüssellänge von 2048 Bit. Die Anpasssoftware verfügt nicht über die Möglichkeit, eine RMA-Datei zu entschlüsseln.

Anonymisierte Exportdateien

Die Anpasssoftware ermöglicht den Export von Kundendaten in eine anonymisierte Kundendatei. Die personenbezogenen Daten des Kunden, wie etwa Geburtsdatum und Name, werden durch generische Werte ersetzt. Die Datei ist nicht verschlüsselt und kann in dieselbe oder eine andere Instanz der Anpasssoftware importiert werden.

Standardexportdateien

Die Anpasssoftware ermöglicht den Export von Kundendaten in eine Standardexportdatei. Diese Datei verwendet ein proprietäres Binärformat und ist nicht verschlüsselt. Die Datei kann in dieselbe oder eine andere Instanz der Anpasssoftware importiert werden. Bei Verwendung dieser Funktion müssen Benutzer der Anpasssoftware sicherstellen, dass Standardexportdateien gemäß den jeweils geltenden lokalen IT-Richtlinien für die Verwaltung unverschlüsselter personenbezogener Daten verarbeitet werden.

Hörsystem

Die Anpasssoftware speichert Kundeninformationen auf dem Hörsystem des Kunden. Personenbezogene Daten wie Name und Geburtsdatum des Kunden werden auf dem Hörsystem nicht gespeichert. Andere nicht personenbezogene Daten werden mithilfe der PBKDF2-Verschlüsselung unter Verwendung eines 128-Bit-Schlüssels gespeichert.

Die Anpasssoftware kann nicht personenbezogene Kundendaten über ein proprietäres kabelgebundenes Gerät (z. B. CPI-3), die mobilen Anwendungen AB Remote Support und AB Remote Support + oder ein NoahLink Wireless Gerät an ein Hörsystem übertragen bzw. von diesem empfangen. Das NoahLink Wireless Gerät verbindet sich per Bluetooth Low Energy (BLE) über einen mit 128 Bit AES-verschlüsselten BLE-Standardkanal mit dem Hörsystem.

8. SOFTWARE-INTEGRITÄT

8.1 ÜBERPRÜFEN DER HERUNTERGELADENEN INSTALLATIONSMEDIEN

Das Installationsmedium für die Target CI-Anpasssoftware kann in einigen Regionen vom Pro Portal oder Sonova Web Client von Advanced Bionics heruntergeladen werden. Das heruntergeladene Installationsmedium kann mit jedem vertrauenswürdigen SHA-256-Hashing-Tool authentifiziert werden.

Der SHA256-Hash für die ZIP-Datei des Standardinstallationsprogramms lautet:
A42B8F41A5A4111D1CDF67394FFBBFBCDF2FB6215EC2696DB310B3AED6D4DD83

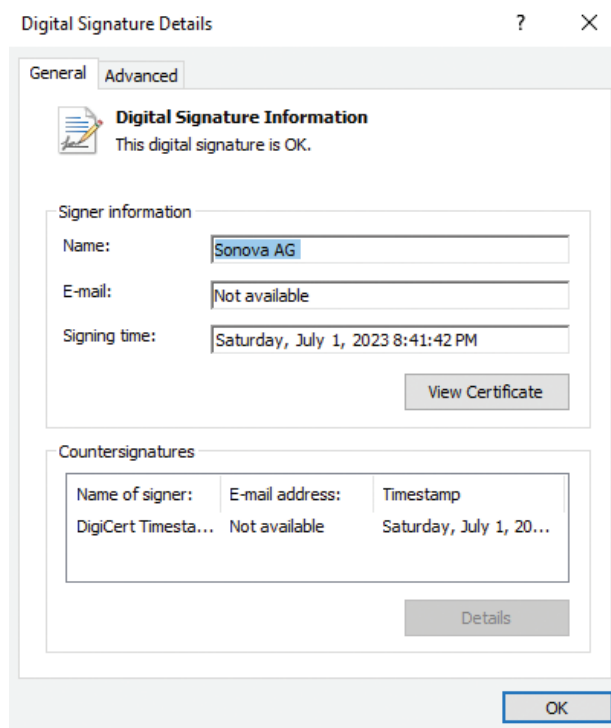
Der SHA256-Hash für die ZIP-Datei des IT Professional-Installationsprogramms lautet:
DDAD362CC3213EFEA702D9F4A61740B34EDF794FE997811B6B2C908CE754B25F

8.2 MANUELLES ÜBERPRÜFEN DER ANPASSSOFTWARE VOR DER INSTALLATION

Benutzer können die folgenden Schritte ausführen, um die Integrität und Echtheit der Anpasssoftware vor der Installation zu überprüfen:

1. Öffnen Sie den Windows Explorer und navigieren Sie zum Stammordner des Installationsmediums der Anpasssoftware. Wenn es sich bei Ihrem Installationsmedium um einen USB-Stick handelt, stecken Sie ihn in einen USB-Anschluss und navigieren Sie zu seinem Stammverzeichnis. Wenn Ihr Installationsmedium eine ZIP-Datei ist, entpacken Sie diese in einen Ordner und navigieren Sie dann dorthin.
2. Klicken Sie mit der rechten Maustaste auf „SonovaVerify.exe“ und wählen Sie „Eigenschaften“ im Kontextmenü aus.
3. Wählen Sie die Registerkarte „Digitale Signaturen“ aus.
4. Doppelklicken Sie auf die SHA256-Signatur „Sonova AG“.

5. Überprüfen Sie, ob die Elemente der Signatur gültig sind. Überprüfen Sie insbesondere, ob oben die Meldung „Die digitale Signatur ist gültig“ angezeigt wird und Name des Signatursgebers und Uhrzeit der Signatur mit dem folgenden Bild übereinstimmen:



6. Klicken Sie auf die Schaltfläche „Zertifikat anzeigen“ und dann auf die Registerkarte „Details“ und überprüfen Sie, ob der Wert im Feld „Fingerabdruck“ mit diesem übereinstimmt: db88d10f0a1bfb12be6c3c46c516e507e14f2593
7. Schließen Sie die Popup-Dialoge und doppelklicken Sie auf „SonovaVerify.exe“.
8. Überprüfen Sie, ob, wie im folgenden Bild dargestellt, „NO ERRORS DETECTED“ (KEINE FEHLER ERKANNT) angezeigt wird:

```
SonovaVerify 0.0.4.0 Copyright 2019-2025 Sonova

Verifying: C:\Program Files (x86)\Advanced Bionics\Target CI\SonovaVerify.DAT
Target: C:\Program Files (x86)\Advanced Bionics\Target CI
Product: Target CI 1.5.11.0

FILES PROCESSED: 779

IGNORED FILES: 3
.\config\App.xml
.\data\
.\sonovaverify.dat

NO ERRORS DETECTED.
Press any key to continue . . .
```

Die Meldung „NO ERRORS DETECTED“ (KEINE FEHLER ERKANNT) bedeutet, dass die Überprüfung der Integrität und Authentizität des Inhalts des Installationsmediums für die Anpasssoftware erfolgreich durchgeführt wurde. Das bedeutet, dass SonovaVerify.exe die Authentizität und Integrität aller Dateien und Ordner überprüft hat. Damit wird sichergestellt, dass der Inhalt des Installationsmediums für die Anpasssoftware nicht manipuliert, beschädigt oder auf andere Weise beeinträchtigt wurde.

SonovaVerify.exe zeigt Warnungen oder Fehlermeldungen an, wenn Dateien oder Ordner fehlen oder dem Installationsmedium unerwartete Dateien oder Ordner hinzugefügt wurden. Falls Warn- oder Fehlermeldungen angezeigt werden, ist die Überprüfung der Integrität und Authentizität des Inhalts des Installationsmediums für die Anpasssoftware fehlgeschlagen. Es wird empfohlen:

- die Installation nicht fortzusetzen
- keine Dateien zu öffnen oder auszuführen, die im Installationsimage der Anpasssoftware enthalten sind und das Problem dem Support von Phonak zu melden (siehe Abschnitt 2.1)

8.3 AUTOMATISCHES ÜBERPRÜFEN DER INTEGRITÄT DER INSTALLIERTEN ANPASSSOFTWARE

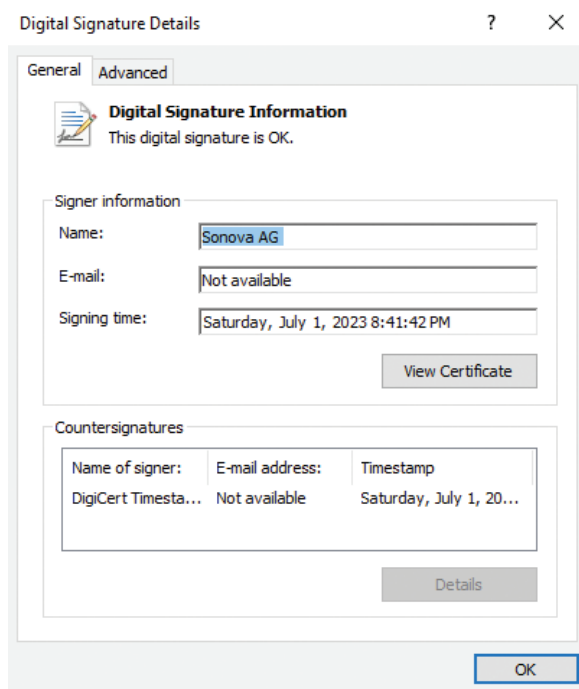
SonovaVerify ist in die Anpasssoftware integriert und wird bei jedem Start der Anwendung ausgeführt, um die Integrität der Programmdateien der Anpasssoftware zu überprüfen. Programmdateien werden mithilfe branchenüblicher Verfahren und Zertifikate, die von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt werden, digital signiert. Die Software informiert den Benutzer in Form von Warnmeldungen, wenn Programmdateien beschädigt sind.

8.4 MANUELLES ÜBERPRÜFEN DER INTEGRITÄT DER INSTALLIERTEN ANPASSSOFTWARE

Benutzer können die folgenden Schritte ausführen, um jederzeit die Integrität und Echtheit der installierten Anpasssoftware zu überprüfen, ohne die Anpasssoftware starten zu müssen:

1. Öffnen Sie den Windows Explorer und navigieren Sie zum Ordner mit der ausführbaren Datei der Anpasssoftware, der sich normalerweise hier befindet: C:\Programmdateien (x86)\Advanced Bionics\Target CI\
2. Klicken Sie mit der rechten Maustaste auf „SonovaVerify.exe“ und wählen Sie „Eigenschaften“ im Kontextmenü aus.
3. Wählen Sie die Registerkarte „Digitale Signaturen“ aus.
4. Doppelklicken Sie auf die SHA256-Signatur „Sonova AG“.

5. Überprüfen Sie, ob die Elemente der Signatur gültig sind, und insbesondere, ob oben die Meldung „Die digitale Signatur ist gültig“ angezeigt wird und Name des Signaturgebers und Uhrzeit der Signatur mit dem folgenden Bild übereinstimmen:



6. Klicken Sie auf die Schaltfläche „Zertifikat anzeigen“ und dann auf die Registerkarte „Details“ und überprüfen Sie, ob der Wert im Feld „Fingerabdruck“ mit diesem übereinstimmt: db88d10f0a1bfb12be6c3c46c516e507e14f2593
7. Schließen Sie die Popup-Dialoge und doppelklicken Sie auf „SonovaVerify.exe“.
8. Überprüfen Sie, ob, wie im folgenden Bild dargestellt, „NO ERRORS DETECTED“ (KEINE FEHLER ERKANNT) angezeigt wird:

```
SonovaVerify 0.0.4.0 Copyright 2019-2025 Sonova

Verifying: C:\Program Files (x86)\Advanced Bionics\Target CI\SonovaVerify.DAT
Target: C:\Program Files (x86)\Advanced Bionics\Target CI
Product: Target CI 1.5.11.0

FILES PROCESSED: 779

IGNORED FILES: 3
.\config\App.xml
.\data\
.\sonovaverify.dat

NO ERRORS DETECTED.
Press any key to continue . . .
```

Die Meldung „NO ERRORS DETECTED“ (KEINE FEHLER ERKANNT) bedeutet, dass die Überprüfung der Integrität und Authentizität des Inhalts des Installationsmediums für die Anpasssoftware erfolgreich durchgeführt wurde. Das bedeutet, dass SonovaVerify.exe die Authentizität und Integrität aller Dateien und Ordner überprüft hat. Damit wird sichergestellt, dass der Inhalt des Installationsmediums für die Anpasssoftware nicht manipuliert, beschädigt oder auf andere Weise beeinträchtigt wurde.

SonovaVerify.exe zeigt Warnungen oder Fehlermeldungen an, wenn Dateien oder Ordner fehlen oder dem Installationsmedium unerwartete Dateien oder Ordner hinzugefügt wurden. Falls Warn- oder Fehlermeldungen angezeigt werden, ist die Überprüfung der Integrität und Authentizität des Inhalts des Installationsmediums für die Anpasssoftware fehlgeschlagen. Es wird empfohlen:

- die Installation nicht fortzusetzen
- keine Dateien zu öffnen oder auszuführen, die im Installationsimage der Anpasssoftware enthalten sind und das Problem dem Support von Phonak zu melden (siehe Abschnitt 2.1)

9. SOFTWARE-PATCHES UND UPDATES

Automatische Updates werden nicht unterstützt. Weitere Informationen finden Sie in Abschnitt 12.

10. DATENVERWALTUNG

10.1 DATENBANKEN

Die Anpasssoftware verwendet eine transaktionale Datenbank zum Speichern von Patientendaten sowie eine Reihe von Infodatenbanken, welche die von der Anwendung benötigten Metadatenkonfigurationen bereitstellen.

Eine detaillierte Liste aller von der Anpasssoftware implementierten Datenbanken finden Sie in Abschnitt 3 „Netzwerk- und Kontextdiagramme“ unter „Bereitstellungsartefakte“.

Wenn die Anpasssoftware als Standalone-Anwendung installiert wird, befindet sich die Patientendatenbank intern in der Anpasssoftware. Die in der Datei „PatientDatabase.sqlite“ gespeicherte Patientendatenbank befindet sich auf demselben Computer wie die Anpasssoftware und ermöglicht das Speichern von Patientendaten. Zum Sichern der Anwendungsdaten können Sie, wenn Target CI als Standalone-Anwendung bereitgestellt ist, eine Sicherungskopie des gesamten Ordners „%ProgramData%\Advanced Bionics\Target CI\Target CI\Data“ erstellen. Schützen Sie Datensicherungen nicht nur vor Datenverlust, sondern auch vor Diebstahl. Wenn die Anpasssoftware als Noah Modul installiert ist, werden die Patientendaten in der vom Noah System bereitgestellten Datenbank gespeichert. Für die Noah Datenbank kann der Netzwerkzugriff konfiguriert werden. Die Noah Datenbank kann auch ohne Netzwerkzugriff konfiguriert und dann auf demselben PC wie die Anpasssoftware installiert werden. Konfigurieren Sie die Noah Datenbankverschlüsselung, um die Daten zu schützen (siehe Dokumentation von HIMSA).

Informationen zum Noah Distributed-Bereitstellungsmodus finden Sie unter dem folgenden Link, über den Sie Anleitungen zum Sichern und Wiederherstellen der Noah Patientendatenbank aufrufen können:

<https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/>

10.2 DATENMIGRATION

Die Anpasssoftware ermöglicht es Benutzern, Patientendatensätze der vorherigen AB Anpasssoftware (SoundWave 3.2) zu migrieren. Damit die Patientendaten migriert werden können, muss der Zugriff auf diese Daten von einer SoundWave 3.2-Installation auf demselben Computer wie Target CI möglich sein.

10.3 HÖRSYSTEMKONFIGURATIONEN

Die Anpasssoftware ermöglicht das Exportieren und Importieren von Gerätekonfigurationen und -einstellungen.

10.4 DATENENTSORGUNG

Hinweise zur Datenentsorgung finden Sie in Abschnitt 5.4 „Demontage und Außerbetriebnahme“ dieses Dokuments sowie im Abschnitt „Entsorgung und gefährliche Materialien“ der Gebrauchsanweisung. Für Noah Installationen stehen detaillierte Anweisungen zum Löschen von Patientenakten unter folgender Adresse zur Verfügung: <https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/deleting-patient-records/>

11. SICHERHEITSUMGEBUNG – GEMEINSAME VERANTWORTUNG

Die Anpasssoftware wurde für einen Verwendungszweck entwickelt, bei dem davon ausgegangen wird, dass die Steuerung von Cybersicherheitsrisiken in der gemeinsamen Verantwortung aller Beteiligten im gesamten Ökosystem für Hörsysteme liegt. Hierzu gehören insbesondere Hörsystemträger, Eltern oder Erziehungsberechtigte von Kindern, die Hörsysteme tragen, Audiologen und Hörakustiker, IT-Administratoren, Hörversorgungseinrichtungen und -anbieter sowie Anbieter von Hörsystemen und Programmiergeräten.

Die folgende Liste enthält Empfehlungen zu bewährten Vorgehensweisen und Sicherheitskontrollen für die Anpassumgebung, in der die Anpasssoftware verwendet wird:

Betriebssystemebene

- Wenden Sie Zugriffskontrollen auf Betriebssystemebene an, z. B. durch:
 - Entfernen von Gästekonten
 - Aktivieren der Windows-Benutzeranmeldung
 - Führen einer Liste autorisierter Bediener, um den Zugriff auf das System zu kontrollieren
 - Festlegen angepasster Benutzer und Rollen
 - Festlegen von Anforderungen für sichere Passwörter und Geheimhalten von Zugangsdaten
 - Aktivierung eines Zeitlimits für inaktive Sitzungen
- Wenden Sie Auditkontrollen auf Betriebssystemebene an.
- Stellen Sie sicher, dass das Betriebssystem auf dem neuesten Stand ist.
- Stellen Sie sicher, dass die installierte Anpasssoftwareversion aktuell ist.
- Verwenden Sie aktuelle Versionen von Malware- und Virenschutz.
- Stellen Sie sicher, dass die AutoRun- und AutoPlay-Funktionen deaktiviert sind.
- Aktivieren Sie Positivlisten für Anwendungen.

Datenschutz

- Bitte stellen Sie sicher, dass keiner der Ordner oder Dateien, die Anwendungsdaten enthalten, im Netzwerk freigegeben ist. Die Standardpfade der Anwendungsdaten sind in der Tabelle in Abschnitt 5.4 aufgeführt. Um zu überprüfen, welche Netzwerkfreigaben von einem Computer bereitgestellt werden, navigieren Sie im Microsoft-Tool „Computerverwaltung“ zu „Computerverwaltung -> Freigegebene Ordner -> Freigaben“ oder führen Sie den PowerShell-Befehl „Get-WmiObject -class Win32_Share“ aus.

- Während der Installation werden die Berechtigungen für den Anwendungsdatenordner gemäß Abschnitt 6.1 festgelegt. Anwendungsdatenordner erben die Zugriffsberechtigungen vom übergeordneten Ordner. Die Verwaltung der Berechtigungen für den übergeordneten Ordner liegt in der Verantwortung des Betreibers der Software.
- Verschlüsseln Sie Patientendaten mithilfe von Drittanbieter-Tools oder -kontrollen auf Betriebssystemebene durch Verwendung einer Laufwerkverschlüsselung (z. B. das kostenlose Microsoft BitLocker), um alle Daten zu schützen. Bei Noah Bereitstellungen sollten Sie die Nutzung der Noah Datenbankverschlüsselung in Betracht ziehen.
- Sorgen Sie für den Schutz externer Medien mit aus der Anpasssoftware exportierten Daten, insbesondere Berichten und Protokollen. Wenn die Daten nicht mehr benötigt werden, sollten sie und/oder die betreffenden Medien sicher gelöscht werden.
- Verwenden Sie USB-Speichermedien mit integrierter Sicherheitsfunktion, beispielsweise verschlüsselte USB-Laufwerke mit integriertem Tastenfeld.
- Gewährleisten Sie stets die Datensicherheit, indem Sie folgende Vorgehensweisen befolgen:
 - Wenn Sie Daten über ungesicherte Kanäle übertragen, anonymisieren oder verschlüsseln Sie die Daten.
 - Schützen Sie Datensicherungen nicht nur vor Datenverlust, sondern auch vor Diebstahl.
 - Entfernen Sie alle Daten von Medien, die nicht mehr verwendet werden oder zur Entsorgung bestimmt sind.
- Benutzer sollten gemäß geltenden Vorschriften und Richtlinien für den Umgang mit Patienteninformationen/personenbezogenen identifizierbaren Informationen (PII)/geschützten Gesundheitsinformationen (PHI) zugelassene Verfahren und Tools zum sicheren Entfernen von auf Wechselmedien gespeicherten Daten anwenden.

IT-Infrastruktur

Betreiben Sie die Anpasssoftware in einer sicheren Netzwerkkumgebung, die vor unbefugtem Zugriff geschützt ist. Es gibt viele wirksame Techniken zum Isolieren und Schützen medizinischer Informationssysteme, insbesondere die Implementierung von Firewall-Schutz, demilitarisierten Zonen (DMZ), virtuellen lokalen Netzen (VLAN) und Netzwerklänen. Halten Sie eine aktive Netzwerkverbindung aufrecht, um Betriebssystemupdates zu beziehen.

Physische Ebene

- Der Arbeitsplatz, auf dem die Anpasssoftware installiert ist, sollte physisch so gesichert sein, dass unbefugtes Personal weder Zugriff darauf hat noch Manipulationen vornehmen kann.
- Der Zugriff auf an den Arbeitsplatz angeschlossene Drucker sollte kontrolliert werden.
- Der Monitor des Arbeitsplatzes, auf dem die Anpasssoftware installiert ist, sollte so aufgestellt werden, dass der Bildschirminhalt nur für den Benutzer sichtbar ist.

Organisationsebene

- Nur professionell geschultes und qualifiziertes Personal ist zur Bedienung des Systems befugt. Bevor einer Person die Befugnis zur Bedienung des Systems gegeben wird, ist sicherzustellen, dass sie die mit der Anpasssoftware gelieferte Gebrauchsanleitung gelesen und vollständig verstanden hat.
- Nur Personal, das zur Wartung und zum Betrieb der Anpasssoftware berechtigt ist, darf über Benutzerkonten für den Rechner verfügen, auf dem die Software installiert ist. Die Computer- und Domänenkonten sowie die damit verbundenen Zugriffsrechte sollten regelmäßig überprüft und deaktiviert werden, wenn der Zugriff auf den Rechner nicht mehr erforderlich ist.
- Wenn Sie verdächtige Aktivitäten auf Ihren Anpasssoftware-Konten oder unerwartete Vorgänge bemerken, wenden Sie sich an Advanced Bionics. Weitere Informationen finden Sie in Abschnitt 2.1.

Weitere Informationen zur gemeinsamen Verantwortung und eine ausführlichere Liste von bewährten Verfahren und Sicherheitskontrollen für die Anpassungsumgebung, in der die Anpasssoftware auf verschiedenen Ebenen eingesetzt wird, finden Sie unter:

- EHIMA-Whitepaper „Best Practices for Secure Fitting of Hearing Devices“ (Best Practices für die sichere Hörsystemanpassung) [EHIMAWhitePaper](#)

12. HERSTELLUNG, SOFTWARE-ENTWICKLUNG UND SICHERHEITSMANAGEMENT

Die Cybersicherheit spielt während der gesamten Software-Entwicklung eine zentrale Rolle. Die Anpasssoftware wird in Übereinstimmung mit den Normen IEC 62304 und IEC 82304 entwickelt.

Die Anpasssoftware wird im Rahmen des Herstellungsprozesses auf Viren und Malware geprüft.

Sicherheitslücken in Komponenten von Drittanbietern, die in der National Vulnerability Database (NVD) des National Institute of Standards and Technology (NIST) aufgeführt sind, werden während des Entwicklungsprozesses bewertet und behoben. Nach dem Inverkehrbringen der Software wird diese weiterhin auf Auftreten der dort aufgeführten Sicherheitslücken überwacht.

Konfigurationsverwaltung

AB entwickelt, dokumentiert und pflegt intern unter Konfigurationskontrolle die Basiskonfiguration jeder freigegebenen Version der Anpasssoftware.

Alle von der Anpasssoftware verwendeten Softwarekomponenten von Drittanbietern werden identifiziert und in der Software-Stückliste (SBOM) dokumentiert. Die SBOM wird von AB im Rahmen des Cybersicherheits-Risikomanagements verwendet, um die Gefährdung durch Cybersicherheitsbedrohungen und bekannt gewordene Sicherheitslücken mithilfe aktueller Tools zum Scan auf Sicherheitslücken zu bewerten und zu überwachen.

Sicherheitsupdates

AB überwacht kontinuierlich die Anpasssoftware auf Sicherheitslücken. Dies umfasst sowohl Sicherheitslücken in der Anpasssoftware selbst als auch in Komponenten von Drittanbietern, die von der Anpasssoftware-Anwendung genutzt werden.

Die Bewertung bekannter Sicherheitslücken erfolgt auf Basis der Konfiguration und Verwendung der Anpasssoftware.

Bei Bedarf können Sicherheitslücken durch eine umfassendere Version der Anpasssoftware behoben werden, die Patches für bestimmte Softwarekomponenten innerhalb des Softwarepakets enthält.

Offenlegung von Sicherheitslücken

Wir verpflichten uns zur Offenlegung von Sicherheitslücken und zur Verbesserung der Sicherheit unserer Produkte und Dienstleistungen.

Die Meldung von vermuteten Sicherheitslücken oder Sicherheitsbedenken im Zusammenhang mit unseren Produkten oder der zugrunde liegenden Software/Infrastruktur wird begrüßt.

Bitte lesen Sie unsere Richtlinien zur Offenlegung von Sicherheitslücken unter <https://www.sonova.com/en/coordinated-vulnerability-disclosure-policy> und befolgen Sie die Anweisungen, um einen Bericht einzureichen.

13. SOFTWAREKOMPONENTEN UND STÜCKLISTE

Die Anpasssoftware umfasst bestimmte COTS-Softwarekomponenten (Commercial Off-the-Shelf, d. h. gewerbliche Standardsoftware).

In der folgenden Tabelle sind alle SOUP (Software of Unknown Provenance, also Software unsicherer Herkunft) aufgeführt, die mit der Anpasssoftware vertrieben werden.

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
AForge.NET	Die AForge.NET-Bibliothek für Mathematik und Medien, die Bestandteil von IceLink und LiveSwitch ist und von diesen benötigt wird	AForge.NET	2.2.5.0
Amplifon. Programmer	Bestandteil der Software-Suite von Amplifon	Amplifon	3.3.4.0
Amplifon. Programmer.Core	Bestandteil der Software-Suite von Amplifon	Amplifon	1.0.4.0
AutoMapper	Automatisiert die Objekt-zu-Objekt-Zuordnung	Jimmy Bogard	10.1.1.0
BenchmarkDotNet	Bibliothek für Benchmark-Tests, die Werkzeuge zur Messung und zum Vergleich der Code-Leistung bereitstellt	BenchmarkDotNet-Community	0.13.0.0
Castle.Core	Eine Kernbibliothek des Castle-Projekts, die Komponenten wie die dynamische Proxy-Generierung und Inversion-of-Control-Container für .NET-Anwendungen bietet	Castle Project	4.4.1
Chessie	Eine funktionale Fehlerbehandlungsbibliothek für F#	Open Source	0.6.0.0
ciAD Hearingloss Simulator	Hörverlustsimulatorbibliothek für Mediaplayer	ciAD (Jürg Haubold)	4.0.0.1
ClosedXML	Vereinfacht das Lesen, Bearbeiten und Schreiben von Excel-Dateien, ohne dass Excel installiert sein muss	ClosedXML Community	0.95.4.0
CommandLine Parser	Bietet eine übersichtliche und prägnante API zum Parsen von Befehlszeilenargumenten	CommandLineParser Community	2.4.3
Common.Logging	Eine portable Logging-Abstraktion für .NET-Anwendungen	Common.Logging Community	3.4.1.0

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
CommonService Locator	Bietet eine einheitliche Schnittstelle für die Dienstsuche, wodurch Anwendungen von bestimmten IoC-Containern entkoppelt werden können	Microsoft	2.0.5.0
Credential Management	Das Credential Management-Paket ist ein Wrapper für die Credential Management-API von Windows.	iLya Lozovyy	1.0.2
CSharpAnalytics	Wird für Google Analytics verwendet	Attack Pattern	1.6.1
Dapper	ORM	Sam Saffron, Marc Gravell, Nick Craver	2.0.78.45418
Destructurama.Attributed	Wird von Nephele-Bibliotheken verwendet	Serilog Contributors	3.1.0.0
Developer Express Suite	Eine umfassende Sammlung von UI-Steuerelementen und Bibliotheken für .NET-Entwickler, die Werkzeuge zur Erstellung funktionsreicher Anwendungen bietet	Developer Express Inc	20.2.10.0
DirectShow 2005	Ermöglicht von .NET-Anwendungen aus den Zugriff auf die Microsoft DirectShow-Funktionalität	Microsoft	2.0
DSL4	DSL 4 Fitting Formula Library	National Centre for Audiology, Kanada	4.2
DSL5	DSL 5 Fitting Formula Library	National Centre for Audiology, Kanada	5.0.34
ExcelNumberFormat	Bietet Funktionen zum Parsen und Formatieren von Excel-Zahlenformaten	Open Source	1.1.0.0
FM.dll	Integraler Bestandteil ihrer Echtzeit-Kommunikationssysteme wie LiveSwitch und IceLink	FM (Frozen Mountain)	2.9.32
FSharp.Core	Die Kernbibliothek für die Programmiersprache F#	Microsoft	6.0.322.10402
FTDI Chip	Ein Treiberpaket von Future Technology Devices International (FTDI), das die Kommunikation zwischen USB-Geräten und Softwareanwendungen ermöglicht	FTDI	3.02.07

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
GNOtometrics.Aurical	GNOtmetrics.Aurical, neu gepackt für Sonova	Natus Medical Incorporated	2.0.1.9
SharedUtilities.dll	Bietet allgemeine Hilfsfunktionen und gemeinsam genutzte Ressourcen für alle Natus-Anwendungen.	Natus Medical Incorporated	1.0.0.0
Hardware.Info	Eine Komponente, die detaillierte Informationen über die Hardwarekonfiguration eines Systems sammelt und bereitstellt	Open Source	11.1.0.1
Himsa.NLWSMAPI.dll	Eine Bibliothek, die mit der Noah Software von HIMSA verbunden ist	HIMSA	2.0.3.0
natus.otometrics.hipro2	HiPro-Kommunikationsbibliotheken	Natus Medical Incorporated	2.0.0.4
Iced.dll	Ermöglicht Echtzeitkommunikation durch Audio-, Video- und Datenstreaming	FM (Frozen Mountain)	1.12.0.0
IceLink	Wird für die Integration von WebRTC-Audio-/Videokonferenzen verwendet	FM (Frozen Mountain)	3.13.100.13250
icudt.dll	Bietet Unicode- und Globalisierungsunterstützung für Softwareanwendungen	FM (Frozen Mountain)	54.1.0.0
IdentityModel	OpenID Connect- und OAuth 2.0-Client-Bibliothek, die von der Komponente „Kona.CommonServices.Authentication“ für die OAuth-2-Authentifizierung verwendet wird	Dominick Baier, Brock Allen	6.2.0.0
IMCInterfaces	Schnittstellenbibliothek für die Kommunikation zwischen Noah Modulen	HIMSA II K/S	4.4.0.2266
iText 7	PDF-Bibliothek zum programmgesteuerten Erstellen, Bearbeiten und Überprüfen von PDF-Dokumenten	iText Software	7.1.16.0
JetBrains.dotMemory	Ein Tool zur Speicherprofilierung, um Speicherlecks zu erkennen und die Speichernutzung in .NET-Anwendungen zu optimieren	JetBrains	111.0.0.0

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
JsonDiffPatch DotNet.dll	Bietet Funktionen zum Vergleichen und Patchen von JSON-Objekten	Open Source	1.0.1.0
LibGit2Sharp	Wird von Bibliotheken von Sonova zur Kommunikation mit Git verwendet	LibGit2Sharp-Mitwirkende	0.26.1.93
LiveSwitch	Wird für die Integration von WebRTC-Audio-/Videokonferenzen verwendet	FM (Frozen Mountain)	1.18.5.32382
log4net.dll	Logging-Framework für .NET	Apache	4.7.0.3189
Mapster	Wird für das Objekt-Mapping in Code verwendet	chaowlert, eric_swann	7.2.0.0
Mapster.Core	Wird für das Objekt-Mapping in Code verwendet	chaowlert, eric_swann	1.2.0.0
MathNet.Numerics	Wird für Anpassalgorithmen (Signalpfad, Zielabgleich usw.) genutzt	Christoph Rüegg, Marcus Cuda, Jorgen van Gael und Mitwirkende	4.11.0
Microsoft.Bcl. AsyncInterfaces	Stellt die Schnittstellen IAsyncEnumerable<T> und IAsyncDisposable sowie Hilfstypen für .NET Standard 2.0 bereit	Microsoft	6.0.21.52210
Microsoft. CodeAnalysis. Common	Wird von den Bibliotheken von Sonova.HardwareAbstraction.Palio.Trafo verwendet	Microsoft	3.900.21.12420
Microsoft. CodeAnalysis. CSharp	Wird von den Bibliotheken von Sonova.HardwareAbstraction.Palio.Trafo verwendet	Microsoft	3.900.21.12420
Microsoft.CSharp.dll	Bietet Kompilierung und Codegenerierung mit C#	Microsoft	4.700.19.56404
Microsoft. Diagnostics. FastSerialization.dll	Wird zur effizienten Serialisierung und Deserialisierung von Diagnosedaten verwendet	Microsoft	1.0.0.0
Microsoft. Diagnostics. NETCore.Client.dll	Eine verwaltete Bibliothek, die die Interaktion mit der .NET Core-Laufzeitumgebung für verschiedene Diagnoseaufgaben ermöglicht, wie z. B. die Ablaufverfolgung und das Anfordern von Speicherausgängen.	Microsoft	0.2.4.27602

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
Microsoft. Diagnostics. Runtime.dll	Stellt APIs zur Untersuchung von laufenden Prozessen und Absturz-Speicherausgügen bereit, sodass Entwickler Debugging- und Diagnosetools erstellen können	Microsoft	2.0.4.26801
Microsoft. Diagnostics.Tracing. TraceEvent.dll	Eine Bibliothek zum Parsen und Verarbeiten von ETW-Ereignissen (Event Tracing for Windows)	Microsoft	2.0.70
Microsoft. DotNet.Platform Abstractions.dll	Bietet APIs für den Zugriff auf Informationen über die .NET-Plattform	Microsoft	3.100.620.31604
Microsoft. Extensions. Dependency Injection. Abstractions	Definiert die Abstraktionen für die Abhängigkeitsinjektion in .NET-Anwendungen	Microsoft	6.0.21.52210
Microsoft. Extensions.Logging	Ermöglicht strukturiertes Logging in .NET-Anwendungen	Microsoft	6.0.21.52210
Microsoft. Extensions.Options	Unterstützt die Konfiguration von Optionen in .NET-Anwendungen	Microsoft	6.0.21.52210
Microsoft. Extensions. Primitives	Stellt Schnittstellen und Klassen für Änderungsverfolgung und Stornierungstoken bereit, die bei der Verwaltung veränderbarer Daten und der Bereinigung von Ressourcen helfen	Microsoft	6.0.21.52210
Microsoft.Identity. Client	Die MSAL-Bibliothek für .NET ist Teil der Microsoft Identity Platform für Entwickler v2.0 (vormals Azure AD). Sie ermöglicht das Abrufen von Sicherheits-Token für den Aufruf geschützter APIs. Sie verwendet den Branchenstandard OAuth2 und OpenID Connect.	Microsoft	4.38.0.0
Microsoft.Identity. Client.Extensions. Msal	Sicherer plattformübergreifender Token-Cache für öffentliche MSAL-Client-Apps	Microsoft	2.19.3.0

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
Microsoft. IdentityModel. JsonWebTokens	Umfasst Typen, die Unterstützung für das Erstellen, Serialisieren und Validieren von JSON Web Token bieten. Wird von Komponenten verwendet, die mit Back-End-Diensten kommunizieren, die JSON Web Token zur Authentifizierung verwenden.	Microsoft	6.8.0.11012
Microsoft. IdentityModel. Logging	Abhängigkeit von Microsoft.IdentityModel.Tokens	Microsoft	6.8.0.11012
Microsoft. IdentityModel. Tokens	Abhängigkeit von SOUP Microsoft.IdentityModel.JsonWebTokens	Microsoft	6.8.0.11012
Microsoft. ML.OnnxRuntime	Eine Inferenz-Engine zum Ausführen von Modellen für maschinelles Lernen im ONNX-Format (Open Neural Network Exchange)	Microsoft	1.12.1
Microsoft. ML.OnnxRuntime. Managed	Der verwaltete .NET-Wrapper für die ONNX-Laufzeitumgebung	Microsoft	1.12.1
Microsoft.Office. Interop.Excel.dll	Als Teil der Office-Interop-Assemblies ermöglicht diese DLL .NET-Anwendungen die Interaktion mit Microsoft Excel	Microsoft	14.0.4733.1000
Microsoft. VisualStudio. TextTemplating.10.0	Bietet Funktionen zur Textvorlagengenerierung in Visual Studio, mit denen Entwickler mithilfe von T4-Vorlagen Code und andere textbasierte Artefakte generieren können	Microsoft	10.0.40219.1
Microsoft.Win32. Registry.dll	Ermöglicht den Zugriff auf die Windows-Registrierung	Microsoft	5.0.20.51904
Microsoft.Win32. SystemEvents.dll	Unterstützt die Systemereignisbehandlung in .NET-Anwendungen	Microsoft	8.0.23.53103
Microsoft.Win32. TaskScheduler.dll	Wird für das Backup-Tool der Anpassungssoftware (d. h. für automatisierte Backups) verwendet	David Hall	2.5.11.0

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
Microsoft.Xaml.Behaviors.Wpf	XAML Behaviors ist eine benutzerfreundliche Möglichkeit, WPF-Anwendungen mit minimalem Programmieraufwand allgemeine und wiederverwendbare Interaktivität hinzuzufügen.	xamlexperienceteam, Microsoft	1.0.1.0
Microsoft DIA SDK	Bietet APIs für die Arbeit mit Debugging-Informationen in PDB-Dateien	Microsoft	2.0.0.0
MS VC++ 2008 Redistributable	Microsoft Visual C++ 2008 Redistributable	Microsoft	9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistributable	Microsoft Visual C++ 2010 Redistributable	Microsoft	10.0.40219.325
Microsoft Visual C++ 2012 Redistributable	Microsoft Visual C++ 2012 Redistributable	Microsoft	11.0.51106.1
Microsoft Visual C++ 2017 Redistributable (x86)	Microsoft Visual C++ 2017 Redistributable	Microsoft	14.16.27024.1
Mono.Cecil	Wird zum Untersuchen, Ändern und Erstellen von .NET-Assemblies verwendet.	Microsoft	0.11.3.0
Moq.dll	Open-Source-.NET-Bibliothek zum Erstellen von Mock-Objekten während Unit-Tests	Moq Community (Open Source)	4.16.1.0
MS-VisualC++ 7.1 Laufzeitbibliotheken	Laufzeitbibliotheken für Microsoft Visual C++	Microsoft	7.10.6030.0
NAL-NL1	NAL-NL1 Fitting Formula Library	Australian Hearing	1.1.0.0
NAL-NL2	NAL-NL2 Fitting Formula Library	Australian Hearing	2.0.11
NAudio.dll	Wird zum Anpassen von Lautstärken und zum Wiedergeben von Audiodateien verwendet	Open Source	1.9.0.0
.NET Framework	.NET-Laufzeit-Framework	Microsoft	4.8.3928.0
Newtonsoft.Json	Wird für die JSON-Serialisierung und -Deserialisierung verwendet	James Newton-King	13.0.3.27908

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
Newtonsoft.Json.Schema.dll	Eine Schema-Validierungsbibliothek für JSON-Daten	James Newton-King	3.0.14.25421
Nibelung	NoahLink Wireless-Anpassbibliotheken	HIMSA	1.3.16.1
Nibelung2.CPD	NoahLink Wireless-Anpassbibliotheken	HIMSA	2.0.3.0
Nlog	Dies ist eine Abhängigkeit von HIMSA Nibelung.CPD (NoahLink Wireless)	Kim Christensen	5.0.4.1331
NoahLink	NoahLink Anpassgerätetreiber	HIMSA	1.55.6.166
NoahLink Wireless-Treiber	NoahLink Wireless-Anpassgerätetreiber	HIMSA	1.1.0.0
NoahLink Wireless Upgrader	NoahLink Wireless Firmware Upgrader	HIMSA	3.1.0.82
ModuleAPI.dll (Noah System)	Eine Komponente des Noah Systems von HIMSA, die APIs zur Integration und Verwaltung audiologischer Daten bereitstellt	HIMSA	4.13.0.5404
NiXPS SDK	Bietet Funktionen zur Verarbeitung von XPS-Dokumenten (XML Paper Specification)	NiXPS NV	2.6.0.0
NPOI	Eine Open-Source-Bibliothek, die das Lesen und Schreiben von Microsoft Office-Dokumenten in .NET-Anwendungen erleichtert	NPOI communi	2.4.1.0
NuGet Package Manager	Ein Tool zur Verwaltung von .NET-Bibliotheken und -Paketen	Microsoft	6.3.0.131
Nunit	Ein Framework für Unit-Tests für .NET-Anwendungen	NUnit Project	3.12.0.0
ONNX Runtime	Engine für Open Neural Network Exchange (ONNX)-Modelle	Microsoft	1.12.20220803.2.7048164

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
Open XML SDK	Bietet Werkzeuge für die Arbeit mit Office Open XML-Dokumenten	Microsoft	2.7.2
OSExtensions.dll	Bibliothek mit Erweiterungen für Betriebssystemfunktionen	Microsoft	1.0.0.0
Otometrics.REMaccess	Otometrics-Abstraktionsschicht oberhalb der Schnittstellenbibliothek für die Kommunikation zwischen Noah Modulen	GN Otometrics	1.0.0.10
Paket.Core.dll	Ein Open-Source-Abhängigkeitsmanager für .NET- und Mono-Projekte	Paket Community (Open Source)	7.1.5.0
Patagames.Pdf	C#-PDF-Bibliothek zum Erstellen und Bearbeiten von PDF-Dokumenten in .NET-Anwendungen	patagames.com	8.57.30.48
Patagames.Pdf.Wpf	C#-PDF-Bibliothek zum Erstellen und Bearbeiten von PDF-Dokumenten in .NET-Anwendungen	Patagames.com	4.19.18.48
Polly	Bibliothek, mit der Entwickler Resilienz- und Fehlerbehandlungsrichtlinien für verschiedene Aspekte wie Wiederholungen (Retry), Überlastungsschutz durch Trennschalter (Circuit Breaker), Schottisolierung (Bulkhead Isolation) und Rückfall (Fallback) auf flüssige und Thread-sichere Weise ausdrücken können	App vNext	7.2.3.0

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
Portable. BouncyCastle	Dies ist eine Abhängigkeit von HIMS A Nibelung.CPD (NoahLink Wireless)	The Legion of the Bouncy Castle Inc	1.8.15362.1
Portable. BouncyCastle. Crypto	Dies ist eine Abhängigkeit von HIMS A Nibelung.CPD (NoahLink Wireless)	The Legion of the Bouncy Castle Inc	1.9.0.1
protobuf-net.dll	Für RC-Blob verwendetes Serialisierungs-Framework.	Open Source	2.3.2.0
Google.Protobuf	Googles offizielle Protocol Buffers-Bibliothek für .NET, welche die Serialisierung und Deserialisierung strukturierter Daten ermöglicht	Google Inc	3.19.3.0
Perfolizer.dll	Eine Open-Source-Bibliothek zur Leistungsanalyse	Open Source	0.2.1.0
Rhino.Mocks.dll	Ein dynamisches Mock-Objekt-Framework für .NET	Rhino Mocks Community	3.6.0.0
Security. Cryptography. NetCore.dll	Bietet kryptografische Funktionen für .NET Core-Anwendungen	HardDev	1.0.1.0
Serilog	Protokollierungskomponente, die für die gesamte Chinook-Anwendung verwendet wird	Serilog Contributors	3.0.1.0
Serilog. Enrichers.Thread	Erweitert Serilog-Ereignisse um Eigenschaften aus dem aktuellen Thread	Serilog Contributors	3.1.0.0
Serilog. Extensions. Logging	Integriert Serilog in die Protokollierungsabstraktionen von Microsoft	Serilog Contributors	3.1.0.0

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
Serilog. Expressions	Ausdrucksbasierte Ereignisfilterung für Serilog	Serilog Contributors	2.0.0.0
Serilog.Sinks. Console	Serilog-Senke, die Protokollereignisse in die Konsole/ das Terminal schreibt	Serilog Contributors	4.0.0.0
Serilog.Sinks. Debug	Serilog-Senke, die Protokollereignisse in das Debug-Ausgabefenster schreibt	Serilog Contributors	2.0.0.0
Serilog.Sinks.File	Schreibt Serilog-Ereignisse in Textdateien im Plain-Text- oder JSON-Format	Serilog Contributors	4.1.0.0
Serilog.Sinks. NUnit.dll	Lässt sich in NUnit integrieren und leitet Protokollereignisse an die Testausgabe von NUnit weiter, was die Testdiagnose erleichtert.	Serilog Contributors	1.0.3.0
Serilog.Sinks. Trace	Serilog-Senke für Diagnose-Traces	Serilog Contributors	2.1.0.0
Serilog.Settings. AppSettings	Unterstützung der XML-Konfiguration (System.Configuration <appSettings>) für Serilog	Serilog Contributors	2.2.2.0
Security. Cryptography. NetCore.dll	Erweiterungen der mit .NET Framework ausgelieferten Sicherheits-APIs	Microsoft	1.0.1.0
SharpBITS API	SharpBITS.NET ist ein .NET-Wrapper der BITS-API sowie eine schlanke Windows-UI-Anwendung für einfacheren Zugriff auf BITS-Uploads und -Downloads.	perpetualKid	2.1.0.0

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
SharpZipLib	#ziplib (SharpZipLib, vormals NzipLib) ist eine Zip-, Gzip-, Tar- und Bzip2-Bibliothek, die vollständig in C# für die .NET-Plattform geschrieben ist. Diese Bibliothek bietet Komprimierungsfunktionen (Zip, Unzip, Stream-Komprimierung usw.). Wir nutzen sie innerhalb der Firmware-Update-App.	Open Source	1.3.3.11
SharpDX	Von LiveSwitch verwendet: SharpDX. Direct3D11, SharpDX. Direct2D1, SharpDX. Mathematics	Alexandre Mutel	4.0.1
SocketIOClient	Stellt einen Client für Socket.IO bereit, der eine bidirektionale, ereignisbasierte Echtzeitkommunikation in .NET-Anwendungen ermöglicht	HeroWong	2.2.4.0
Superpower	Parser-Kombinator-Bibliothek für C#	Datalust, Superpower Contributors, Sprache Contributors	2.3.0.0
SQLite.Interop	SQLite 3.36.0 Native Interop Library. Es handelt sich um eine Datenbank (SQLite) zum Speichern von Patientendaten (im Standalone-Modus), unseren Produktkatalogressourcen und den Metadaten für Anpassung, Zubehör und Hörsysteme. SQLite ist gemeinfrei.	SQLite Development Team	1.0.115

SOUP	FUNKTIONS- BESCHREIBUNG	HERSTELLER	VERSION
System Buffers	Stellt Ressourcen-Pooling aller Art für leistungskritische Anwendungen bereit, die häufig Objekte zuweisen und freigeben	microsoft, dotnetframework	4.6.28619.01
System.Collections.Immutable	Wird von den Bibliotheken von Sonova. HardwareAbstraction. Palio.Trafo verwendet	Microsoft	7.0.22.51805
System.ComponentModel.Annotations	Stellt Attribute bereit, mit denen Metadaten für Objekte definiert werden, die als Datenquellen dienen	microsoft, dotnetframework	4.6.26515.06
System.Configuration.ConfigurationManager	Implementiert Typen, welche die Verwendung von Konfigurationsdateien unterstützen.	Microsoft	5.0.20.51904
System.CodeDom.dll	Stellt Klassen bereit, mit denen Quellcode generiert und zu ausführbaren Dateien oder Assemblies kompiliert werden kann	Microsoft	8.0.23.53103
System.Data.SQLite	Wird von den Bibliotheken von Sonova. HardwareAbstraction. Palio.Trafo verwendet	SQLite Development Team	1.0.115.0
System.Diagnostics.DiagnosticSource	Eine Protokollierungsbibliothek, mit der Entwickler Diagnosedaten nachverfolgen und überwachen können	Microsoft	6.0.21.52210
System.Diagnostics.PerformanceCounter	Stellt APIs für die Interaktion mit Windows-Leistungszählern bereit	Microsoft	7.0.22.51805

SOUP	FUNKTIONS- BESCHREIBUNG	HERSTELLER	VERSION
System.Drawing.Common	Bietet Zugriff auf die GDI+-Grafikfunktionalität.	Microsoft	8.0.324.11603
System.Formats.Asn1.dll	Unterstützt die Kodierung und Dekodierung von Daten im Format „Abstract Syntax Notation One“ (ASN.1)	Microsoft	6.0.21.52210
System.IdentityModel.Tokens.Jwt	Umfasst Typen, die Unterstützung für das Erstellen, Serialisieren und Validieren von JSON Web Token bieten. Wird von Komponenten verwendet, die mit Back-End-Diensten kommunizieren, die JSON Web Token zur Authentifizierung verwenden.	Microsoft	6.8.0.11012
System.IO.Abstractions	Satz von Abstraktionen, die dabei helfen, Dateisysteminteraktionen testbar zu machen.	Tatham Oddie & Friends	12.0.10.46693
System.IO.Hashing.dll	Bietet Hash-Funktionen innerhalb von .NET, darunter Algorithmen zur Berechnung von Prüfsummen und kryptografischen Hashes.	Microsoft	6.0.222.6406
System.IO.Packaging.dll	Ermöglicht das Lesen und Schreiben von Paketdateien.	Microsoft	6.0.21.52210

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
System.IO.Ports.dll	Stellt Klassen für die Kommunikation über serielle Schnittstellen bereit, sodass .NET-Anwendungen mit Hardware interagieren können, die über serielle Schnittstellen angeschlossen ist	Microsoft	8.0.23.53103
System.Net.Http.WinHttpHandler.dll	Ein spezialisierter HTTP-Handler für Windows	Microsoft	6.0.422.16404
System.Numerics.Vectors	Implementiert hardwarebeschleunigte numerische Typen, die für Hochleistungsverarbeitungs- und Grafikanwendungen geeignet sind	microsoft, dotnetframework	4.6.26515.06
System.Memory	Implementiert Typen für die effiziente Darstellung und Zusammenführung verwalteter, gestapelter und nativer Speichersegmente und Abfolgen solcher Segmente sowie Primitive zum Parsen und Formatieren UTF-8-codierten Texts, der in diesen Speichersegmenten gespeichert ist	microsoft, dotnetframework	4.6.31308.01
System.Reactive.dll		Open Source	5.0.0.1

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
System. Reflection. DispatchProxy	Stellt eine Klasse zum dynamischen Erstellen von Proxytypen bereit, die eine angegebene Schnittstelle implementieren und von einem angegebenen DispatchProxy-Typ abgeleitet sind. Methodenaufrufe der generierten Proxyinstanz leiten an diesen DispatchProxy-Basistyp weiter.	Microsoft	4.700.20.21406
System. Reflection. Metadata	Dieses Paket implementiert maschinennahe Lese- und Schreibfunktionen für .NET-Metadaten (ECMA-335). Es ist leistungsoptimiert und die ideale Wahl zum Erstellen komplexerer Bibliotheken, die ein eigenes Objektmodell bereitstellen sollen, wie z. B. Compiler	Microsoft	5.0.20.51904
System. Reflection. TypeExtensions	Bietet Erweiterungsmethoden für die Reflection-API	Microsoft	4.700.19.56404
System.Runtime. Compiler Services.Unsafe	Stellt die System.Runtime.CompilerServices.Unsafe Klasse, die generische, low-level-Funktionalität zur Bearbeitung von Zeigern bereitstellt	microsoft, dotnetframework	6.0.21.52210

SOUP	FUNKTIONS- BESCHREIBUNG	HERSTELLER	VERSION
System.Security. AccessControl	Implementiert Basisklassen, welche die Verwaltung von Zugriffs- und Auditkontrolllisten für sicherungsfähige Objekte ermöglichen	Microsoft	6.0.21.52210
System.Security. Permissions	Stellt Typen bereit, die Code Access Security (CAS) unterstützen	Microsoft	5.0.20.51904
System.Security. Principal. Windows	Implementiert Klassen zum Abrufen des aktuellen Windows-Benutzers und zur Interaktion mit Windows-Benutzern und -Gruppen	Microsoft	5.0.20.51904
System.Security. Cryptography. Cng.dll	Bietet kryptografische Funktionen unter Verwendung von Cryptography Next Generation (CNG) APIs	Microsoft	5.0.20.51904
System.Security. Cryptography. Pkcs.dll	Bietet Klassen zur Verarbeitung von Public Key Cryptography Standards (PKCS), einschließlich signierter und verschlüsselter Daten	Microsoft	6.0.1923.31806
System.Security. Cryptography. ProtectedData. dll	Bietet Methoden zum Schutz und zur Aufhebung des Schutzes von Daten unter Verwendung der Windows Data Protection API (DPAPI) für die sichere Datenspeicherung	Microsoft	6.0.21.52210

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
System.Security.Cryptography.Xml.dll	Ermöglicht XML-Verschlüsselung und digitale Signaturen und unterstützt so die sichere Verarbeitung von XML-Daten in .NET-Anwendungen	Microsoft	6.0.822.36306
System.ServiceModel.Http.dll	Bietet HTTP-basierte Kommunikationsfunktionen für Windows Communication Foundation (WCF)-Dienste	Microsoft	4.700.19.56502
System.ServiceModel.Primitives.dll	Enthält grundlegende Klassen für WCF-Dienste, einschließlich Basisklassen und Schnittstellen für Dienstverträge und Kanäle	Microsoft	4.700.19.56502
System.Text.Encoding.CodePages	Bietet Unterstützung für Codepage-basierte Verschlüsselungen, einschließlich Windows-1252, Shift-JIS und GB2312	Microsoft	5.0.20.51904
System.Text.Encodings.Web	Implementiert Typen zum Kodieren und Escape-Maskieren von Zeichenfolgen zur Verwendung in JavaScript, HyperText Markup Language (HTML) und Uniform Resource Locators (URLs). Ist eine Abhängigkeit von SOUP IdentityModel.	microsoft, dotnetframework	6.0.21.52210

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
System.Text.Json	Implementiert leistungsstarke und ressourcenschonende Typen, die Objekte in JSON-Text (JavaScript Object Notation) serialisieren und JSON-Text in Objekte deserialisieren, einschließlich UTF-8-Unterstützung. Implementiert ferner Typen zum Lesen und Schreiben von UTF-8-codiertem JSON-Text und zum Erstellen eines schreibgeschützten In-Memory-Dokumentobjektmodells (DOM) für den wahlfreien Zugriff auf die JSON-Elemente in einer strukturierten Datenansicht	Microsoft	6.0.222.6406
System.Threading.Tasks.Extensions	Implementiert zusätzliche Typen, die das Schreiben von nebenläufigem und asynchronem Code vereinfachen	microsoft, dotnetframework	4.6.28619.01
System.Threading.Channels	Bietet eine Reihe von Synchronisierungsdatenstrukturen für den Datenaustausch zwischen Produzenten und Konsumenten und unterstützt so die parallele Programmierung mit hoher Leistung	Microsoft	6.0.21.52210

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
System.ValueTuple	Stellt die System.ValueTuple-Strukturen bereit, welche die zugrunde liegenden Typen für Tupel in C# und Visual Basic implementieren Ergänzt Unterstützung für Werttupel, da diese erst in späteren Versionen von .NET Framework enthalten sind	microsoft, dotnetframework	4.6.26515.06
TestStack.BDDfy.dll	Ein Framework für verhaltensgetriebene Entwicklung (BDD) für .NET	TestStack-Community	4.3.2.0
Thrift	Wird für die Remotelink-Protokolldefinition verwendet	Apache	0.13.0.0
Unity.Container	Der Unity Container (Unity) ist ein vollständig ausgestatteter und erweiterbarer Dependency-Injection-Container	Unity Container Project	5.8.13.0
Unity.Konfiguration	Der Unity Container (Unity) ist ein vollständig ausgestatteter und erweiterbarer Dependency-Injection-Container	Unity Container Project	5.2.5.0
Unity.Abstractions	Der Unity Container (Unity) ist ein vollständig ausgestatteter und erweiterbarer Dependency-Injection-Container	Unity Container Project	3.3.1.0

SOUP	FUNKTIONS-BESCHREIBUNG	HERSTELLER	VERSION
Unity. Interception. Configuration	Der Unity Container (Unity) ist ein vollständig ausgestatteter und erweiterbarer Dependency-Injection-Container	Unity Container Project	5.1.7.0
Unity. Interception	Der Unity Container (Unity) ist ein vollständig ausgestatteter und erweiterbarer Dependency-Injection-Container	Unity Container Project	5.5.5.0
Unity. Registration ByConvention	Der Unity Container (Unity) ist ein vollständig ausgestatteter und erweiterbarer Dependency-Injection-Container	Unity Container Project	2.1.9.0
Unity. ServiceLocation	Der Unity Container (Unity) ist ein vollständig ausgestatteter und erweiterbarer Dependency-Injection-Container	Unity Container Project	2.1.2.0
WAP BT Dongle Driver	Treiber für WAP BT-Dongle (Anpass-Dongle)	iAnywhere Solutions	3.0.0.6095
WebSync	Wird zur Integration des Anpassdatenkanals verwendet	FM (Frozen Mountain)	4.9.32.0
WPFHexaEditor. dll	Ein Hexadezimal-Editor-Steurelement für WPF-Anwendungen	FM (Frozen Mountain)	2.1.6
WpfScreen Helper.dll	Eine Hilfsbibliothek für WPF-Anwendungen, die Bildschirm- und Monitorinformationen bereitstellt	FM (Frozen Mountain)	2.1.0.0

SOUP	FUNKTIONS- BESCHREIBUNG	HERSTELLER	VERSION
Xceed Extended WPF Toolkit	Eine Sammlung von WPF-Steuererelementen und -Hilfsprogrammen, die WPF-Anwendungen um zusätzliche UI-Komponenten erweitern	Xceed	3.5.0.0
xmlunit-core.dll	Eine Bibliothek zum Testen und Vergleichen von XML-Ausgaben	XMLUnit Community	2.9.0.205
Xps to Pdf render (NiXPS)	Konvertiert programmgesteuert erstellte XPS-Dateien in das PDF-Format; wird für Berichtsfunktionen in der Anpass-App verwendet	NiXPS	2.6.7.0

14. REFERENZEN

Titel	URL
Gebrauchsanweisung (in elektronischer Form)	https://ifu.advancedbionics.com/
Advanced Bionics Datenschutzrichtlinie	https://advancedbionics.com/privacy
HIMSA	https://www.himsa.com/
Noah System 4	https://www.himsa.com/products/all-about-noah-system-4/
Backup und Wiederherstellung der Daten in Ihrer Noah Datenbank	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/backing-up-and-restoring-the-data-in-your-noah-database/
Kapazität der Noah System Datenbank ist erreicht	https://www.himsa.com/support/noah-4-knowledge-base/the-learning-center-2/noah-system-database-capacity-has-been-reached/
Welche Ports verwendet TeamViewer?	https://community.teamviewer.com/English/kb/articles/4139-ports-used-by-teamviewer
BCP 195	https://www.rfc-editor.org/info/bcp195
LiveSwitch Server Security Documentation (Sicherheitsdokumentation zum LiveSwitch-Server)	https://developer.liveswitch.io/liveswitch-server/server/security.html
EHIMA-Whitepaper „Best Practices for Secure Fitting of Hearing Devices“ (Best Practices für die sichere Hörsystemanpassung)	https://www.ehima.com/wp-content/uploads/2021/09/EHIMA_Cybersecurity-FSW-Security-Whitepaper_v1-Sep2021.pdf

 Advanced Bionics LLC
28515 Westinghouse Place
Valencia, CA 91355, United States
Tel.: +1.661.362.1400

info.us@advancedbionics.com

 Advanced Bionics
Logistic Services GmbH
Rheinmetallstraße 18A
99610 Sömmerda, Germany

info.switzerland@advancedbionics.com

Informationen über weitere AB Standorte finden Sie auf
advancedbionics.com/contact

AB – A Sonova brand

Informieren Sie sich bitte bei Ihrem lokalen Vertreter von AB über
die Zulassung und Verfügbarkeit in Ihrer Region.

Die Bluetooth®-Wortmarke und -Logos sind eingetragene Marken
der Bluetooth SIG, Inc. und jede Verwendung dieser Marken durch
die Sonova AG ist lizenziert.



029-S391-01