secunet konnektor

secunet Konnektor

Version 2.0.0

Hinweise zur sicheren Lagerung und Lieferkette

Version 1.7, 10.10.2018

Vertraulich / Confidential

secunet

secunet Security Networks AG

Inhaltsverzeichnis

Dokumentenhistorie

Version	Datum	Änderung	Autor
0.97	16.04.2018	Draft Version	secunet / SRC
0.98	27.04.2018	Einarbeitung der Kommentare von Prüfstelle und Zertifizierungsstelle	secunet / SRC
1.0	02.05.2018	Review durch secunet und Version zur Evaluierung	secunet / SRC
1.1	09.05.2018	Einarbeitung der Kommentare von Prüfstelle	secunet / SRC
1.2	18.05.2018	Korrekturen und Einarbeitung weiterer Kommentare von der Prüfstelle	secunet / SRC
1.3	22.07.2018	Korrekturen und Einarbeitung weiterer Kommentare des BSI	secunet / SRC
1.4	13.08.2018	Korrekturen und Einarbeitung weiterer Kommentare des BSI	secunet
1.5	27.09.2018	Korrekturen und Einarbeitung weiterer Kommentare des BSI	secunet / SRC
1.6	28.09.2018	Korrekturen und Einarbeitung weiterer Kommentare der Prüfstelle	secunet / SRC
1.7	10.10.2018	Korrekturen und Einarbeitung weiterer Kommentare des BSI	secunet / SRC

Dokumenteninformationen

Name	Wert
Dokumentenversion	Version 1.7
Datum	10.10.2018
Klassifizierung	Vertraulich / Confidential
Produktname	secunet Konnektor
Produktversion	2.0.0
Hersteller	secunet Security Networks AG

1 Einleitung

Dieses Dokument beschreibt die sichere Lieferkette bei Auslieferung des secunet Konnektor 2.0.0 der secunet Security Networks AG und ist Teil von [ALC_DEL]. Um die Sicherheit des secunet Konnektor zu gewährleisten, unterliegt der Lieferprozess definierten Anforderungen an die sichere Lieferkette.

Insbesondere ist das Schutzziel der sicheren Lieferkette die **Integrität** des secunet Konnektors. Es muss sichergestellt werden, dass der secunet Konnektor

- Während der Lagerung oder dem Transport nicht unbemerkt manipuliert oder ausgetauscht werden kann
- Während der Lagerung oder dem Transport nicht unbemerkt gestohlen werden kann
- Keine Geräte von außen in die Lieferkette eingebracht werden können.

Die sichere Lieferkette stellt keine **Vertraulichkeitsanforderung** an den secunet Konnektor. So wird nicht verhindert das Konnektoren gestohlen werden können. Dennoch wird durch Anforderungen bzgl. **Integrität** sichergestellt, dass keine individuellen Informationen einzelner Konnektoren (wie z.B. Seriennummern von Bauteilen) durch einen Angreifer unbemerkt abgegriffen werden können, da dies immer als Manipulationsversuch erkannt werden muss.

Die in diesem Dokument beschriebene sichere Lieferkette für den secunet Konnektor schließt nicht aus, dass in einer Lieferung neben dem Konnektor auch weitere eHealth Produkte, wie eHealth Kartenterminals ausgeliefert werden, solange die in diesem Dokument gestellten Anforderungen an die sichere Lieferkette für den secunet Konnektor eingehalten werden.

2 Lieferwege

Produzierte Konnektoren verlassen mit einem Großtransport die Produktionsstätte zu genau einem Großlager. Im Folgenden ist der direkte Lieferweg vom Großlager bis zum Leistungserbringer skizziert.

Vom Großlager kann ein Konnektor per Einzelversand in einer sicheren Versandtasche zum Leistungserbringer versandt werden, wo dieser bis zur Installation durch einen DVO sicher verwahrt wird. Ein Anbieter eines Praxisverwaltungssystems (PVS-Anbieter) kann durch Einzelversand, Kleintransport, mittlerer Transport oder Großtransport Konnektoren aus dem Großlager erhalten und selbst in ein Kleinlager oder mittleres Lager verbringen. Der PVS-Anbieter verschickt über Kleintransport Konnektoren zu beauftragten Dienstleistern vor Ort (DVO), die diese Konnektoren in Kleinlager und mobile Lager verbringen. Der PVS-Anbieter kann auch selbst die Rolle des DVO übernehmen. Ein unabhängiger DVO erhält Konnektoren über Kleintransport und verwahrt die Konnektoren bis zur Installation im Kleinlager und Transport diese zur Installation mit einem Kleintransport zum Leistungserbringer. Erfolgt die Installation zu einem späteren Zeitpunkt, ist der Leistungserbringer nach Annahme des Gerätes für die sichere Lagerung verantwortlich.

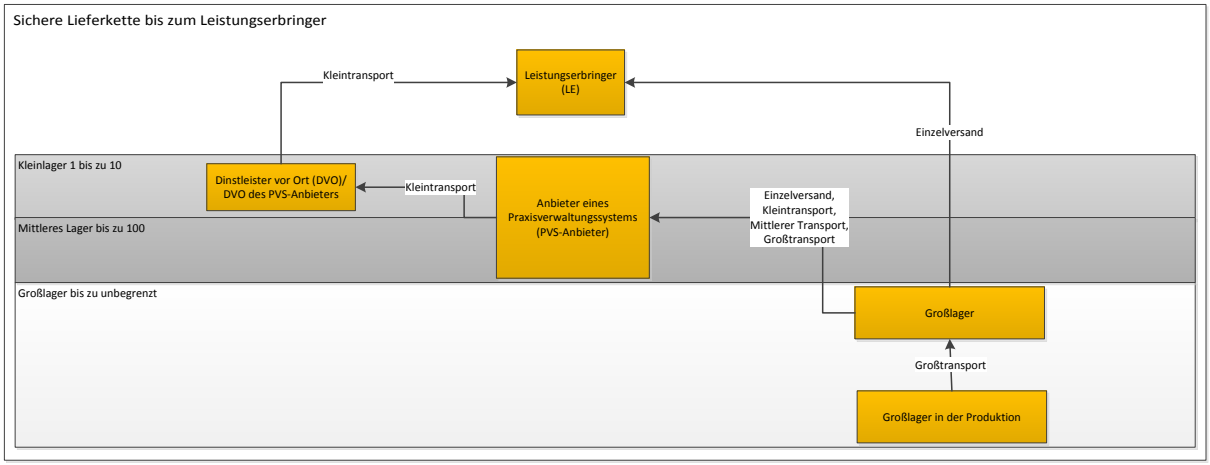

Abbildung 1: Darstellung der sicheren Lieferkette

Der Lieferweg des secunet Konnektors sieht ein Großlager vor. Neben dem oben beschriebenen Lieferweg sind aber weitere Zwischenstationen möglich. So können Konnektoren vom Großlager an weitere Zwischenhändler mit Großlager, Mittlerem Lager oder Kleinlager geliefert werden, bevor diese an einen PVS-Anbieter geliefert werden. Dabei gibt es keine Einschränkungen bzgl. der Anzahl der Zwischenhändler. Abhängig von der Anzahl der transportierten Geräte ist eine entsprechende Transportart (Kleintransport, mittlerer Transport, Großtransport) zu verwenden. Bis auf die Auslieferung an den Leistungserbringer (Kleintransport oder Einzelversand) gibt es keine weiteren Einschränkungen zur Transportart. Zudem sind auch Lieferungen von einem PVS-Anbieter zu einem anderen PVS-Anbieter oder von DVO zu DVO möglich.

Alle Teilnehmer der sicheren Lieferkette müssen sich an die Anforderungen zur sicheren Lagerung und Lieferkette halten.

Alle Detailanforderungen zu den einzelnen Lagern (Kleinlager, mittleres Lager, Großlager) und Transportarten werden in den Kapiteln 4 und 5 detailliert aufgeführt

3 Definitionen

3.1 Rollen

Fahrer:

Der Fahrer ist eine natürliche Person. Er transportiert den bzw. die Konnektoren von einem Ort zum nächsten Bestimmungsort. Der Fahrer kann die Rolle Transporteur bzw. Kurier haben. Beim Transport zum Installationstermin ist der Fahrer ggf. gleichzeitig der Servicetechniker (DVO). Der Kurier bildet eine besondere Form des Fahrers und ist gesondert beschrieben.

Servicetechniker (DVO):

Der Servicetechniker oder auch Dienstleister vor Ort (DVO) ist eine natürliche Person und führt die Installation und Konfiguration des Konnektors beim Leistungserbringer (LE) durch. Der DVO ist häufig auch Inhaber und Betreiber eines kleinen Lagers bzw. mobilen Lagers. Zudem kann der DVO als Lieferant (Transporteur / Fahrer) des Konnektors zum Leistungserbringer auftreten. Die Rolle des DVO wird entweder vom PVS-Anbieter übernommen oder ist ein von diesem beauftragter Dienstleister.

Transporteur:

Der Transporteur ist eine natürliche Person und Angestellter eines Versandunternehmens bzw. Speditionsunternehmens oder Lagers. Der Transporteur verantwortet mit seinen Mitteln den sicheren Transport im Sinne dieses Dokuments.

Kurier:

Der Kurier ist eine natürliche Person und transportiert einzelne Konnektoren zum Leistungserbinger, in Einzelfällen auch zum DVO. Der Kurier kommt z. B. beim Einzelversand von Konnektoren zum Einsatz.

Versandunternehmen:

Das Versandunternehmen oder auch Speditionsunternehmen stellt die erforderlichen Versandvoraussetzungen (Fahrzeug, Fahrer und ggf. zusätzliche Transportmittel) für die Lieferung von Konnektoren von einem Versandort zum nächsten Bestimmungsort gemäß den jeweiligen Anforderungen dieses Dokuments.

Versender:

Der Versender ist eine natürliche Person, welche namentlich in den Lieferdokumenten beim Versand der Konnektoren benannt wird. Der Versender gehört der jeweiligen Institution an, die sich für den Versandschritt verantwortlich zeichnet.

Empfänger:

Der Empfänger ist eine natürliche Person, welche namentlich in den Lieferdokumenten im Zuge des Versands der Konnektoren benannt wird. Der Empfänger gehört der jeweiligen Institution an, an welche die jeweilige Lieferung adressiert ist (z. B. Mitarbeiter im Großlager, mittlere Lager oder kleine Lager oder Mitarbeiter beim Leistungserbringer).

Empfangsberechtigter:

Bei dem Empfangsberechtigten handelt es sich um eine natürliche Personen auf Seiten des Empfängers. Der Empfangsberechtigte wird namentlich in den Lieferdokumenten genannt und verfügt über die notwendigen Rechte um auf der Seite des Empfängers die Konnektoren in Empfang zu nehmen. Nur empfangsberichtigte Personen dürfen Lieferungen von Konnektoren entgegennehmen. Es darf für eine Lieferung mehrere empfangsberechtigte Personen geben.

Leistungserbringer:

Als Leistungserbringer werden im deutschen Gesundheitssystem Personen oder Unternehmen bezeichnet, die Leistungen für die Mitglieder der gesetzlichen (GKV) Krankenversicherung erbringen. Der Leistungserbringer (LE) ist in der Lieferkette der letzte Empfänger der Konnektoren.

Hersteller:

Der Hersteller bzw. Produzent der Konnektoren ist eine juristische Person. Der Hersteller im Sinne dieser Spezifikation ist die Firma secunet.

Lager:

Ein Versender oder Empfänger (sofern nicht der Leistungserbringer) bewahrt Konnektoren vor Versand oder nach Empfang in einem Klein-, Mittel-, Groß oder Mobillager auf. Die Anforderungen an die Lager werden in Kapitel 4 erläutert.

Lagerist:

Bei dem Lageristen handelt es sich um eine natürliche Personen die in einem Lager beschäftigt ist.

PVS-Anbieter

Zugelassene Konnektoren können nur bei einem Praxisverwaltungssystem-Anbieter (PVS-Anbieter bzw. entsprechende Organisationseinheiten) bestellt werden. Der PVS-Anbieter ist zudem der Ansprechpartner des Leistungserbringers rund um den zugelassenen Konnektor. Bei Fragen zur sicheren Lieferung und zur Installation des Konnektors wendet sich der Leistungserbringer an seinen zuständigen PVS-Anbieter. Der PVS-Anbieter kann selbst die Rolle des Dienstleisters vor Ort (DVO) übernehmen oder einen externen DVO beauftragen. Zudem kann der PVS-Anbieter auch als Lieferant (siehe Rolle Fahrer bzw- Servicetechniker (DVO)) des Konnektors zum Leistungserbringer auftreten.

3.2 Informationen

Versandinformationen und Liefer-AVIS:

Der Liefer-AVIS oder die Versandinformation ist die Ankündigung des Lager- bzw. Warenzugangs. Das Liefer-AVIS (bzw. die Versandinformation) wird vom Versender an den Empfänger der Ware gesendet, bevor die Ware in Empfang genommen wird. Die Begriffe Liefer-AVIS und Versandinformation werden in diesem Dokument synonym verwendet. Zum Mindestumfang des Liefer-AVIS, siehe Kapitel 7.1.

Ausweisdokument:

Unter Ausweisdokument wird ein gültiger Lichtbildausweis, der zum Identitätsnachweis herangezogen wird, verstanden. Als zulässige Ausweisdokumente für die Identitätsfeststellung im Rahmen der sicheren Lieferkette können Personalausweis (bzw. ein entsprechender gültiger Identitätsnachweis eines EU-Landes), Reisepass oder Aufenthaltstitel verwendet werden.

Gerätesiegel und Siegelband

Als Gerätesiegel werden die Sicherheitssiegel bezeichnet, die direkt auf dem Gehäuse des Konnektors angebracht sind. Diese Siegel sind speziell auf die Materialeigenschaften des Gehäuses angepasst. Insbesondere ist die Klebekraft der Siegel auf den Untergrund zugeschnitten, so dass die Siegel mit hoher Wahrscheinlichkeit nicht rückstandslos und zerstörungsfrei entfernt werden können. Gerätesiegel sind zudem mit einer eindeutigen Seriennummer gegen Austausch geschützt. Abbildung 2 zeigt ein Beispiel für ein Gerätesiegel. Die Merkmale der Sicherheitssiegel sowie Anweisungen zu deren Prüfung sind der Bedienungsanleitung secunet Konnektor, Abschnitt „Manipulationsversuche erkennen“ zu entnehmen (siehe [1]).

Abbildung 2: Beispiel für Gerätesiegel

Der Siegelhersteller wurde von secunet ausgewählt, da er die oben genannten Anforderungen an die Herstellung von Gerätesiegeln erfüllt und sehr viel Erfahrung auf dem Gebiet der Herstellung von Sicherheitssiegeln hat.

Der Konnektor wird in einer Transportverpackung geliefert. Die Transportverpackung ist mit einem Siegelband gesichert, das speziell für den Untergrund der Transportverpackung geeignet ist. Das Siegelband kann mit hoher Wahrscheinlichkeit nicht rückstandslos und zerstörungsfrei von der Trans-

portverpackung entfernt werden. Die Siegelbänder werden ebenfalls vom oben genannten Hersteller der Gerätesiegel hergestellt. Abbildung 3 zeigt das Siegelband der Transportverpackung intakt und teilweise geöffnet. Die Merkmale des Siegelbandes sowie Anweisungen zu dessen Prüfung sind der Bedienungsanleitung secunet Konnektor, Abschnitt „Transportverpackung prüfen“ zu entnehmen (siehe [1]).

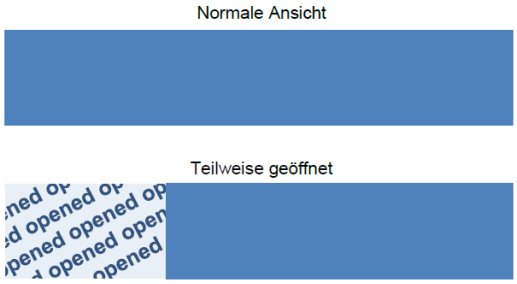

Abbildung 3: Siegelband der Transportverpackung.

Plomben:

Plomben werden verwendet, um Transportfahrzeuge (Laderaum) oder Transportboxen gegen unbemerktes öffnen zu schützen. Es dürfen nur Plomben verwendet werden, die eine eindeutige Seriennummer haben und damit gegen Austausch der Plombe geschützt sind.

Für die Absicherung der Konnektoren (Laderaum oder Transportboxen) dürfen nur Sicherheitsplomben verwendet werden, die

- Eine eindeutige und irreversible Nummerierung aufweisen, z.B. Prägung oder permanente Laserbeschriftung.
- Aus bruchfestem Material bestehen, so dass die Plomben nur mit Werkzeugen (z.B. Bolzenschneider) durch Zerstörung der Plombe entsiegelt werden können.
- Die Plomben mit einer bestimmten Seriennummer nicht einfach zu beschaffen sind (z.B. individualisierte Plomben oder Bestellung sehr hoher Stückzahlen notwendig)

Dazu können zum Beispiel Metallbandplomben mit Kugelkopf, Kabelplomben mit bruchfestem Kunststoffkörper oder Stahlseilplomben verwendet werden.

Bei Plomben für Transportboxen gilt: Die Transportboxen dürfen nicht von außen zugänglich sein. Der entsprechende Fahrzeugbereich muss immer außerhalb der Lade- und Entladezeiten verschlossen sein. Zudem dürfen nicht mehr als 10 Konnektoren pro Transportbox ausgeliefert werden.

Neben der Sicherung von Transportboxen können Plomben auch zur Sicherung der Transportfahrzeuge (Laderaum) verwendet werden. Da im Laderaum der Transportfahrzeuge wesentlich größere Stückzahlen transportiert werden können als in einer einzelnen Transportbox und da die Laderaum-

Plombe sich nicht im abgeschlossenen Fahrzeug selbst befindet, sondern an einem von außen zugänglichen Bereich des Fahrzeuges angebracht wird, dürfen für die Absicherung des Laderaums der Transportfahrzeuge nur Plomben verwendet werden, die nach ISO 17712:2013 zertifiziert sind.

Sichere Versandtasche:

Sichere Versandtaschen werden verwendet, um Konnektoren bei Einzelversand zusätzlich vor unbemerkte Manipulationen zu schützen. Es dürfen nur sichere Versandtaschen verwendet werden, die eine eindeutige Seriennummer haben und damit gegen Austausch der Versandtasche geschützt sind. Die Versandtasche muss einen reißfesten Taschenkörper und manipulationssichere Siegelverschlüsse mit Manipulationsanzeige bei Öffnungsversuchen besitzen. Zudem müssen sicherheitsrelevante Aufdrucke wir Seriennummer vor Fälschung geschützt sein (z.B. durch Sicherheitsdruck unter dem Siegelverschluss). Unbemerktes Öffnen an den Seiten muss durch geeignete Schweißnähte verhindert werden.

4 Lager

Im Folgenden werden die Anforderungen an die Lagerarten Kleinlager, mittleres Lager und Großlager beschrieben.

Um ein gleiches Sicherheitsniveau in jeder Ausprägung der Lagerhaltung zum Schutz der Integrität eines jeden Konnektors zu wahren, wird ein Verhältnis von organisatorischen und physikalischen Maßnahmen gewählt, das entsprechend der Menge der gelagerten Konnektoren angepasst ist. Dies bedeutet für kleinere Mengen die Umsetzung von mehr organisatorischen Maßnahmen da z. B. der Zugriff und die Inventur eingeschränkt sind. Bei größeren Mengen kommen mehr physikalische Maßnahmen zum Einsatz, um den Zugriff und die Inventur zur unterstützen und das Schutzziel zu erreichen. Welche Maßnahmen im Detail gefordert sind, werden im Kapitel 4 erläutert. In Kapitel 4.4 werden diese für alle Lagerarten gegenübergestellt und begründet, warum ein gleichbleibendes Sicherheitsniveau für alle Lagerarten gegeben ist.

4.1 Kleinlager (bis zu 10 Geräte)

Im Folgenden werden die Anforderungen an den Zugriffsschutz der Konnektoren für ein Kleinlager beschrieben. In einem Kleinlager dürfen maximal 10 Geräte gelagert werden. Entsprechend der Lagergröße wird von einer geringen Anzahl von zugriffsberechtigten Mitarbeitern im Vergleich zu größeren Lagerarten (mittleres Lager, Großlager) ausgegangen. Es dürfen maximal 3 Mitarbeiter Zugriff auf die Konnektoren haben.

4.1.1 Technische Maßnahmen

Die Geräte müssen in einem gesicherten Lagerraum gelagert werden. Für den Lagerraum gelten die nachfolgenden Anforderungen:

- Abgeschlossener Raum (Schlüssel nur im Besitz berechtigter Mitarbeiter)
- Blickdichte Lagerung (z. B. blickdichte Verglasung oder ohne Fenster)
- Eingeschränkter Zutritt (z. B. nur berechtigte Mitarbeiter); Eine entsprechende Liste berechtigter Mitarbeiter ist zu führen.
- Bauliche Sicherungsmaßnahmen des Lagerraums, die bei einem Einbruchsversuch zu erkennbaren Einbruchsspuren führen. Ein Einbruchsversuch darf nicht beim nächsten Betreten des Lagers unbemerkt bleiben.
    - Wände: Der Lagerraum muss aus massiven Wänden bestehen, die nur mit großem Aufwand (z. B. Einsatz eines Stemmhammers, etc.) überwunden werden können und bei denen davon ausgegangen werden kann, dass sich die Spuren des Einbruches nicht über Nacht vertuschen lassen (z.B. neue Wände einziehen).
    - Fenster: Die Fenster müssen gegen unbemerktes öffnen gesichert sein (z. B. Pilzkopfzapfen-Beschläge, abschließbare Fenstergriffe, nachträgliche angebrachte Aufschraubsicherungen, etc.). Jeder erfolgreiche Einbruch muss zu erkennbaren Spuren führen (Glasbruch, starke Beschädigungen der Fensterrahmen durch Hebelkräfte, etc.).

- Türen: Die Türen müssen gegen unbemerktes öffnen gesichert sein (z.B. Pilzkopfzapfen-Beschläge, Sicherheitsschloss mit Zertifikat oder zugehöriger Sicherheitskarte). Jeder erfolgreiche Einbruch muss zu erkennbaren Spuren führen (starke Beschädigungen der Tür oder am Schloss, etc.).

4.1.2 Organisatorische Maßnahmen

- Es dürfen nicht mehr als 3 Mitarbeiter Zugriff auf die Konnektoren haben. Nur diese dürfen im Besitz eines Schlüssels für den Lagerraum sein oder Zugang zu einem Schlüssel haben. Schlüssel die nicht im Besitz eines Mitarbeiters sind müssen sicher verwahrt werden (z. B. Schlüsseltresor). Für jeden Schlüssel muss jederzeit Nachvollziehbar sein, in wessen Besitz sich dieser befindet.
- Im Lager / beim Servicetechniker (DVO) werden maximal 10 Geräte gelagert.
- Der Lagerraum ist immer zu verschließen (Fenster und Türen).
- Beim Zugriff auf den Lagerraum wird ein Eingangsprotokoll geführt.
- Es ist eine Bestandsliste für alle Geräte zu führen (siehe Kapitel 7.3). Der Bestand der Geräte wird regelmäßig anhand der Bestandsliste kontrolliert. Die Überprüfung muss mindestens alle 3 Monate durchgeführt werden.
- Der Lagerraum ist bei Dienstbeginn und bei jedem Betreten des Lagers auf Einbruchspuren zu untersuchen. Die Überprüfung muss mindestens alle 24 Stunden durchgeführt werden. Ggf. ist dazu eine Vertreterregelung einzuführen.
- Die Mitarbeiter müssen regelmäßig und mindestens einmal im Jahr hinsichtlich der in diesem Dokument definierten Sicherheitsanforderungen an Lagerung und Umschlag von Konnektoren geschult werden.

4.1.3 Empfang und Versand

<u>Versandinformationen:</u>

- Die Versandinformationen müssen dem Empfänger vor der Auslieferung der Geräte übersendet werden (siehe Kapitel 7.1 bzw. 7.2). Insbesondere dürfen die Versandinformationen nicht mit der Lieferung der Geräte an den Empfänger übermittelt werden.

<u>Lieferzeitpunkt:</u>

- Wird eine Lieferung von Geräten nicht innerhalb von 12 Stunden nach dem angekündigten Liefertermin geliefert, muss der Versender kontaktiert werden. Die Lieferzeit darf maximal 3-mal vom Versender benannten Fahrer entgegen der angekündigten Lieferzeitankündigung und insgesamt um max. 12 Stunden verschoben werden. Ansonsten muss direkt mit dem Versender ein neuer separater Liefertermin abgestimmt werden. Außerhalb des angegeben Lieferzeitraumes dürfen keine Geräte vom Empfänger angenommen und vom Fahrer ausgeliefert werden. Die Geräte verbleiben im Bestand des Fahrers.

<u>Identifikation:</u>

- Identifikation beim Empfang / Versand von Geräten

- Empfangsberechtigter (Lager) identifiziert Fahrer anhand der elektronischen Versandinformation (Name, Vorname) mit dem Ausweisdokument des Fahrers.
- Fahrer identifiziert den Empfangsberechtigten anhand der in den Versandinformationen hinterlegten Daten (Name, Vorname) mit dem Ausweisdokument des Empfangsberechtigten.
- Kann die Identität nicht bestätigt werden
  - Darf die Ware nicht angenommen bzw. ausgeliefert werden
  - Fahrer kann nicht bestätigt werden; Annahme wird vom Empfangsberechtigten verweigert
  - Empfangsberechtigter kann nicht bestätigt werden; Geräte verbleiben im Bestand des Fahrers

Annahme und Prüfung:

- Der oder die Empfangsberechtigten (Lager) überprüfen im Beisein des Fahrers die Vollständigkeit und Unversehrtheit der Gerätekartons (keine Öffnungsspuren, keine Beschädigungen des Siegelbandes) und vergleicht die Seriennummern der gelieferten Geräte (auf dem Gerätekarton) mit den Versandinformationen.
- Ist eine Lieferung unvollständig bzw. bestehen Abweichungen zur Versandankündigung (z. B. fehlerhafte Angaben wie abweichende Seriennummern, etc.) oder sind Manipulationsspuren an den Gerätekartons erkennbar, gilt der Verdacht auf Integritätsverletzung und der Versender muss unverzüglich darüber informiert werden. Die Lieferung darf in diesen Fällen nicht angenommen werden. Es sind die Schritte aus Kapitel 4.1.4 durchzuführen.
- Nach Erhalt und Überprüfung der Geräte werden diese unmittelbar im vorgesehenen Lagerbereich eingelagert. Der Empfangsberechtigte muss die Anforderungen an die Lagerung entsprechend der Lagergröße einhalten.

Verfügbarkeit von Informationen:

- Der Versender muss die Kontaktdaten des Empfängers für jeden Konnektor nachhalten und anhand von Seriennummer und MAC Adressen zuordnen können. Auf Anfrage muss der Versender die Kontaktdaten eines Empfängers an den Leistungserbringer bei Nennung von Seriennummer und MAC-Adressen ausgeben (Prüfung der sicheren Lieferkette).
- Diese Informationen müssen auch nach Beendigung des Vertriebes von Konnektoren nachgehalten und für mindestens 5 Jahre verfügbar gemacht werden können. Alle Teilnehmer der sicheren Lieferkette, die an diesen Versender Konnektoren geliefert haben, müssen über entsprechende Nachfolgeregeln informiert werden. Dabei ist z.B. zu regeln, unter welchen Kontaktdaten die Informationen in Zukunft abgefragt werden können, falls sich diese ändern.
- Alle Seriennummern und MAC Adressen der nach Geschäftsaufgabe noch im Bestand befindlichen Geräte müssen an den Hersteller übermittelt werden (konnektorlieferung@secunet.com). Dieser veranlasst die unverzügliche Sperrung der Zertifikate für diese Geräte, die nicht mehr als Teil der sicheren Lieferkette betrachtet werden können.

Zudem sind die für den Empfänger relevanten Punkte aus den Kapiteln 5.1.2, 5.2.2, 5.3.2 oder 5.4.2 zu beachten.

Schlägt eine der oben genannten Prüfungen fehl, gilt der Verdacht auf Integritätsverletzung.

4.1.4 Maßnahmen bei Verdacht auf Integritätsverletzung

Kann eine Manipulation oder ein Austausch von gelagerten Geräten nicht ausgeschlossen werden so gilt der Verdacht auf Integritätsverletzung. Auch bei Verlust von Geräten (Diebstahl) kann eine Integritätsverletzung der verbliebenen Geräte nicht mehr ausgeschlossen werden. Ein Verdacht auf Integritätsverletzung kann für eine einzelne Lieferung (Prüfung bei der Annahme) oder für den Lagerbestand (Prüfung auf Einbruchsspuren) gelten.

Im Folgenden werden die Maßnahmen beschrieben, die bei einem Verdacht auf Integritätsverletzung von Konnektoren durchzuführen sind. Ein Verdacht auf Integritätsverletzung kann durch reguläre Prüfungen (wie z.B. im Kapitel „Empfang und Versand“ beschrieben) oder durch anlassbezogene Prüfungen (z.B. Verdacht auf Einbruch) entstehen. Bei Verdacht auf Integritätsverletzung ist zunächst die Ursache für den Verdacht zu prüfen. Kann ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden sind die folgenden Maßnahmen umzusetzen:

- Sofortige Prüfung der Lieferung/des Lagerbestandes nach Anzahl und Seriennummern (Vergleich mit Versandinformationen bzw. Bestandsliste.)
- Die Seriennummern aller Geräte der Lieferung/des Bestandes, inklusiver ggf. fehlender Geräte, müssen unverzüglich dem Hersteller mittgeteilt werden. Dazu ist der Hersteller unverzüglich über die E-Mail Adresse konnektorlieferung@secunet.com zu informieren.
    - Bei einem Verdacht auf Integritätsverletzung bei Konnektor Lieferungen ist der Versender verantwortlich den Hersteller zu informieren.
    - Bei einem Verdacht auf Integritätsverletzung bei im Lagerbestand befindlichen Geräten ist der Lagerbetreiber verantwortlich den Hersteller zu informieren.

  Die E-Mail muss authentisch und integritätsgeschützt übertragen werden. Der Hersteller muss den Eingang der Sperrinformationen auf sicheren Weg bestätigen. Siehe Kapitel 7.5 zum sicheren Austausch der Informationen.
  Der Hersteller veranlasst anhand der Seriennummer die unverzügliche Sperrung der Konnektor-Zertifikate.
- Bei Verdacht auf Integritätsverletzung einer Lieferung müssen alle Geräte vom Versender direkt an den Hersteller zurückgeschickt werden.
  Bei Verdacht auf Integritätsverletzung des Lagerbestandes müssen alle Geräte im Lagerbestand vom Lagerbetreiber direkt an den Hersteller zurückgeschickt werden.

4.2 Mittleres Lager (bis zu 100 Geräte)

Im Folgenden werden die Anforderungen an den Zugriffsschutz der Konnektoren für ein mittleres Lager beschrieben. In einem mittleren Lager dürfen maximal 100 Geräte gelagert werden. Entsprechend der Lagergröße wird von einer größeren Anzahl von zugriffsberechtigten Mitarbeitern im Vergleich zum Kleinlager ausgegangen. Dennoch muss sich die Anzahl der Zugriffsberechtigten Personen soweit in Grenzen halten, das Schlüsselmanagement und organisatorische Maßnahmen zum Zugriffsschutz noch realistisch umsetzbar sind. Es dürfen maximal 10 Mitarbeiter Zugriff auf die Konnektoren haben.

4.2.1 Technische Maßnahmen

Die Geräte müssen in einem gesicherten Lagerraum gelagert werden. Für den Lagerraum gelten die nachfolgenden Anforderungen:

- Abgeschlossener Raum (Schlüssel nur im Besitz berechtigter Mitarbeiter oder in einem Schlüsseltresor); Eine entsprechende Liste berechtigter Mitarbeiter ist zu führen.
- Blickdichte Lagerung (z. B. blickdichte Verglasung oder ohne Fenster)
- Eingeschränkter Zutritt (z. B. nur berechtigte Mitarbeiter)
- Alarmanlage (Einbruchsalarm) mit baulichen Sicherungsmaßnahmen, die ein Eindringen ohne auslösen des Alarms verhindern.
    - Wände: Das durchdringen der Wände muss zu einem Alarm führen (z. B. Abdeckung durch Bewegungsmelder, Alarmtapete, etc.)
    - Fenster: Der Zugang durch Fenster muss zu einem Alarm führen (z. B. Abdeckung durch Bewegungsmelder, Glasbruchdetektoren, etc.).
    - Türen: Die Türen müssen gegen unbemerktes öffnen gesichert sein (z. B. Pilzkopfzapfen-Beschläge, Sicherheitsschloss mit Zertifikat oder zugehöriger Sicherheitskarte). Jeder erfolgreiche Einbruch muss zu einem Alarm führen (z. B. Abdeckung durch Bewegungsmelder, Anbindung der Tür ans Alarmsystem, etc.).
- Oder Videoüberwachung mit baulichen Sicherungsmaßnahmen die Zugriff auf die Konnektoren ohne Aufzeichnung durch die Kamera verhindern.
- Die Videoüberwachung muss jeden Zugriff auf die Konnektoren lückenlos überwachen. Die Aufnahmen müssen Integritätsgeschützt gesichert werden. Es darf nicht möglich sein Aufnahmen zu manipulieren oder zu entfernen, ohne dass dies bei Überprüfung der Aufzeichnungen festgestellt werden kann (z. B. sichere Speicherung). Die Aufnahmen müssen mindesten bis zur nächsten Überprüfung gespeichert werden.

4.2.2 Organisatorische Maßnahmen

- Es dürfen nicht mehr als 10 Mitarbeiter Zugriff auf die Konnektoren haben. Nur diese dürfen im Besitz eines Schlüssels für den Lagerraum sein oder Zugang zu einem Schlüssel haben. Schlüssel, die nicht im Besitz eines Mitarbeiters sind, müssen sicher verwahrt werden (z. B. Schlüsseltresor). Für jeden Schlüssel muss jederzeit Nachvollziehbar sein, in wessen Besitz sich dieser befindet. Es müssen definierte Verfahrensanweisungen zur Ausgabe und Rücknahme von Schlüsseln umgesetzt werden und solche Prozesse protokolliert werden.
- Im Lager werden maximal 100 Geräte gelagert.
- Der Lagerraum ist immer zu verschließen (Fenster und Türen).
- Beim Zugriff auf den Lagerraum wird ein Eingangsprotokoll geführt
- Es ist eine Bestandsliste für alle Geräte zu führen (siehe Kapitel 7.3). Der Bestand der Geräte wird regelmäßig anhand der Bestandsliste kontrolliert. Die Überprüfung muss mindestens alle 3 Monate durchgeführt werden.
- Regelmäßige Überprüfung der Videoüberwachung / Alarmanlage. Die Alarmanlage ist bei jedem Dienstbeginn auf Meldungen zu prüfen. Wird keine Alarmanlage verwendet, müssen die

Videoaufnahmen des Lagerraums mindestens bei jedem Dienstbeginn geprüft werden. Die Überprüfung muss mindestens alle 24 Stunden durchgeführt werden. Ggf. ist dazu eine Vertreterregelung einzuführen.
- Die Mitarbeiter müssen regelmäßig und mindestens einmal im Jahr hinsichtlich der in diesem Dokument definierten Sicherheitsanforderungen an Lagerung und Umschlag von Konnektoren geschult werden.

4.2.3 Empfang und Versand

Versandinformationen:

- Die Versandinformationen müssen dem Empfänger vor der Auslieferung der Geräte übersendet werden (siehe Kapitel 7.1 bzw. 7.2). Insbesondere dürfen die Versandinformationen nicht mit der Lieferung der Geräte an den Empfänger übermittelt werden.

Lieferzeitpunkt:

- Wird eine Lieferung von Geräten nicht innerhalb von 12 Stunden nach dem angekündigten Liefertermin geliefert, muss der Versender kontaktiert werden. Die Lieferzeit darf maximal 3-mal vom Versender benannten Fahrer entgegen der angekündigten Lieferzeitankündigung und insgesamt um max. 12 Stunden verschoben werden. Ansonsten muss direkt mit dem Versender ein neuer separater Liefertermin abgestimmt werden. Außerhalb des angegeben Lieferzeitraumes dürfen keine Geräte vom Empfänger angenommen und vom Fahrer ausgeliefert werden. Die Geräte verbleiben im Bestand des Fahrers.

Identifikation:

- Identifikation beim Empfang / Versand von Geräten
    - Empfangsberechtigter (Lager) identifiziert Fahrer anhand der elektronischen Versandinformationen (Name, Vorname) mit dem Ausweisdokument des Fahrers.
    - Fahrer identifiziert den Empfangsberechtigten anhand der in den Versandinformationen hinterlegten Daten (Name, Vorname) mit dem Ausweisdokument des Empfangsberechtigten.
    - Identität kann nicht bestätigt werden
        - Fahrer kann nicht bestätigt werden; Annahme wird vom Empfangsberechtigten verweigert
        - Empfangsberechtigter kann nicht bestätigt werden; Geräte verbleiben im Bestand des Fahrers

Annahme und Prüfung:

- Der oder die Empfangsberechtigten (Lager) überprüfen im Beisein des Fahrers die Vollständigkeit und Unversehrtheit der Gerätekartons (keine Öffnungsspuren, keine Beschädigungen des Siegelbandes) und vergleicht die Seriennummern der gelieferten Geräte (auf dem Gerätekarton) mit den Versandinformationen.

- Ist eine Lieferung unvollständig bzw. bestehen Abweichungen zur Versandankündigung (z. B. fehlerhafte Angaben wie abweichende Seriennummern, etc.) oder sind Manipulationsspuren an den Gerätekartons erkennbar, gilt der Verdacht auf Integritätsverletzung und der Versender muss unverzüglich darüber informiert werden. Die Lieferung darf in diesen Fällen nicht angenommen werden. Es sind die Schritte aus Kapitel 4.2.4 durchzuführen.
- Nach Erhalt und Überprüfung der Geräte werden diese unmittelbar im vorgesehenen Lagerbereich eingelagert. Der Empfangsberechtigte muss die Anforderungen an der Lagerung entsprechend der Lagergröße einhalten (siehe Kap. 4.1, 4.2 oder 4.3).

Verfügbarkeit von Informationen:

- Der Versender muss die Kontaktdaten des Empfängers für jeden Konnektor nachhalten und anhand von Seriennummer und MAC Adressen zuordnen können. Auf Anfrage muss der Versender die Kontaktdaten an den Leistungserbringer bei Nennung von Seriennummer und MAC-Adressen ausgeben (Prüfung der sicheren Lieferkette).
- Diese Informationen müssen auch nach Beendigung des Vertriebes von Konnektoren nachgehalten und für mindestens 5 Jahre verfügbar gemacht werden können. Alle Teilnehmer der sicheren Lieferkette, die an diesen Versender Konnektoren geliefert haben, müssen über entsprechende Nachfolgeregeln informiert werden. Dabei ist z.B. zu regeln, unter welchen Kontaktdaten die Informationen in Zukunft abgefragt werden können, falls sich diese ändern.
- Alle Seriennummern und MAC Adressen der nach Geschäftsaufgabe noch im Bestand befindlichen Geräte müssen an den Hersteller übermittelt werden (konnektorlieferung@secunet.com). Dieser veranlasst die unverzügliche Sperrung der Zertifikate für diese Geräte, die nicht mehr als Teil der sicheren Lieferkette betrachtet werden können.

Zudem sind die für den Empfänger relevanten Punkte aus den Kapiteln 5.1.2, 5.2.2, 5.3.2 oder 5.4.2 zu beachten.

Schlägt eine der oben genannten Prüfungen fehl, gilt der Verdacht auf Integritätsverletzung.

4.2.4 Maßnahmen bei Verdacht auf Integritätsverletzung

Kann eine Manipulation oder ein Austausch von gelagerten Geräten nicht ausgeschlossen werden so gilt der Verdacht auf Integritätsverletzung. Auch bei Verlust von Geräten (Diebstahl) kann eine Integritätsverletzung der verbliebenen Geräte nicht mehr ausgeschlossen werden. Ein Verdacht auf Integritätsverletzung kann für eine einzelne Lieferung (Prüfung bei der Annahme) oder für den Lagerbestand (Prüfung auf Einbruchsspuren) gelten. Im Einbruchfall gilt:

- Eine sofortige Überprüfung der Videoaufnahmen (z. B. Wo wurde sich aufgehalten) oder Alarmmeldungen (z. B. wo wurde detektiert) ist durchzuführen. Kann ein bestehender Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden müssen die im Folgenden beschriebenen Maßnahmen ergriffen werden. Das gilt auch bei Zweifel an der Authentizität oder Integrität der Videoaufnahmen oder der Alarmanlage.

Im Folgenden werden die Maßnahmen beschrieben, die bei einem Verdacht auf Integritätsverletzung von Konnektoren durchzuführen sind. Ein Verdacht auf Integritätsverletzung kann durch reguläre

Prüfungen (wie z.B. im Kapitel „Empfang und Versand“ beschrieben) oder durch anlassbezogene prüfungen (z.B. Verdacht auf Einbruch) entstehen. Bei Verdacht auf Integritätsverletzung ist zunächst die Ursache für den Verdacht zu Prüfen. Kann ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden sind die folgenden Maßnahmen umzusetzen:

- Sofortige Prüfung der Lieferung/des Lagerbestandes nach Anzahl und Seriennummern (Vergleich mit Versandinformationen bzw. Bestandsliste)
- Die Seriennummern aller Geräte der Lieferung/des Bestandes, inklusiver ggf. fehlender Geräte, müssen unverzüglich dem Hersteller mittgeteilt werden. Dazu ist der Hersteller unverzüglich über die E-Mail Adresse konnektorlieferung@secunet.com zu informieren.
    - Bei einem Verdacht auf Integritätsverletzung bei Konnektor Lieferungen ist der Versender verantwortlich den Hersteller zu informieren.
    - Bei einem Verdacht auf Integritätsverletzung bei im Lagerbestand befindlichen Geräten ist der Lagerbetreiber verantwortlich den Hersteller zu informieren.

  Die E-Mail muss authentisch und integritätsgeschützt übertragen werden. Der Hersteller muss den Eingang der Sperrinformationen auf sicheren Weg bestätigen. Siehe Kapitel 7.5 zum sicheren Austausch der Informationen.
  Der Hersteller veranlasst anhand der Seriennummer die unverzügliche Sperrung der Konnektor-Zertifikate.
- Bei Verdacht auf Integritätsverletzung einer Lieferung müssen alle Geräte vom Versender direkt an den Hersteller zurückgeschickt werden.
  Bei Verdacht auf Integritätsverletzung des Lagerbestandes müssen alle Geräte im Lagerbestand vom Lagerbetreiber direkt an den Hersteller zurückgeschickt werden.

4.3 Großlager (ab 101 Geräte)

Im Folgenden werden die Anforderungen an den Zugriffsschutz der Konnektoren für ein Großlager beschrieben. In einem Großlager dürfen mehr als 100 Geräte gelagert werden. Entsprechend der Lagergröße wird von einer hohen Anzahl von zugriffsberechtigten Mitarbeitern im Vergleich zu den anderen Lagerarten (Kleinlager, mittleres Lager) ausgegangen. Durch die hohe Anzahl der Mitarbeiter wird ein elektronisches Zugangskontrollsystem zur Umsetzung von Zugriffsrechten gefordert.

4.3.1 Technische Maßnahmen

Die Geräte müssen in einem gesicherten Lagerraum gelagert werden. Für den Lagerraum gelten die nachfolgenden Anforderungen:

- Elektronisches Zugangskontrollsystem (Zutrittskontrollanlage, ZKA) mit eingeschränkten Zutrittsrechten (Zugangskarten nur im Besitz berechtigter Mitarbeiter) mit Protokollierung.
    - Die Einzelkomponenten des Zugangskontrollsystems müssen mindestens der Anlagenklasse B nach VdS 2348 entsprechen oder ein vergleichbares Schutzniveau bieten. Insbesondere dürfen die Sicherheitskomponenten der ZKA nicht für unbefugte zugänglich sein und müssen vor Manipulation geschützt sein. Die Zugangskarten dürfen nicht fälschbar oder kopierbar sein.
    - Die Protokolle der ZKA müssen mindestens 6 Monate aufbewahrt werden.

- Alarmanlage (Einbruchsalarm) mit definierter Alarmkette und Aufschaltung auf Wachschutz. Der Wachschutz muss spätestens 30 Minuten nach Alarmierung vor Ort sein.
- Videoüberwachung der äußeren baulichen Anlagen
- Angemessene bauliche Sicherungsmaßnahmen des Großlagers, die sicherstellen, dass Zugang auf das Gelände durch die Videoüberwachung aufgezeichnet wird und bei unbefugtem Zugriff auf die Konnektoren ein Alarm ausgelöst wird.
    - Wände: Das Durchdringen der Wände muss zu einem Alarm führen (z. B. Abdeckung durch Bewegungsmelder, Alarmtapete, etc.).
    - Fenster: Der Zugang durch Fenster muss zu einem Alarm führen (z. B. Abdeckung durch Bewegungsmelder, Glasbruchdetektoren, etc.).
    - Türen: Die Türen müssen bei unbefugtem Öffnen zu einem Alarm führen (z. B. Abdeckung durch Bewegungsmelder, Anbindung der Tür ans Alarmsystem, etc.).
    - Die Videoüberwachung muss jeden Zutritt auf das Gelände, der Zugang zu den Konnektoren ermöglichen kann, lückenlos überwachen. Die Aufnahmen müssen integritätsgeschützt gesichert werden. Es darf nicht möglich sein, Aufnahmen zu manipulieren oder zu entfernen, ohne dass dies bei Überprüfung der Aufzeichnungen festgestellt werden kann (z. B. sichere Speicherung). Die Aufnahmen müssen mindesten bis zur nächsten Überprüfung gespeichert werden.
    - Elektronische Erfassung des Wareneingangs und -ausgangs (siehe Kapitel 7.3).
    - Äußerer Perimeterschutz: Das Lagergelände muss durch bauliche Maßnahmen (z.B. Mauer, Zaun) gegen Betreten durch Unbefugte geschützt sein.
- In einem Großlager werden neben den Konnektoren üblicherweise auch andere Güter gelagert. Die Konnektoren müssen in einem gesonderten Bereich gelagert werden.

4.3.2 Organisatorische Maßnahmen

- Im Lager können mehr als 100 Geräte gelagert werden.
- Es müssen definierte Verfahrensanweisungen zur Ausgabe und Rücknahme von Zugangskarten umgesetzt werden und solche Prozesse protokolliert werden.
- Den gesonderten Bereich für Konnektoren dürfen nur zutrittsberechtigte Personen betreten. Wenn keine diesbezüglichen Einschränkungen durch das elektronisches Zugangskontrollsystem umgesetzt sind, müssen die Zutrittsbeschränkungen organisatorisch geregelt werden. Das ist insbesondere in den regelmäßigen Schulungen zu berücksichtigen (siehe unten).
- Der Bestand der Geräte wird elektronisch festgehalten und regelmäßig anhand der Bestandsliste kontrolliert. Die Überprüfung muss mindestens alle 6 Monate durchgeführt werden.
- Regelmäßige Überprüfung der Videoüberwachung und der Alarmanlage. Die Alarmanlage und die Videoüberwachung sind bei jedem Dienstbeginn auf Meldungen zu prüfen. Die Überprüfung muss mindestens alle 24 Stunden durchgeführt werden. Ggf. ist dazu eine Vertreterregelung einzuführen.
- Die Mitarbeiter müssen regelmäßig und mindestens einmal im Jahr hinsichtlich der in diesem Dokument definierten Sicherheitsanforderungen an Lagerung und Umschlag von Konnektoren geschult werden.

4.3.3 Empfang und Versand

Versandinformationen:

- Die Versandinformationen müssen dem Empfänger vor der Auslieferung der Geräte übersendet werden (siehe Kapitel 7.1 bzw. 7.2). Insbesondere dürfen die Versandinformationen nicht mit der Lieferung der Geräte an den Empfänger übermittelt werden.

Lieferzeitpunkt:

- Wird eine Lieferung von Geräten nicht innerhalb von 12 Stunden nach dem angekündigten Liefertermin geliefert, muss der Versender kontaktiert werden. Die Lieferzeit darf maximal 3-mal vom Versender benannten Fahrer entgegen der angekündigten Lieferzeitankündigung und insgesamt um max. 12 Stunden verschoben werden. Ansonsten ist direkt mit dem Versender ein neuer separater Liefertermin abzustimmen. Außerhalb des angegeben Lieferzeitraumes dürfen keine Geräte vom Empfänger angenommen und vom Fahrer ausgeliefert werden. Die Geräte verbleiben im Bestand des Fahrers.

Identifikation:

- Identifikation beim Empfang / Versand von Geräten
    - Empfangsberechtigter (Lager) identifiziert Fahrer anhand der elektronischen Versandinformationen (Name, Vorname) mit dem Ausweisdokument des Fahrers.
    - Fahrer identifiziert den Empfangsberechtigten anhand der in den Versandinformationen hinterlegten Daten (Name, Vorname) mit dem Ausweisdokument des Empfangsberechtigten
    - Identität kann nicht bestätigt werden
        - Fahrer kann nicht bestätigt werden; Annahme wird vom Empfangsberechtigten verweigert
        - Empfangsberechtigter kann nicht bestätigt werden; Geräte verbleiben im Bestand des Fahrers

Annahme und Prüfung –Stufe 1:

- Der oder die Empfangsberechtigten (Lager) überwachen die ordnungsgemäße Verladung aus dem Transportfahrzeug (z. B. Prüfung der Plombe etc., siehe dazu Transportarten in Kapitel 5) und überprüft im Beisein des Fahrers die Unversehrtheit der Transportverpackung (keine Öffnungsspuren, keine Beschädigungen der Umverpackung) und vergleicht die Seriennummern der Versandinformationen mit den vom Fahrer mitgeführten Informationen (z.B. Liefer-AVIS des Fahrers). Unter Transportverpackung wird in diesem Fall die äußere sichtbare Umverpackung der Liefercharge verstanden (Transportfolie, sichtbare Gerätekartonseiten, etc.).

- Ist eine Lieferung unvollständig bzw. bestehen Abweichungen zur Versandankündigung (z. B. fehlerhafte Angaben wie abweichende Seriennummern, etc.) oder sind Manipulationsspuren an der Transportverpackung erkennbar, gilt der Verdacht auf Integritätsverletzung und der Versender muss unverzüglich darüber informiert werden. Die Lieferung darf in diesen Fällen nicht angenommen werden. Es sind die Schritte aus Kapitel 4.3.4 durchzuführen.
- Nach Erhalt der Geräte werden diese unmittelbar in einen geschützten Lagerbereich (Zugang nur für Berechtigte Mitarbeiter) für die weitere Überprüfung gebracht.

Annahme und Prüfung –Stufe 2:

- Die berechtigten Mitarbeiter vergleichen die Seriennummern der gelieferten Geräte (auf dem Gerätekarton) mit den Versandinformationen, prüfen die Unversehrtheit der Gerätekartons (Keine Öffnungsspuren, keine Beschädigungen des Siegelbandes)und melden den einwandfreien Erhalt oder etwaige Abweichungen zur angekündigten Bestellinformation zum frühestmöglichen Zeitpunkt (spätestens binnen 24 Stunden nach Erhalt der Anlieferung) dem Versender.
- Ist eine Lieferung unvollständig bzw. bestehen Abweichungen zur Versandankündigung (z. B. fehlerhafte Angaben wie abweichende Seriennummern, etc.) oder sind Manipulationsspuren an den Gerätekartons erkennbar, gilt der Verdacht auf Integritätsverletzung und der Versender muss unverzüglich vom Empfangsberechtigten darüber informiert werden. Es sind die Schritte aus Kapitel 4.3.4 durchzuführen. Die Eingangskontrolle und die Rückmeldung an den Versender haben binnen 24 Stunden ab Eingang der Lieferung zu erfolgen.
- Nach positiver Überprüfung der Geräte werden diese unmittelbar im vorgesehenen Lagerbereich eingelagert. Der Empfangsberechtigte muss die Anforderungen an die Lagerung entsprechend der Lagergröße einhalten. Werden Abweichungen bei der Prüfung festgestellt, dürfen die Geräte nicht in den Lagerbestand überführt werden.

Verfügbarkeit von Informationen:

- Der Versender muss die Kontaktdaten des Empfängers für jeden Konnektor nachhalten und anhand von Seriennummer und MAC Adressen zuordnen können. Auf Anfrage muss der Versender die Kontaktdaten an den Leistungserbringer bei Nennung von Seriennummer und ggf. MAC-Adressen ausgeben (Prüfung der sicheren Lieferkette).
- Diese Informationen müssen auch nach Beendigung des Vertriebes von Konnektoren für mindestens 5 Jahre nachgehalten und verfügbar gemacht werden können. Alle Teilnehmer der sicheren Lieferkette, die an diesen Versender Konnektoren geliefert haben, müssen über entsprechende Nachfolgeregeln informiert werden. Dabei z.B. zu regeln, unter welchen Kontaktdaten die Informationen in Zukunft abgefragt werden können, falls sich diese ändern.
- Alle Seriennummern und MAC Adressen der nach Geschäftsaufgabe noch im Bestand befindlichen Geräte müssen an den Hersteller übermittelt werden (konnektorlieferung@secunet.com). Dieser veranlasst die unverzügliche Sperrung der Zertifikate für diese Geräte, die nicht mehr als Teil der sicheren Lieferkette betrachtet werden können.

Zudem sind die für den Empfänger relevanten Punkte aus den Kapiteln 5.1.2, 5.2.2, 5.3.2 oder 5.4.2 zu beachten.

Schlägt eine der oben genannten Prüfungen fehl, gilt der Verdacht auf Integritätsverletzung.

4.3.4 Maßnahmen bei Verdacht auf Integritätsverletzung

Kann eine Manipulation oder ein Austausch von gelagerten Geräten nicht ausgeschlossen werden so gilt der Verdacht auf Integritätsverletzung. Auch bei Verlust von Geräten (Diebstahl) kann eine Integritätsverletzung der verbliebenen Geräte nicht mehr ausgeschlossen werden. Ein Verdacht auf Integritätsverletzung kann für eine einzelne Lieferung (Prüfung bei der Annahme) oder für den Lagerbestand (Prüfung auf Einbruchsspuren) gelten. Im Einbruchfall gilt:

- Eine Sofortige Überprüfung der Einträge der Zutrittskontrollanlage auf Unregelmäßigkeiten und eine sofortige Überprüfung der Videoaufnahmen (z. B. Wo wurde sich aufgehalten) und Alarmmeldungen (z. B. wo wurde detektiert) ist durchzuführen. Kann ein bestehender Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden müssen die im Folgenden beschriebenen Maßnahmen ergriffen werden. Das gilt auch bei Zweifel an der Authentizität oder Integrität der Videoaufnahmen oder der Alarmanlage.

Im Folgenden werden die Maßnahmen beschrieben, die bei einem Verdacht auf Integritätsverletzung von Konnektoren durchzuführen sind. Ein Verdacht auf Integritätsverletzung kann durch reguläre Prüfungen (wie z.B. im Kapitel „Empfang und Versand“ beschrieben) oder durch anlassbezogene Prüfungen (z.B. Verdacht auf Einbruch) entstehen. Bei Verdacht auf Integritätsverletzung ist zunächst die Ursache für den Verdacht zu prüfen. Kann ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden sind die folgenden Maßnahmen umzusetzen:

- Sofortige Prüfung der Lieferung/des Lagerbestandes nach Anzahl und Seriennummern (Vergleich mit Versandinformationen bzw. Bestandsliste)
- Die Seriennummern aller Geräte der Lieferung/des Bestandes, inklusiver ggf. fehlender Geräte, müssen unverzüglich dem Hersteller mittgeteilt werden. Dazu ist der Hersteller unverzüglich über die E-Mail Adresse konnektorlieferung@secunet.com zu informieren.
    - Bei einem Verdacht auf Integritätsverletzung bei Konnektor Lieferungen ist der Versender verantwortlich den Hersteller zu informieren.
    - Bei einem Verdacht auf Integritätsverletzung bei im Lagerbestand befindlichen Geräten ist der Lagerbetreiber verantwortlich den Hersteller zu informieren.

  Die E-Mail muss authentisch und integritätsgeschützt übertragen werden. Der Hersteller muss den Eingang der Sperrinformationen auf sicheren Weg bestätigen. Siehe Kapitel 7.5 zum sicheren Austausch der Informationen.
  Der Hersteller veranlasst anhand der Seriennummer die unverzügliche Sperrung der Konnektor-Zertifikate.
- Bei Verdacht auf Integritätsverletzung einer Lieferung müssen alle Geräte
    - im Falle der Annahme und Prüfung –Stufe 1 vom Versender direkt an den Hersteller zurückgeschickt werden.
    - im Falle der Annahme und Prüfung –Stufe 2 vom Empfänger direkt an den Hersteller zurückgeschickt werden.

Bei Verdacht auf Integritätsverletzung des Lagerbestandes müssen alle Geräte im Lagerbestand vom Lagerbetreiber direkt an den Hersteller zurückgeschickt werden.

4.4 Vergleich der Lagerarten

In einem Kleinlager werden nur wenige Konnektoren gelagert. Zudem kann davon ausgegangen werden, dass die Zahl der Mitarbeiter sehr beschränkt ist (z. B. nur ein Mitarbeiter). In einem Großlager dagegen können beliebig viele Konnektoren gelagert werden. Mit steigender Lagerkapazität steigt auch die Anzahl der Mitarbeiter des Lagers, insbesondere von Mitarbeitern, die Zugriff auf die Konnektoren haben. Organisatorische Maßnahmen, wie zum Beispiel das Abschließen des Lagerraums nach jeden Zutritt oder die manuelle Protokollierung des Bestandes, die für ein Kleinlager durchführbar sind, sind in einem Großlager gegebenenfalls nicht mehr sinnvoll umsetzbar. Zudem steigt die Möglichkeit, dass bei entsprechendem Durchsatz von Mitarbeitern nicht mehr sichergestellt werden kann, dass alle Mitarbeiter untereinander bekannt sind. Mit zunehmender Lagergröße sind daher organisatorische Maßnahmen durch technische oder physikalische Maßnahmen zu ersetzen. Dabei bleibt das Sicherheitsniveau für alle Lagerarten auf einem gleichbeliebenden Mindestlevel, um Angriffe auf die sichere Lieferkette abzuwehren oder zu erkennen.

In den folgenden Tabellen werden für die einzelnen Lagerarten die Maßnahmen gegenübergestellt. Dabei werden die Umsetzungen der Zutrittsbeschränkung, der Einbruchserkennung und des Lagerbestandes diskutiert. Nach jeder Tabelle wird begründet, warum ein gleichbleibendes Sicherheitsniveau für alle Lagerarten gegeben ist.

Zutrittsbeschränkung:

	Kleinlager	**Mittleres Lager**	**Großlager**
Zutrittsbeschränkung	Abgeschlossener Raum (Schlüssel nur im Besitz berechtigter Mitarbeiter oder in einem Schlüsseltresor)	Abgeschlossener Raum (Schlüssel nur im Besitz berechtigter Mitarbeiter oder in einem Schlüsseltresor)	Elektronisches Zugangskontrollsystem. Die Konnektoren müssen in einem gesonderten Bereich gelagert werden.
	Eingeschränkter Zutritt (z. B. nur berechtigte Mitarbeiter)	Eingeschränkter Zutritt (z. B. nur berechtigte Mitarbeiter)	Elektronisches Zugangskontrollsystem mit eingeschränkten Zutrittsrechten (Zugangskarten nur im Besitz berechtigter Mitarbeiter)
	Der Lagerraum ist immer zu verschließen (Fenster und Türen)	Der Lagerraum ist immer zu verschließen (Fenster und Türen)	Zugang zum Lager nur für Mitarbeiter mit Zugangskarte. Den gesonderten Bereich für Konnektoren dürfen nur Zutrittsberechtigte Personen betreten. Wenn keine diesbezüglichen Einschränkungen durch das elektronisches Zugangskontrollsystem umgesetzt sind müssen die Zutrittsbeschränkungen organisatorisch geregelt

			werden.
	Beim Zugriff auf den Lagerraum wird ein Eingangsprotokoll geführt	Beim Zugriff auf den Lagerraum wird ein Eingangsprotokoll geführt	Elektronisches Zugangskontrollsystem mit Protokollierung
	Es dürfen nicht mehr als 3 Mitarbeiter Zugriff auf die Konnektoren haben. Nur diese dürfen im Besitz eines Schlüssels für den Lagerraum sein oder Zugang zu einem Schlüssel haben. Schlüssel die nicht im Besitz eines Mitarbeiters sind, müssen sicher verwahrt werden (z. B. Schlüsseltresor). Für jeden Schlüssel muss jederzeit Nachvollziehbar sein, in wessen Besitz sich dieser befindet	Es dürfen nicht mehr als 10 Mitarbeiter Zugriff auf die Konnektoren haben. Nur diese dürfen im Besitz eines Schlüssels für den Lagerraum sein oder Zugang zu einem Schlüssel haben. Schlüssel die nicht im Besitz eines Mitarbeiters sind, müssen sicher verwahrt werden (z. B. Schlüsseltresor). Für jeden Schlüssel muss jederzeit Nachvollziehbar sein, in wessen Besitz sich dieser befindet.	Es gibt keine Einschränkung der Anzahl von Mitarbeitern, die Zugriff auf die Konnektoren haben.
	Keine Anforderungen an Schlüsselmanagement	Es müssen definierte Verfahrensanweisungen zur Ausgabe und Rücknahme von Schlüsseln umgesetzt werden und solche Prozesse protokolliert werden.	Es müssen definierte Verfahrensanweisungen zur Ausgabe und Rücknahme von Zugangskarten umgesetzt werden und solche Prozesse protokolliert werden.

Tabelle 1: Zutrittsbeschränkung der einzelnen Lagerarten

Für Kleinlager und mittlere Lager sind analoge Anforderungen an die Zutrittsbeschränkung gestellt. Diese beinhalten physikalische Anforderungen an den Lagerraum (z. B. abgeschlossener Raum) und organisatorische Anforderungen (der Lagerraum ist immer zu verschließen). Beim Großlager ist der gesamte Lagerbereich nur für Mitarbeiter mit Zugangskarten zugänglich. Die Konnektoren werden in einem gesonderten Bereich gelagert zu dem nur berechtigte Personen Zutritt haben. Das ist technisch durch das Zugangskontrollsystem oder organisatorisch umzusetzen.

Bei max. 3 berechtigten Mitarbeitern in einem Kleinlager ist das Schlüsselmanagement überschau ohne zusätzliche Maßnahmen durchsetzbar. Für ein mittleres Lager mit bis zu 10 berechtigten Mitarbeitern müssen Prozesse zur Ausgabe und Rücknahme von Schlüsseln umgesetzt werden, um das Schlüsselmanagement zu unterstützen. In einem Großlager kann nicht mehr davon ausgegangen werden, dass bei Verwendung von physischen Schlüsseln der Lagerraum nach jedem Zutritt verschlossen wird. Zudem ist ein geeignetes Schlüsselmanagement nicht mehr durchzusetzen. Um die Anforderung der Zutrittsbeschränkung in einem Großlager umzusetzen wird daher ein elektronisches Zugangskontrollsystem gefordert. Für Zugangskarten müssen ebenfalls Prozesse zur Ausgabe und Rücknahme umgesetzt werden.

In allen Lagerarten wird der Zutritt auf berechtigte Mitarbeiter beschränkt und protokolliert. Das geschieht bei Kleinlager und Mittleren Lager mittels Eingangsprotokoll. Für ein Großlager ist durch das elektronische Zugangskontrollsystem eine Protokollierung umzusetzen.

Einbruchserkennung:

	Kleinlager	Mittleres Lager	Großlager
Einbruchserkennung	Bauliche Sicherungsmaßnahmen des Lagerraums, die bei einem Einbruchsversuch zu erkennbaren Einbruchsspuren führen. Ein Einbruchsversuch darf zum Beispiel nicht beim nächsten Betreten des Lagers unbemerkt bleiben. (Siehe Anforderungen an Wände, Fenster und Türen in Kapitel 4.1.1.)	Alarmanlage (Einbruchsalarm) mit baulichen Sicherungsmaßnahmen, die ein Eindringen ohne auslösen des Alarms verhindern. (Siehe Anforderungen an Wände, Fenster und Türen in Kapitel 4.2.1.) oder Videoüberwachung mit baulichen Sicherungsmaßnahmen die Zugriff auf die Konnektoren ohne Aufzeichnung durch die Kamera verhindern. (Siehe Anforderungen Videoüberwachung in Kapitel 4.2.1.)	Angemessene bauliche Sicherungsmaßnahmen des Großlagers Alarmanlage (Einbruchsalarm) mit definierter Alarmkette und Aufschaltung auf Wachschutz Videoüberwachung der äußeren baulichen Anlagen, die sicherstellen, dass Zugang auf das Gelände durch die Videoüberwachung aufgezeichnet wird und bei unbefugtem Zugriff auf die Konnektoren ein Alarm ausgelöst wird. (Siehe Anforderungen an Wände, Fenster, Türen und Videoüberwachung in Kapitel 4.3.1.)
	Der Lagerraum ist mindesten bei jedem Betreten des Lagers auf Einbruchspuren zu untersuchen.	Regelmäßige Überprüfung der Videoüberwachung / Alarmanlage. Wird keine Alarmanlage verwendet, müssen die Videoaufnahmen des Lagerraums mindestens bei jedem Dienstbeginn geprüft werden.	Regelmäßige Überprüfung der Videoüberwachung und der Alarmanlage

Tabelle 2: Einbruchserkennung der einzelnen Lagerarten

In einem Kleinlager sind für Lageräume Anforderungen an die baulichen Sicherungsmaßnahmen (Wände, Fenster, Türen) gestellt, die es einem Einbrecher unmöglich machen, unbemerkt einzubrechen. Ein Einbruch muss zum Beispiel zu erkennbaren Spuren an der Lagerraumtür (Schloss aufgebrochen) oder möglichen Fenstern (Glasbruch) führen. Bei Zutritt ist der Lagerraum auf solche Spuren zu untersuchen. Mit zunehmender Lagergroße steigt auch die Gefahr, dass solche Spuren übersehen oder zu spät erkannt werden. Für mittlere Lager ist daher mindestens Videoüberwachung des Lagerraumes oder eine Alarmanlage zur Absicherung zu verwenden. Mit der Alarmanlage wird der Einbruchsversuch direkt erkannt. Die baulichen Maßnahmen müssen das Alarmsystem dahingehend unterstützen, das Zugang ohne Auslösen eines Alarmes ausgeschlossen ist. Bei Videoüberwachung müssen die Videoaufnahmen des Lagerraums regelmäßig und mindestens bei jedem Dienstbeginn geprüft werden. Für ein Großlager wird Videoüberwachung der Außenhaut und eine Alarmanlage gefordert. Bei einem Großlager kann von einer Größe ausgegangen werden, bei der Einbruchsspuren leichter übersehen werden oder auf der Videoüberwachung verdächtige Personen nicht mehr zuverlässig als solche erkannt werden (hohe Mitarbeiterzahl, Einbruch während der Betriebszeit). Daher werden zur Absicherung sowohl Alarmanlage als auch Videoüberwachung gefordert. Zudem wird auch eine entsprechende bauliche Sicherung des Großlagers gefordert, die es unmöglich macht, wäh-

rend oder außerhalb der Betriebszeiten unbemerkt Zutritt zu erlangen. In allen Fällen werden Einbruchsversuche spätestens bei Dienstbeginn festgestellt und es können weiter Schritte unternommen werden.

Lagerbestand:

	Kleinlager	mittleres Lager	Großlager
Lagerbestand	Beim Zugriff auf den Lagerraum wird ein Eingangsprotokoll geführt	Beim Zugriff auf den Lagerraum wird ein Eingangsprotokoll geführt	Elektronische Erfassung des Wareneingangs und -ausgangs (siehe Kapitel 7.3).
	Es ist eine Bestandsliste für alle Geräte zu führen (siehe Kapitel 7.3). Der Bestand der Geräte wird regelmäßig anhand der Bestandsliste kontrolliert	Es ist eine Bestandsliste für alle Geräte zu führen (siehe Kapitel 7.3). Der Bestand der Geräte wird regelmäßig anhand der Bestandsliste kontrolliert	Der Bestand der Geräte wird elektronisch festgehalten und regelmäßig anhand der Bestandsliste kontrolliert
	Die Überprüfung muss mindestens alle 3 Monate durchgeführt werden.	Die Überprüfung muss mindestens alle 3 Monate durchgeführt werden.	Die Überprüfung muss mindestens alle 6 Monate durchgeführt werden.

Tabelle 3: Lagerbestand der einzelnen Lagerarten

In einem Kleinlager und mittleren Lager wird jeder Zutritt protokolliert. Zudem werden Bestandslisten geführt, die regelmäßig und bei jedem Wareneingang und Warenausgang kontrolliert werden. Eine vollständige Überprüfung des Lagerbestandes muss mindesten alle 3 Monate durchgeführt werden, da bei einer größeren Anzahl von Geräten Abweichungen vom Soll-Bestand nicht mehr sofort auffallen. In einem Großlager ist diese Art der Lagerbestandserfassung nicht mehr sinnvoll umzusetzen, da sowohl Anzahl der berechtigten Mitarbeiter, als auch Anzahl der vertreibenden Konnektoren sehr groß sein kann. Der Zutritt zum Lager wird durch das elektronische Zugangskontrollsystem protokolliert. Zudem wird eine elektronische Erfassung des Wareneingangs und -ausgangs gefordert, die sicherstellt, dass sämtliche Lieferungen von Konnektoren erfasst werden. Durch die elektronisch gestützte Erfassung des Bestandes sind Abweichungen vom SOLL weitestgehend ausgeschlossen. Es wird daher nur alle 6 Monate eine vollständige Inventur gefordert. In allen Fällen ist sichergestellt, dass der Lagerbestand und der Wareneingang und -ausgang erfasst ist.

5 Transport

Im Folgenden werden die Anforderungen an die Transportarten Kleintransport, mittlerer Transport und Großtransport sowie Einzelversand beschrieben. Im Wesentlichen sind für alle Transportarten die gleichen Anforderungen und Maßnahmen definiert. Die einzelnen Transportarten können aber das geforderte Sicherheitsniveau aber unterschiedlich erreichen, z. B. durch Transport mit zwei Fahrern oder Absicherung durch eine Alarmanlage. In Kapitel 5.6 werden die unterschiedlichen Umsetzungen gegenübergestellt und begründet, warum ein gleichbleibendes Sicherheitsniveau gegeben ist.

5.1 Kleintransport (bis max. 10 Geräte)

Im Folgenden werden die Anforderungen an den Zugriffsschutz der Konnektoren beim Transport für einen Kleintransport beschrieben

5.1.1 Technische Maßnahmen

Die Geräte müssen in einem gesicherten Fahrzeug transportiert werden. Für Kleintransport gelten die nachfolgenden Anforderungen:

- Fester Aufbau
- Entweder zwei Fahrer oder
- Ein Fahrer (z. B. Transporteur oder Servicetechniker(DVO)) und
    - Alarmanlage oder
    - Verplombte (mit eindeutiger Seriennummer) Transportbox
- Blickdichte Lagerung im Fahrzeug (z. B. Decke oder blickdichte Verglasung oder ohne Fenster)

5.1.2 Organisatorische Maßnahmen

- Der Fahrer / Servicetechniker (DVO) transportiert nur so viele Geräte im mobilen Lager, wie er am Tag installieren kann, jedoch maximal 10. Die Geräte dürfen nicht über Nacht im Kleintransporter verbleiben, sondern müssen wieder in einem sicheren Lager eingelagert werden.
- Das Fahrzeug ist immer zu verschließen.
- Der Transport darf insgesamt (inkl. möglicher Verzögerungen) nicht länger als 24 Stunden dauern. Wenn dieser Zeitraum überschritten wird, verbleiben die Geräte im Bestand des Versenders und die Ursache für die Verzögerung ist zu prüfen. Besteht ein Verdacht auf Integritätsverletzung sind die Maßnahmen aus Kapitel 5.1.3 durchzuführen.
- Verzögerungen der Lieferung müssen dem Empfangsberechtigten unter Nennung der neuen Lieferzeit unverzüglich mitgeteilt werden.
- Bei Transportbox mit Plombe
    - Die Seriennummer der jeweils verwendeten Plombe muss vom Fahrer zwecks Überprüfung notiert werden.
    - Überprüfung der Seriennummer und Unversehrtheit der Transportbox und Plombe vor jedem Fahrtantritt
    - Werden für eine Teilauslieferung einzelne Konnektoren aus der Transportbox entnommen, muss danach die Transportbox wieder geschlossen und mit einer neuen Plombe gesichert werden. Die neue Seriennummer muss vom Fahrer zwecks Überprüfung notiert werden.
- Bei Transport mit zwei Fahrern
    - Es muss stets mindestens ein Fahrer in Gegenwart der Geräte sein (z. B. im Fahrzeug oder beim Empfangsberechtigten). Die Geräte dürfen niemals unbeaufsichtigt bleiben.
- Bei Fahrzeug mit Alarmanlage

    - Bei einem Alarmfall muss der Alarm vom Fahrer / DVO sofort bemerkt werden (z. B. akustisch, Smartphone-Nachricht)
- Versandinformationen mit den Seriennummern der Geräte muss stets vom Fahrer / DVO mitgeführt werden. Die Versandinformationen sind immer so beim Fahrer zu halten, dass kein unbemerkter Austausch oder eine Manipulation möglich sind.
- Identifikation
    - Fahrer / DVO identifiziert den Empfangsberechtigten anhand der in den Versandinformationen hinterlegten Daten (Name, Vorname) mit dem Ausweisdokument des Empfangsberechtigten
    - Empfangsberechtigter (Leistungserbringer) identifiziert den DVO anhand der Angaben in den Versandinformationen (Name, Vorname) mit dem Ausweisdokument des DVO.
    - Empfangsberechtigter (Lager) identifiziert Fahrer anhand der elektronischen Versandinformation (Name, Vorname) mit dem Ausweisdokument des Fahrers.
    - Kann die Identität nicht bestätigt werden
        - Darf die Ware nicht angenommen bzw. ausgeliefert werden
        - Empfangsberechtigter kann nicht bestätigt werden; Geräte verbleiben im Bestand des Fahrers / DVO.
        - Fahrer / DVO kann nicht bestätigt werden; Annahme wird vom Empfangsberechtigten verweigert.
- Empfangsberechtigter (Lager) überprüft im Beisein des Fahrers die Vollständigkeit und Unversehrtheit der Gerätekartons (keine Öffnungsspuren, keine Beschädigungen des Siegelbandes) und vergleicht die Seriennummern der gelieferten Geräte mit den Versandinformationen.
- Die Fahrer müssen hinsichtlich der in diesem Dokument definierten Sicherheitsanforderungen an Umschlag und Transport von Konnektoren eingewiesen werden.

Der Kleintransport wird zum Beispiel vom DVO verwendet, um die Konnektoren an den Leistungserbringer auszuliefern. Kann bei der Auslieferung die Identität des Empfangsberechtigten nicht vom DVO bestätigt werden oder umgekehrt die Identität des DVO nicht vom Empfangsberechtigten bestätigt werden, verbleibt der Konnektor im Bestand des DVOs. Dieser muss sich an den PVS-Anbieter wenden, der den Leistungserbringer und DVO bei der Nachverfolgung des Lieferschrittes unterstützt. Wenn der Grund für die Nicht-Bestätigung nicht zweifelsfrei geklärt werden kann, muss der PVS-Anbieter sich unter Angabe der Seriennummer des Konnektors an den Hersteller wenden (E-Mail Adresse konnektorlieferung@secunet.com). Der TOE wird bis zur endgültigen Klärung im sicheren Lager des DVO gelagert. Bleiben Zweifel an der Einhaltung der sicheren Lieferkette bestehen, muss der Konnektor unverzüglich gesperrt werden und vom DVO an den Hersteller zurück gesendet werden.

Schlägt eine der oben genannten Prüfungen fehl, gilt der Verdacht auf Integritätsverletzung.

5.1.3 Maßnahmen bei Verdacht auf Integritätsverletzung

Kann eine Manipulation oder ein Austausch von gelieferten Geräten nicht ausgeschlossen werden (Alarmfall oder Bruch/Austausch der Plombe) so gilt der Verdacht auf Integritätsverletzung. Auch bei Verlust von Geräten (Diebstahl) kann eine Integritätsverletzung der verbliebenen Geräte nicht mehr ausgeschlossen werden. Im Alarmfall gilt:

- Der Fahrer muss sofort zum Fahrzeug zurückkehren (Ankunft nach max. 10 Minuten) und die Ursache für den Alarm ermitteln. Kann ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden, müssen die im Folgenden beschriebenen Maßnahmen ergriffen werden. Das gilt in jedem Fall wenn die Ankunftszeit des Fahrers beim Fahrzeug nach Auslösen des Alarmes länger als 10 Minuten beträgt.
- Auch wenn nach Prüfung der Alarmursache der Verdacht auf Integritätsverletzung nicht mehr besteht, müssen mindestens alle Gerätekartons auf Unversehrtheit geprüft und der Gerätebestand gegen die Versandinformationen geprüft werden. Kann ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden, müssen die im Folgenden beschriebenen Maßnahmen ergriffen werden.

Im Folgenden werden die Maßnahmen beschrieben, die bei einem Verdacht auf Integritätsverletzung von Konnektoren durchzuführen sind. Ein Verdacht auf Integritätsverletzung kann durch reguläre Prüfungen (wie z.B. Prüfungen bei Fahrtantritt) oder durch anlassbezogene Prüfungen (z.B. Verdacht auf Einbruch im Fahrzeug) entstehen. Kann ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden, sind die folgenden Maßnahmen umzusetzen:

- Sofortige Prüfung des Lieferbestandes nach Anzahl und Seriennummern (Vergleich mit Versandinformationen)
- Die Seriennummern aller Geräte der Lieferung, inklusiver ggf. fehlender Geräte, müssen unverzüglich dem Hersteller mittgeteilt werden. Dazu ist der Hersteller unverzüglich durch den Versender über die E-Mail Adresse konnektorlieferung@secunet.com zu informieren.
  Die E-Mail muss authentisch und integritätsgeschützt übertragen werden. Der Hersteller muss den Eingang der Sperrinformationen auf sicheren Weg bestätigen. Siehe Kapitel 7.5 zum sicheren Austausch der Informationen.
  Der Hersteller veranlasst anhand der Seriennummer die unverzügliche Sperrung der Konnektor-Zertifikate.
- Alle Geräte einer Lieferung müssen bei Verdacht auf Integritätsverletzung vom Versender direkt an den Hersteller zurückgeschickt werden.

5.2 Mittlerer Transport (bis max. 100 Geräte)

Im Folgenden werden die Anforderungen an den Zugriffsschutz der Konnektoren beim Transport für einen mittleren Transport beschrieben.

5.2.1 Technische Maßnahmen

Die Geräte müssen in einem gesicherten Fahrzeug transportiert werden. Für den mittleren Transport gelten die nachfolgenden Anforderungen:

- Fester verschlossener nicht einsehbarer Aufbau
- Mindestens ein Fahrer (Transporteur) und
    - Verplombter (mit Seriennummer) Laderaum oder
    - Alarmanlage

5.2.2 Organisatorische Maßnahmen

- Der Fahrer transportiert nur maximal 100 Geräte.
- Das Fahrzeug ist immer zu verschließen.
- Der Transport darf insgesamt (inkl. möglicher Verzögerungen) nicht länger als 24 Stunden dauern. Wenn dieser Zeitraum überschritten wird, verbleiben die Geräte im Bestand des Versenders und die Ursache für die Verzögerung ist zu prüfen. Besteht ein Verdacht auf Integritätsverletzung sind die Maßnahmen aus Kapitel 5.2.3 durchzuführen.
- Verzögerungen der Lieferung müssen unter Nennung der neuen Lieferzeit dem Empfangsberechtigten unverzüglich mitgeteilt werden.
- Bei Fahrzeug mit Plombe
    - Die Plombe wird vom Fahrer im Beisein des Versenders am Laderaum des Fahrzeuges angebracht. Seriennummer der verwendeten Plombe wird vom Versender Nachgehalten und in den Versandinformationen für den Empfänger angegeben.
    - Überprüfung der Seriennummer (anhand der Versandinformationen) und Unversehrtheit der Plombe vor jedem Fahrtantritt
- Bei Fahrzeug mit Alarmanlage
    - Bei einem Alarmfall muss der Alarm vom Fahrer sofort bemerkt werden (z. B. akustisch, Smartphone-Nachricht)
- Versandinformationen mit den Seriennummern der Geräte muss stets vom Fahrer mitgeführt werden. Die Versandinformationen sind immer so beim Fahrer zu halten, dass kein unbemerkter Austausch oder eine Manipulation möglich sind.
- Identifikation
    - Fahrer identifiziert den Empfangsberechtigten anhand der in den Versandinformationen hinterlegten Daten (Name, Vorname) mit dem Ausweisdokument des Empfangsberechtigten.
    - Empfangsberechtigter (Lager) identifiziert Fahrer anhand der elektronischen Versandinformation (Name, Vorname) mit dem Ausweisdokument des Fahrers.
    - Kann die Identität nicht bestätigt werden
        - Darf die Ware nicht angenommen bzw. ausgeliefert werden
        - Empfangsberechtigter kann nicht bestätigt werden; Geräte verbleiben im Bestand des Fahrers.
        - Fahrer kann nicht bestätigt werden; Annahme wird vom Empfangsberechtigten verweigert.
- Bei Fahrzeug mit Plombe:

    - Empfangsberechtigter (Lager) überprüft im Beisein des Fahrers die Seriennummer der Plombe mit den Versandinformationen und öffnet gemeinsam mit dem Fahrer den Laderaum.
- Empfangsberechtigter (Lager) überprüft im Beisein des Fahrers die Unversehrtheit der Gerätekartons (Siegelband) und vergleicht die Seriennummern der gelieferten Geräte mit den Versandinformationen
- Die Fahrer müssen hinsichtlich der in diesem Dokument definierten Sicherheitsanforderungen an Umschlag und Transport von Konnektoren eingewiesen werden.

Schlägt eine der oben genannten Prüfungen fehl, gilt der Verdacht auf Integritätsverletzung.

5.2.3 Maßnahmen bei Verdacht auf Integritätsverletzung

Kann eine Manipulation oder ein Austausch von gelieferten Geräten nicht ausgeschlossen werden (Alarmfall oder Bruch/Austausch der Plombe) so gilt der Verdacht auf Integritätsverletzung. Auch bei Verlust von Geräten (Diebstahl) kann eine Integritätsverletzung der verbliebenen Geräte nicht mehr ausgeschlossen werden. Im Alarmfall gilt:

- Der Fahrer muss sofort zum Fahrzeug zurückkehren (Ankunft nach max. 10 Minuten) und die Ursache für den Alarm ermitteln. Kann ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden, müssen die im Folgenden beschriebenen Maßnahmen ergriffen werden. Das gilt in jedem Fall wenn die Ankunftszeit des Fahrers beim Fahrzeug nach Auslösen des Alarmes länger als 10 Minuten beträgt.
- Auch wenn nach Prüfung der Alarmursache der Verdacht auf Integritätsverletzung nicht mehr besteht, müssen mindestens alle Gerätekartons auf Unversehrtheit geprüft und der Gerätebestand gegen die Versandinformationen geprüft werden. Kann ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden, müssen die im Folgenden beschriebenen Maßnahmen ergriffen werden.

Im Folgenden werden die Maßnahmen beschrieben, die bei einem Verdacht auf Integritätsverletzung von Konnektoren durchzuführen sind. Ein Verdacht auf Integritätsverletzung kann durch reguläre Prüfungen (wie z.B. Prüfungen bei Fahrtantritt) oder durch anlassbezogene Prüfungen (z.B. Verdacht auf Einbruch im Fahrzeug) entstehen. Kann ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden sind die folgenden Maßnahmen umzusetzen:

- Sofortige Prüfung des Lieferbestandes nach Anzahl und Seriennummern (Vergleich mit Versandinformationen)
- Die Seriennummern aller Geräte der Lieferung, inklusiver ggf. fehlender Geräte, müssen unverzüglich dem Hersteller mittgeteilt werden. Dazu ist der Hersteller unverzüglich durch den Versender über die E-Mail Adresse konnektorlieferung@secunet.com zu informieren.
  Die E-Mail muss authentisch und integritätsgeschützt übertragen werden. Der Hersteller muss den Eingang der Sperrinformationen auf sicheren Weg bestätigen. Siehe Kapitel 7.5 zum sicheren Austausch der Informationen.
  Der Hersteller veranlasst anhand der Seriennummer die unverzügliche Sperrung der Konnektor-Zertifikate.

- Alle Geräte einer Lieferung müssen bei Verdacht auf Integritätsverletzung vom Versender direkt an den Hersteller zurückgeschickt werden.

5.3 Großtransport (ab 101 Geräte)

Im Folgenden werden die Anforderungen an den Zugriffsschutz der Konnektoren beim Transport für einen Großtransport beschrieben.

5.3.1 Technische Maßnahmen

Die Geräte müssen in einem gesicherten Fahrzeug transportiert werden. Für den Großtransport gelten die nachfolgenden Anforderungen:

- Fester verschlossener nicht einsehbarer Aufbau
- Mindestens ein Fahrer (Transporteur) und
    - Verplombter (mit Seriennummer) Laderaum oder
    - Alarmanlage
- Werden große Stückzahlen auf Paletten transportiert, müssen die Palette mit den Geräten mit einer Umverpackung (Transportfolie) umwickelt werden.

5.3.2 Organisatorische Maßnahmen

- Der Fahrer kann mehr als 100 Geräte transportieren.
- Das Fahrzeug ist immer zu verschließen.
- Der Transport darf insgesamt (inkl. möglicher Verzögerungen) nicht länger als 24 Stunden dauern. Wenn dieser Zeitraum überschritten wird, verbleiben die Geräte im Bestand des Versenders und die Ursache für die Verzögerung ist zu prüfen. Besteht ein Verdacht auf Integritätsverletzung sind die Maßnahmen aus Kapitel 5.4.3 durchzuführen.
- Verzögerungen der Lieferung müssen dem Empfangsberechtigten unter Nennung der neuen Lieferzeit unverzüglich mitgeteilt werden.
- Bei Fahrzeug mit Plombe
    - Die Plombe wird vom Fahrer im Beisein des Versenders am Laderaum des Fahrzeuges angebracht. Seriennummer der verwendeten Plombe wird vom Versender Nachgehalten und in den Versandinformationen für den Empfänger angegeben.
    - Überprüfung der Seriennummer (anhand der Versandinformationen) und Unversehrtheit der Plombe vor jedem Fahrtantritt
- Bei Fahrzeug mit Alarmanlage
    - Bei einem Alarmfall muss der Alarm vom Fahrer sofort bemerkt werden (z. B. akustisch, Smartphone-Nachricht)
- Versandinformation mit den Seriennummern der Geräte muss stets vom Fahrer mitgeführt werden. Die Versandinformationen sind immer so beim Fahrer zu halten, dass kein unbemerkter Austausch oder eine Manipulation möglich sind.

- Identifikation
    - Fahrer identifiziert den/ die Empfangsberechtigten anhand der in den Versandinformationen hinterlegten Daten (Name, Vorname) mit dem Ausweisdokument des Empfangsberechtigten
    - Empfangsberechtigter (Lager) identifiziert Fahrer anhand der elektronischen Versandinformation (Name, Vorname) mit dem Ausweisdokument des Fahrers.
    - Kann die Identität nicht bestätigt werden
        - Darf die Ware nicht angenommen bzw. ausgeliefert werden
        - Empfangsberechtigter kann nicht bestätigt werden; Geräte verbleiben im Bestand des Fahrers.
        - Fahrer kann nicht bestätigt werden; Annahme wird vom Empfangsberechtigten verweigert.
- Bei Fahrzeug mit Plombe:
    - Empfangsberechtigter (Lager) überprüft im Beisein des Fahrers die Seriennummer der Plombe mit den Versandinformationen öffnet gemeinsam mit dem Fahrer den Laderaum..
- Empfangsberechtigter (Lager) überprüft im Beisein des Fahrers die Unversehrtheit der Gerätekartons (Siegelband) und vergleicht die Seriennummern der gelieferten Geräte mit den Versandinformationen.
- Die Fahrer müssen hinsichtlich der in diesem Dokument definierten Sicherheitsanforderungen an Umschlag und Transport von Konnektoren eingewiesen werden.

Schlägt eine der oben genannten Prüfungen fehl, gilt der Verdacht auf Integritätsverletzung.

5.3.3 Maßnahmen bei Verdacht auf Integritätsverletzung

Kann eine Manipulation oder ein Austausch von gelieferten Geräten nicht ausgeschlossen werden (Alarmfall oder Bruch/Austausch der Plombe) so gilt der Verdacht auf Integritätsverletzung. Auch bei Verlust von Geräten (Diebstahl) kann eine Integritätsverletzung der verbliebenen Geräte nicht mehr ausgeschlossen werden. Im Alarmfall gilt:

- Der Fahrer muss sofort zum Fahrzeug zurückkehren (Ankunft nach max. 10 Minuten) und die Ursache für den Alarm ermitteln. Kann ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden, müssen die im Folgenden beschriebenen Maßnahmen ergriffen werden. Das gilt in jedem Fall wenn die Ankunftszeit des Fahrers beim Fahrzeug nach Auslösen des Alarmes länger als 10 Minuten beträgt.
- Auch wenn nach Prüfung der Alarmursache der Verdacht auf Integritätsverletzung nicht mehr besteht, müssen mindestens alle Gerätekartons auf Unversehrtheit geprüft und der Gerätebestand gegen die Versandinformationen geprüft werden. Kann ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden, müssen die im Folgenden beschriebenen Maßnahmen ergriffen werden.

Im Folgenden werden die Maßnahmen beschrieben, die bei einem Verdacht auf Integritätsverletzung von Konnektoren durchzuführen sind. Ein Verdacht auf Integritätsverletzung kann durch reguläre Prüfungen (wie z.B. Prüfungen bei Fahrtantritt) oder durch anlassbezogene Prüfungen (z.B. Verdacht

auf Einbruch im Fahrzeug) entstehen. Kann ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden sind die folgenden Maßnahmen umzusetzen:

- Sofortige Prüfung des Lieferbestandes nach Anzahl und Seriennummern (Vergleich mit Versandinformationen)
- Die Seriennummern aller Geräte der Lieferung, inklusiver ggf. fehlender Geräte, müssen unverzüglich dem Hersteller mittgeteilt werden. Dazu ist der Hersteller unverzüglich durch den Versender über die E-Mail Adresse konnektorlieferung@secunet.com zu informieren.
  Die E-Mail muss authentisch und integritätsgeschützt übertragen werden. Der Hersteller muss den Eingang der Sperrinformationen auf sicheren Weg bestätigen. Siehe Kapitel 7.5 zum sicheren Austausch der Informationen.
  Der Hersteller veranlasst anhand der Seriennummer die unverzügliche Sperrung der Konnektor-Zertifikate.
- Alle Geräte einer Lieferung müssen bei Verdacht auf Integritätsverletzung vom Versender direkt an den Hersteller zurückgeschickt werden.

5.4 Einzelversand

Neben dem Versand von Geräten von einem Lager über weitere Zwischenlager und schließlich zum Endkunden (Leistungserbringer) können auch direkt einzelne Konnektoren an den Leistungserbringer ausgeliefert werden. Der Bestellprozess kann dabei auch im Auftrag des Leistungserbringes von einem Dienstleister (z. B. Praxisverwaltungssystem, PVS) durchgeführt werden. Empfänger ist dabei in der Regel der Leistungserbringer. In Einzelfällen kann auch der DVO Empfänger eines Einzelversandes sein. Dieser ist damit aber wieder Teil der sicheren Lieferkette und muss sich an die Anforderungen an Transport und Lagerung halten.

Der Versand einzelner Geräte kann auch durch die Transportart „Kleintransport (1-10 Geräte)“ durchgeführt werden.

Zugriffsschutz der Konnektoren beim Transport:

5.4.1 Technische Maßnahmen

- Kurier-Fahrzeug
  - Geschlossenes Fahrzeug mit festem Aufbau
  - Sichere Versandtasche (mit Seriennummer). Die sichere Versandtasche darf nach Verschließen nicht mehr ohne größeren Aufwand geöffnet werden können, ohne dass sichtbare Spuren entstehen.
  - Blickdichte Umverpackung der Versandtasche

5.4.2 Organisatorische Maßnahmen

- Der Fahrer (Kurier) transportiert den Konnektor direkt zum Leistungserbringer.
- Das Fahrzeug ist immer zu verschließen.

- Die Versandtasche ist immer beim Kurier zu tragen, wenn dieser das Fahrzeug verlässt.
- Der Transport darf insgesamt (inkl. möglicher Verzögerungen) nicht länger als 24 Stunden dauern. Wenn dieser Zeitraum überschritten wird, verbleiben die Geräte im Bestand des Versenders und die Ursache für die Verzögerung ist zu prüfen. Besteht ein Verdacht auf Integritätsverletzung sind die Maßnahmen aus Kapitel 5.4.3 durchzuführen.
- Verzögerungen der Lieferung müssen dem Empfangsberechtigten unter Nennung der neuen Lieferzeit unverzüglich mitgeteilt werden.
- Die Seriennummer und Unversehrtheit der Versandtasche muss vor jedem Fahrtantritt überprüft werden.
- Versandinformation mit der Seriennummer des Gerätes muss stets vom Fahrer / DVO mitgeführt werden – aber NICHT in der Versandtasche oder Umverpackung. Die Versandinformationen sind immer so beim Fahrer zu halten, dass kein unbemerkter Austausch oder eine Manipulation möglich sind.
- Identifikation
    - Fahrer (Kurier) identifiziert den Empfangsberechtigten anhand der in den Versandinformationen hinterlegten Daten (Name, Vorname) mit dem Ausweisdokument des Empfangsberechtigten
    - Empfangsberechtigter (Leistungserbringer) identifiziert den Kurier anhand der Angaben in den Versandinformationen (Name, Vorname) mit dem Ausweisdokument des Kuriers.
    - Kann die Identität nicht bestätigt werden
        - Darf die Ware nicht angenommen bzw. ausgeliefert werden
        - Empfangsberechtigter kann nicht bestätigt werden; Geräte verbleiben im Bestand des Fahrers (Kuriers) und müssen zurückgesendet werden
        - Fahrer (Kurier) kann nicht bestätigt werden; Annahme wird vom Empfangsberechtigten verweigert
- Empfangsberechtigter (Leistungserbringer) überprüft im Beisein des Fahrers (Kurier) die Unversehrtheit der Versandtasche (keine Öffnungsspuren, korrekte Seriennummer der Versandtasche) und vergleicht die Seriennummern der gelieferten Geräte mit den Versandinformationen.

Schlägt eine der oben genannten Prüfungen fehl, gilt der Verdacht auf Integritätsverletzung.

5.4.3 Maßnahmen bei Verdacht auf Integritätsverletzung

Kann eine Manipulation oder ein Austausch von gelieferten Geräten nicht ausgeschlossen werden (Manipulationsspuren an der Versandtasche) so gilt der Verdacht auf Integritätsverletzung. Im Folgenden werden die Maßnahmen beschrieben, die bei einem Verdacht auf Integritätsverletzung von Konnektoren durchzuführen sind. Ein Verdacht auf Integritätsverletzung kann durch reguläre Prüfungen (wie z.B. Prüfungen bei Fahrtantritt) oder durch anlassbezogene Prüfungen (z.B. Verdacht auf Manipulation der Versandtasche) entstehen. Kann ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden sind die folgenden Maßnahmen umzusetzen:

- Die Seriennummer des Gerätes muss unverzüglich dem Hersteller mittgeteilt werden. Dazu ist der Hersteller unverzüglich durch den Versender über die E-Mail Adresse konnektorlieferung@secunet.com zu informieren.
  Die E-Mail muss authentisch und integritätsgeschützt übertragen werden. Der Hersteller muss den Eingang der Sperrinformationen auf sicheren Weg bestätigen. Siehe Kapitel 7.5 zum sicheren Austausch der Informationen.
  Der Hersteller veranlasst anhand der Seriennummer die unverzügliche Sperrung der Konnektor-Zertifikate.
- Das Gerät der Lieferung muss bei Verdacht auf Integritätsverletzung vom Versender direkt an den Hersteller zurückgeschickt werden.

Der erste Schritt ist auch bei Diebstahl des Gerätes durchzuführen.

5.5 Regelungen bei Unfall

Tritt während eines Transportes von Konnektoren ein Unfall, ist unverzüglich der Versender zu informieren, damit dieser weitere Schritte planen kann und den Empfänger über mögliche Verspätungen informieren kann. Die Konnektoren dürfen nur dann an den Empfänger ausgeliefert werden, wenn keine Zweifel an der Integrität der Konnektoren bestehen. Dabei gilt:

- Auch wenn nach Prüfung der Unfallsituation der Verdacht auf Integritätsverletzung nicht besteht, müssen mindestens alle Transportverpackungen auf Unversehrtheit geprüft und der Gerätebestand gegen die Versandinformationen geprüft werden. Kann ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden, müssen die im Folgenden beschriebenen Maßnahmen ergriffen werden.

Bei Verdacht auf Integritätsverletzung sind die folgenden Maßnahmen umzusetzen:

- Sofortige Prüfung des Lieferbestandes nach Anzahl und Seriennummern (Vergleich mit Versandinformationen)
- Die Seriennummern aller Geräte der Lieferung, inklusiver ggf. fehlender Geräte, müssen unverzüglich dem Hersteller mittgeteilt werden. Dazu ist der Hersteller unverzüglich durch den Versender über die E-Mail Adresse konnektorlieferung@secunet.com zu informieren.
  Die E-Mail muss authentisch und integritätsgeschützt übertragen werden. Der Hersteller muss den Eingang der Sperrinformationen auf sicheren Weg bestätigen.
  Der Hersteller veranlasst anhand der Seriennummer die unverzügliche Sperrung der Konnektor-Zertifikate.
- Alle Geräte dieser Lieferung müssen bei Verdacht auf Integritätsverletzung vom Versender direkt an den Hersteller zurückgeschickt werden.

5.6 Vergleich der Transportarten

Für die Umsetzung der Transportsicherung sind für die Transportarten Kleintransport, mittlerer Transport, Großtransport sowie Einzelversand unterschiedliche Möglichkeiten zur Umsetzung der Sicherheitsanforderung gegeben. Ziel dabei ist es, sicherzustellen, dass Geräte nicht unbemerkt manipuliert oder ausgetauscht werden können und dass Diebstahl frühzeitig bemerkt wird. Im Folgenden werden diese diskutiert.

Transport mit zwei Fahrern:

Es muss stets mindestens ein Fahrer in Gegenwart der Geräte sein. Dadurch ist sichergestellt, dass keine Geräte unbemerkt manipuliert, ausgetauscht oder gestohlen werden können. Unbemerkte Angriffe auf den sicheren Transport können daher ausgeschlossen werden. Bei physischen Angriffen auf den Transport, wird der Hersteller vom Versender kontaktiert und veranlasst die Sperrung aller Geräte der Lieferung anhand der Seriennummern.

Transport mit verplombter Transportbox oder verplombtem Laderaum:

Vor jedem Fahrtantritt muss die Seriennummer kontrolliert werden und die Unversehrtheit der Plombe geprüft werden. Wenn eine Manipulation oder Austausch der Plombe nicht ausgeschlossen werden kann, hatte ein Angreifer möglicherweise die gesamte Abwesenheit des Fahrers Zeit Geräte zu manipulieren. Damit die unbemerkte Manipulation oder der unbemerkte Austausch von Geräten ausgeschlossen werden kann, müssen alle Geräte zum Hersteller zurückgeschickt werden. Sind Geräte entwendet worden, wird der Hersteller vom Versender kontaktiert und veranlasst die Sperrung aller Geräte der Lieferung anhand der Seriennummern.

Transport mit Alarmanlage:

Bei einem Alarmfall muss der Alarm vom Fahrer sofort bemerkt werden. Das kann durch ständigen Aufenthalt in Hörweite des Alarmes oder durch Meldungen der Armanalage an ein Smartphone sichergestellt werden. Im Alarmfall muss der Fahrer sofort zum Fahrzeug zurückkehren und spätestens nach 10 Minuten das Fahrzeug erreichen. Es ist umgehend die Ursache des Alarms zu ermitteln. Zudem ist das Auto genauestens auf mögliche Einbruchsspuren zu untersuchen. Kann ein Einbruchsversuch unter Berücksichtigung des Autos (bspw. Fahrzeugalter, Zustand und Modell) nicht zweifelsfrei ausgeschlossen werden, gilt der Verdacht auf Integritätsverletzung. Auch wenn durch die vorangegangenen Prüfungen der Verdacht auf Integritätsverletzung nicht mehr besteht, müssen mindestens alle Gerätekartons (bzw. die Transportverpackungen) auf ihre Unversehrtheit und der Gerätebestand gegen die Versandinformationen geprüft werden. Kann der Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden oder erreicht der Fahrer das Fahrzeug erst später als 10 Minuten nach Auslösen des Alarms, muss der Hersteller vom Versender kontaktiert werden, der die Sperrung der Geräte anhand der Seriennummern veranlasst (siehe 7.4).

Einzelversand mit Versandtasche:

Die sicheren Versandtaschen haben eine eindeutige Seriennummer. Die Versandtasche ist zudem immer beim Kurier zu tragen, wenn dieser das Fahrzeug verlässt. Dadurch ist sichergestellt, dass keine Geräte unbemerkt manipuliert, ausgetauscht oder gestohlen werden können. Angriffe auf den

sicheren Transport können daher ausgeschlossen werden. Die Versandtasche dient der zusätzlichen Absicherung, da der Kurier auch ein vom Großlager beauftragtes Versandunternehmen sein kann.

6 Anforderungen an den PVS-Anbieter

Die zugelassenen secunet Konnektor werden bei einem Praxisverwaltungssystem-Anbieter (PVS-Anbieter bzw. entsprechende Organisationseinheit) bestellt. Der PVS-Anbieter ist zudem der Ansprechpartner des Leistungserbringers rund um den zugelassenen secunet Konnektor und u. a. bei Fragen zur sicheren Lieferung und zur Installation des Konnektors. In Dokument Hinweise und Prüfpunkte für Endnutzer (siehe [2]) werden dabei bestimmet Fälle definiert bei denen sich der Leistungserbringer an den PVS-Anbieter wenden muss. Der PVS-Anbieter verpflichtet sich dazu den Leistungserbringer bei entsprechenden Fragestellungen zu unterstützen:

- Kann der Leistungserbringer die sichere Lieferkette des secunet Konnektors nicht nachvollziehen, muss er sich an seinen PVS-Anbieter wenden. Dieser muss den Leistungserbringer bei der erneuten Überprüfung der sicheren Lieferkette unterstützen. Die Unterstützung kann darin bestehen, dass der PVS-Anbieter prüft ob die Prüfung korrekt durchgeführt wurde und dem Leistungserbringer ggf. die einzelnen Schritte erklärt. Bei Bedarf kann auch eine neue Überprüfung mit Anleitung des PVS-Anbieters durchgeführt werden. Die Prüfung MUSS aber immer vom Arzt selbst durchgeführt werden. Kann die Einhaltung der sicheren Lieferkette nicht Zweifelsfrei bestätigt werden, organisiert der Leistungserbringer die Rücksendung des Konnektors und übermittelt die Seriennummer des Konnektors zur Sperrung unverzüglich an den Hersteller (E-Mail Adresse konnektorlieferung@secunet.com).
- Um sicherzustellen, dass die Versandinformationen des Leistungserbringers authentisch sind, muss dieser sich an seinen PVS-Anbieter wenden. Der PVS-Anbieter muss den Leistungserbringer bei dem Abgleich der Versandinformationen unterstützen. Falls der PVS-Anbieter selbst der Versender des Konnektors ist, kann dieser den Abgleich direkt mit dem Leistungserbringer durchführen. Ansonsten muss der PVS-Anbieter dem Leistungserbringer die Kontaktdaten des Versenders an den Leistungserbringer mitteilen. Das ist entweder ein vom Leistungserbringer beauftragter DVO oder der Lieferant des Großlagers.
- Bei der Annahme des Konnektors muss der Leistungserbringer die Identität des Lieferanten anhand der Versandinformationen prüfen. Kann die Identität nicht bestätigt werden, muss sich der Leistungserbringer an den PVS-Anbieter wenden. Dieser kann den Leistungserbringer bei der Nachverfolgung des Lieferschrittes unterstützen. Bleiben Zweifel an der Einhaltung der sicheren Lieferkette bestehen, muss der PVS-Anbieter die Seriennummer des Konnektors zur Sperrung unverzüglich an den Hersteller (E-Mail Adresse konnektorlieferung@secunet.com) übermitteln. Kann die Identität des Empfangsberechtigten durch den DVO nicht bestätigt werden so kann der PVS-Anbieter ebenfalls bei der Klärung unterstützen, siehe auch Kapitel 5.1.2.
- Entsteht der Verdacht eines Manipulationsversuches bei der Prüfung der Transportverpackung und ggf. der Versandtasche des Konnektors darf der Leistungserbringer diesen nicht annehmen und den PVS-Anbieter kontaktieren. Dieser muss die Seriennummer des Konnektors zur Sperrung unverzüglich an den Hersteller (E-Mail Adresse konnektorlieferung@secunet.com). Treten während der Prüfung Unklarheiten auf, wie zum Beispiel Fragen zu den Sicherheitsmerkmalen der Versandtasche muss der PVS-Anbieter den Leistungserbringer bei der Prüfung unterstützen.
- Nach Annahme des Konnektors findet ein erster Abgleich der Seriennummer und der MAC Adressen auf dem Typenschild des Konnektors (siehe [2], Abbildung 2) mit den Versandinformationen statt. Ebenso werden die Siegelnummern beider Gerätesiegel abgeglichen. Stimmen die Daten nicht überein, darf der Konnektor nicht in Betrieb genommen werden

und er Leistungserbringer muss sich an den PVS-Anbieter wenden. Dieser organisiert die Rücksendung des Konnektors und übermittelt die Seriennummer des Konnektors zur Sperrung unverzüglich an den Hersteller (E-Mail Adresse konnektorlieferung@secunet.com).

- Zudem findet eine Prüfung der Gerätesiegel und des Gehäuses statt. Entsteht ein Manipulationsverdacht, darf der Konnektor nicht in Betrieb genommen werden und er Leistungserbringer muss sich an den PVS-Anbieter wenden. Dieser organisiert die Rücksendung des Konnektors und übermittelt die Seriennummer des Konnektors zur Sperrung unverzüglich an den Hersteller (E-Mail Adresse konnektorlieferung@secunet.com).

7 Versandinformationen, Bestandsliste und Sperrprozess

7.1 Versandinformationen bis einschließlich DVO

- Seriennummern der Geräte
- WAN MAC Adressen der Geräte
- LAN MAC Adressen der Geräte
- Lieferadresse und Kontaktdaten der empfangsberechtigten Personen
- Adresse und Kontaktdaten des Versenders (Transporteurs)
- Voraussichtlicher Lieferzeitpunkt (Tag, Uhrzeit)
- Name des Fahrers / DVOs
- Seriennummer der Gerätesiegel
- Seriennummer der Plombe (Nur bei Mittleren und Großtransport mit Plombe)

Die MAC Adressen dürfen nicht auf der Transportverpackung sichtbar sein.

Die Versandinformationen müssen dem Empfänger auf elektronischem Weg vor der Auslieferung der Geräte übersendet werden. Dabei muss die Vertraulichkeit und Integrität der Versandinformationen sichergestellt sein. Insbesondere dürfen die Versandinformationen nicht auf gleichem Weg wie die Geräte an den Empfänger ausgeliefert werden.

Der Schutz der Versandinformationen muss durch verschlüsselten E-Mail-Austausch sichergestellt werden. Für die Verschlüsselung (Vertraulichkeit) und Signatur (Integrität) von Versandinformationen dürfen nur kryptographische Verfahren gemäß [TR-02102] verwendet werden.

Es sollten vom Empfänger immer mehrere empfangsberechtigte Personen benannt werden, damit der Vertretungsfall bei Anlieferung der Geräte geregelt ist. Der Bestellprozess muss daher den Empfänger die Möglichkeit anbieten mindesten zwei empfangsberechtigte Personen zu benennen.

Werden diese Versandinformationen beim Transport mitgeführt, so müssen diese stets vom Fahrer mitgeführt werden und dürfen nicht bei den Geräten verbleiben.

7.2 Versandinformationen für Leistungserbringer

- Seriennummer der Geräte
- WAN MAC Adressen der Geräte
- LAN MAC Adressen der Geräte
- Seriennummer der Versandtasche (bei Einzelversand)
- Lieferadresse und Kontaktdaten der empfangsberechtigten Personen
- Adresse und Kontaktdaten des Versenders bzw. DVOs mit Telefonnummer.
- Voraussichtlicher Lieferzeitpunkt (Tag, Uhrzeit)
- Name des Fahrers / DVOs
- Seriennummer der Gerätesiegel

Die MAC Adressen dürfen nicht auf der Transportverpackung sichtbar sein.

Die Versandinformationen müssen dem Empfänger vor der Auslieferung der Geräte übermittelt werden. Insbesondere dürfen die Versandinformationen nicht auf gleichem Weg wie die Geräte an den Empfänger ausgeliefert werden.

Es sollten vom Empfänger immer mehrere empfangsberechtigte Personen benannt werden, damit der Vertretungsfall bei Anlieferung der Geräte geregelt ist. Der Bestellprozess muss daher den Empfänger die Möglichkeit anbieten mindesten zwei empfangsberechtigte Personen zu benennen.

Werden diese Versandinformationen beim Transport mitgeführt, so müssen diese stets vom Fahrer mitgeführt werden und dürfen nicht bei den Geräten verbleiben.

7.3 Bestandsliste

Alle Lagerarten müssen eine Bestandsliste für die eingelagerten Geräte führen. Die Bestandsliste muss immer den aktuellen Warenbestand nachhalten und jeden Wareneingang und Warenausgang erfassen. Je nach Lagergröße kann die Bestandsliste manuell geführt werden (z. B Nachhalten der Liefer-AVIS bei Eingang und Ausgang von Konnektoren) oder durch elektronische Inventarlisten geführt werden. Es müssen in der Bestandliste mindestens die folgenden Informationen für jeden Konnektor enthalten sein:

- Seriennummer der Geräte
- WAN MAC Adressen der Geräte
- LAN MAC Adressen der Geräte
- Seriennummer der Versandtasche (bei Einzelversand)
- Seriennummer der Gerätesiegel

Diese Informationen müssen getrennt von den Konnektoren aufbewahrt werden und vor Manipulation während eines Einbruches geschützt sein (z. B. Tresor bei Drucksachen oder Integritätsschutz bei elektronischen Daten).

Bei Versand von Konnektoren müssen neben den oben genannten Informationen auch die folgenden Daten für mindestens 5 Jahre nachgehalten werden:

- Lieferadresse und Kontaktdaten (inkl. Telefonnummer) des Empfängers

Anhand der Seriennummer und der MAC Adressen muss der Empfänger des Konnektors ermittelt werden. Dies ist für die Prüfung der sicheren Lieferkette durch den Leistungserbringer erforderlich.

7.4 Sperrprozess

In einigen Fällen (z. B. Manipulationsverdacht oder Verlust/Diebstahl von Konnektoren) muss die Sperrung der Konnektor-Zertifikate veranlasst werden. Insbesondere müssen Konnektoren immer dann gesperrt werden, wenn ein Verdacht auf Integritätsverletzung nicht zweifelsfrei ausgeräumt werden kann. Um die Sperrung zu veranlassen, muss die Seriennummer eines entsprechenden Konnektors an den Hersteller übermittelt werden. Nur Sperraufträge durch Teilnehmer der sicheren Lieferkette oder durch den Endnutzer werden angenommen. Der Hersteller kann dabei die sichere Lieferkette anhand der Seriennummer nachverfolgen und feststellen, ob der Sperrauftrag für den betroffenen Konnektor zulässig ist.

Um als Teilnehmer der sicheren Lieferkette die Sperrung von Konnektoren zu beauftragen müssen die Seriennummer aller vom Verdacht auf Integritätsverletzung betroffenen Geräte über die E-Mail Adresse konnektorlieferung@secunet.com an den Hersteller übermittelt werden. Die E-Mail muss authentisch und integritätsgeschützt übertragen werden. Der Hersteller muss den Eingang der Sperrinformationen auf sicheren Weg bestätigen.

Wenn die Bestätigung durch den Hersteller ausbleibt, ist der Hersteller unverzüglich telefonisch zu kontaktieren. Über die Service-Hotline kann dazu Auskunft über den Sperrstatus erteilt werden. Falls die Sperrung der betroffenen Geräte noch nicht erfolgt ist, sind weitere Schritte mit dem Service-Mitarbeiter zu planen.

Der Schutz der Sperrinformationen und der Eingangsbestätigung des Herstellers muss durch verschlüsselten E-Mail-Austausch sichergestellt werden. Für die Verschlüsselung (Vertraulichkeit) und Signatur (Integrität) von Versandinformationen dürfen nur kryptographische Verfahren gemäß [TR-02102] verwendet werden.

Anhand der Seriennummer kann der Konnektor eindeutig identifiziert werden, insbesondere können die darin verbauten gSMC-Ks ermittelt werden (ICCSN). Der Hersteller wendet sich zur Sperrung direkt und unverzüglich an den PKI Betreiber und gibt die Notwendigen Informationen weiter. Dieser kann die zu Sperrenden Zertifikate der gSMC-Ks in eine CRL aufnehmen und so die Zertifikate zurückziehen. Dabei werden jeweils alle in einem Konnektor verbauten gSMC-Ks gesperrt. Dieser Prozess ist durch die gematik festgelegt und klar geregelt.

Die secunet hält alle durchgeführten Sperrungen von Konnektoren in Ihren Systemen nach. Bei Bedarf kann secunet über die Service-Hotline Auskunft über den Sperrstatus von Konnektoren erteilen.

7.5 Austausch von Informationen

In diesem Dokument wird an mehreren Stellen der Austausch bestimmter Informationen (wie z.B Versandinformationen, Sperrinformationen, etc) gefordert.

Der Schutz dieser Informationen (Vertraulichkeit und Integrität) muss grundsätzlich durch verschlüsselten E-Mail-Austausch sichergestellt werden. Für die Verschlüsselung (Vertraulichkeit) und Signatur (Integrität) von Versandinformationen dürfen nur kryptographische Verfahren gemäß [TR-02102] verwendet werden.

Eine Ausnahme ist die Übertragung der Versandinformationen für Leistungserbringer (siehe Kapitel 7.2). Diese können durch verschlüsselten E-Mail-Austausch, wie oben beschrieben, gesicherten werden. Alternativ wird eine Überprüfung der Versandinformationen durch den Leistungserbringer in [2] beschrieben.

8 Einhaltung und Überwachung der Sicherheitsanforderungen

Die Lagerung, der Transport und der Umschlag von Konnektoren darf nur von Teilnehmern der sicheren Lieferkette durchgeführt werden. Alle Lager und Transportunternehmen die in die Lieferkette von Konnektoren eingebunden sind müssen Teilnehmer der sicheren Lieferkette sein und die folgenden Anforderungen berücksichtigen.

Alle Teilnehmer der sicheren Lieferkette für die Auslieferung von secunet Konnektor müssen sich vertraglich dazu verpflichten die in diesem Dokument gestellten Anforderungen an die sichere Lagerung und Lieferkette einzuhalten. Dazu sind die mindestens die folgenden Punkte entsprechend im Vertrag aufzunehmen:

- Der Vertragspartner verpflichtet sich dazu, alle in diesem Dokument gestellten Anforderungen an die sichere Lagerung und Lieferkette streng einzuhalten.
- Der Vertragspartner verpflichtet sich dazu, bei der Unterbeauftragung weiterer Zwischenhändler, Speditionsunternehmen, PVS-Anbieter oder DVOs, diese wiederum vertraglich zu verpflichten, die in diesem Dokument gestellten Anforderungen an die sichere Lagerung und Lieferkette streng einzuhalten.
- Der Vertragspartner verpflichtet sich dazu die Überprüfung der Einhaltung der in diesem Dokument gestellten Anforderungen an die sichere Lagerung und Lieferkette durch das BSI, den Hersteller secunet und ggf. eine vom Hersteller beauftragte Prüfstelle zuzulassen.

Zudem muss der Vertragspartner garantieren, dass auch bei Geschäftsaufgabe (z.B. durch Konkurs) die Möglichkeit zur Überprüfung der sicheren Lieferkette durch den Leistungserbringer für mindestens 5 Jahre weiter besteht. Dazu sind ggf. entsprechende Nachfolgeregeln zu definieren, siehe dazu auch „Verfügbarkeit von Informationen“ in den Kapiteln 4.1.3, 4.2.3 und 4.3.3. Dabei gilt insbesondere:

- Die Seriennummern aller noch im Bestand befindlichen Konnektoren müssen unverzüglich dem Hersteller über die E-Mail Adresse konnektorlieferung@secunet.com gemeldet werden.
- Die Informationen über Seriennummer, MAC Adressen und Empfänger für jeden ausgelieferten Konnektor müssen integritätsgeschützt für mindestens 5 Jahre aufbewahrt werden und bei Bedarf Auskunft zu den Empfängern einzelner Konnektoren bei Angabe von Seriennummer und MAC Adressen erteilt werden können. Dabei ist z.B. zu regeln, unter welchen Kontaktdaten die Informationen in Zukunft abgefragt werden können, falls sich diese ändern.

9 Referenzen

[1] Modularer Konnektor Version 2.0.0, Bedienhandbuch, Für Administratoren und Benutzer, Version 1.0, Secunet Security Networks AG

[2] secunet(konnektor Version 2.0.0, Sichere Lieferkette – Hinweise und Prüfpunkte für Endnutzer, Version 1.5, Secunet Security Networks AG