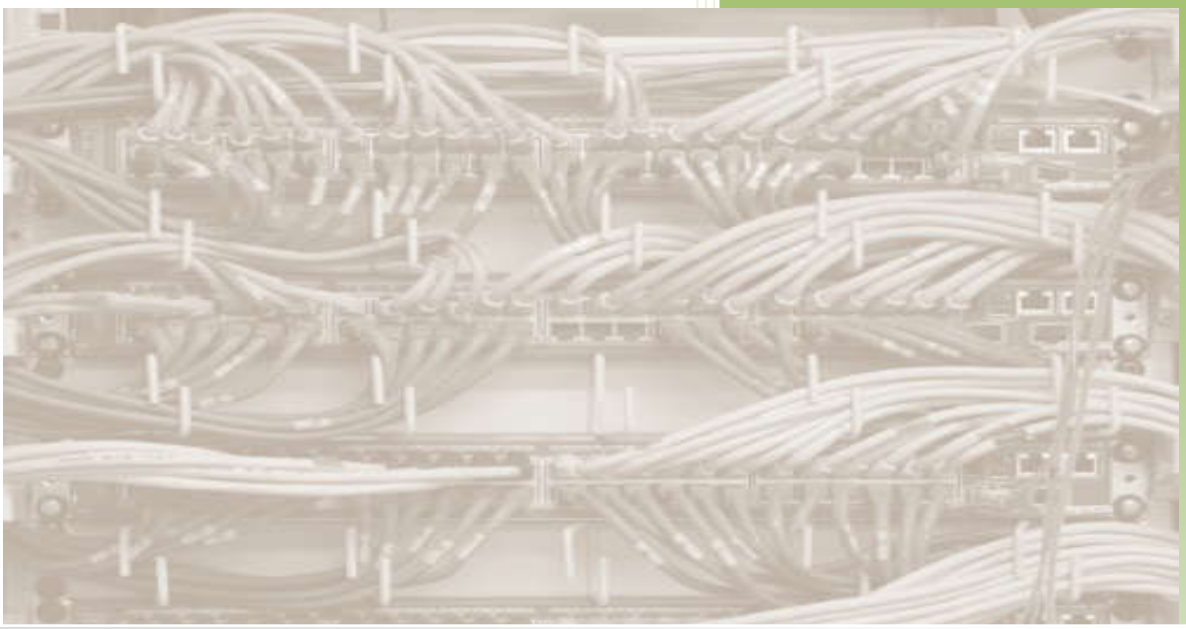

Technische Mindestanforderung Bereich: Netzwerk-Komponenten und angeschlossene Geräte

Verantwortlich:

Robert Gladewitz

Stephan Schnappauf

DBFZ Leipzig

Stand: 18.03.2021

Nächste Überprüfung: 05.2024

Gültigkeit: 03.2025

Inhalt

1 Allgemeines

1.1 Ziel des Dokuments und allgemeine Vorgaben

Dieses Dokument legt die technischen Mindestanforderungen für Netzwerk-Komponenten (Komponenten der Informations- und Kommunikationstechnik mit Ethernet Netzwerkinfrastrukturabhängigkeit) für Ausschreibungen und Verträge fest. Grundsätzlich sind Abweichungen vertraglich festzulegen und im Vorfeld mit der IT des DBFZ abzusprechen.

Alle gesetzten Vorgaben definieren – in Anlehnung an den IT-Sicherheitskatalog von BNetzA und BSI - eine Minimalanforderung zur Sicherstellung der Verfügbarkeit der zu schützenden Systeme und Daten, der Integrität der verarbeiteten Informationen und Systeme und der Gewährleistung der Vertraulichkeit der mit den Systemen verarbeiteten Informationen. Nachweislich höherwertige Komponenten können verwendet werden und können je nach Ausschreibung und Vertrag zu einer Höherwertung führen.

Alle technischen Mindestanforderungen des DBFZ sind unter https://www.dbfz.de/tma verfügbar.

1.2 Verwendete Abkürzungen

ADS	Active Directory Services
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
GA	Gebäudeautomatisierung
IEEE	Institute of Electrical and Electronics Engineers
IKT	Informations- und Kommunikationstechnik
POE	Power over Ethernet
SNMP	Simple Network Management Protocol
VLAN	Virtual LAN
VSS	Virtual Switching System

1.3 Geltungsbereich

Dieses Dokument legt Mindestanforderungen für alle Netzwerk- und Infrastrukturkomponenten fest, die innerhalb des DBFZ zum Einsatz kommen sollen. Mit inbegriffen sind hierbei Komponenten bzw. Teilsysteme, die im Bereich der Prozessautomation eingesetzt werden sollen und steuerbar sind bzw. durch die Bereitstellung der Daten mittelbar einen Einfluss auf die Steuerung von verfahrenstechnischen Anlagen haben.

2 Vorgaben

Für die Festlegung der Vorgaben werden grundlegend drei Netzwerktypen/-bereiche unterschieden. Diese werden im Dokument wie folgt weitergeführt:

- Backbone-Netz **Backbone**
- Gebäudeleittechnik / Prozessleittechnik - **GA Netz**
- Backbone und Arbeitsplatznetz **Büronetz**

Da sich die Anforderungen aufgrund der verschiedenen Anwendungsgebiete unterscheiden, werden die Mindestanforderungen für alle Netze zusätzlich einzeln betrachtet.

2.1 Anforderungen für alle Netzwerktypen

2.1.1 Gesicherter Bereich

Grundsätzlich müssen alle Netzwerkkomponenten mit zentralen Aufgaben, wie Switches, Router und Umsetzer, in gesicherten Bereichen installiert werden. Hierbei ist sicherzustellen, dass nach der Inbetriebnahme nur eingeschränkter Zugriff auf alle Netzwerkkomponenten besteht.

Grundlegend müssen alle Geräte, die an eines der genannten Netzwerke angeschlossenen werden, durch eine Authentifizierung auf Basis von IEEE 802.1x autorisiert und authentifiziert werden.

Endgeräte, die eine Authentifizierung mittels IEEE 802.1x nicht unterstützen, dürfen nur unter folgenden Voraussetzungen eingesetzt werden:

1. das Gerät befindet sich in einem gesicherten Bereich,
2. die Anschlussdose für das Gerät befindet sich in einem gesicherten Bereich und
3. der angeschlossene Netzwerkswitch befindet sich in einem gesicherten Bereich

Ein gesicherter Bereich bezeichnet hierbei einen abgeschlossenen, nur eingeschränkt zugänglichen, also nicht öffentlichen Bereich. Dies gilt beispielsweise für Server, die sich im Serverraum befinden, der zutrittsbeschränkt und zusätzlich überwacht ist. Zulässig als gesicherte Bereiche sind auch Technikräume, wenn diese dadurch abgesichert werden können, dass sie nur durch einen eingeschränkten und definierbaren Personenkreis zugänglich sind.

Ein größerer Bereich mit vielen zulässigen Benutzergruppen, wie zum Beispiel das Technikum, gilt nicht als gesicherter Bereich im Sinne der Netzwerktechnik.

Oben genannte Bedingungen sind zwingend. Ausnahmen müssen durch die IT schriftlich genehmigt werden, da diese Komponenten ein potenzielles Risiko für den Betrieb des Netzes bzw. der Anlagensicherheit darstellen.

2.1.2 Definitionen für IEEE 802.1x

Im DBFZ wird bereits eine ausgebaute und redundant abgesicherte 802.1x Infrastruktur zur Verfügung gestellt. Aktuell werden in der 802.1x Infrastruktur folgende 802.1x EAP Typen unterstützt:

- EAP-TLS
- EAP-TTLS
- EAP-MSCHAPV2
- EAP-MD5
- EAP-PEAP

Die EAP Typen EAP-TLS und EAP-TTLS sind nach Möglichkeit zu bevorzugen.

Zertifikate oder notwendige Kennwörter für GA Komponenten werden auf Anfrage vom DBFZ bereitgestellt.

2.1.3 Absicherung der Konfigurationsmechanismen

Im Fall, dass die Geräte eine Fernadministration/Fernkonfiguration unterstützen, muss die Kommunikation durch geeignete Verschlüsselungsmechanismen abgesichert werden. Geräte, die eine Verschlüsselung der Fernadministration/Fernkonfiguration nicht unterstützen, sind für den Einsatz im DBFZ nicht zulässig.

2.1.3.1 WEB Basiert

Für WEB basierte Konfigurationsoberflächen bedeutet diese eine Absicherung durch das https Protokoll. Hierbei muss, wenn die Geräte dies unterstützen, eine TLS Version größer 1.1 eingesetzt werden. Die Verwendung vom veralteten SSL3 Standard muss vermieden werden.

2.1.3.2 SSH

Eine weitere verbreitete Konfigurationsmöglichkeit besteht auf Basis von SSH. Für SSH muss mindestens die Version 2 eingesetzt werden, wenn das Gerät dies unterstützt. Es ist bei Verwendung von SSH sowohl eine benutzer-/kennwortbasierte als auch zertifikatsbasierte Authentifizierung zulässig.

2.1.3.3 Eigene Software zur Konfiguration

Wenn eine spezielle Software zur Konfiguration verwendet wird, muss die Kommunikation zwischen Software und Gerät ebenfalls verschlüsselt werden, wenn diese über das Netzwerk durchgeführt werden soll. Ein reines Encoding oder eine binäre Übertragung reichen zur Absicherung nicht aus.

2.1.3.4 IP Zugriffseinschränkungen

Geräte mit IP basierten Zugriffseinschränkungen müssen so konfiguriert werden, dass nur berechtigte IP Bereiche eine Konfiguration durchführen können. Bei Ausschreibungen sind Geräte, die IP basierte Einschränkungen unterstützen, durch eine bessere Wertung zu bevorzugen.

2.2 Anforderungen Infrastrukturkomponenten Backbone

Der Backbone bildet das Kernnetzwerk am DBFZ und stellt alle Netzwerkdienste auf Basis einer Sternverkabelung zu den Client Netzen und GA Netzen bereit.

Alle Backbone Komponenten sind redundant auszulegen. Dies bedeutet, dass das Netzwerk durch den Ausfall einer Komponente nicht beeinträchtigt werden darf.

Auf Virtualisierung ist in diesem Bereich vollständig zu verzichten, um Risiken durch diese Technologien auszuschließen. Weitere Vorgaben werden in der folgenden Tabelle aufgeschlüsselt.

Mindestanforderung	Notwendigkeit	Hinweise/Einschränkungen
Redundante Netzteile	Ja	
SNMP	Ja (RMON)	Mit Statusinformationen
Modularer Aufbau	Ja	
19 Zoll	Ja	
POE	Optional	Je nach Ausschreibung/Anforderung
Firewall	Ja	Stateful Inspection muss unterstützt werden
Cluster	VSS Technologie	Alle Module muss VSS Clustering unterstützen
Layer 3	Ja	Inclusive Unterstützung von Filterregeln für Pakete
Normen/Standards	IEEE 802.1d IEEE 802.1p IEEE 802.1q IEEE 802.1s IEEE 802.1w IEEE 802.1x IEEE 802.3x IEEE 802.3ad IEEE 802.3ae IEEE 802.3ak IEEE 802.3aq IEEE 802.3an	
Remotezugriff	SSH	
QoS	802.1p L2 Prioritization Standard QOS	
VLAN	Ja	Anzahl VLAN > 500
Routing	Statisch, OSPF, RIP2, IS-IS	
Paketfilter	ACL basiert	OSI Layer 2, 3 und 4
CU-Ports	10G	1G Kompatibel
LWL Ports	40G/10G	
NON Blocking	Alle verwendete Ports	
STP	RSTP und PVSTP	

Tabelle 1: Mindestanforderung Switches Backbone

Ausnahmen oder Anpassungen müssen durch die IT genehmigt und schriftlich festgelegt werden. Wenn geforderte Technologien zur Ausschreibungszeit/Vertragszeit noch nicht

zur Verfügung stehen, müssen diese umgehend nach Veröffentlichung, spätestens aber nach einem Jahr des Zuschlags oder Vertragsabschluss, ohne weitere Kosten zur Verfügung gestellt werden

2.3 Anforderungen Infrastrukturkomponenten Client Netz

Aufgrund der vorhandenen Infrastruktur und der Interoperabilität zwischen anderen Instituten ist am Standort Cisco als Hersteller in diesem Bereich vorgeschrieben. Der Bereich Client Netze betrifft alle Komponenten, an deren angeschlossenen Geräte sich Benutzer anmelden können.

Es sind bei gleicher Ausstattung und Leistung grundsätzlich Switches mit höherer Portanzahl zu bevorzugen.

Mindestanforderung	Notwendigkeit	Hinweise/Einschränkungen
Normen/Standards	IEEE 802.1D Spanning Tree Protocol IEEE 802.1Q VLAN IEEE 802.1s IEEE 802.1w IEEE 802.1X IEEE 802.1ab LLDP, IEEE 802.3ad, IEEE 802.3ac, IEEE 802.3af, IEEE 802.3at	
19 Zoll	Ja	
Layer	Layer 2	
Stack	FlexStack oder vergleichbar	4 Geräte pro Stack
POE	PoE+	
Remotezugriff	SSH	
QoS	802.1p L2 Prioritization Standard QOS	
Zertifikate	EN 55022 Class A, EN 55024	
CU Ports	24/48 (1 GBit)	
SFP	SFP+ (10GBit)	
VLAN	Ja	Anzahl VLAN > 500
Paketfilter	ACL	OSI Layer 2, 3, 4
Routing	Statisch, OSPF, RIP2, IS-IS	
Non Blocking	erforderlich für alle Ports	
STP	RSTP und PVS	
GVRP	erforderlich	
Syslog	erforderlich	Syslog Server Unterstützung

Tabelle 2: Mindestanforderungen Switches Client Netze

Grundlegend muss für jeden angeschlossenen Port, bei denen ein gesicherter Bereich nicht gewährleistet werden kann, wie folgt konfiguriert werden:

Konfiguration	Anforderung	Hinweise/Einschränkungen
Port Security	Aktiviert	
Authentifizierungs-protokolle	dot1x **# authentication port-control auto**	MAB ist nur im Ausnahmefall zulässig
VLAN	1 **# switchport mode access**	
PAE	Authentificator **# dot1x pae authenticator**	
Spanning Tree	Port Fast **# spanning-tree portfast**	

Tabelle 3: Interface Konfigurationsvorgaben Client Netz

2.4 Anforderungen für Netzwerkkomponenten von Forschungsanlagen

Alle Forschungsanlagen am DBFZ sind in gesonderten TECH-Netzen vom Verwaltungsnetz und dem Internet getrennt. Für die Integration in diese Netze werden zwei Möglichkeiten vorgegeben.

2.4.1 Integration der Einzelkomponenten direkt in die DBFZ Infrastruktur

Hierbei wird die DBFZ Infrastruktur direkt genutzt. Die IT Abteilung am DBFZ stellt Netzwerkports bereit, an die Geräte werden direkt angeschlossen können. Hierbei muss die MAC/Hardwareadresse des Geräts in der IT bekannt gegeben werden.

Eine zusätzliche Unterteilung durch weitere Layer 2 Netzwerkgeräte ist ausdrücklich nicht gestattet. Bei Ausbau durch bspw. weitere Geräte ist auch ein weiterer Netzwerkport pro zu integrierendes Gerät zu verwenden.

2.4.2 Abtrennung in eigene Netze

Für diesen Fall müssen alle Geräte der Anlage in einem eigenen Netz mit eigenen Hardware- und Netzwerkkomponenten installiert werden. Typisch für solch eine Umgebung ist die Verwendung eines Rechners/Servers als Leitrechner oder Steuerungsrechner, der in beiden Netzen integriert ist. Ein Routing zwischen den Netzen ist bei der Verwendung dieses Aufbaus nicht zulässig. Eine Mischung von Netzkomponenten zwischen DBFZ und Anlagenkomponenten ist nicht möglich.

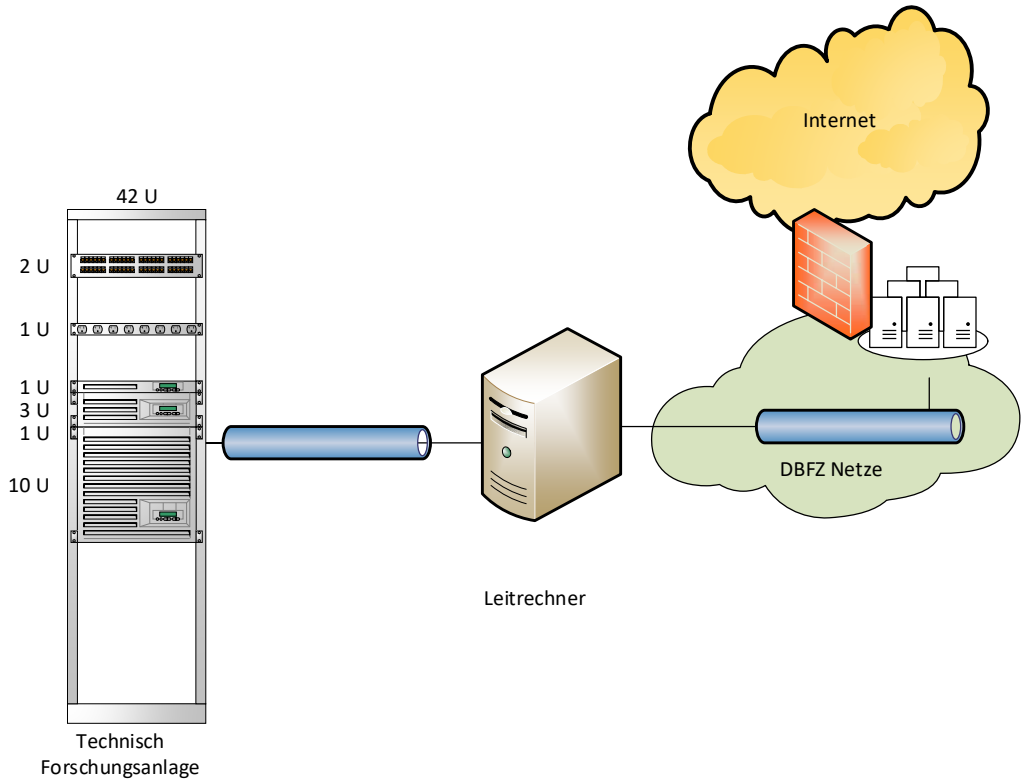

Abbildung 1: Forschungsanlage mit Leitrechner

Für den Leitrechner darf weder Routing noch Bridging für die Netzwerkports aktiv sein, die eine Verbindung mit dem DBFZ Netz haben. Hierbei muss der Leitrechner eine Authentifizierung per 802.1x am DBFZ Netz unterstützen.

Die IP Bereiche müssen vor der Integration mit dem DBFZ abgestimmt werden. Folgende Netzbereiche sind ausdrücklich nicht zugelassen:

- Alle Public-IP Adressbereiche
- 172.16.0.0/12 (172.16.0.0 – 172.31.255.255)
- 192.168.128.0/17 (192.168.128.0 – 192.168.255.255)

Für die Segmentierung der Netze im IPv4 wird grundsätzlich ein Class C Netz (Netzmaske 24 Bit) vorgeschrieben. Wenn mehr Geräte in einem Netz eingesetzt werden sollen, muss ein internes Routing mit entsprechenden Routingkomponenten erfolgen.

Für IPv6 werden Netze mit einer 64-Bit Maske vorgeschrieben. IPv6 Netzbereiche werden vom DBFZ auf Anfrage vergeben. Eigene LocalLink Netze sind aber zulässig.

Die Vorgaben für die verwendeten aktiven Netzwerkkomponenten werden wie folgt definiert:

Tabelle 4: Vorgaben Switch technische Anlage

Mindestanforderung	Notwendigkeit	Hinweise/Einschränkungen
Normen/Standards	IEEE 802.1D Spanning Tree Protocol IEEE 802.1Q VLAN IEEE 802.1s IEEE 802.1w IEEE 802.1X IEEE 802.1ab LLDP, IEEE 802.3ad, IEEE 802.3ac, IEEE 802.3af, IEEE 802.3at	
19 Zoll	Optional	
Layer	Layer 2	oder Layer 3

Um eine Fehlverhalten bei Steckverbindungen zu vermindern, werden für technische Anlagen Kabelfarben für CAT/RJ45 Kabel vorgeschrieben. Für technische Versuchsanlagen mit eigenem Leitrechner werden für alle CAT-Kabel folgende Kabelfarben festgelegt:

Komponentenart	Kabelfarbe CAT/RJ45Kabel
internes Anlagen-Netzwerk	Orange
Serial über CAT/RJ45 Kabel	Gelb
Video über CAT/RJ45 Kabel	Grün
Anbindung DBFZ Netz (vom Leitrechner)	Grau

Tabelle 5: CAT Kabelfarben technische Anlagen

Für alle Kabel, die keine CAT-Kabel sind, sind keine Kabelfarben vorgeschrieben.

2.5 Anforderungen Infrastrukturkomponenten GA Netz

Das GA Netz definiert alle Komponenten, die Geräte für die Gebäudeautomatisierung und Prozessautomatisierung anbinden. Grundsätzlich wird das GA Netzwerk innerhalb eines Gebäudes unabhängig von anderen Netzkomponenten des DBFZ betrieben und muss auch so geplant werden. Hierzu gehören alle Kabelverbindungen inklusive der CAT Kupferverkabelung innerhalb eines Gebäudes.

Die gebäudeübergreifende Anbindung wird durch den vorhandenen Backbone und Clientnetzbereiche des DBFZ sichergestellt.

Grundlegend wird für die GA Netz Verkabelungsstruktur der Gebäude eine Sternverkabelung vorgegeben. Ausnahmen dürfen nur umgesetzt werden, wenn sicherheitstechnisch keine Einschränkungen bestehen und sich die Ausfallsicherheit hierdurch nicht verschlechtert.

2.5.1 Netzintegrierte Switches

Für Ethernet Switches, die in die DBFZ Netze direkt eingebunden werden müssen, gelten gesonderte Vorgaben. Diese Switches sind nur nach Absprache mit der IT Abteilung des DBFZ in die Infrastruktur einzubinden.

Mindestanforderung	Notwendigkeit	Hinweise/Einschränkungen
Normen	IEEE 802.1D Spanning Tree IEEE 802.3 IEEE 802.3u IEEE 802.3x IEEE 802.3z IEEE 802.1D IEEE 802.1w IEEE 802.1p IEEE 802.1Q IEEE 802.3ab	
SNMP	min. v3	Inklusive Verschlüsselung, RMON Standard
Spanning Tree	RSTP und PVSTP	
LACP	Ja	
Verwaltung	ssh/ssl	
MAC Adressen	<10000	
VLANs	Ja	

Tabelle 6: Mindestanforderungen Switches GA Netze

Die 802.1x Infrastruktur wird bereits durch das DBFZ bereitgestellt. Vor der endgültigen Abnahme müssen alle Komponenten, die am Netzwerk abgeschlossen sind, über 802.1x Mechanismen autorisiert und authentifiziert sein.

Während definierter Test- und Einführungsphasen dürfen nach Absprache mit der IT, GA Netze auch ohne Authentifizierung betrieben werden. Spätestens zum Abschluss dieser Phase sind diese Netze dann endgültig durch Authentifizierung und Autorisierung über 802.1x abzusichern.

Wenn möglich, ist die VLAN Konfiguration des Ports auf Basis der 802.1x Zugangspakte durch den Radius festzulegen. Nur wenn diese automatische Zuweisung technisch bedingt nicht möglich ist, ist eine statische VLAN Zuweisung zulässig.

2.5.2 Andere Geräte im GA Netz

Alle anderen Geräte mit Netzwerkzugriff sind als Netzwerkclients zu betrachten. Diese müssen, wenn ein gesicherter Bereich nicht vorhanden ist, mittels 802.1x am jeweiligen Switch autorisiert und authentifiziert werden.

3 Service und Maintenance, fakultativ: Garantie

Für alle Komponenten muss in Ausschreibungen und Vergaben ein vierjähriger Servicevertrag abgeschlossen werden. Folgende Voraussetzungen müssen in einem Servicefall erfüllt werden:

- Maximal 24 Stunden Erstreaktionszeit,
- Erfüllung vordefinierter Wiederherstellungszeiten,
- fachkundiger Hardware- und Softwaresupport ohne Wartezeiten,
- die Serviceunterstützung bei Hardwarefehlern muss vor Ort ausgeführt werden,
- Unterstützung für Softwarefehler kann Remote durchgeführt werden

Seitens des DBFZ werden für alle Infrastrukturkomponenten folgende Reaktions- und Wiederherstellungszeiten definiert.

Mängelklasse	Reaktionszeit	Wiederherstellungszeit
Betriebsverhindernder Mangel	4 Stunden	24 Stunden
Betriebsbehindernder Mangel	24 Stunden	48 Stunden
Leichter Mangel	48 Stunden	eine Woche

Tabelle 7: Reaktions- und Wiederherstellungszeiten

Software-Updates, Sicherheitsupdates und neue Feature-Packs während des gesamten Zeitraums sind im Beschaffungsprozess festgelegten Pauschalfestpreis enthalten. Das Gleiche gilt für die Anpassungen an neue Technologien, wie zum Beispiel neuer Verschlüsselung oder Authentifizierungstechnologien.

Alle angebotenen Komponenten müssen eine unselbstständige Garantie mit Vorortaustausch für einen Zeitraum von vier Jahren beinhalten. Deshalb wird über die Mängelhaftung nach Ziffer 13 EVB-IT Systemlieferungs-AGB hinausgehend der Abschluss einer individuellen Garantievereinbarung oder Servicevereinbarung in der folgenden Form angestrebt:
Alternativ kann für alle Komponenten einen Wartungsvertrag inklusive kostenlosem Hardwaretausch angeboten werden. Dieser muss ebenfalls den kostenlosen Austausch aller Komponenten ermöglichen und notwendige Softwareupdates / -upgrades während des Wartungszeitraums beinhalten.

Der Auftragnehmer garantiert für die Dauer von vier Jahren, dass die Sache frei von jeglichen Sachmängeln im Sinne des § 434 BGB ist. Dies gilt auch für solche Mängel, die erst nach Gefahrübergang auftreten (unselbständige Garantie).

Für Geräte, die für Projekte oder kurze Laufzeiten angeschafft werden, ist sicherzustellen, dass für die Laufzeit Software-Updates, Sicherheitsupdates und neue Feature-Packs kostenlos zur Verfügung stehen. Ein Servicevertrag muss für solche Geräte nur abgeschlossen werden, wenn andere Prozesse oder GA Komponenten durch Ausfälle oder Fehler beeinflusst werden.