Leistungsbeschreibung
Business Client Protect, Kaspersky.

1 Allgemein

Die Telekom Deutschland GmbH (im Folgenden Telekom genannt) verkauft, installiert, hält instand und betreibt (je nach vereinbartem Leistungsumfang) mit Business Client Protect (im Folgenden BCP genannt) eine Client Security Lösung zur Absicherung von mobilen Arbeitsplätzen, Desktop PCs und Server-Systemen.

Mit BCP erhält die Unternehmens-IT die Kontrolle darüber, wer was an welchem Client anschließen darf, welche Programme darauf laufen dürfen und mittels einer zentralen Konsole die Remote Verwaltung aller geschützten Endpoints. Diese Kontrolle wird mit einer Verschlüsselungsoption, AntiVirus und einer Personal Firewall oder der Absicherung virtueller Instanzen ergänzt. BCP bietet einen Schutz zur Absicherung der Daten und Schutz vor Viren, Malware sowie vor Trojanern.

1.1 Funktionalitäten

1.1.1 Verschlüsselung

Die Verschlüsselung erfolgt nach AES-256 Standard und umfasst Datenträger, Dateien oder Ordner. Für Wechseldatenträger kann eine Zwangsverschlüsselung eingerichtet werden.

1.1.2 Kontrolle des Datenflusses

Festlegen von Richtlinien mit denen der Datenfluss auf und von Wechseldatenträgern und sonstigen Peripheriegeräten kontrolliert wird, sowie mit denen Programme und Berechtigungen im Betriebssystem reguliert werden können.

Die eingesetzte Technologie unterstützt:

- Sperren von Laufwerken (Floppy, CD/DVD, USB, Firewire und andere)
- Sperren von Geräten (Smartphones, Kameras, MP3-Player usw.)
- Dateifilter
- Überwachung der Anwendungsausführung
- Sperren von Anwendungen (Blacklist)
- Freigabe der erlaubten Applikationen (Whitelist)
- Kombination von Blacklist- und Whitelistmodus für optimale Absicherung.

1.1.3 AntiVirus

Die eingesetzte Technologie unterstützt die automatische Verteilung von Updates, Patches und Schutz auf Signaturbasis (Unterstützung von MAC und Windows[1]). Zusätzlich ist ein System zur Angriffsüberwachung auf Client-Basis Bestandteil.

1.1.4 Mobile EndPoint Security

Über die eingesetzte Software werden folgende Technologien unterstützt:

- Überwachung installierter Anwendungen auf mobilen Geräten gemäß Gruppenrichtlinien.
- Containerisierung, um Unternehmensdaten und -anwendungen in verschlüsselten Containern zu isolieren.
- Bietet die Möglichkeit, Anwendungen zentral über SMS, E-Mail und PC im Voraus zu konfigurieren und bereitzustellen.
- Externe Tools zum Diebstahlschutz, z. B.
  - SIM-Überwachung
  - Remote-Sperrung
  - Remote-Löschen der Daten
  - GPS-Tracking.

1.1.5 Inventarisierung

Die Technologie-Komponente ermöglicht ein Inventar-Management, sodass neben der Hardware der Bestand an Software inventarisiert und geprüft wird (z. B. Ablaufdaten Softwarelizenzen etc.).

1.1.6 Server-Schutz

Die eingesetzte Technologie unterstützt:

- Collaboration-Server
  - Schutz für SharePoint-Farmen, einschließlich Front-End, SQL-Server, Programmen, Suche, Index, etc.
  - Verhindert externe Uploads unangemessener Inhalte, setzt interne Kommunikationsrichtlinien durch und blockiert die Speicherung von Dateien nach Dateityp oder Textinhalt.
- E-Mail-Server
  - Schutz des E-Mail-Verkehrs auf Basis von Microsoft Exchange, IBM Lotus Domino und Linux.
  - Reduzierung der Systembelastung durch leistungsstarke Anti-Viren-Engine und Load-Balancing-Verfahren für Serverressourcen.
- Web-Server
  - Verbesserung der Leistung und senken die Ressourcenauslastung für Viren Scanning durch Leistungsstarke Anti-Viren-Engine und optimierter, intelligenter Scan- und Load-Balancing-Verfahren.
  - Unterstützung Windows- und Linux basierter Plattformen.

2 Leistungen der Telekom

Business Client Protect basiert auf der Lösungen des Herstellers Kaspersky.

Die Telekom verkauft dem Kunden die erforderliche Software, installiert sie bei Vereinbarung gemäß Ziffer 2.2, betreibt sie bei Vereinbarung gemäß Ziffer 2.3 und hält sie bei Vereinbarung gemäß Ziffer 3 instand.

2.1 Kauf

Die Telekom übereignet dem Kunden das vereinbarte Software-Paket.

2.2 Installation

Im Rahmen der Installationsleistung wird ein telefonischer Konfigurationsworkshop durchgeführt. Im Rahmen dieses Workshops unterstützt die Telekom den Kunden mit Hilfe eines Konfigurationsdokumentes (Pre-Implementation Worksheet) bei der Zusammenstellung aller für die Installation von Business Client Protect erforderlichen Angaben.

Hierbei werden alle erforderlichen Daten für die Erstellung des Konfigurationsdokumentes gemeinsam mit dem Kunden erarbeitet.

Die Installation beinhaltet die Installation der Managementkonsole, die Basiskonfiguration der vereinbarten Features für fünf Clients sowie das Anlegen des Kunden in der Betriebsdatenbank. Die Basiskonfiguration beinhaltet eine Standard-Konfiguration ohne kundenindividuelle Anpassungen. Darüber hinaus kann die Implementierung weiterer Clients zusätzlich beauftragt werden.

Erforderliche Besonderheiten (z. B. Notwendigkeit einer statischen IP-Adresse bzw. Verfügbarkeit des DSL-Anschlusses) werden bei Vertragsschluss vereinbart.

2.2.1 Consulting

a) Konfigurationsworkshop via WebEx
   Besprechung der Anforderungen. Abfrage der Kundenanforderung an Hand eines PreIMP Worksheets. Festlegung des Kundenansprechpartners. Das Worksheet dient als Basis der Installation und wird dem Kunden für die Dokumentation zur Verfügung gestellt.
b) Tagesworkshop
   Durchführung eines individuelles Kundenconsultings.

2.2.2 Montage

a) Installation Managementkonsole
   - Abstimmen der Active Directory-Konfiguration für die Management Komponenten
   - Installation der Management Komponenten/Konsole inkl. Datenbank
   - Integration Management-Komponenten in die Active Directory-Struktur
   - Funktionstest der Active Directory-Verbindung, der Updates der Management Komponenten, der Logfiles und Dienste
   - Rollout der Software auf max. fünf Clients.
   - Kundenübergabe / -einweisung (max. 15 Minuten)
   - Anlege des Kunden in den Telekom-Systemen.
   - Übergabe bei Betrieb S an den Kunden.
   - Übergabe bei Betrieb L an den Kunden und den Betrieb.

[1] Die im Dokument genannten Produkt- und Firmennamen sind Marken der jeweiligen Eigentümer.

b) Basisinstallation Kaspersky Core
AntiVirus & Firewall
- Festlegen des Umgang bei einem Virenfund.
- Zuweisung der Funktionalität eines vorhandenen Userprofils.
- Rollout von Software und Profil.

Rollout aller Funktionen über vorhandene Softwareverteilung oder Active Directory auf max. fünf Clients.

c) Basisinstallation Kaspersky Select
AntiVirus & Firewall
- Festlegen des Umgang bei einem Virenfund.
- Zuweisung der Funktionalität eines vorhandenen Userprofils.
- Rollout von Software und Profil.

Gerätekontrolle
- Konfiguration von max. drei User Profilen (z. B. erlaubten/gesperrten Peripheriegeräten und/oder Zeitschaltung).
- Sperren bzw. Freigabe von bestimmten Devices an Hand von drei Profilen.

Webkontrolle
- Konfiguration von max. drei User Profilen (z. B. nach Kategorien Erotik, Glücksspiel usw., nach URL und/oder Zeitschaltung)

Programmkontrolle
- Konfiguration von max. drei User Profilen (z. B. Programme und Berechtigungen im Betriebssystem etc.).
- Konfiguration von unerwünschten Applikationen.
- Einstellung der Signalisierung am Client (Informationen etc.)

Sicherheit für Datei Server
- Initial-Installation

Mobile Endpoint Security und Mobile Device Management
- Rollout und Konfiguration auf max. drei Mobilen Geräten.
- Anlegen von max. drei Profilen. (z. B. erlaubte/gesperrte Apps, Erstellung verschlüsselter Ordner etc.)

Rollout aller Funktionen über vorhandene Softwareverteilung oder Active Directory auf max. fünf Clients.

d) Basisinstallation Kaspersky Advanced
AntiVirus & Firewall
- Festlegen des Umgang bei einem Virenfund.
- Zuweisung der Funktionalität eines vorhandenen Userprofils.
- Rollout von Software und Profil.

Gerätekontrolle
- Konfiguration von max. drei User Profilen (z. B. erlaubten/gesperrten Peripheriegeräten und/oder Zeitschaltung).
- Sperren bzw. Freigabe von bestimmten Devices an Hand von drei Profilen.

Webkontrolle
- Konfiguration von max. drei User Profilen (z. B. nach Kategorien Erotik, Glücksspiel usw. nach URL und/oder Zeitschaltung)

Programmkontrolle
- Konfiguration von max. drei User Profilen (z. B. Programme und Berechtigungen im Betriebssystem etc.).
- Konfiguration von unerwünschten Applikationen.
- Einstellung der Signalisierung am Client (Informationen etc.)

Sicherheit für Datei Server
- Initial-Installation

Mobile Endpoint Security und Mobile Device Management
- Rollout und Konfiguration auf max. drei Mobilen Geräten.
- Anlegen von max. drei Profilen. (z. B. erlaubte/gesperrte Apps, Erstellung verschlüsselter Ordner etc.)

Datenschutz (Verschlüsselung)
- Verschlüsselung nach AES-256 Standard für max. drei Clients.

Image-Management
- Initial-Installation

Lizenz-Management
- Initial-Installation

Patch-Management
- Initial-Installation

Softwareinstallation
- Initial-Installation

Vulnerability Scanning
- Initial-Installation

Rollout aller Funktionen über vorhandene Softwareverteilung oder Active Directory auf max. fünf Clients.

e) Basisinstallation Kaspersky Total (Server)
Installation jeweils eines Servers mit folgender Funktion:
Collaboration-Server (Schutz für SharePoint-Farmen einschließlich Front-End, SQL-Server, Programmen, Suche, Index, etc.)
- Initial-Installation

E-Mail-Server (Schutz des E-Mail-Verkehrs auf Basis von Microsoft Exchange, IBM Lotus Domino und Linux)
- Initial-Installation

Web-Server (optimierte, intelligente Scan- und Load-Balancing-Verfahren)
- Initial-Installation

2.3 Betrieb

Die Telekom bietet die Betriebspakete
- S (Reaktives Management)
- L (Shared Management)

an.

Beim Betriebspaket S obliegt das Lösungsmanagement dem Kunden. Dazu gehören Datensicherungen, Patch- und Releasemanagement, Monitoring und Überwachung, Incidentmanagement sowie Changemanagement. Die Telekom erbringt auf Abruf die unter Ziffer 2.3.1 Betriebspaket S beschriebenen Leistungen.

Für das Betriebspaket L ist beim Kunden eine statische IP-Adresse und ein VPN-Gateway Voraussetzung. Der entsprechende Internet-Zugang sowie die statische IP-Adresse sind nicht Bestandteil dieser Leistung.

Kunden die einen bestehenden Managementvertrag zu den Produkten Customized Network Protect oder Business Network Protect haben, benötigen keinen gesonderten VPN-Zugang. Das Management erfolgt über die bestehende VPN-Verbindung.

Sofern keine durch die Telekom betriebene Firewall vorhanden ist, muss für den dauerhaften Managementzugriff ein entsprechendes VPN-Gateway (bevorzugt Cisco ASA5505-BUN-K9) bereitgestellt werden. Dem Zugriff auf das zu betreibende System über die VPN-Verbindung muss zugestimmt werden. Während der Arbeiten an Business Client Protect ist die Telekom berechtigt, die Software außer Betrieb zu nehmen.

Die Telekom erbringt bei Betrieb L die unter Ziffer 2.3.2 Betriebspaket L beschriebenen Leistungen. Changemanagement ist nicht Leistungsbestandteil und kann als zusätzliche Leistung beauftragt werden (s. Ziffer 2.4).

2.3.1 Betriebspaket S
- Bereitstellung einer 1st Level-Hotline täglich von 0.00 bis 24.00 Uhr (Störungsannahme)
- Bereitstellung 2nd Level Support an Werktagen (montags bis freitags) 8.00 bis18.00 Uhr (außerhalb der Zeiten mittels Herbeiruf)
- Ggf. Unterstützung durch gesicherte Remoteverbindung
- Herstellung des 3rd-Levelkontakts zum Hersteller (Einstellung Ticket durch die Telekom)

2.3.2 Betriebspaket L
- Bereitstellung einer 1st Level-Hotline täglich von 0.00 bis 24.00 Uhr (Störungsannahme)
- Bereitstellung 2nd Level Support an Werktagen (montags bis freitags) 8.00 bis18.00 Uhr (außerhalb der der Zeiten mittels Herbeiruf)
- Ggf. Unterstützung durch gesicherte Remoteverbindung
- Kontakt zum Hersteller bereitstellen (3rd Level Zugang)
- Überwachung der VPN Verbindung und Verfügbarkeit per SNMP
- Einspielen von Patches und Fixes / Einspielung neuerer Softwareversion in Abstimmung mit dem Kunden
- Unterstützung bei Datenwiederherstellung verschlüsselter Festplatten
- Regelmäßige Sicherung der Kundenkonfiguration (Sicherung der Datenbank und Zertifikate einmal die Woche und gesamtes Backup einmal pro Monat)
- Folgende Komponenten werden überwacht: Server auf Erreichbarkeit, ServicePorts der Anwendungen, Auslastung des Arbeitsspeichers, CPUs und Festplatte der Server (wegen Sicherung der Backups).
- Servicelevel S24 oder S72 gemäß der unter Ziffer 3 beschriebenen Parameter.

Begriffsdefinition:

a) Einspielen von Patches und Fixes
In Absprache mit dem Kunden führt die Telekom Anpassungen und Aktualisierungen der eingesetzten Software auf den aktuellen Entwicklungsstand des Herstellers durch. Die Softwareupdates werden von der Telekom zuvor geprüft und freigegeben. Major-Release-Wechsel und Lizenz-Upgrades sind nicht Leistungsbestandteil.

b) Überwachung der VPN Verbindung
Die VPN Verbindung des Kunden wird im Betriebszentrum der Telekom täglich von 0.00 bis 24.00 Uhr aktiv überwacht. Wird ein Incident erkannt, erfolgt eine Information des Kunden durch die Hotline. Mittels der VPN-Verbindung erfolgt das Monitoring,

welches die Erreichbarkeit des Kundensystems überwacht.

c) Überwachung und Monitoring
Die Lösung des Kunden wird im Betriebszentrum der Telekom täglich von 0.00 bis 24.00 Uhr aktiv überwacht. Wird ein Incident erkannt, erfolgt eine Information des Kunden (an den bei der Installation festgelegten Ansprechpartner des Kunden) durch die Telekom. Zusätzlich erfolgt ein Monitoring, welches die Erreichbarkeit der Securitylösung überwacht.

d) Sicherung der Kundenkonfiguration (Datenbank und Zertifikate)
Das Betriebszentrum der Telekom erstellt regelmäßig (Sicherung der Datenbank und Zertifikate einmal die Woche und gesamtes Backup einmal pro Monat) oder vor Durchführung eines Changes ein Backup der eingesetzten Lösung, welches im Falle eines Restores in ein Austauschsystem eingespielt wird.

e) Incident Management
Die Telekom übernimmt die Analyse und Beseitigung aller Störungen an der Lösung. Die Störung wird entweder proaktiv durch die permanente Überwachung erkannt oder durch den Kunden an die Hotline gemeldet.

2.3.3 Hotline
Das Telekom-Eingangstor steht dem Kunden unter einer Servicerufnummer zur Verfügung.

2.4 AddOn Change
Die Telekom erbringt das AddOn Change nach Vereinbarung als zusätzliche Leistung im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten gegen gesondertes Entgelt, das sich nach den zum Zeitpunkt der Auftragserteilung gültigen Listenpreisen richtet.
Voraussetzung hierfür ist das vereinbarte Betriebspaket L.
AddOn Change beinhaltet monatlich max. fünf Changes (z. B. Konfigurationsanpassungen, Einrichtung verschlüsselter Devices, Container Verschlüsselung, Offline Freigabe für USB Devices etc.).
Änderungen, die an Werktagen (montags bis freitags) eingehen, werden innerhalb von 24 Arbeitsstunden bearbeitet. Diese werden ausschließlich nach Absprache mit dem Kunden durchgeführt. Die Clientkonfiguration erfolgt über zentral gespeicherte Richtlinien oder über Gruppenrichtlinien. Changerequests beinhalten nicht das Anlegen von neuen Richtlinien.

3 Service

Der Service umfasst die Annahme von Störungsmeldungen, die Instandsetzung des Lösungssystems, soweit die auftretenden Störungen bei ordnungsgemäßem Gebrauch entstanden sind sowie Unterstützung des Kunden bei unklaren oder wiederkehrenden Fehlerzuständen und Zugang zum Herstellersupport. In der Regel erfolgt die Instandsetzung durch Einspielen der zuletzt gesicherten Version.

3.1 Standard
Es werden bei Betriebspaket L die Servicelevel S24 und S72 angeboten (Parameter siehe u. s. Tabelle).
Die Servicelevel S24 und S72 inklusive der sichergestellten Entstörzeiten beziehen sich ausschließlich auf die von der Telekom installierten Software. Die zugesicherten Entstörzeiten setzen die einwandfreie Funktion der darunterliegenden Kunden-Systeme (Hardware, VM etc.) voraus.
Weiterhin sind alle softwarebedingten Störungen von den zugesicherten Entstörfristen ausgeschlossen. Bei softwarebedingten Störungen handelt es sich um Störungen, die auf Softwarefehler zurückzuführen sind. Hierbei muss eine Reaktion und Interaktion des Herstellers vorweggehen, damit eine überarbeitete Softwareversion zur Einspielung von Patches/Updates/Upgrades bereitgestellt werden kann.
Im Einzelnen erbringt die Telekom folgende Service-Leistungen:

3.1.1 Annahme der Störungsmeldung
Die Telekom nimmt täglich von 0.00 bis 24.00 Uhr Störungsmeldungen des Kunden unter einer Service-Rufnummer entgegen.

3.1.2 Servicebereitschaft
Die Servicebereitschaft richtet sich nach dem mit dem Kunden vereinbarten Servicelevel.

3.1.3 Reaktionszeit
Die Reaktionszeit richtet sich nach dem vereinbarten Servicelevel.

3.1.4 Zwischenmeldung
Die Telekom erteilt auf Wunsch unter der angegebenen Rückrufnummer entsprechend des mit dem Kunden vereinbarten Servicelevels nach Ablauf der Reaktionszeit eine Zwischenmeldung über den Bearbeitungsstand und den Ausblick auf weitere Maßnahmen.

3.1.5 Entstörungsfrist
Die Telekom beseitigt die Störung in Abhängigkeit vom mit dem Kunden vereinbarten Servicelevel nach Eingang der Störungsmeldung innerhalb der angegebenen Frist. Die Frist ist eingehalten, wenn innerhalb des vereinbarten Zeitraums die Funktionalität wiederhergestellt ist oder dem Kunden ein adäquater Ersatz zur Verfügung gestellt wurde.

3.1.6 Rückmeldung
Die Telekom informiert den Kunden nach Beendigung der Störung.

3.2 Individuelle Serviceleistungen
Die Telekom erbringt jeweils nach Vereinbarung im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten gegen gesondertes Entgelt, das sich nach den zum Zeitpunkt der Auftragserteilung gültigen Listenpreisen richtet, weitere individuelle Serviceleistungen.

4 Mitwirkungspflichten des Kunden

Der Kunde und die Telekom werden zu Beginn des Projektes je einen verantwortlichen technischen Projektleiter benennen. Die beiden Projektleiter sind die verantwortliche Verbindung der Vertragspartner. Um das Projekt zu einem erfolgreichen Abschluss zu bringen, sind eine Aufteilung der Aufgaben und eine definierte Zuständigkeit für Projektabläufe zwingend notwendig.
Die Mitwirkung des Kunden umfasst folgende Leistungen:

- Informationsfluss zum Projektleiter der Telekom (d. h. Sicherstellen des Informationsaustausches/Weiterleitung von Informationen kundenseitig).
- Ggf. Vorbereitung von Projekt- und Statusmeetings.
- Bereitstellung aller für das Projekt erforderlichen Unterlagen des Kunden wie aktuelle Netzpläne, aktuelle IP-Adressen, Software-Releasestände der bestehenden Systeme, Konfigurationen der bestehenden Systeme.
- Einplanung und Bereitstellung von Ressourcen kundenseitig (Personal, Räume etc.)
- Koordination der Mitarbeiter kundenseitig bzgl. der Vor-Ort Installationen in Zusammenarbeit mit dem Projektleiter der Telekom.
- Vorbereitung der Vor-Ort Installationen kundenseitig hinsichtlich des Zutritts, Stromversorgung, Verteilerschränke, etc.
- Die für die Technik benötigten Räumlichkeiten, einschließlich der passiven Verkabelung und der aktiven Netzwerkkomponenten werden vom Auftraggeber im Projekt bereitgestellt.
- Für die gesamte Projektlaufzeit ist der ungehinderte Zugang für das Personal der Telekom zu allen für die Systemlösung relevanten Räumen im Rahmen der Installationsleistungen sicherzustellen.
- Bereitstellung aller benötigten Zugänge, Daten (z. B. Benutzername, Passwort, Lizenzkeys etc.), Parameter, Wartungs- und Nutzungsverträge sowie alle sonstigen Informationen, die für die Projektabwicklung/Betrieb notwendig sind.
- Ein VPN-Gateway muss bereitgestellt werden (Betriebspaket L).
- Dem Zugriff auf das zu betreibende System über eine VPN-Verbindung muss zugestimmt werden (Betriebspaket L).
- Der Kunde muss den Backup Speicher im Netzwerk und den Zugriff darauf bereitstellen (Betriebspaket L).

Bei auftretenden Störungen oder Problemen:

- Rechtzeitige Übermittlung von detaillierten Fehlerbeschreibungen, aktive Mitarbeit bei der Fehlereingrenzung bzw. Fehlerverifikation.
- Benennung eines Ansprechpartners für den Störungsfall.
- Sicherstellung der Kompatibilität der zum Einsatz kommenden Applikationen mit den vorhandenen Betriebssystemversionen.

Werden Mitwirkungspflichten nicht oder nur teilweise erbracht, kann dies terminliche als auch kostenrelevante Auswirkungen haben. Bei Verstoß gegen Mitwirkungspflichten übernimmt die Telekom keine Verantwortung für den Betrieb der Systeme und daraus abgeleitete Forderungen des Kunden bzw. Dritter. Beim Einsatz von Full Disk Encryption (FDE) verpflichte sich der Kunde eine Datensicherung, sowie ein CheckDisk (chkdsk) vor der Einrichtung der FDE vorzunehmen. Die Telekom übernimmt keine Haftung der daraus möglich entstehenden Datenverluste.

5 Vertragslaufzeit, Kündigung und vorzeitige Vertragsbeendigung

5.1 Die Mindestvertragslaufzeiten für den Betrieb (Ziffer 2.3) und für die Serviceleistungen (Ziffer 3) betragen zwei Jahre; sie beginnen mit dem Tag, an dem die Telekom die vertragliche Leistung aufnimmt.

5.2 Das Vertragsverhältnis ist für beide Vertragspartner mit einer Frist von drei Monaten frühestens zum Ablauf der Mindestvertragslaufzeit schriftlich kündbar. Soweit keine Kündigung erfolgt, verlängert sich die Vertragslaufzeit jeweils um ein Jahr, wenn nicht spätestens drei Monate vor ihrem Ablauf schriftlich gekündigt wird.

5.3 Kündigt die Telekom den Vertrag vorzeitig aus einem vom Kunden zu vertretenden wichtigen Grund, ist der Kunde verpflichtet, der Telekom einen in einer Summe fälligen pauschalierten Schadensersatz in Höhe der Hälfte der bis zum Ablauf der vereinbarten Ver-

tragslaufzeit zu entrichtenden restlichen monatlichen Preise zu zahlen. Der Schadensbetrag ist höher anzusetzen, wenn die Telekom einen höheren Schaden nachweist. Er ist niedriger anzusetzen bzw. entfällt, wenn der Kunde nachweist, dass ein wesentlich geringerer oder überhaupt kein Schaden eingetreten ist.

Servicelevel-Parameter Betrieb L

Service-level	Entstörungsfrist	Service-bereitschaft	Störungs-annahme	Reaktions-zeit	Zwischen-meldungen	Termin-vereinbarung
S72	72 Stunden, nicht an Sonn- und Feiertagen	Montag bis Samstag (an Werktagen) 8.00 bis 20.00 Uhr	täglich, 0.00 bis 24.00 Uhr	2 Stunden	nur bei Statusänderung	maximale Zeitspanne von 2 Stunden
S24	24 Stunden, nicht an Sonn- und Feiertagen	Montag bis Samstag (an Werktagen) 8.00 bis 20.00 Uhr	täglich, 0.00 bis 24.00 Uhr	1 Stunde	bei jeder Statusänderung, mindestens alle 4 Stunden	maximale Zeitspanne von 2 Stunden