Leistungsbeschreibung
Customized Network Protect.

Die Telekom Deutschland GmbH (im Folgenden Telekom genannt) bietet mit Customized Network Protect Leistungen zum Schutz von Kundennetzen vor Angriffen aus dem Internet.

1 Konzepte und Workshops

1.1 Konzepte

Die Telekom erarbeitet zusammen mit dem Kunden ein Konzept zur sicheren Anbindung eines Kundennetzwerks über eine managed Network Security Infrastruktur an das Internet.
Für die Realisierung der managed Network Security Infrastruktur wird ein Security PreImplemetation Workshop vorausgesetzt.

1.2 Workshop und Dokumentation

1.2.1 Security Pre-Implemetation Workshop

Die Telekom initiiert vor Realisierung auf Basis eines mit dem Kunden abgestimmten Konzepts zur sicheren Anbindung eines Kundennetzwerks über eine managed Network Security Infrastruktur an das Internet einen Pre-Implemetation Workshop. Resultat des Workshops ist ein Pre-Implemetation Worksheet. Das Pre-Implemetation Worksheet beinhaltet folgende Merkmale:
Rahmenbedingungen der Installation
- IP Design und Topologie Darstellung
- Detaillierter Netzplan
- Konfigurationsparameter
- Beizustellendes Kundenequipment

Das Pre-Implementation Worksheet wird dem Kunden in elektronischer Form übermittelt.

1.2.2 Security Detailkonzept

Bei Vereinbarung mit dem Kunden erstellt die Telekom zusätzlich gegen gesondertes Entgelt auf Basis eines mit dem Kunden abgestimmten Konzepts zur sicheren Anbindung eines Kundennetzwerks über eine managed Network Security Infrastruktur an das Internet ein Detailkonzept.. Das Detailkonzept stellt die technische Dokumentation der im Rahmen der Realisierung beauftragten IT-Security Lösung dar.
Das Security Detailkonzept ist in vier eigenständige Dokumente unterteilt, die wahlweise kombinierbar sind:
- Detailkonzept Firewall;
- Detailkonzept Intrusion Prevention System und Applikationskontrolle;
- Detailkonzept Contentweb und Mail;
- Detailkonzept UTM.

Diese werden dem Kunden in elektronischer Form übermittelt.

1.2.2.1 Detailkonzept Firewall

Das Detailkonzept Firewall beinhaltet die technische Dokumentation einer PAP-Struktur (ein Paketfilter, ein Application Level Gateway, ein Paketfilter) und folgende Merkmale:
- Überblick Systemlösung (Lösungsbeschreibung, Management)
- Anforderungen an die Sicherheit (Virenschutz, WAN-Verbindung, Web-Server, etc.)
- Netzstruktur und -aufbau
- Beschreibung Services, Kommunikation und Regeln (Domain Name System, Beschreibung der Sicherheitskomponenten, d.h. externe und interne FW etc.)
- Beschreibung des Reporting
- Beschreibung des Monitoring/Alarming
- Festlegung der Ansprechpartner für Incident und Changes
- Anhang (Auszug Regelwerk, detaillierter Netzplan)

1.2.2.2 Detailkonzept Intrusion Prevention System und Applikationskontrolle

Das Detailkonzept Intrusion Prevention System und Applikationskontrolle beinhaltet folgende Merkmale:
- Überblick Systemlösung (Lösungsbeschreibung, Management)
- Beschreibung Sicherheit IPS, Signaturen, Regeln etc.

1.2.2.3 Detailkonzept Webcontent und eMail

Das Detailkonzept Webcontent und eMail beinhaltet folgende Merkmale:
- Überblick Systemlösung (Lösungsbeschreibung, Management)
- Beschreibung Virenscan, Proxy, Antispam etc.

1.2.2.4 Detailkonzept Unified Threat Management (UTM)

Das Detailkonzept Unified Threat Management (UTM) beinhaltet folgende Merkmale:
- Überblick Systemlösung (Lösungsbeschreibung, Management)
- Anforderungen an die Sicherheit (AV, Mailsystem, WAN-Verbindung, Web-Server, etc.)
- Netzstruktur & -aufbau
- Beschreibung Services, Kommunikation und Regeln (DNS, Beschreibung der Sicherheitskomponenten, d.h. externe und interne FW, Proxy, Antispam, Mailserver-Security etc.)
- Beschreibung des Reporting
- Beschreibung des Monitoring/Alarming
- Festlegung der Ansprechpartner für Incidents und Changes
- Anhang (Auszug Regelwerk, detaillierter Netzplan).

2 Technologiemodule

Die Telekom verkauft dem Kunden die im Vertrag aufgeführte Security Hard- und Software und installiert sie bei Vereinbarung gemäß Ziffer 3. Die Option auf weiterentwickelte Versionen der Software gehört nicht zum Leistungsumfang dieses Vertrages.
Die Telekom liefert, installiert und betreibt auf Basis eines technischen Konzeptes die für die Sicherheitsinfrastruktur benötigte Hard- und Software.

2.1 Firewall/UTM-Module

Die Firewall- oder UTM-Module sind für die Filterung des Datenverkehrs zwischen verschiedenen Netzwerksegmenten mit unterschiedlichen Vertrauensbeziehungen bzw. unterschiedlichen Security Niveaus notwendig. Der generelle Einsatzort einer Firewall ist daher immer der Übergang zwischen einem LAN und dem Internet. Die Ausfallsicherheit kann mittels einer High Availability Lösung erreicht werden.
Voraussetzung für das Betreiben weiterer Security Module ist ein vorhandenes Vertragsverhältnis über eine Firewall oder ein UTM-Management.

2.2 VPN-Security Module

VPN-Security Module bieten den Schutz der Kommunikationswege zwischen dem Unternehmensnetzwerk und außenliegenden Standorten (z. B. Filialen, mobilen Endgeräten oder bei der M2M Anbindung) wird im Detailkonzept festgelegt. Die Ausfallsicherheit kann mittels einer High Availability Lösung erreicht werden.

2.3 Intrusion Detection- /Intrusion Prevention Module

IDS/IPS Module überwachen Warnungen, die von Sensoren im LAN-Segment hinter der Firewall des Unternehmens erzeugt werden. Gemäß den Sicherheitsrichtlinien werden diese Daten zugelassen oder abgewiesen. Der Monitoring-Service analysiert die Sicherheitswarnungen. Sie werden gefiltert, klassifiziert und mit Blick auf ihre Korrelation überprüft, um Sicherheitsvorfälle zu priorisieren und zu eskalieren.

2.4 Content-Security-Web Modul

Das Content-Security-Web Modul ermöglicht die Überprüfung von Datenverkehr der User am zentralen Gateway auf Virusbefall. Als weitere Option bestehen die Möglichkeiten der Einbindung der URL Filtering, Caching, Proxy sowie SSL Proxy Funktionalität.

2.5 Content-Security-Mail Modul

Das Content-Security-Mail Modul überprüft eingehende Daten am zentralen Gateway oder Mail Forwarder auf Virusbefall und AntiSPAM.

2.6 DMZ-Module
Die Telekom erbringt jeweils nach Vereinbarung im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten gegen gesondertes Entgelt, das sich nach den bei Auftragserteilung gültigen Listenpreisen richtet, folgende Leistungen:

2.6.1 DNS System
Die Telekom verkauft, installiert und betreibt auf Basis des Detailkonzeptes die zur Nutzung des Domain Name Services in firewallgesicherten Netzwerken benötigte Hard- und Software (DNS-Server).
Der DNS-Server kann sowohl als Secondary- als auch als Primary-DNS-Server installiert werden. Die Installation beinhaltet die Eintragung einer Zone; die Eintragung weiterer Zonen erfolgt gegen gesonderte Berechnung.

2.6.2 Loadbalancing Systeme
Die Telekom ermöglicht mit den Loadbalancing Systemen ein- und ausgehende Daten (Web, Mail, etc.) am zentralen Gateway einer Lastverteilung zu unterziehen.

2.7 High Availability
Mit dem High Availability Pack wird die Ausfallsicherheit der Sicherheitsinfrastruktur-Systeme erhöht. Hierzu sind zwei identische Sicherheitsinfrastruktur-Systeme (identische Hard- und Software) erforderlich. Die Voraussetzung für das Betreiben des High Availability Pack ist ein vorhandenes Vertragsverhältnis über ein Firewall-Management.

3 Installation

Die Telekom unterstützt den Kunden mit Hilfe der unter Ziffer 1 (Konzepte und Workshops) beschriebenen Dokumente bei der Zusammenstellung aller für die Installation erforderlichen Angaben zu netzseitigen Parametern wie z. B. IP-Adressen, Netzen und Routing-Tabellen. Die Implementierung beinhaltet eine Konfiguration, die Montage und Installation auf Basis des erarbeiteten technischen Konzepts sowie die Inbetriebnahme.
Die Installation erfolgt durch die Telekom in Abstimmung mit dem Kunden. Die Hardware ist mit der Software, den notwendigen Lizenzen und mit allen zum Betrieb im Kundennetz erforderlichen Daten sowie mit den im Konfigurationsdokument enthaltenen Daten vorkonfiguriert. Die Betriebskonfiguration (Regelwerk) erfolgt im Rahmen der Inbetriebnahme durch die Telekom in Absprache mit dem Kunden und nach Maßgabe der im Security-Workshop (Ziffer 1.2.21) erfassten Positionen.
Die Besonderheiten bezüglich des Betriebes und der Servicezeiten (z. B. Notwendigkeit einer statischen IP-Adresse bzw. Verfügbarkeit des DSL-Anschlusses) bei einem Company Connect, eines DSL Business oder eines asymmetrischen DSL-An-schlusses werden bei Vertragsabschluss vereinbart.
Das Patchmanagement innerhalb eines Releases der installierten Lösung ist in der Dienstleistung enthalten.
Die Installationsleistung im Rahmen von Releasewechseln führt die Telekom gegen gesonderte Berechnung durch.
Die hierzu erforderlichen Arbeiten erfolgen werktags (montags bis freitags) von 8.00 bis 18.00 Uhr in Absprache mit dem Kunden. Dabei ist die Telekom zur Außerbetriebnahme der Sicherheitsinfrastruktur berechtigt.

4 Sicherheitsinfrastruktur-Management

4.1 Grundleistung
Die Telekom überwacht und betreibt aufgebaute Sicherheitsinfrastruktur-Systeme über einen gesicherten Zugang täglich von 0.00 bis 24.00 Uhr.
Als Ersatzzugang für den Betrieb der Sicherheitsinfrastruktur-Systeme kann ein mit dem LAN des Kunden verbundener Zweitweg (ISDN, DSL, MPLS) genutzt werden. Wird der Zweitweg über einen ISDN- oder MPLS Anschluss realisiert, so muss dieser der Telekom während der Vertragslaufzeit ausschließlich für diesen Zweck zur Verfügung stehen.
Der Internet-Zugang, Universal- oder MPLS-Anschluss ist nicht Gegenstand dieses Vertrages. Voraussetzung für das Sicherheitsinfrastruktur-Management ist ein Servicevertrag (s. Ziffer 6) für Hardware und Betriebssystem. Ein Ersatzzugang muss zur Verfügung stehen, um die unter Ziffer 6 beschriebenen Services bei Ausfall der Regelanbindung einhalten zu können.

4.1.1 Monitoring und Reaktion auf Alarme
Wird eine Abweichung von herstellerspezifischen vordefinierten Security Parametern der Telekom erkannt, wird ein Alarm an das zentrale Management-Zentrum der Telekom gesendet.
Die Security Parameter werden mit Abschluss der Konzeptionsphase und Festlegung der Sicherheitsinfrastruktur-Systeme dem Sicherheitskonzept zugefügt.
Bei einer Unregelmäßigkeit der überwachten Security Parameter wird im Management-Zentrum der Telekom ein Alarm ausgelöst und angemessene Maßnahmen eingeleitet.
Die autorisierten Mitarbeiter des Kunden werden mittels E-Mail und/oder Telefonat über die festgestellten Unregelmäßigkeiten, die ergriffenen Maßnahmen und deren Status informiert.
Die gemanagten Security Komponenten kommunizieren über eine gesicherte Verbindung über das Internet mit der zentralen Security Management Installation der Telekom. Hierbei werden ausschließlich Verschlüsselungs- und zertifikatsbasierende Authentifizierungsverfahren eingesetzt.

4.1.2 Backup
Die Telekom erstellt täglich die zur Wiederherstellung der Sicherheitsinfrastruktur-Funktionalität benötigten Daten. Dieses Backup umfasst die im Detailkonzept definierten Router, die Firewall-/UTM Systeme, die DMZ-Systeme und das Betriebssystem der Plattform, auf der die Sicherheitsinfrastruktur-Systeme implementiert sind.

4.1.3 Updates, Patches und Fixes
In Absprache mit dem Kunden führt die Telekom Anpassungen der Firewall- und Betriebssystem-Software an den aktuellen Entwicklungsstand des Herstellers durch. Minor- und Major-Releasewechsel sowie Lizenz-Upgrades sind davon ausgenommen und erfordern eine besondere Beauftragung. Die hierzu erforderlichen Arbeiten erfolgen werktags (montags bis freitags) von 8.00 bis 18.00 Uhr. Dabei ist die Telekom zur Außerbetriebnahme der Firewall berechtigt.

4.1.4 User Helpdesk
Der User Helpdesk der Telekom ist werktags (montags bis freitags von 8.00 bis 18.30 Uhr und samstags von 8.00 bis 13.00 Uhr) erreichbar und kann von autorisierten Mitarbeitern des Kunden in Anspruch genommen werden.

4.1.5 Change Management
Die Telekom nimmt die nachfolgend beschriebenen Änderungen an der Sicherheitsinfrastruktur-Konfiguration innerhalb der nachstehend beschriebenen Kategorien werktags (montags bis freitags von 8.00 bis 18.30 Uhr und samstags von 8.00 bis 13.00 Uhr) vor. Die Änderungsaufträge werden durch einen gesicherten Informationsaustausch zwischen der Telekom und autorisierten Mitarbeitern des Kunden vereinbart und nach ihrer Ausführung dokumentiert.
Änderungswünsche der Kategorie I, die an Werktagen (montags bis freitags) bis 11.00 Uhr eingehen, werden am gleichen Tag bearbeitet. Ansonsten werden die Änderungen am nächsten Werktag bearbeitet.

4.1.5.1 Firewall Module Änderungskategorie I
Dieses Modul beinhaltet bis zu zehn Änderungen der Kategorie I im Monat. Eine Änderung umfasst:
- Anlegen neuer bzw. Löschen bestehender User aus dem Firewall-Regelwerk.
- Anlegen neuer bzw. Löschen bestehender User-Gruppen aus dem Firewall-Regelwerk.

4.1.5.2 Firewall Module Änderungskategorie II
Dieses Modul beinhaltet bis zu zehn Änderungen der Kategorie II im Monat. Eine Änderung umfasst:
- Einpflegen und Ändern von Regeln und Rechten sowie von Netzobjekten.
- Anpassen der Routing-Tabelle an die Erfordernisse des Kunden.

Änderungen der Kategorie II werden am nächsten Arbeitstag durchgeführt.

4.1.5.3 Firewall Module Änderungskategorie III
- Arbeiten im Zusammenhang mit der Implementierung neuer Netzstränge im Kundennetz.
- Ergänzungen des Regelwerkes bzw. implementieren von Services, die über die jeweils gültigen Standard-Dienste der eingesetzten Firewall-Software hinausgehen.
- Anpassungen der Firewall bei der Einrichtung eines VPN's (ausgenommen VPN's zu Systemen, die sich nicht im Management der Telekom befinden). Dies umfasst auch Änderungen und Löschungen.
- Anpassungen der Firewall zum Betreiben einer Dial in-/Dial out-Lösung. Dies umfasst auch Änderungen und Löschungen.
- Inbetriebnahme neuer Interfaces.
- Einrichten einer separaten Authentifikations-Lösung, die über

die jeweils gültigen Standard-Dienste der eingesetzten Firewall-Software hinausgeht. Dies umfasst auch Änderungen und Löschungen.

Diese Änderungen können gegen gesonderte Berechnung auch einzeln beauftragt werden. Änderungen der Kategorie III werden nach Absprache mit dem Kunden durchgeführt.

4.1.5.4 Emergency Request

Das Emergency Request kann nur von einem autorisierten Mitarbeiter des Kunden telefonisch beauftragt werden. Das Request kann nur die Sperrung eines Protokolls bzw. eines Dienstes beinhalten. Die Sperrung wird grundsätzlich für alle Benutzer/Gruppen getätigt/aktiviert.

Die Emergency Requests werden unverzüglich und innerhalb von zwei Stunden nach Eingang und erfolgter Authentifizierung des Requesters implementiert.

Eine Deaktivierung der Sperrung wird als eine normale Änderung der Kategorie I betrachtet. Hierfür gilt die bereits definierte bzw. vertraglich vereinbarte Bearbeitungsdauer.

4.1.5.5 Zusätzliche Firewall Änderungen

Über die Leistungen der Änderungskategorien I bis III und Emergency Requests hinausgehende Änderungen werden gegen gesondertes Entgelt, das sich nach den bei Auftragserteilung gültigen Listenpreisen richtet, durchgeführt.

4.1.5.6 UTM/DMZ Module

Bei den UTM- und DMZ-Modulen (z. B. Content Web Modul/ Content Mail Modul, DNS System etc.) sind alle Änderungen an der Konfiguration im Betriebspaket enthalten.

4.2 Zubuchbare Leistungen (ausschließlich für Ziffer 2.1 Firewall)

Die Telekom nimmt die unter Ziffer 4.1.5 beschriebenen Änderungen an der Sicherheitsinfrastruktur-Konfiguration innerhalb der beschriebenen Kategorien werktags (montags bis freitags) von 8.00 bis 18.00 Uhr vor. Die Änderungsaufträge werden durch einen gesicherten Informationsaustausch zwischen der Telekom und autorisierten Mitarbeitern des Kunden vereinbart und nach ihrer Ausführung dokumentiert.

Änderungswünsche der Kategorie I, die an Werktagen (montags bis freitags) bis 11.00 Uhr eingehen, werden am gleichen Tag bearbeitet. Ansonsten werden die Änderungen am nächsten Tag bearbeitet.

5 Zusätzliche Leistungen

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, insbesondere folgende zusätzliche Leistungen:

5.1 Erstellung eines Security Detailkonzeptes als technische Dokumentation.

5.2 Erweiterte Konzepte

Konzepterstellungen, die über die in die in Ziffer 1.2 beschriebenen Leistungen hinausgehen (z. B. managed Endpoint Security, Fernzugriff, etc.).

5.3 Individuelle Consultingleistungen, die über die in Ziffer 1, 3 und 4 beschriebenen Leistungen hinausgehen.

5.4 Kundenindividuelle Betriebsleistungen, die über die in Ziffer 4 beschriebenen Leistungen hinausgehen.

5.5 Reporting

Der Reporting-Service bietet Kunden die Möglichkeit standardisierte Reports über die Performance ihrer Security-Netzwerkkomponenten abzurufen. Die Reports lassen sich über Filter-Kriterien anhängig von den eingesetzten Security-Komponenten und deren Hersteller individuell gestalten. Ein Download in HTML- und PDF-Datenformat ist möglich.

Standard-Reporting

Für die gemäß Ziffer 2.1 bis 2.6 angebotenen Module erbringt die Telekom Reporting-Leistungen.

Der Umfang des Reportings richtet sich nach dem vom jeweiligen Hersteller für die Appliance definierten Standardreport.

6 Service

6.1 Der Service umfasst die Annahme von Störungsmeldungen, die Instandsetzung der Appliance Systeme, 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 Austausch der Hardware-Komponenten und Einspielen der von der Telekom gesicherten Konfiguration.

Es werden die Servicelevel S72, S24 und S8 angeboten (siehe Servicelevel-Parameter für die Entstörung).

Im Einzelnen erbringt die Telekom folgende Service-Leistungen:

6.1.1 Störungsannahme

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

6.1.2 Servicebereitschaft

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

6.1.3 Reaktionszeit

Die Reaktionszeit ist die Zeit zwischen einer Störungsmeldung durch den Kunden und der Rückmeldung über den Beginn der Aktivitäten der Telekom. Diese Rückmeldung erfolgt in Abhängigkeit des vereinbarten Servicelevels ab der Störungsmeldung. Zeiten außerhalb der Servicebereitschaft werden auf die Reaktionszeit nicht angerechnet.

6.1.4 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.

6.1.5 Terminvereinbarung

Die Telekom vereinbart mit dem Kunden, soweit erforderlich, einen Termin für den Besuch eines Servicetechnikers. Dieser Termin wird mit einer Zeitspanne, die abhängig vom mit dem Kunden vereinbarten Servicelevel ist, angegeben.

Ist die Leistungserbringung aus vom Kunden zu vertretenden Gründen nicht möglich, wird ein neuer Termin vereinbart und die gegebenenfalls zusätzlich erforderliche Anfahrt berechnet. Die Entstörungsfrist verlängert sich entsprechend.

6.1.6 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.

6.1.7 Rückmeldung

Die Telekom informiert den Kunden nach Beendigung der Störung.

6.2 Ausnahmen bei softwarebedingten Störungen

Die Telekom ist von den Servicelevel-Parametern freigestellt, sofern sie nachweist, dass der Mangel auf eine softwarebedingte Störungen (Bug) zurückzuführen ist. Softwarebedingte Störungen sind Störungen, die auf Softwarefehler/Programmierfehler zurückzuführen sind. Hierbei muss eine Reaktion und Interaktion des Herstellers vorrausgehen, damit eine überarbeitete Softwareversion zur Einspielung von Patches/Updates/Upgrades bereitgestellt werden kann.

6.3 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.

7 Pflichten und Obliegenheiten des Kunden

7.1 Um den sicheren Betrieb des Internetgateways durch die Telekom nicht zu gefährden, verpflichtet sich der Kunde,

- von dem gesicherten Netz aus keine weiteren Übergänge in das Internet zu betreiben,
- ein Virenschutzprogramm in aktueller Fassung im Netz zu betreiben und
- auf allen Systemen, die Internetdienste nutzen, stets aktuelle Sicherheitsschutzprogramme zu betreiben.

Die Einhaltung dieser Pflichten ist zwingende Voraussetzung für den sicheren Betrieb des Internetgateways. Die Telekom weist darauf hin, dass ein Schutz des Kundenetzes vor Angriffen aus dem Internet nicht oder nur eingeschränkt vorhanden ist, wenn diese Pflichten verletzt werden. Die Telekom ist in diesem Fall von jeder Haftung freigestellt.

7.2 Der Kunde verpflichtet sich, auf seinem System stets das aktuelle Update der Software einzusetzen. Das Update muss aus Gründen der Kompatibilität mit der Management-Software auf der Telekom-Plattform zuvor von der Telekom freigegeben worden sein. Das Vorliegen des aktuellen Updates ist zwingende

Voraussetzung für die Sicherstellung des fehlerfreien Betriebs von Customized Network Protect. Die Telekom weist darauf hin, dass ein Schutz des Kundenetzes vor Angriffen aus dem Internet nicht oder nur eingeschränkt vorhanden ist, wenn die Installation der Updates unterbleibt. Die Telekom ist in diesem Fall von jeder Haftung freigestellt.

7.3 Der Kunde verpflichtet sich für den Fall und zu dem Zeitpunkt, dass seitens des Herstellers der Hard- oder Software generell keine Pflegeleistungen mehr erbracht werden, („End of Maintenance"), das Nachfolgeprodukt bzw. ein alternatives Produkt einzusetzen. Das Nachfolgeprodukt muss aus Gründen der Kompatibilität mit der Management-Software auf der Telekom-Plattform zuvor von der Telekom freigegeben worden sein. Der Einsatz des Nachfolgeproduktes ist zwingende Voraussetzung für die Sicherstellung des fehlerfreien Betriebs von Customized Network Protect. Der Telekom steht für den Fall, dass der Kunde dieser Verpflichtung nicht nachkommt, das Recht zu, den Vertrag vorzeitig mit einer Frist von zwei Wochen zum Monatsende zu kündigen. Die Telekom weist darauf hin, dass ein Schutz des Kundennetzes vor Angriffen aus dem Internet während dieser Zeit nicht oder nur eingeschränkt vorhanden ist. Die Telekom ist in diesem Fall von jeder Haftung freigestellt, sofern sie nachweist, dass der Mangel bei Installation des Nachfolgeproduktes nicht aufgetreten wäre.

7.4 Der Kunde verpflichtet sich, einen Ansprechpartner zu benennen.

Der Ansprechpartner verantwortet folgende Maßnahmen:

- Sicherstellung des ständigen Informationsflusses zur Telekom
- Bereitstellung der erforderlichen Unterlagen wie aktuelle Netzpläne, aktuelle IP-Adressen, Software-Releasestände der bestehenden Systeme, Konfigurationen der bestehenden Systeme.
- Einplanung und Bereitstellung von kundenseitigen Ressourcen (Personal, etc.) und Sicherstellung des Zugangs für die Telekom zu den für die Systemlösung relevanten Räumen.
- Koordination der kundenseitig erforderlichen Mitarbeit bzgl. der Vor-Ort Installationen
- Bereitstellung der für die Realisierung benötigten passiven Verkabelung und der aktiven Netzwerkkomponenten
- Bereitstellung der benötigten Zugänge und Daten (z. B. Benutzername, Passwort, Lizenzkeys etc.)

7.5 Der Kunde verpflichte sich bei einer auftretenden Störungen zur

- Übermittlung von Fehlerbeschreibungen und der Mitarbeit bei der Fehlereingrenzung bzw. Fehlerverifikation
- Benennung eines Ansprechpartners
- Sicherstellung der Kompatibilität der zum Einsatz kommenden Applikationen mit den vorhandenen Betriebssystemversionen.

8 Vertragslaufzeit, Kündigung und vorzeitige Vertragsbeendigung

8.1 Die Mindestvertragslaufzeiten für das Sicherheitsinfrastruktur-Management (Ziffer 4), für die Zusätzlichen Leistungen (Ziffer 5) und für die Serviceleistungen (Ziffer 6) betragen zwei Jahre; sie beginnen mit dem Tag, an dem die Telekom die vertragliche Leistung aufnimmt.

8.2 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.

8.3 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 Vertragslaufzeit 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 für die Entstörung

Servicelevel	Störungsannahme (Ziffer 6.1.1)	Servicebereitschaft (Ziffer 6.1.2)	Reaktionszeit (Ziffer 6.1.3)	Zwischenmeldungen (Ziffer 6.1. 4)	Terminvereinbarung (Ziffer 6.1.5)	Entstörfrist (Ziffer 6.1.6)
S72	täglich von 0.00 bis 24.00 Uhr	montags bis samstags 8.00 bis 20.00 Uhr, nicht an gesetzlichen Feiertagen	2 Stunden	bei jeder Statusänderung	maximale Zeitspanne von zwei Stunden	72 Stunden[1)]
S24	täglich von 0.00 bis 24.00 Uhr	montags bis samstags 8.00 bis 20.00 Uhr, nicht an gesetzlichen Feiertagen	1 Stunde	bei jeder Statusänderung, mindestens alle vier Stunden	maximale Zeitspanne von zwei Stunden	24 Stunden[1)]
S8	täglich von 0.00 bis 24.00 Uhr	täglich von 0.00 bis 24.00 Uhr	1 Stunde	bei jeder Statusänderung, mindestens alle zwei Stunden	maximale Zeitspanne von zwei Stunden	8 Stunden

1) Ausgenommen an Sonn- und Feiertagen.