Leistungsbeschreibung Business Network Protect.

Die Telekom Deutschland GmbH (im Folgenden Telekom genannt) verkauft, installiert, hält instand und betreibt je nach vereinbartem Leistungsumfang mit dem standardisierten Produkt Business Network Protect (BNP) eine integrative Security-Lösung, die mehrere Infrastruktur-Security-Features in einer Appliance vereint, zum Schutz von Kundennetzen vor Angriffen aus dem Internet.
Diese Leistung wird nur innerhalb Deutschlands angeboten.
Die Dimensionierung richtet sich nach Anzahl der IT-Arbeitsplätze und entsprechender technischer Parameter (z. B. Firewall- oder VPN-Durchsatz) und dem vereinbarten Leistungsumfang für den Betrieb des Gerätes durch die Telekom.
Die Telekom bietet folgende BNP Produktmodule an, die entsprechend den Anforderungen des Kunden auf Appliances der Hersteller WatchGuard und Fortinet beruhen:
- Plug-and-play BNP (nur WatchGuard),
- BNP Classic (WatchGuard und Fortinet).

1 Funktionalitäten

1.1 Firewall-System
Folgende Security-Technologien werden unterstützt:
- Stateful Inspection
- Network Hiding durch NAT und PAT
- Port Forwarding
- IP-basierende Filterlisten

1.2 Content Security
Die eingesetzte Technologie unterstützt
a) Content Web AntiVirus zur Untersuchung des Traffics auf Virus- und Schadcode-Befall
b) Content Web URL-Filter zur Filterung von URLs oder URL-Gruppen
c) Content Application Control zur Untersuchung des Traffics nach typischen Applikationsmustern
d) Content Mail AntiVirus zur Untersuchung des Mail-Traffics nach Viren und Malware-Befall
e) Content Mail Anti Spam zur Kennzeichnung betroffener Mails über Hersteller-Datenbanken oder White/Blacklists
f) Content Mail Type Filter zur Filterung vordefinierter MIME-Types

1.3 Intrusion Prevention System
Über die eingesetzte Appliance ein- und ausgehende Verbindungen werden in Realtime auf bekannte Schwachstellen verschiedenster Betriebssysteme und Applikationen überprüft. Ferner findet eine Anomalieüberprüfung im IPS statt.

1.4 https-Proxy
Installation eines selbstsignierten Zertifikats auf der UTM zum Aufbrechen von SSL-verschlüsseltem Traffics.

1.5 VPN (nur BNP Classic)
Die eingesetzte Technologie unterstützt SSL-VPN und IPSec-VPN.

2 Kauf

Die Telekom verkauft dem Kunden die erforderliche Hard- und Software der Produktmodule, installiert sie bei Vereinbarung gemäß Ziffer 3, betreibt sie bei Vereinbarung gemäß Ziffer 4 und hält sie bei Vereinbarung gemäß Ziffer 6 instand.

3 Installation

3.1 Plug-and-play BNP
Einbinden (Anschalten) der Plug&Play BNP Appliance in die LAN Infrastruktur des Kunden.
Zur Inbetriebnahme muss der Kunde die Plug-and-play BNP Hardware an seinen Router für den Internet-Anschluss anschalten. Plug-and-play BNP baut dann automatisch eine Verbindung über den Internet-Anschluss mit der Plattform auf und erhält, nach erfolgreicher Authentifizierung seine Konfigurationsdaten.

3.2 Business Network Protect Classic
Die Telekom unterstützt den Kunden mit Hilfe eines Konfigurations-Dokumentes (Pre-Implementation Worksheet) bei der Zusammenstellung aller für die Installation von Business Network Protect erforderlichen Angaben zu netzseitigen Parametern wie IP-Adressen, Netzen und Routing-Tabellen. Die Implementierung beinhaltet eine Standard-Konfiguration ohne kundenindividuelle Anpassungen, die Montage und Installation sowie die Remote-Inbetriebnahme.
In Zusammenarbeit mit einem Experten der Telekom werden alle erforderlichen Daten für die Erstellung des Konfigurations-Dokumentes gemeinsam mit dem Kunden erarbeitet. Das Pre-Implementation Worksheet wird genutzt, um evtl. Einschränkungen bzw. Probleme, die später auftreten könnten, auszuschließen bzw. im Vorfeld zu klären.
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 und mit den im Konfigurationsdokument enthaltenen Daten vorkonfiguriert. Die Betriebskonfiguration (Regelwerk) erfolgt durch die Telekom in Absprache mit dem Kunden.
Die Besonderheiten bezüglich des Betriebes und der Servicezeiten bei einem Anschluss (z. B. Notwendigkeit einer statischen IP-Adresse bzw. Verfügbarkeit des DSL-Anschlusses) werden bei Vertragsabschluss vereinbart.

4 Betrieb von Business Network Protect

4.1 Plug-and-play BNP
Die Telekom bietet folgende Betriebspakete an:

4.1.1 Betriebspaket Helpdesk-Service Plus

4.1.2 Einbindung in Managementumgebung
Plug-and-play BNP wird in die Managementumgebung des Betriebszentrums passiv eingebunden.

4.1.3 Release Management (Updates/Patches/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 der Telekom.

4.1.4 Zusätzliche Leistungen
Gegen gesondertes Entgelt, das sich nach den zum Zeitpunkt der Auftragserteilung gültigen Listenpreisen richtet, erhält der Kunde folgende zusätzliche Leistungen:

4.1.4.1 Hotline Unterstützung
Hotline-Unterstützung durch die Experten der Telekom betreffend Installation, Konfiguration und Management von Plug-and-play BNP.

4.1.4.2 ATP/APT Blocker
Die Lösung prüft verdächtige Dateien zunächst auf der eingesetzten Appliance.
Identifizierte verdächtige Dateien werden automatisiert in einer cloudbasierten Sandbox des jeweiligen Herstellers analysiert, emuliert und ausgeführt, um das Bedrohungspotenzial zu bestimmen.
Voraussetzung zur Nutzung des ATP/APT Blockers ist eine gültige herstellerspezifische Lizenz.

4.2 Business Network Protect Classic
Für den Betrieb von Business Network Protect ist beim Kunden eine statische IP-Adresse Voraussetzung. Der entsprechende Internet-Zugang sowie die statische IP-Adresse sind nicht Bestandteil dieser Leistung. Während der Arbeiten an

Business Network Protect ist die Telekom berechtigt, die Appliance außer Betrieb zu setzen.
Die Telekom bietet folgende Betriebspakete an:

4.2.1 Betriebspaket S

4.2.1.1 Einbindung in Managementumgebung
Business Network Protect wird in die Managementumgebung des Betriebszentrums passiv eingebunden.

4.2.1.2 Release Management (Updates/Patches/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 der Telekom.
Gegen gesondertes Entgelt, das sich nach den zum Zeitpunkt der Auftragserteilung gültigen Listenpreisen richtet, erhält der Kunde Hotline-Unterstützung durch die Experten der Telekom betreffend Konfiguration und Management von Business Network Protect.

4.2.2 Betriebspaket M

4.2.2.1 Überwachung / Monitoring
Die Appliance 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. Zusätzlich erfolgt ein Monitoring, welches die Erreichbarkeit der Appliance überwacht.

4.2.2.2 Release Management (Updates/Patches/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 der Telekom.

4.2.2.3 Backup / Restore
Das Betriebszentrum der Telekom erstellt täglich ein Backup der eingesetzten Appliance, welches im Falle eines Restores in ein Austauschsystem eingespielt wird.

4.2.3 Betriebspaket L
Die Telekom betreibt täglich von 0.00 bis 24.00 Uhr für den Kunden proaktiv sein Business Network Protect. Dies beinhaltet zusätzlich zu den unter Ziffer 4.2.2 beschriebenen Leistungen folgende weitere Leistungen:

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

4.2.3.2 Change-Management Kategorie I
Die Telekom nimmt die nachfolgend beschriebenen Änderungen an der Appliance-Konfiguration innerhalb der nachstehend beschriebenen Kategorie während der Regelarbeitszeit(an Werktagen, montags bis freitags, von 8.00 bis 20.00 Uhr) vor. Die Änderungsaufträge werden durch einen gesicherten Informationsaustausch zwischen der Telekom und dem autorisierten Mitarbeiter des Kunden vereinbart und nach ihrer Ausführung dokumentiert.

- Anlegen neuer bzw. Löschen bestehender User aus dem Appliance-Regelwerk
- Anlegen neuer bzw. Löschen bestehender User- Gruppen aus dem Appliance-Regelwerk
- Einpflegen und Ändern von Regeln und Rechten sowie von Netzobjekten
- Anpassen der Routing-Tabelle an die Erfordernisse des Kunden.

Änderungen der Kategorie I, die an Werktagen (montags bis freitags) eingehen, werden innerhalb von sechs Arbeitsstunden bearbeitet.

5 Zusätzliche Leistungen (nur Business Network Protect Classic)
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 Reporting
Das Reporting bietet dem Kunden die Möglichkeit, auf das Reportingtool der Managementsoftware, die zentral im Betriebszentrum der Telekom eingesetzt wird, zuzugreifen. Der Umfang des Reportings richtet sich nach den vom jeweiligen Hersteller definierten Standardreports. Im Standardreporting sind zehn Reports enthalten.

5.2 Hochverfügbarkeit (High Availibility)
Mit Hilfe eines zweiten, gleichen Produktmoduls bietet sich die Möglichkeit des Aufbaus einer Hochverfügbarkeitslösung (Hot Stand By). Fällt z. B. Appliance A aus, so übernimmt die zweite, im Hot Stand By befindliche Appliance B automatisch deren Funktionen.

5.3 Backup-Zugang
Um bei Ausfall des Internetzuganges den Zugang zu den Komponenten und eine qualifizierte Störungseingrenzung denn noch zu ermöglichen, kann ein optionaler Backup-Zugang (mit fester IP-Adresse) für Managementzwecke gebucht werden. Die Funktion des ausschließlich für diese Zwecke bereitgestellten Anschlusses wird regelmäßig von der Telekom überprüft. Anschluss und Router sind nicht Bestandteil der Leistung.

5.4 Kundenindividuelle Leistungen
Die Telekom erbringt bei Vereinbarung weitere kundenindividuelle Leistungen.

5.5 Loadbalancing
Mit der Funktionalität Load Balancing wird im weitesten Sinne ein Mechanismus zum Aufbau eines Server Clusters in einer der angeschlossenen DMZ's abgebildet oder der Verteilung der IP basierenden Anfragen auf einzelne DMZ Server Systeme verstanden. Sofern der Ausfall eines Systems erkannt wird werden die Anfragen automatisch an ein anderes System abgegeben.

5.6 Endpoint Security
Die Telekom betreibt auf Kundenwunsch IPSec oder SSL-VPN Clients mit weiteren Funktionalitäten wie Personal Firewall, AV und AntiSpam. Die betrieblichen Leistungen beschränken sich auf eine zentrale Administration und das entsprechende Management sowie eine Endpoint Kontrolle, ein Support für die jeweiligen Clients ist nicht beinhaltet.

5.7 Change-Management Kategorie II

- 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 Software hinausgehen.
- Anpassungen der Appliance bei der Einrichtung eines VPN. Dies umfasst auch Änderungen und Löschungen.
- Anpassungen der Appliance zum Betreiben einer dial in-/dial out-Lösung. Dies umfasst auch Änderungen und Löschungen.
- Inbetriebnahme neuer Interfaces.

Änderungen der Kategorie II, die an Werktagen (montags bis freitags) eingehen, werden innerhalb von 24 Arbeitsstunden bearbeitet.
Änderungen der Kategorie II werden nach Absprache mit dem Kunden durchgeführt.

5.8 Edge-Management
Die Telekom betreibt auf Kundenwunsch die installierten Edge-Appliances an den Außenstellen und überwacht die Verfügbarkeit der Devices.

5.9 ATP/APT Blocker
Die Lösung prüft verdächtige Dateien zunächst auf der eingesetzten Appliance.
Identifizierte verdächtige Dateien werden automatisiert in einer cloudbasierten Sandbox des jeweiligen Herstellers analysiert, emuliert und ausgeführt, um das Bedrohungspotenzial zu bestimmen.
Voraussetzung zur Nutzung des ATP/APT Blockers ist eine gültige herstellerspezifische Lizenz.

- Betrieb S/M:
  Bei einem erkannten kritischen Security Event wird eine Benachrichtigung an den Ansprechpartner des Kunden gesendet.
- Betrieb L:
  Bei einem erkannten kritischen Security Event, wird eine Benachrichtigung an das Management-Zentrum der Telekom und an den Ansprechpartner des Kunden gesendet.

Innerhalb der in den Servicelevel-Parametern hinterlegten Reaktionszeiten werden die erkannten kritischen Security Events durch das Management-Zentrum der Telekom bewertet und der Ansprechpartner des Kunden über die eingeleiteten Maßnahmen telefonisch informiert.

Dem Kunden wird monatlich ein Reportbericht über die abgewehrten Bedrohungen zur Verfügung gestellt. Der Umfang des Reportberichtes richtet sich nach dem vom jeweiligen Hersteller festgelegten Standard Reporting.

6 Service

Der Service umfasst die Annahme von Störungsmeldungen, die Instandsetzung der Appliance Systems, 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 Erstkonfiguration, die vom Kunden bereitzustellen ist; die ausgetauschte Hardware-Komponente geht in das Eigentum des Kunden bzw. der Telekom über.

6.1 Es werden die Servicelevel S72, S24, S8 und S4 angeboten (Parameter s. untenstehende Tabelle).
Im Einzelnen erbringt die Telekom folgende Service-Leistungen:

6.1.1 Annahme der Störungsmeldung
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 Telekom teilt auf Wunsch innerhalb der für den mit dem Kunden vereinbarten Servicelevel vorgesehenen Zeitintervallen Zwischenergebnisse mit, wenn eine Rückrufnummer angegeben wurde.

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 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 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, sofern sie nachweist, dass ein Angriff aus dem Internet bei Einhaltung der Pflichten nicht aufgetreten wäre.

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 Business 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, sofern sie nachweist, dass der Mangel bei Installation der jeweils aktuellsten Softwareversion nicht aufgetreten wäre.

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 Business 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.

8 Vertragslaufzeit, Kündigung und vorzeitige Vertragsbeendigung

8.1 Die Mindestvertragslaufzeiten für den Betrieb (Ziffer 4) 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 in Textform (z. B. per Brief oder E-Mail) kündbar. Soweit keine Kündigung erfolgt, verlängert sich die Vertragslaufzeit jeweils um ein Jahr, wenn nicht spätestens drei Monate vor ihrem Ablauf in Textform (z. B. per Brief oder E-Mail) 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	Störungs-annahme (Ziffer 6.1.1)	Servicebereitschaft (Ziffer 6.1.2)	Reaktionszeit (Ziffer 6.1.3)	Zwischenmeldungen (Ziffer 6.1.4)	Termin vereinbarung (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	nur bei Statusänderung	maximale Zeitspanne von zwei Stunden	72 Stunden
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
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
S4	täglich von 0.00 bis 24.00 Uhr	täglich von 0.00 bis 24.00 Uhr	30 Minuten	bei jeder Statusänderung, mindestens jede Stunde	maximale Zeitspanne von einer Stunde	4 Stunden