Leistungsbeschreibung
htp Net Business Secure

1 Allgemeines

htp Net Business Secure ist eine Zusatzleistung, die nur bei Beauftragung oder Bestehen eines htp Internetfestverbindungsanschlusses, wie z.B. htp Net Business Direct, beauftragt werden kann. Der Leistungsumfang für das Produkt htp Net Business Secure ergibt sich aus dem Auftrag und dieser Leistungsbeschreibung.

2 Leistungsmerkmale

Um das durch die Festverbindung mit dem Internet verbundene Netzsegment des Kunden gegen unerwünschte Datenübertragungen aus dem und in das Internet zu schützen, betreibt htp an zentraler Stelle ein Security Gateway. Dieses Gateway wird gemeinsam von mehreren Kunden genutzt, die über virtuelle Systeme voneinander getrennt sind. Die Netzsegmente und virtuellen Systeme anderer Kunden auf diesem Gateway gehören per Definition zum Internet.

htp sorgt dafür, dass die erforderlichen Lizenzen für den Softwareeinsatz vorliegen und die eingesetzte Software durch erforderliche Patches und Fixes aktualisiert wird. htp gewährleistet damit nicht, dass eine Penetration des Netzsegments des Kunden vollständig verhindert wird. Auch der Einsatz dieses Security Gateways kann keinen hundertprozentigen Schutz des eigenen Netzwerkes vor unbefugten Zugriffen von außen bieten.

htp stellt mit htp Net Business Secure folgende Security-Dienste bereit:

2.1 Basisleistung: Firewall-Dienst

Der Firewall-Dient ist Bestandteil der Basisleistung. Der Firewall-Dienst filtert ein- und ausgehende Datenpakete auf Basis bestimmter IP-, TCP-, UDP- und ICMP-Protokollmerkmale. Dabei bestimmt eine vom Kunden vorgegebene Regelbasis das Kommunikationsschema zwischen dem internen Netz des Kunden und dem Internet.
Es wird ausschließlich das Internet-Übertragungsprotokoll in der Version 4 (IPv4) unterstützt. Die Kommunikation über IP-fremde Schicht-3-Protokolle (OSI-Modell) wird generell unterbunden.
Die innerhalb einer bestehenden IP Verbindung transferierten IP Pakete werden auf Grund der eingesetzten Stateful Inspection Technik erkannt und durchgeleitet.
Der Kunde teilt htp die initiale Regelbasis zu Vertragsbeginn mit dem von htp zur Verfügung gestellten Dokument „Technische Anlage zur Konfiguration“ schriftlich mit.

2.2 Optionale Leistung: AntiVirus-Dienst

Diese Leistung steht nur zur Verfügung, wenn sie vom Kunden explizit schriftlich beauftragt wurde. Der AntiVirus-Dienst analysiert den http-Datenverkehr mit dem Ziel TCP-Port 80 zwischen dem internen Netz des Kunden und einem Server im Internet. Vom AntiVirus-Dienst erkannte schadhafte Inhalte, wie Viren, Trojaner oder Malware werden am Security Gateway blockiert und nicht in das Netz des Kunden weitergeleitet. Die betroffene Anfrage des Clients wird mit einem entsprechenden Hinweis beantwortet. Verschlüsselte Inhalte, wie passwortgeschützte Archive oder SSL gesicherter Datenverkehr, und Dateien mit einer Größe von mehr als 10 MB werden nicht analysiert und unverändert durchgeleitet.

2.3 Optionale Leistung: URL-Filter-Dienst

Diese Leistung steht nur zur Verfügung, wenn sie vom Kunden explizit schriftlich beauftragt wurde. Der URL-Filter-Dienst analysiert die URLs der http-Anfragen mit dem Ziel TCP-Port 80 aus dem internen Netz des Kunden in Richtung Internet. Nicht erlaubte URLs werden vom Gateway mit einem Hinweis an den anfragenden Client blockiert; erlaubte URLs werden unverändert weitergeleitet.
Der Filter analysiert einzelne Elemente einer Webseite, so dass durch das selektive Blockieren auch nur bestimmte Inhalte einer Webseite nicht angezeigt werden könnten.

htp stellt dem Kunden für die Administration des Dienstes einen Webservice bereit, über den der Kunde die Filtereigenschaften wie folgt konfigurieren kann.

- Kategorie-Filter: Mit diesem Filter können bestimmte Themenbereiche, wie z.B. Pornografie, Gewalt, Jobsuche, freigeschaltet oder blockiert werden. Die Zuordnung einer URL zu einem bestimmten Themenbereich ist vom Hersteller der eingesetzten Software vorgegeben und wird vom Hersteller fortlaufend gepflegt. Für den Filter unbekannte URLs können auf Wunsch blockiert werden.
- URL-Black-List: URL-Einträge der Black-List werden vom URL-Filter generell blockiert. Die Listeneinträge werden vom Kunden vorgenommen und können Wildcardzeichen enthalten.
- URL-White-List: URL-Einträge der White-List werden vom URL-Filter generell weitergeleitet. Die Einträge können Wildcardzeichen enthalten.

Der Zugang zu diesem Webservice erfolgt über eine gesicherte SSL Verbindung. Der Kunde erhält zur Authentisierung von htp einen Benutzernamen und ein Kennwort.

3 IP-Adressen, Routing, NAT

Die offiziellen IPv4-Adressen für das Subnetz des Kunden erhält der Kunde im Rahmen seines bezogenen Internet-Festverbindungsanschlusses. Auf Wunsch des Kunden können die offiziellen IP-Adressen auch auf dem externen Interface des htp Security Gateways terminieren. Die Konfiguration des dann erforderliche NAT-Dienstes („Network Address Translation“) beauftragt der Kunde zusammen mit der Firewall-Regelbasis (siehe Punkt 2.1). Es wird statisches und dynamisches NAT unterstützt.

Der Kunde benennt htp mit der Beauftragung die für die Konfiguration des Dienstes erforderliche IP-Konfiguration (IP-Adressen, Subnetzmasken, Default-Gateway-Adresse für das interne Interface).

4 Service Level Agreement (SLA)

Störungen werden von htp unverzüglich im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten und den nachfolgenden Bedingungen beseitigt. Für die Entgegennahme von Störungsmeldungen und technischen Fragen hat htp Servicerufnummern eingerichtet. Hinsichtlich der Servicebereitschaft, der Reaktions- und der Entstörzeit bietet htp die folgenden Optionen an:

standard Service

Servicebereitschaft	Werktags (außer samstags), 8 - 18 Uhr
Störungsannahme	Hotline: 0800-4877587 (htp plus)
Reaktionszeit	1 Stunde
Entstörzeit	8 Stunden

premium Service

Servicebereitschaft	24x7
Störungsannahme	Hotline: 0800-4872273 (htp care)
Reaktionszeit	1 Stunde
Entstörzeit	8 Stunden

Die Servicebereitschaft ist der Zeitraum, innerhalb der htp zur Durchführung von Instandsetzungsmaßnahmen verpflichtet ist.
Die Reaktionszeit ist der Zeitraum ab Eingang der Störungsmeldung, innerhalb der htp mit der Entstörung beginnt und den Kunden telefonisch über mögliche Fehlerursachen und die voraussichtliche Ausfalldauer unterrichtet. Die Reaktion gilt bei Nichterreichbarkeit des Kunden mit dem Anrufversuch als erfolgt.
Nach Ablauf der Reaktionszeit beginnt die Entstörzeit, innerhalb der htp die Leistung wieder herzustellen hat. Falls Entstörarbeiten über die Zeiten der Servicebereitschaft hinausgehen, werden sie zu Beginn der folgenden Servicebereitschaftszeit fortgesetzt. Nach Beseitigung der Störung erhält der Kunde eine telefonische Abschlussmeldung oder eine Abschlussmeldung von einem Techniker vor Ort. Die Störung gilt bei Nichterreichbarkeit des Kunden mit dem Anrufversuch als beseitigt.

5 Verfügbarkeit

Die Verfügbarkeit der Leistung htp Net Business Secure ist abhängig vom beauftragten Service Level:

Service Level	Verfügbarkeit
basic Service	99,5%
premium Service	99,9%

Die angegebene Verfügbarkeit gilt im Jahresmittel bezogen auf die Zeiten der Servicebereitschaft je Kalenderjahr.
Bei der Option „premium Service“ wird das Security Gateway von htp in einem Cluster aus zwei Knoten betrieben. Dabei befinden sich die Clusterknoten in zwei unterschiedlichen htp Rechenzentren.

htp behält sich das Recht vor, technische Änderungen oder Wartungsarbeiten an ihrem Netz vorzunehmen. Diese bleiben bei der Berechnung der Verfügbarkeit unberücksichtigt. htp wird dabei die Belange des Kunden berücksichtigen und Wartungsarbeiten grundsätzlich in einem außerhalb der üblichen Arbeitszeit liegenden Zeitfenster von 4:00 bis 07:00 Uhr durchführen. htp behält sich vor, diese Wartungszeiten nach angemessener Ankündigung aufgrund technischer oder betrieblicher Erfordernisse zu ändern.