Spezielle Geschäftsbedingungen und Leistungsbeschreibung R-SEC

Teil A: Spezielle Geschäftsbedingungen der R-KOM für R-SEC

1 Geltungsbereich und Definitionen

1.1 Diese speziellen Geschäftsbedingungen R-KOM Regensburger Telekommunikationsgesellschaft mbH (nachfolgend R-KOM) gelten für die Verträge zwischen den Kunden und R-KOM über die Bereitstellung und Überlassung des IT-Security-Systems R-SEC.

1.2 R-KOM erbringt ihre Leistungen ausschließlich auf Grundlage
- des Einzelvertrages,
- dieser Speziellen Geschäftsbedingungen und Leistungsbeschreibung der R-KOM Regensburger Telekommunikationsgesellschaft mbH für die Erbringung der Dienstleistung „R-SEC“,
- der Besonderen Geschäftsbedingungen der R-KOM für Werk- und Dienstleistungen,
- der Allgemeinen Geschäftsbedingungen der R-KOM Regensburger Telekommunikationsgesellschaft mbH.

Im Falle von Widersprüchen gelten die Regelungen in der oben genannten Reihenfolge.

1.3 Das R-SEC-Angebot und diese Bedingungen richten sich ausschließlich an Unternehmer im Sinn von § 14 BGB und gilt unabhängig von sonstigen Leistungen (insb. Telekommunikationsdienstleistungen) der R-KOM.

1.4 Begriffsdefinitionen im Zusammenhang mit den Leistungen von R-SEC ergeben sich aus der Leistungsbeschreibung von R-SEC, die als Teil B diesem Vertrag beigefügt und in vollem Umfang Vertragsbestandteil ist.

2 Zustandekommen des Vertrages

2.1 R-KOM erstellt durch die Ausfertigung des Angebots-/Vertragsblattes „R-SEC“ eine Preis- und Leistungsinformation auf der Basis der Kundenanfrage und übersendet diese zur Unterschrift an den Kunden. Beiliegend erhält der Kunde pro Firewall ein Spezifikationsblatt, in dem die Leistungsmerkmale des R-SEC Dienstes festgehalten sind.

2.2 Das Spezifikationsblatt nennt die vom Kunden gewünschte Konfiguration des Systems. Zusätzlich benennt der Kunde auf dem Spezifikationsblatt eine Liste mit Personen, die autorisiert sind Änderungen am R-SEC Dienst zu beauftragen.

2.3 Der Vertrag kommt durch Unterschrift beider Parteien oder durch einen Kundenauftrag mit nachfolgender Auftragsbestätigung der R-KOM zustande.

2.4 Nach Abschluss des Vertrages sind Vertragsanpassungen und Konfigurationsänderungen für R-SEC durch autorisierte Ansprechpartner des Kunden durch formlosen Auftrag möglich.

3 Leistungen der R-KOM

3.1 Die Leistungen der R-KOM ergeben sich aus der Leistungsbeschreibung von R-SEC (Teil B).

3.2 Zur Sicherstellung einer ordnungsgemäßen Funktion des Systems ist es ausschließlich R-KOM und ihren Mitarbeitern und Erfüllungsgehilfen oder Beauftragten vorbehalten, die Konfiguration des Systems zu erstellen und ggf. zu verändern.

4 Mitwirkungspflichten des Kunden

4.1 Voraussetzung für den Einsatz von R-SEC ist ein permanent verfügbarer Internetanschluss mit mindestens einer festen IP-Adresse pro Firewall-System, die ausschließlich für die Firewall zur Verfügung steht. Diese IP-Adresse muss aus dem Internet uneingeschränkt erreichbar sein. Der Kunde hat dafür zu sorgen, dass diese Voraussetzungen in seinem Betrieb jederzeit erfüllt werden. Für Störungen in diesem Bereich ist der Kunde allein verantwortlich. Bei Nichterreichbarkeit der Firewall bei Anschlüssen, die nicht von R-KOM bereitgestellt sind haftet R-KOM nicht bei Unterschreitung der vereinbarten SLA, nicht bei eingeschränkter Funktionalität der Firewall, wie auch nicht für die über diese Firewall bereitgestellten Anbindungen und Dienste.

4.2 Der Kunde ist nicht berechtigt, Änderungen an dem System ohne Absprache mit R-KOM vorzunehmen oder vornehmen zu lassen. Er hat bei Auftragserteilung Ansprechpartner zu benennen, die autorisiert sind, Änderungen am System bei R-KOM in Auftrag zu geben. Für die Beauftragung von Änderungen im System muss sich der jeweilige Ansprechpartner bei der R-KOM als Berechtigter (Nennung von vereinbarten Kennzeichen) identifizieren. Der Kunde muss bei Änderungen der Ansprechpartner (z.B. beim Verlassen der Firma) dies umgehend R-KOM schriftlich mitteilen. R-KOM haftet nicht dafür, dass der Kunde seine Mitteilungspflicht hier unterlassen hat.

5 Bereitstellung des Firewall-Systems

5.1 R-KOM vereinbart mit dem Kunden einen Termin, zu dem das System an den Kunden übergeben bzw. beim Kunden vor Ort installiert wird.

5.2 Wird das System dem Kunden übersandt oder zur Abholung bereitgestellt, ist der Kunde selbst für die ordnungsgemäße Installation und Inbetriebnahme verantwortlich. Im Übrigen installiert R-KOM das System vor Ort beim Kunden. Nach erfolgter Installation hat der Kunde die ordnungsgemäße Installation und Inbetriebnahme in einer von R-KOM bereitgestellten Inbetriebnahmeerklärung zu bestätigen, wenn nicht wesentliche Mängel vorliegen, die den Kunden zur Verweigerung der Abnahme berechtigen. Äußert sich der Kunde innerhalb einer Woche nach Übergabe der Inbetriebnahmeerklärung nicht, gilt die Installation des Systems als abgenommen. In der Inbetriebnahmeerklärung wird auch der Installationstermin angegeben.

6 Vergütung

6.1 Die Vergütung ergibt sich aus der Preisliste für R-SEC.

6.2 Die Vergütung wird dem Kunden monatlich im Voraus in Rechnung gestellt.

7 Haftung

7.1 Die mit der Nutzung des Internet verbundenen Gefahren und die sich hierdurch für die Kundenumgebung ergebenden Sicherheitsrisiken sind vielfältig und unterliegen einer laufenden Änderung und Weiterentwicklung. R-KOM setzt zum Schutz des Kunden im Rahmen von R-SEC marktgängige, erprobte und ausgereifte Firewall-Systeme ein. Diese Hard- und Software-Systeme basieren auf dem jeweiligen aktuellen Stand der Technik. Dem Kunden ist bekannt, dass es nach dem derzeitigen Stand der Technik nicht möglich ist, Software absolut fehlerfrei herzustellen und zu erhalten. Zudem kann sich die Erkennungs- und Schutzheuristik von R-SEC nach dem derzeitigen Stand der Technik nur gegen bekannte und/oder wahrscheinliche Angriffsszenarien richten, etwaige zukünftige und bisher nicht bekannte Angriffsstrategien können damit nicht erfasst werden.

7.2 Aus diesen Gründen wird ausdrücklich darauf hingewiesen, dass R-SEC keinen vollständigen, 100-prozentigen Schutz gegen sämtliche Angriffe oder Virenbefall oder andere Schäden bieten kann, sondern lediglich das vorhandene Risiko – soweit nach dem derzeitigen Stand der Technik möglich – minimieren kann. R-KOM haftet daher nicht für Schäden aus bisher nicht bekannten Angriffsstrategien, die aufgrund des derzeitigen Stands der Technik von R-SEC nicht erkannt werden konnten.

7.3 R-KOM haftet darüber hinaus nicht für Schäden, die durch den Kunden selbst, insbesondere durch fehlerhafte Installation, Nichteinhaltung der Systemvoraussetzungen oder unbefugte Systemänderungen, oder durch unbefugten Zugriff Dritter, der nicht durch das Firewall-System verhindert werden konnte, verursacht werden.

7.4 Im Übrigen richtet sich die Haftung nach den Bestimmungen in den AGB. Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

8 Datenschutz und Geheimhaltung

8.1 R-KOM wird die jeweils geltenden Datenschutzbestimmungen einhalten. Zum Zweck der Erkennung und Eindämmung von Spam, Viren und anderen Schadprogrammen ist es aber unabdingbar, dass übermittelte Daten zwischengespeichert und geprüft werden. R-KOM wird die Kenntnisnahme von diesen Daten auf das für die Leistungserbringung erforderliche Maß beschränken und dafür Sorge tragen, dass unbefugte Dritte keine Kenntnis von diesen Daten erlangen. Eine Weitergabe solcher Daten an Dritte ist ausgeschlossen.

8.2 Der Kunde erklärt sich ausdrücklich mit einer Kenntnisnahme von übermittelten Daten durch R-KOM zu dem in 8.1 genannten Zweck einverstanden. Er wird hierauf im Auftragsformular gesondert und hervorgehoben hingewiesen.

8.3 Der Kunde ist verpflichtet, die jeweils geltenden Datenschutzbestimmungen einzuhalten. Auf Verlangen wird R-KOM eine den gesetzlichen Bestimmungen entsprechende Datenschutzvereinbarung zeichnen.

8.4 Die Parteien sind verpflichtet, über alle Informationen, insbesondere Geschäfts- und Betriebsgeheimnisse, von denen sie im Rahmen des Vertrags oder anderweitig Kenntnis erlangen, auch nach Beendigung des Vertrags Stillschweigen zu bewahren.

9 Vertragslaufzeit und Kündigung

9.1 Die Mindestlaufzeit des Vertrags beträgt 12 Monate, wenn nicht eine längere Mindestlaufzeit vereinbart wurde.

9.2 Die Kündigung bedarf mindestens der Textform. Maßgebend für die Wahrung von Fristen ist der Eingang bei R-KOM. Mit der Kündigung hat der Kunde den gewünschten Deinstallationstermin zu nennen.

9.3 Die dem Kunden während der Nutzung leihweise überlassenen R-SEC Firewall Systeme werden inklusive allem Zubehör, wie z.B. Netzteile, Kabel und Adapter, abgebaut und an R-KOM zurückgegeben. Bei Nichtrückgabe von Systemkomponenten verrechnet R-KOM die Systeme gemäß der R-SEC Preisliste.

Teil B: Leistungsbeschreibung R-SEC

1 Zielgruppe

1.1 Die R-KOM bietet mit dem Produkt R-SEC ihren Kunden umfassende Schutzmechanismen für die Anbindung Ihrer internen LAN-Netze an das öffentliche Internet an. Darüber hinaus können mit R-SEC kostengünstige und sichere VPN Verbindungen aufgebaut und somit ein sicherer Zugriff von verschiedenen Standorten auf das Firmennetzwerk gewährt werden. Zur Realisierung von R-SEC wird ein Firewallsystem, dass aus einer oder mehreren Firewalls besteht konfiguriert, eingesetzt und gewartet.

2 R-SEC Funktionsumfang und Leistungsmerkmale

2.1 Begriffsdefinitionen:

Firewall: Hardware, die den Datenverkehr zwischen dem Internet und dem Firmennetz überwacht um verdächtige Aktivitäten zu melden und zu blockieren. Der Begriff bezeichnet ein einzelnes Gerät bzw. bei Verwendung von Hochverfügbarkeit ein aus mehreren Geräten bestehendes Cluster.

Netzwerk: Ein Netzwerk beschreibt im Folgenden immer ein IPv4- oder IPv6-Netzwerk, entsprechend ist unter einer IP-Adresse eine IPv4 Adresse oder IPv6-Adresse zu verstehen.

intern wird für das auf Kundenseite liegende, zu schützende Netzwerk verwendet, „extern" für das Netzwerk über das die Verbindung ins öffentliche Internet hergestellt wird.

UTM: Bereitstellung von verschiedenen Sicherheitsfunktionalitäten die gebündelt auf einer Applikationsplattform (hier Firewall-System) verfügbar ist um eine erweiterte Sicherheit für das gesamte Netzwerk zu erhalten.

Dienst: IPv4 oder IPv6 basierter Dienst, dem feste TCP und/oder UDP Portnummern zugeordnet werden können.

Weitere Begriffsdefinitionen sind unter „Anhang-1 – Begriffsdefinitionen" zu finden

2.2 Verfügbare Firewall-Systeme (Produktvarianten)

Zur Realisierung von R-SEC wird dem Kunden während der Vertragslaufzeit ein Firewall System von R-KOM zur Verfügung gestellt, konfiguriert und gewartet, mit dem die im Rahmen des R-SEC Produktes verfügbaren und vom Kunden gewünschten Dienste und Leistungsmerkmale realisiert werden. Die zugehörigen Firewalls werden standardmäßig an den Internetanschlüssen des Kunden betrieben, wodurch für den Kunden bestimmte Pflichten entstehen.

Die Dimensionierung der eingesetzten Firewalls geschieht in Absprache mit dem Kunden und richtet sich nach der Anzahl der zu schützenden Rechner, der Anzahl zu schützender Netze, der Interfaceanzahl und der Bandbreite des Internetanschlusses sowie der sonstigen Anforderungen des Kunden bezüglich der anzuschließenden Systeme und Sicherheitsfunktionalitäten (z.B. dedizierter DMZ-Port, zusätzliche UTM-Service).

2.3 Die Benutzerzahl sowie die für die einzelnen Dienste nutzbare Bandbreite ist abhängig von den jeweiligen verwendeten Basis-Diensten (nur Standard-Firewall-Dienste) sowie zusätzlich gebuchten UTM-Diensten (IPS, AntiVirus, Malware usw.) oder der jeweiligen VPN-Vernetzung. R-KOM kann keine Garantie übernehmen das die in der jeweiligen Produktvariante definierte Firewall alle Leistungen im Zusammenspiel der verschiedenen Funktionalitäten mit der maximalen Performance verarbeiten kann. Die Angaben im Leistungsumfang der jeweiligen Produktvariante basieren auf Messungen und Erfahrungen bezogen auf einer Business-Standardnutzung. Spezielle Kundenanwendungen können zusätzliche Systeme und Firewalls notwendig machen. Ein Upgrade auf eine höherwertigere Produktvariante während der Vertragslaufzeit kann bei Bedarf durch den Kunden beauftragt werden.

2.4 R-SEC stellt dem Kunden, in Abhängigkeit von der gewählten Variante, verschiedene Lösungen und Systemleistungen in den R-SEC Produktvarianten zur Verfügung. Anhang-1 (Produktmatrix R-SEC) stellt eine Übersicht der Leistungsmerkmale der jeweiligen R-SEC Produktvariante dar.

2.5 Eine ausführliche Erläuterung der einzelnen Leistungsmerkmale erfolgt im Anhang-3 (Begriffe - Detailbeschreibung). Für die Produktvariante R-SEC Enterprise werden die Leistungsmerkmale projektbezogen definiert, dokumentiert und sind deshalb nicht in dieser Leistungsbeschreibung aufgeführt.

3 Standardleistungsumfang R-SEC

R-SEC umfasst, in Abhängigkeit von der gewählten Produktvariante gem. R-SEC Produktmatrix, folgende Standard-Leistungen

3.1 Basisleistungspakte – Gültig für alle Produktvarianten

- Bereitstellung der in der Produktvariante definierten Firewall für den vereinbarten Vertragszeitraum
- Grundkonfiguration der Firewall in Absprache mit dem Kunden (Installation, inkl. Festlegung der jeweiligen Firewall-Policies). Die Bereitstellung von Leistungsmerkmale bzw. deren Erstkonfiguration sind dabei im Basispreis im Umfang von maximal einer Arbeitsstunde ohne Aufpreis enthalten.
- Vor-Ort-Installation im R-KOM Einzugsgebiet (ab R-SEC Business) oder Zusendung der Firewall an Standorte innerhalb und außerhalb des R-KOM Einzugsgebiets bei allen sonstigen Produktvarianten.
- Überwachung des Systems an 24 Stunden am Tag und 365 Tagen im Jahr
- Sicherheitsupdates der Firewall sowie Aktualisierung der optional zubuchbaren UTM-Dienste (hierfür ist ein Zugang zum zentralen Updateserver notwendig, wodurch zusätzliche Kosten für die Aktualisierung entstehen können).
- Austausch der Firewall bei einem Hardwaredefekt gemäß dem vereinbarten Service-Level.

3.2 Die Bereitstellung und Konfiguration von zusätzlichen Regeln und Leistungsmerkmale sowie Änderungen in der Basiskonfiguration werden nach der jeweils aktuellen Preisliste R-SEC abgerechnet.

3.3 Leistungspakete UTM (optional zubuchbar)

In Ergänzung können zusätzliche UTM (Unified Threat Management) Funktionalitäten optional zum Standardpaket für alle R-SEC Produktvarianten gebucht werden. UTM Funktionalitäten können nur im jeweiligen Gesamtpaket genutzt werden und sind nicht einzeln zu beziehen. Im UTM Leistungspaket sind die nachfolgend aufgeführten UTM-Standardleistungsmerkmale verfügbar:

- Intrusion Prevention System (IPS)
- Antivirus
- WEB-Filterung
- WEB Rating

Mit der Bereitstellung der UTM-Funktionalitäten reduzieren sich die Leistungs- und Performancewerte der genutzten R-SEC Produktvariante. Weitere Details sind der Produktmatrix (Anhang 1) zu entnehmen. Die Laufzeit des UTM-Leistungspakets richtet sich an die Vertragslaufzeit der jeweiligen Firewall und Produktvariante pro gewähltem Standort.

4 VPN-Konfiguration / Vernetzungslösungen

Für die Anbindung und die Vernetzung von Außenstellen zu einem zentralen Firewall-System sowie für die Integration von Homeoffice-Außendienstmitarbeitern in eine zentrale Sicherheits- und Vernetzungslösung sind die nachfolgenden Leistungsmerkmale optional nutzbar.

4.1 Leistungsumfang IPSEC Site-to-Site VPN

R-KOM konfiguriert eine verschlüsselten IP Verbindung mittels IPSEC zwischen zwei vorgegebenen Standorten (IP Netzen) an denen jeweils eine R-SEC Firewall installiert ist. Die IP-Netze aller beteiligten Tunnel-Endpunkte dürfen sich nicht überschneiden. Die Authentifizierung geschieht via IKE über einen pre-shared Key (PSK).

4.2 Remote Access SSL VPN

Bei dieser VPN Konfiguration können sich z.B. Außendienstleister via SSL über das Internet in das Firmennetz „einwählen". Eine feste IP-Adresse des Einwählenden wird nicht benötigt. Hierfür muss die von R-KOM vertriebene SSL-VPN Client Software verwendet und ihre Installationsvoraussetzungen erfüllt werden. Die Installation und Verwaltung der Client Software ist nicht im Leistungsumfang der R-SEC Produkte enthalten. Für die Realisierung einer SSL-VPN für eine externe Einwahl ist das Leistungsmerkmal Remote Access VPN Token erforderlich.

4.3 Remote Access VPN Token:

Bereitstellung eines Hardware-Token oder Software-Mobile Tokens (elektronische Lizenz) durch die R-KOM. Bei der Bereitstellung eines Software-Mobile Tokens sind mindestens 5 SW-Mobile Token pro zu nutzender VPN-Firewall zu bestellen. Mit dem Token kann eine zweifache Authentifizierung (1. Authentifizierung: Password des Nutzers – 2. Authentifizierung: – Eingangscode des Tokens) durchgeführt werden. Der Kunde hat den Verlust eines Tokens umgehend an R-KOM, für die Sperrung des Zugangstokens, zu melden. R-KOM übernimmt keine Haftung bei Verlust des Tokens und der Nicht-Meldung des Verlusts an R-KOM. Abweichend von der Mindestvertragslaufzeit von 12 Monaten gelten für die Bereitstellung von Mobil-Tokens eine Mindestlaufzeit von 6 Monaten.

5 Bereitstellung

Die zur Realisierung von R-SEC notwendige Firewall wird entsprechend der Konfigurationsangaben des Kunden konfiguriert. Innerhalb des R-KOM Einzugsgebiets wird R-SEC ab der Variante Business durch einen R-KOM Mitarbeiter vor Ort installiert und in Betrieb genommen, ansonsten zugeschickt oder zur Abholung bereitgestellt. Innerhalb und auf Anfrage ggf. auch außerhalb des Einzugsgebiets ist gegen gesonderte Berechnung nach R-SERVICE für alle R-SEC Varianten eine Vor-Ort-Installation möglich. Schnittstelle und Übergabepunkt im Verantwortungsbereich des Kunden sind die Ethernet Ports (LAN-Seite), an denen Equipment betrieben wird, das nicht von R-KOM verwaltet wird.

6 Aktualisierung der verwendeten R-SEC Systeme

Die in den R-SEC Produktvarianten eingesetzten Systeme und Applikationen werden kontinuierlich unter Berücksichtigung von verschiedensten Anforderungen (z.B. Behebung von Sicherheitslücken, Aktualisierung auf neue Versionen, neue Sicherheitsfunktionalitäten) weiterentwickelt. R-KOM hält sich das Recht vor, Änderungen bei den eingesetzten Applikationen / Programmen durchzuführen. R-KOM informiert den Kunden frühzeitig über die notwendigen Änderungen, soweit nicht Gefahr im Verzug ist. Die Aktualisierung betrifft auch den notwendigen Austausch von Systemhardware (Firewalls).

7 Kundennetzwerk

Der Anschluss des Kundennetzwerkes an das Firewallsystem erfolgt über die durch die Konfiguration vorgegebenen Ethernet Ports. Dieser Abschluss entspricht auch dem Demarkationspunkt zwischen dem Kunden und R-KOM für die Bereitstellung des R-SEC Services. R-KOM wird im Netzwerk des Kunden (Lokales LAN) keine Konfigurationen vornehmen. Der Kunde hat bei der Inbetriebnahme, bei Wartungs- und Entstörmaßnahmen, geschultes Personal bereitzustellen. Konfigurationen die sich auf Kundenanschlüsse im lokalen LAN des Kunden auswirken müssen zwischen dem Kunden und R-KOM vereinbart werden. Störungen die sich wegen Änderungen der Kundenkonfigurationen im lokalen LAN ergeben sind keine Störungen gemäß der Definition von R-SEC da der Kunde hier die Verantwortung zur frühzeitigen Meldung und Beauftragung von entsprechenden Konfigurationsmaßnahmen trägt.

8 Zusatzleistungen gegen gesondertes Entgelt

R-KOM erbringt nach Beauftragung im Rahmen der technischen und betrieblichen Möglichkeiten gegen gesondertes Entgelt folgende Zusatzleistungen:

8.1 Konfigurationsänderungen

Änderungen der Basiskonfiguration nach der Erstinstallation werden gemäß der Preisliste R-SEC im 15-Minuten Intervall abgerechnet (jedes angefangene 15-Minuten Intervall wird voll verrechnet). Unter Änderungen fallen alle Konfigurationsänderungen an den verwendeten Firewalls, die nicht durch eine Verlegung, Aktivierung eines Firewall-Dienstes oder ein Produktupgrade bereits abgegolten sind. Änderungen sind z.B. Konfiguration einer zusätzlichen Firewall-Regel, Freischaltung eines weiteren FW-Ports, Anfragen bezüglich der aktuellen Konfiguration oder Tätigkeiten die in Entstörung und Wartung der verwendeten Systeme nicht abgegolten sind.

Die Konfigurationsänderung kann nur durch den im Vertrag hinterlegten autorisierten Ansprechpartner bei der R-KOM beauftragt werden. Bei der Beauftragung einer Änderung muss sich der Beauftragte gegenüber R-KOM authentifizieren.

8.2 Verlegung

Die räumliche Verlegung der R-SEC Firewall liegt im Verantwortungsbereich des Kunden. Die mit einer Verlegung ggf. erforderlichen Konfigurationsänderungen sind vom Kunden, nach der jeweils aktuellen Preisliste R-SERVICE, zu vergüten.

8.3 Höherwertiger Entstörungsservice

Für R-SEC bietet R-KOM auch den Entstörungsservice unter den R-HELP Kategorien mit den zu unter Punkt 8.3 geänderten Serviceparametern für

- R-HELP Grün (Reaktionszeit: 2 Stunden, Regelentstörzeit: 12 Stunden – Servicebereitschaft auch Samstag 6:00 bis 20:00)
- R-HELP Rot (Reaktionszeit: 1 Stunde, Regelentstörzeit: 8 Stunden, Servicebereitschaft – 24 x 7)

an.

8.4 Hochverfügbarkeits-Firewall (High-Availability Configuration)

Ab der Produktvariante R-SEC Business können für redundante Anbindungen und zum Schutz des Ausfalls einzelner Anschlüsse redundante Firewalls bereitgestellt werden. Diese Firewalls können im Betriebsmodus Active/Standby betrieben werden. Umfang und notwendige Konfiguration werden zusammen mit dem Kunden definiert und gegen gesondertes Entgelt abgerechnet.

8.5 Vor-Ort-Service

Vor-Ort-Service wird nach der aktuellen Preisliste R-SERVICE berechnet und ist auf Anfrage auch außerhalb des R-KOM Einzugsgebiets möglich.

8.6 Änderung des Produktvariante:

Die Änderung der Produktvariante (Upgrade) wird nach der aktuellen Preisliste für R-SEC abgerechnet. Mit der Produktänderung beginnt eine neue Mindestvertragslaufzeit. Bei längeren Laufzeiten des bestehenden Vertrags greift die Restlaufzeit.

9 Leistungsstörungen / Service Level Agreement

R-KOM gewährleistet die Erbringung ihrer Leistungen nach dem anerkannten und üblichen Stand der Technik und unter Einhaltung aller anwendbaren Sicherheitsvorschriften für den ordnungsgemäßen Betrieb des Netzes. Die Entstörung inklusive Vor-Ort-Einsatz für R-SEC ist innerhalb des R-KOM Einzugsgebiets kostenlos sofern es sich um einen Defekt der Hardware/Software bei sachgemäßer Handhabung oder um ein durch R-KOM verursachtes Problem handelt. Ansonsten werden Entstörungen oder Vor-Ort-Einsatz nach der aktuellen Preisliste R-SERVICE berechnet. Falls die Ursache einer Störung im Verantwortungsbereich des Kunden liegt, sind die entstandenen Kosten der Entstörung vom Kunden zu tragen. Alternativ zum Vor-Ort-Einsatz kann das Produkt der R-KOM zugeschickt werden.

9.1 Technische Verfügbarkeit:

Die technische Verfügbarkeit für den Service R-SEC beträgt je Standort 99,9 % über das Jahr gemittelt. Die technische Verfügbarkeit beinhaltet nicht die Verfügbarkeit der Zuführungsleistung (Anschluss) zum jeweiligen Standort.

9.2 Störungen an Leistungen von R-SEC werden von R-KOM unverzüglich gemäß den nachfolgend genannten Entstörungsfristen im Rahmen der technischen und betrieblichen Möglichkeiten beseitigt.

9.3 Störungsannahme:

R-KOM -Service-Center-
Tel. 09 41 / 60822 66

9.4 Serviceparameter für R-SEC

Störungsannahme	0:00 Uhr bis 24:00 Uhr an 365 Tagen im Jahr
Servicebereitschaft	$7^{\underline{00}}$ Uhr bis $18^{\underline{00}}$ Uhr von Montag bis Freitag, außer an den gesetzlichen Feiertagen
Reaktionszeit	2 Stunden
Regelentstörzeit	24 Stunden
Wartungsfenster	Täglich - 3:00 Uhr bis 5:00 Uhr 0:00 bis 6:00 am ersten Dienstag im Monat

9.5 Servicebereitschaft:

Unter der Servicebereitschaft sind die Zeiträume zu verstehen, in denen die R-KOM zur Durchführung von Instandsetzungsmaßnahmen verpflichtet ist. Während der Servicebereitschaft

- versucht R-KOM, die Störungsursache vom Betriebsgelände der R-KOM aus zu ermitteln (Ferndiagnose),
- berät die R-KOM den Kunden bei Bedarf telefonisch über geeignete Test- und/oder Fehlerbehebungsmaßnahmen,
- meldet die R-KOM die Störung weiter an Zulieferer und Servicepartner, wenn als Störungsursache ein Fehler in deren Zuständigkeitsbereich zu vermuten ist,
- und sucht R-KOM ggf. den Kundenstandort zur Eingrenzung und Behebung der Störung auf.

9.6 Regelentstörzeit:

Die Regelentstörzeit ist die Zeitspanne, die unter normalen Umständen maximal bis zur Behebung der Störung verstreicht. Die Messung der Regelentstörzeit beginnt mit dem Eingang der Störungsmeldung und endet mit der Behebung der Störung. Die Messung endet auch, wenn der Kunde zur Abstimmung nicht erreichbar ist oder aber die Mitarbeiter der R-KOM sowie deren Servicepartner keinen Zutritt zum Gelände des Kunden oder zu den Installationsräumen der auf dem Kundengelände betriebenen Netztechnik erhalten. Sollte der Eingang der Störungsmeldung außerhalb der vereinbarten Servicebereitschaft erfolgen, beginnt die Messung der Regelentstörzeit mit dem Beginn der nächsten Servicebereitschaftszeit.

9.7 Wartungsfenster:

R-KOM kann Dienste während des Wartungsfensters unterbrechen, wenn dies technisch und betrieblich notwendig ist. Zur Pflege und Wartung der R-SEC Firewall Produkte wird ggf. ein Zeitfenster benötigt innerhalb dessen die Firewall nicht oder nur eingeschränkt verwendet werden kann. Dieses Zeitfenster ist vom Kunden nach Absprache innerhalb der offiziellen R-KOM Servicebereitschaft zu gewähren. Dies ist z.B. für Firmware Upgrades oder größere Konfigurationsänderungen nötig, nach denen ein Neustart durchgeführt werden muss. R-KOM wird sich bemühen die Häufigkeit der Wartung auf ein Minimum zu beschränken.

9.8 Zur Entstörung prüft R-KOM den Anschluss ausschließlich mit dem für R-SEC bereitgestellten Systemkomponenten.

9.9 Absicherung der Regelentstörzeit:

Bei einer von R-KOM zu vertretenden Überschreitung der Regelentstörzeit erhält der Kunde eine Gutschrift bis zur Höhe des monatlichen Grundentgelts für den betroffenen Anschluss, die mit den Forderungen von R-KOM aus diesem Vertragsverhältnis verrechnet wird. Weitergehende Ansprüche des Kunden bestehen nur bei Vorsatz oder grober Fahrlässigkeit.

Anhang 1: R-SEC Produkt-Matrix	Produktvariante		
	Basic	**Business**	**Premium**
FW-System			
Maximale empfohlene Internet Bandbreite (mit FW-Funktion) ***	bis 250 Mbit/s	Bis 500 Mbit/s	Bis 1000 Mbit/s
Anzahl empfohlener Benutzer / Endpoints im LAN	Bis 30	Bis 50	Bis 140
Hardware-Definition			
Interface WAN	1 x GE RJ45	2 x GE RJ45	2 x GE RJ45
Interface intern (Switch-Ports)	4 x GE RJ45	7 x GE RJ45	14 x GE RJ45
DMZ-Port – Anzahl	Nein	Ja – 1 x GE RJ45	2 x 1 GE RJ45
SFP/Optische Übergabe (1 Gbit)	Nein	Nein	4 x SFP / 4 x SFP shared
SFP+ (10GE)	Nein	Nein	2 x SFP+
System-Performance (HW-und Service abhängig)**			
Firewall Durchsatz	3000 Mbit/s	4.000 Mbit/s	10.000 Mbit/s
IPS Durchsatz	800 Mbit/s	1.000 Mbit/s	2.000 Mbit/s
Threat Protection Durchsatz (bei aktivem UTM)	400 Mbit/s	500 Mbit/s	1.000 Mbit/s
IP-SEC Durchsatz	1.000 Mbit/s	4.000 Mbit/s	8.000 Mbit/s
SSL-VPN Durchsatz	200 Mbit/s	600 Mbit/s	1.000 Mbit/s
Leistungsmerkmale**			
Statisches Routing	Ja	Ja	Ja
Port Forwarding	Ja	Ja	Ja
NAT	Ja	Ja	Ja
Dynamisches Routing	Nein	Nein	OSPF, BGP
Policy-based Routing	Ja	Ja	Ja
DHCP Einwahl	Ja	Ja	Ja
DHCP-Server für lokales LAN	Ja	Ja	Ja
DNS-Weiterleitung	Nein	Ja	Ja
VLAN (IEEE 802.1Q)	Ja	Ja	Ja
Multi-WAN	Ja	Ja	Ja
DMZ (Anzahl)	Nein	Ja (1)	Ja (2)
Paketfilter	Ja	Ja	Ja
zeitgesteuerte Regeln	Nein	Ja	Ja
Antivirus (AV)	UTM	UTM	UTM
Intrusion Prevention System (IPS)	UTM	UTM	UTM
Dateityp-Filter	UTM	UTM	UTM
Web-Filter	UTM	UTM	UTM
Web-Rating	UTM	UTM	UTM
Application Control	Nein	UTM	UTM
Logging	Ja	Ja	Ja
Echtzeit Systemüberwachung	Ja	Ja	Ja
Automatische Benachrichtigung per E-Mail	Nein	Nein	Ja
Read-Only Login für Administratoren	Nein	Ja	Ja
Leistungsmerkmale VPN-Konfiguration**			
IPSEC Site-to-Site VPN	Ja *	Ja *	Ja *
Maximale IPSEC Site-to-Site VPN Verbindungen	50	100	1000
SSL Remote-Access VPN	Ja*	Ja *	Ja *
Anzahl Token	20	70	200
SSL Gruppen- und Nutzerverwaltung	Ja	Ja	Ja
Sonstige Leistungsmerkmale			
Transparent L2 Mode	Nein	Ja	Ja
Hochverfügbarkeit möglich	Nein	Ja *	Ja *
Unterbringung der Geräte bei R-KOM	Ja *	Ja *	Ja *
Umgebungsbedingungen	0-40°C, 5-90%rF	0-40°C, 5-90%rF	0-40°C, 5-90%rF
Stromverbrauch	15 W	15 W	40 W

* Durch diesen Service entstehen ggf. weitere Kosten, die Sie der aktuellen Preisliste entnehmen können
** Die Leistungsmerkmale / Performancewerte der jeweiligen Produktvariante sind abhängig davon ob UTM-Dienste zusätzlich aktiviert sind. UTM Dienste und SSL-VPN Verbindungen benötigen entsprechende Performance-Werte der verwendeten Produktvariante (Firewall). Der parallele Betrieb von verschiedenen Leistungsmerkmalen führt zu einer Reduzierung der Leistungsfähigkeit auf den jeweils geringsten Performancewert der genutzten Leistungsmerkmale.
*** Die Bereitstellung der Internetanbindung ist nicht im Leistungsumfang von R-SEC enthalten.

Anhang 2 Abkürzungsverzeichnis:

DHCP	Dynamic Host Configuration Protocol: Protokoll zur automatischen Vergabe von IP-Adressen.
DNS	Domain Name Service: Dienst zur Zuordnung von Domainnamen zu IP-Adressen.
DMZ	Demilitarized Zone: Bezeichnung für ein von der Firewall geschütztes Kundennetzwerk, auf das vom Internet aus kontrolliert zugegriffen werden darf.
FTP	File Transfer Protocol: Protokoll zur Dateiübertragung.
HTTP	Hypertext Transfer Protocol: Protokoll zur Übertragung von Webinhalten.
IKE	Internet Key Exchange: Protokoll zum Schlüsselaustausch beim Aufbau von VPN Verbindungen.
IMAP	Internet Message Access Protocol: Protokoll zum Abholen von E-Mail Nachrichten.
IPSEC	IP Secure: Ein Standard zur Verschlüsselung und Authentifizierung von Daten in IP Netzen.
NAT	Network Address Translation: Bezeichnet allgemein das Umschreiben von IP-Adressen.
OSPF	Open Shortest Path First: Dynamisches Routingprotokoll.
PAT	Port Address Translation: Bezeichnet das Umsetzen von Port und IP-Adresse auf eine andere IP-Adresse.
POP3	Post Office Protocol Version 3: Protokoll zum Abholen von E-Mail Nachrichten.
PKI	Public Key Infrastructure: Infrastruktur bestehend aus der Zertifizierungsstelle und den ausgegebenen Zertifikaten.
PSK	Pre-Shared Key: Geheimer Schlüssel, den nur autorisierten Systeme kennen.
RIP	Routing Information Protocol: Dynamisches Routingprotokoll.
RTP	Real-Time Transport Protocol: Protokoll zur Übertragung von Echtzeitdaten.
SIP	Session Initiation Protocol: Protokoll zum Aufbau von VoIP Verbindungen.
SMTP	Simple Mail Transfer Protocol: Protokoll zum Versenden von E-Mail Nachrichten.
Stateful Packet Inspection	Mechanismus in Firewalls, der Antwortdaten einer vorausgegangenen Anfrage zuordnen kann.
TCP	Transmission Control Protocol: Protokoll zur Übertragung von IP Daten.
UDP	User Datagram Protocol: Protokoll zur Übertragung von IP Daten.
URL	Uniform Ressource Locator: Format zur Spezifikation von z.B. Webadressen, wie http://www.r-kom.de
VLAN	Virtual Local Area Network: Ein virtuelles lokales Netzwerk innerhalb eines physikalischen Netzwerks.
VoIP	Voice-over-IP: Telefonieren über IP-Datennetze.
VPN	Virtual Private Network: Verschlüsselte Zusammenschaltung von IP Netzen.
Zertifikat	Die durch eine Zertifizierungsstelle beglaubigte Identität.

Anhang 3 - Beschreibung Leistungsmerkmale (Detail)

AntiVirus(UTM): Die Firewall bietet die Möglichkeit FTP, HTTP, POP3, IMAP und SMTP Datenströme nach bekannten Virensignaturen zu durchsuchen und ggf. zu unterbinden. Die Virensignaturdatenbank wird regelmäßig über das Internet aktualisiert.
Dateityp-Filter: Mit dieser Option kann die Firewall Dateien welche per FTP-, HTTP-, POP3-, IMAP- oder SMTP-Protokoll übertragen werden anhand ihrer Dateiendung blockieren oder erlauben. So kann z.B. die Übertragung von EXE-Dateien blockiert werden.
DHCP-Server für lokales LAN: Hiermit kann die Firewall den angeschlossenen Geräten (Clients) automatisch IP-Adressen aus einem festzulegenden IP-Netz zuteilen. Voraussetzung ist, dass diese Geräte (Clients) das DHCP Protokoll wie in IEEE RFC 2131 spezifiziert unterstützen.
DNS-Weiterleitung: Mit dieser Option kann die IP-Adresse der Firewall auf den angeschlossenen Geräten fest als DNS zur Namensauflösung eingetragen werden. Die Firewall nimmt die DNS-Anfragen entgegen, leitet sie an die Nameserver des Providers weiter und speichert intern das Ergebnis. Folgende DNS-Anfragen können somit schneller beantwortet werden.
DMZ: DMZ steht für demilitarisierte Zone und bezeichnet ein an die Firewall angeschlossenes, zu schützendes, vom internen abweichendes Netz, auf das vom öffentlichen Internet aus kontrolliert zugegriffen werden soll. Innerhalb dieses kontrollierten Netzes können z.B. öffentliche Webserver betrieben werden. Zum Aufbau einer DMZ ist jeweils ein dedizierter physikalischer Ethernet Port an der Firewall oder eine VLAN-Konfiguration notwendig.
Dynamisches Routing: Bei Bedarf kann die Firewall an einem beim Kunden verwendeten dynamischen Routing-Protokoll teilnehmen. Abhängig vom jeweiligen Typ werden dabei RIP Version 1 und Version 2, OSPF und BGPv4 unterstützt.
Hochverfügbarkeit: Bei dieser Option werden zwei oder mehr Firewalls parallel in einem Cluster betrieben, so dass bei einem Ausfall einer Firewall die jeweils andere Firewall ohne Unterbrechung übernimmt. Größere Firmware Updates können während des Betriebs mit äußerst kurzen Ausfallzeiten durchgeführt werden.
Integrierter Switch: Die Hardware der Firewall verfügt über einen integrierten Layer-2 Switch. Die Anzahl der Switchports ist vom jeweiligen Firewall-Modell abhängig.
Interface Anzahl: Hierbei handelt es sich um die Anzahl der für die Firewall physikalisch sichtbaren Netzwerkschnittstellen innerhalb des Systems. VLANs nach dem Standard 802.1q sind hiervon ausgenommen. Ein integrierter Switch wird von der Firewall wie eine einzelne Netzwerkschnittstelle betrachtet.
Intrusion Detection Prevention(UTM): Ist dieses Leistungsmerkmal aktiv, untersucht die Firewall den durch sie laufenden Datenverkehr nach bekannten Angriffsmustern und kontrolliert die sachgemäße Nutzung bekannter Dienste. Werden hier Unregelmäßigkeiten festgestellt, protokolliert die Firewall den Datenverkehr und kann ihn auch unterbinden. Die hierzu notwendige Datenbank mit Angriffssignaturen wird regelmäßig aus dem Internet aktualisiert.
IPSEC Site-to-Site VPN: Bezeichnet den Aufbau einer verschlüsselten IP Verbindung mittels IPSEC zwischen zwei vorgegebenen IP Netzen an verschiedenen Standorten. Die IP-Netze aller beteiligten Tunnel-Endpunkte dürfen sich nicht überschneiden. Die Authentifizierung geschieht via IKE über einen pre-shared Key (PSK).
Für den häufigen Fall einer sog. „hub-and-spoke“ VPN-Konfiguration bestehend aus einer Zentrale (hub) mit einer oder mehreren Außenstellen (spoke), wobei der Zugriff ins Internet für alle Außenstellen über die Zentrale und deren Firewall erfolgt.
Logging/Reporting: R-KOM erstellt periodisch definierbare Berichte etwa über die Nutzung des WWW, an geblockten Attacken. Diese Berichte stehen dem Kunden anschließend im Kundenportal über einen SSL-verschlüsselten Webzugang zum Download zur Verfügung. Gleichzeitig kann über ein Web Frontend der aktuelle Zustand der Firewall überwacht und Datenströme in Echtzeit betrachtet werden.
NAT: Network Address Translation. Damit ist sowohl die Übersetzung offizieller externer IP-Adressen nach internen (ggf. privaten) IP-Adressen möglich, als auch die sog. Port Address Translation (PAT), d.h. die Zuordnung externer IP-Adressen und Ports zu internen IP-Adressen/Ports. Dieses Leistungsmerkmal steht im Transparent L2 Mode nicht zur Verfügung.
Paketfilter: Über Paketfilter-Regeln können gezielt bestimmte Dienste bzw. IP-Adressen gesperrt oder erlaubt werden. Durch den vorhandenen Stateful-Inspection Mechanismus wird die gesamte Kommunikation in beide Übertragungsrichtungen nach Verbindungsaufbau diesen Regeln zugeordnet und gefiltert.
Policy-based Routing: Ermöglicht das Routing von Paketen nicht nur anhand der Zieladresse, sondern darüber hinaus anhand weiterer Kriterien wie Quell IP-Adresse, Quell-, Zielport oder Protokoll.
Port Forwarding: Hierbei werden Datenströme die an einen bestimmten TCP/UDP-Port der Firewall gerichtet sind, für den Sender unsichtbar an ein konfiguriertes Ziel (IP/Port) weitergeleitet. Das Zielsystem kann sich auch innerhalb des LANs befinden und wäre somit aus dem Internet erreichbar. Dieses Leistungsmerkmal steht im Transparent L2 Mode nicht zur Verfügung. Durch Managementzugänge belegte TCP-Ports der Management-IP-Adresse können abhängig vom Produkttyp ggf. nicht weitergeleitet werden.
Read-Only Login für Administratoren: Mit diesem Leistungsmerkmal erhält der Kunde auf Wunsch einen Benutzernamen und ein Passwort mit dem man sich per HTTPS auf das Webinterface der Firewall einloggen kann. Diesem Benutzer werden ausschließlich Leserechte auf ein Subset der Webinterface-Optionen gewährt. RKOM ist nicht verpflichtet die Nutzer dieses Logins bezüglich der Nutzung des Webinterfaces zu schulen oder zu unterrichten. Diese Obliegenheit und die damit verbundenen Kosten sind ausschließlich vom Kunden zu tragen.
SSL Gruppen- und Nutzerverwaltung: Aufgrund dieser Option kann die Firewall zwischen verschiedenen SSL Remote-Access VPN Gruppen und Nutzer unterscheiden und entsprechend behandeln. Somit können verschiedene Regeln, also Zugriffsrechte, je nach Gruppe verwendet werden. Man kann z.B. der SSL VPN Gruppe EDV andere Rechte einräumen als der Gruppe Vertrieb.
SSL Remote-Access VPN: Bei dieser VPN Konfiguration können sich z.B. Außendienstleister via SSL über das Internet in das Firmennetz „einwählen“. Eine feste IP-Adresse des Einwählenden wird nicht benötigt. Hierfür muss die von R-KOM vertriebene SSL-VPN Client Software verwendet und ihre Installationsvoraussetzungen erfüllt werden. Die Installation und Verwaltung der Client Software ist nicht im Leistungsumfang der R-SEC Produkte enthalten.
Statisches Routing: Ermöglicht das Weiterleiten von IP-Paketen anhand der Ziel-IP-Adresse an fest eingetragene Gateways. Einige Provider stellen ihren Kunden im Businessbereich, Ethernet Schnittstellen und permanenter Layer-3 Verbindung zum Zugangsrouter zur Verfügung. Zu deren Realisierung wird statisches Routing benötigt. Die ggf. zusätzlich beim Provider entstehenden Kosten für eine feste IP-Adresse, Anschlussbereitstellung oder Anschlussnutzung müssen vom Kunden getragen werden.
Transparent L2 Mode: Wird diese Option gewählt, arbeitet die Firewall als Layer-2 Gerät (Bridge) und ist auf Layer-3 nicht sichtbar. Eine bestehende Layer-3 Netztopologie muss demnach nicht verändert werden. Zur Verwaltung der Firewall ist dennoch eine feste IP-Adresse notwendig (siehe Voraussetzungen). Leistungsmerkmale die auf einer Manipulation von Layer-3 Daten basieren (z.B. NAT, Port Forwarding, ...) sind in diesem Modus nicht möglich oder nur eingeschränkt verwendbar.
Echtzeit Systemüberwachung: Das Firewallsystem wird in das zentrale Netzwerkmanagementsystem des R-KOM NOC eingebunden von wo aus Systemparameter 24 Stunden am Tag, an 365 Tagen im Jahr überwacht werden.
Umgebungsbedingungen: Dies sind die von den Herstellern geforderten Umgebungsbedingungen bezüglich Temperatur und nicht kondensierender Luftfeuchtigkeit. Die Geräte sind ausschließlich zur Verwendung in geschlossenen Räumen geeignet. Es ist die Pflicht des Kunden die Hardware nur innerhalb der vorgegebenen Umgebungsbedingungen zu betreiben und für ausreichenden Überspannungsschutz und sachgemäße Handhabung zu sorgen.
Unterbringung der Geräte bei der R-KOM: Hierbei wird die notwendige Hardware zur Realisierung des R-SEC Produkts im Rechenzentrum der R-KOM installiert und betrieben. Für die Unterbringung, Strom und Klimatisierung entstehen ggf. weitere Kosten die auf Anfrage individuell berechnet werden müssen. R-KOM prüft zusammen mit dem Kunden für die Unterbringung bei R-KOM die technische Machbarkeit.
VLAN (IEEE 802.1Q): Die Firewall unterstützt VLAN nach dem IEEE Standard 802.1Q. Über einen 802.1Q fähigen Switch können somit zusätzliche virtuelle Interfaces auf der Firewall geschaffen werden.
Web Filter (UTM): Bietet die Möglichkeit zur Filterung des HTTP-Datenverkehrs. Es können Seiten mit aktiven Inhalten wie Java oder Active-X generell geblockt werden, aber auch konkrete URLs oder Seiten mit bestimmten Schlüsselwörtern können geblockt werden. Über eine Whitelist können bestimmte URLs von dieser Regelung ausgenommen werden.
Web Rating(UTM): Hierbei handelt es sich um eine Erweiterung zur „Web Filter“ Option, die eine Klassifizierung der URLs ermöglicht. Basierend darauf können anschließend Webseiten aufgrund ihrer Klassifizierung (z.B. Pornografie, Malware, Spiele…) geblockt oder erlaubt werden. Mit dieser Erweiterung lässt sich z.B. ein ausreichender Jugendschutz realisieren. Die Klassifizierung geschieht unter Zuhilfenahme einer permanent aktualisierten Datenbank, welche regelmäßig über das Internet aktualisiert wird.
Zeitgesteuerte Regeln: Diese aktivieren oder deaktivieren vorhandene Regeln zu festgelegten Uhrzeiten.