Leistungsbeschreibung
WiTCOM MANAGED FIREWALL

1. ALLGEMEINES

WiTCOM Wiesbadener Informations- und Telekommunikations GmbH (im Folgenden WiTCOM), bietet auf Grundlage der „Allgemeinen Geschäftsbedingungen der WiTCOM GmbH“ und zusätzlich der „Besonderen Geschäftsbedingungen der WiTCOM GmbH für Telekommunikationsdienste“ ihren Geschäftskunden den Service „WiTCOM MANAGED FIREWALL“ an.

1.1 Managed IT-Security Dienstleistungen

Managed Dienstleistungen ermöglichen Kunden ohne bzw. mit nur eingeschränktem Security Know How ein hohes Maß an Sicherheit für deren Netzwerk. Managed IT-Security Dienstleistungen werden in enger Abstimmung mit dem Kunden nach dessen Beauftragung durch WiTCOM durchgeführt. Die hierfür notwendigen Services sind Bestandteil der im Folgenden beschriebenen Leistung.

2. STANDARDLEISTUNG

2.1 WiTCOM MANAGED FIREWALL

Die Dienstleistung WiTCOM MANAGED FIREWALL beinhaltet die mietweise Überlassung eines Firewallsystems pro Kunde für die Vertragslaufzeit.

Die aktuell zum Einsatz kommenden Komponenten verfügen über Schnittstellen (Ethernet, PPPoE) zum Weitverkehrsnetz WAN (Ethernet, PPPoE) und zu lokalen Rechnernetzwerk (LAN).

Die für den Einsatz infrage kommende Firewall Plattform sowie Software werden entsprechend den Anforderungen des Kunden durch WiTCOM ausgewählt und in dem individuellen Angebot von WiTCOM an den Kunden mitgeteilt.

Der Kunde hat weder Anspruch auf Bereitstellung neuwertiger Komponenten oder einer Firewall eines von ihm gewünschten Herstellers, noch hat er Anspruch auf besondere Softwareversionen.

2.2 Konfiguration des Basis Regelwerks

Die WiTCOM MANAGED FIREWALL wird vor Bereitstellung durch WiTCOM entsprechend dem durch den Kunden bei Beauftragung mitgeteilten, individuellen Regelwerk konfiguriert.

Der mögliche Umfang des kundenspezifischen Regelwerks ist von der Leistungsfähigkeit des Firewall Systems abhängig und kann limitiert sein.

Eine spätere Anpassung der Sicherheitseinstellung an geänderte Sicherheitsanforderungen des Kunden kann als zusätzliche Leistung beauftragt werden.

2.3 Installation der WiTCOM MANAGED FIREWALL

Die Standardleistung beinhaltet die Installation der Firewall Komponente vor Ort beim Kunden, bzw. am Kundensystem durch WiTCOM, soweit der Kundenstandort innerhalb des WiTCOM Erschließungsgebietes liegt. Arbeiten an der Inhouse-Verkabelung sind nicht in der Leistung enthalten. Im Übrigen erfolgt die Installation der Firewall Komponenten, entsprechend den bei WiTCOM bzw. bei deren Unterlieferanten zur Zeit der Ausführung gültigen Regeln für die Standardinstallation.

Soll die Installation außerhalb des WiTCOM Erschließungsgebiets erfolgen, stimmt WiTCOM die Vorgehensweise individuell mit dem Kunden ab.

2.4 Softwarepflege der WiTCOM MANAGED FIREWALL

WiTCOM aktualisiert standardmäßig die Firewall-Software (Applikation und Betriebssystem) der betreuten Systeme mit Softwareversionen sofern sie relevant für die Sicherheitsfunktionen des Firewall-Systems sind.

Die Installation der Patches und Updates erfolgt in der Regel unter Berücksichtigung der Betriebssicherheit des Systems und dem korrekten Zusammenspiel aller Komponenten der Security Umgebung. WiTCOM übernimmt keine Garantie für die Qualität der Hersteller-Patches und Updates.

2.5 Störungsbeseitigung

Die Standardleistung beinhaltet den nachfolgend beschriebenen Service. Eine individuelle Servicevereinbarung kann gegen gesondertes Entgelt vereinbart werden.

2.6 Störungsannahme

WiTCOM nimmt Störungsmeldungen täglich von 0.00 Uhr bis 24.00 Uhr unter der Technischen-Hotline-Nummer 08000-948266 (08000-WiTCOM) entgegen. Bei der Störungsmeldung ist es wichtig das WiTCOM folgende Informationen vorliegen: Service-ID, Firmenname, Ansprechpartner, ggf. der Standort (falls es mehrere Lokationen gibt) und die Details der Störung.

2.7 Entstörung

Der Kunde meldet die Störung im Regelfall telefonisch der Hotline unter Angabe seiner Kundendaten, idealerweise unter Angabe der Service-ID.

Nach Meldung der Störung durch den Kunden untersucht WiTCOM die Ursache der Störung und leitet ggf. die Entstörung ein. Wird hierbei festgestellt, dass nicht der Dienst WiTCOM MANAGED FIREWALL, sondern der Internetzugang des Kunden von einer Störung betroffen ist, gilt ausschließlich die für den Internetzugang vereinbarte Regelung zur Störungsbeseitigung.

Wird hierbei festgestellt, dass der Dienst WiTCOM MANAGED FIREWALL gestört ist, wird die erforderliche Entstörung terminlich insbesondere dann abgesprochen, wenn zur Störungsbehebung auf das Kundensystem vor Ort oder remote zugegriffen werden muss.

Während der Servicebereitschaftszeit wird der Kunde nach der ersten Rückmeldung weiterhin regelmäßig über den Stand der Störungsbehebung unterrichtet, sofern er dieses wünscht.

Die Servicebereitschaft besteht täglich von 0 Uhr bis 24 Uhr.

2.8 Remote Diagnose

Geht die Störungsmeldung im Zeitraum Montag bis Freitag, jeweils 8.00 Uhr bis 16.00 Uhr bei der WiTCOM Technische Hotline ein, beginnt eine Remote Diagnose innerhalb einer Stunde, sofern WiTCOM über gültige Zugangsdaten sowie über einen Remote-Zugriff auf das System beim Kunden verfügt. Kann eine Diagnose remote nicht erfolgen, koordiniert WiTCOM mit dem Kunden einen Termin vor Ort. Außerhalb dieser Zeiten, sowie an gesetzlichen Feiertagen, beginnt sie spätestens am nächsten Arbeitstag.

Die Entstörzeit ist auf maximal 24 Stunden begrenzt. Sollte in dieser Zeit der Fehler nicht behoben werden können, kann ein Hardwaretausch veranlasst werden.

Während der Entstörung muss ein Ansprechpartner beim Kunden vor Ort zur Verfügung stehen. Sollte dieser im Bedarfsfall nicht erreichbar sein, wird für diesen Zeitraum die Entstörzeit ausgesetzt.

2.9 Hardwaretausch

Wird im Zuge der Entstörung festgestellt, dass die Fehlerursache ein Hardwaredefekt oder ein anderer, nicht Remote zu behebender Fehler ist, kann ein Hardwaretausch eingeleitet werden.

Der Austausch der betroffenen Hardware erfolgt durch den WiTCOM Service innerhalb von längstens 3 Arbeitstagen.

WiTCOM vereinbart hierzu mit dem Kunden einen Termin. Der Termin wird mit einer maximalen Zeitspanne von zwei Stunden angegeben (z.B. „Zwischen 10.00 und 12.00 Uhr"). Ist der Austausch im vereinbarten Zeitraum aus von dem Kunden zu vertretenden Gründen nicht möglich, wird ein neuer Termin vereinbart und eine gegebenenfalls zusätzlich erforderliche Anfahrt berechnet.

Die Zeit zwischen dem ursprünglich vereinbarten Termin und dem Zeitpunkt des tatsächlichen Hardwaretausches wird nicht auf die Maximal-Frist von 3 Arbeitstagen angerechnet.

3. ZUSÄTZLICHE LEISTUNGEN

WiTCOM erbringt jeweils nach Vereinbarung im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten gegen gesondertes Entgelt insbesondere die folgenden zusätzlichen Leistungen.

Die zusätzlichen Leistungen sind stets separat zu beauftragen. Grundlage ist das individuelle Angebot der WiTCOM an den Kunden, das entsprechend der kundenseitigen Anforderungen erstellt wird.

3.1 Regelwerksänderungen

WiTCOM führt im Auftrag des Kunden individuelle Änderungen seines bestehenden Regelwerks aus. Dieses kann erforderlich werden, wenn sich das Nutzungsverhalten des Kunden ändert oder er ein abweichendes Sicherheitsprofil benötigt.

Die Beauftragung kann ausschließlich per Fax und nur durch einen autorisierten Mitarbeiter des Kunden erfolgen.

Änderungen mit genauer Vorgabe werden im Zeitraum Montag bis Freitag, jeweils 8.00 bis 16.00 Uhr, innerhalb von 12 Stunden eingepflegt. Damit die Änderung noch am gleichen Tag wirksam werden kann, muss der Auftrag bis 12.00 Uhr vorliegen.

Trifft der Auftrag außerhalb dieser Zeiten oder an gesetzlichen Feiertagen ein, erfolgt die Änderung im Lauf des nächstfolgenden Werktages.

Grundlage für die Regeländerungen ist stets ein korrekt und vollständig ausgefüllte Change Request Formular, mit allen erforderlichen Angaben z.B. Source IP Adresse, Destination IP Adresse, Dienst und Schaltanweisung.

Änderungen ohne genaue Vorgabe werden zunächst durch WiTCOM mit dem Kunden technisch geklärt. Ab dem Zeitpunkt, zu dem die Klärung abgeschlossen ist, werden sie wie Änderungen mit genauer Vorgabe behandelt.

Die Anzahl der möglichen Regeln ist begrenzt und hängt von der aktuellen Ausbaustufe der WiTCOM MANAGED FIREWALL ab.

Auf Wunsch berät WiTCOM oder ein Partner den Kunden bei der Definition der individuellen Regelwerksänderungen. Hierbei handelt es sich ebenfalls um eine kostenpflichtige Leistung.

3.2 Upgrade der WiTCOM MANAGED FIREWALL

WiTCOM führt im Auftrag des Kunden die Umstellung einer in Betrieb befindlichen WiTCOM MANAGED FIREWALL auf eine höhere Ausbaustufe durch.

Die Mindestvertragslaufzeit für die geänderten WiTCOM MANAGED FIREWALL erneuert sich im Zeitpunkt der Inbetriebnahme des umgestellten Dienstes WiTCOM MANAGED FIREWALL.

3.3 Managed VPN

VPN's (Virtual Private Network) stellen den sicheren Austausch von Daten innerhalb einer definierten Nutzergruppe sicher.

Managed VPN stellt die Etablierung solcher Nutzergruppen sicher, unabhängig davon, ob der einzelne User über einen Internet Anschluss mit statischen oder mit dynamischen IP Adressen verfügt. Die so entstandenen VPNs sind voll vermascht (any to any). Ein bestehendes Managed VPN kann an die eventuellen Änderungen der Community angepasst werden.

Im Rahmen dieser Dienstleistung richtet WiTCOM auf Wunsch des Kunden ein Managed VPN, basierend auf der WiTCOM MANAGED FIREWALL ein und betreut dieses.

3.4 Managed Content Filtering

Mit dieser Option lassen sich die Zugriffe aus dem Netzwerk des Kunden auf das World-Wide-Web einschränken. Hierzu stehen verschiedene Kategorien zur Verfügung (z.B. Ausschluss von Webseiten mit jugendgefährdenden Inhalten).

Zusätzlich können weitere URL-Adressen individuell festgelegt werden, die unabhängig von der Kategorisierung, nicht angezeigt werden sollen oder für den Zugriff freigegeben werden sollen.

Über nicht zulässige Inhalte hinaus wird der Nutzer mit dieser Zusatzleistung auch vor Phishing Sites, Spyware und Malicious Code geschützt.

Die den Kategorien zugeordneten Internetadressen und schädlichen Webseiten werden regelmäßig überprüft und zentral aktualisiert.

Im Rahmen dieser Dienstleistung richtet WiTCOM auf Wunsch des Kunden die Zusatzleistung Managed Content Filtering auf der WiTCOM MANAGED FIREWALL ein und betreut diese.

3.5 Managed E-Mail Anti Virus und Schutz

Bei dieser Zusatzleistung werden alle für den Kunden eingehenden Mails durch ein zentrales E-Mail Anti Virus Gateway auf böswillige Inhalte gescannt.

Die Mails werden hierbei u.a. auf schädliche Programmtypen wie „Trojanische Pferde", „Hoaxes", „Würmer" und „Visual Basic Script" überprüft:

Das E-Mail Anti Virus Gateway wird zentral gepflegt. und permanent aktualisiert. Verseuchte Mails werden vom Gateway automatisch erkannt und unschädlich gemacht.

Managed E-Mail Anti Virus beinhaltet auch die Erkennung und Markierung von Spam-Mails. Soweit vom Kunde gewünscht, können diese Mails auch direkt nach ihrer Identifikation zentral gelöscht werden.

Im Rahmen dieser Dienstleistung richtet WiTCOM auf Wunsch des Kunden den Dienst Managed E-Mail Antivirus ein und betreut diesen.

3.6 Sonstige Leistungen

Sonstige Dienstleistungen (z.B. Arbeiten an der Inhouse-Verkabelung) können individuell zwischen dem Kunden und WiTCOM vereinbart werden.

4. Bereitstellung

Die Bereitstellung der WiTCOM MANAGED FIREWALL erfolgt innerhalb von vier bis sechs Wochen nach technisch geklärtem Auftragseingang.

5. PREISE UND ZAHLUNGSBEDINGUNGEN

WiTCOM erhebt eine einmalige Pauschale für die Bereitstellung und Konfiguration der WiTCOM MANAGED FIREWALL sowie einen monatlichen Grundpreis für das Management der WiTCOM MANAGED FIREWALL. Das Gleiche gilt für die Bereitstellung und Nutzung der zusätzlichen Leistungen.

Die Preise für die beschriebenen Leistungen ergeben sich aus dem individuellen Angebot der WiTCOM an den Kunden. Grundlage für die Berechnung aller Preise ist der mit der individuellen Leistungserbringung verbundene Aufwand (Material und Zeit). Sämtliche Preise verstehen sich netto, zuzüglich der gesetzlichen Mehrwertsteuer.

Die Rechnungsstellung erfolgt in der Regel monatlich, sofern nicht etwas anderes vereinbart wurde. Soweit eine monatliche Grundgebühr zu zahlen ist, ist diese jeweils zum Ersten eines jeden Monats fällig und wird entsprechend in Rechnung gestellt. Sofern eine einmalige Installationsgebühr erhoben wird, wird sie mit der ersten Rechnung für Leistungsentgelte in Rechnung gestellt. Die Rechnungsbeträge werden mit Zugang der Rechnung fällig und sind sofort ohne Abzug zahlbar.

6. MINDESTVERTRAGSLAUFZEIT

Die Vertragslaufzeit beginnt mit dem Tag der Inbetriebnahme der WiTCOM MANAGED FIREWALL. Die Mindestvertragslaufzeit beträgt 24 Monate. Nach Ablauf der Mindestvertragslaufzeit kann der Vertrag schriftlich mit einer Frist von 3 Monaten zum Ende der Laufzeit gekündigt werden. Andernfalls verlängert er sich um weitere 12 Monate.

7. GEWÄHRLEISTUNG

WiTCOM übernimmt die Gewähr für den technisch korrekten Ablauf ihrer hiermit angebotenen Dienstleistungen gemäß dem gegenwärtigen Stand der Technik. Firewall-Systeme erhöhen den Sicherheitsstandard eines Netzwerkes, können jedoch aufgrund der sich ständig weiterentwickelnden Angriffstechniken keinen 100%igen Schutz bieten. WiTCOM übernimmt daher keine Gewährleistung für den Umfang des Schutzes eines Netzwerkes gegen Angriffe von innen oder außen. Eine Garantie oder die Zusicherung von Eigenschaften des Firewall-Systems wird durch WiTCOM nicht erteilt.

8. HAFTUNG

Firewall-Systeme erhöhen den Sicherheitsstandard eines Netzwerkes, können jedoch aufgrund der sich ständig weiterentwickelnden Angriffstechniken keinen 100%igen Schutz vor Angriffen auf das Netzwerk bieten. WiTCOM schließt daher jede Haftung für Schäden, die aus Angriffen Dritter auf das Netz des Endkunden resultieren, grundsätzlich aus.

Virus Scanner erhöhen den Schutz des eigenen Netzes vor der Infektion mit böswilligen Softwaretools. Dennoch kann dadurch kein 100% Schutz gewährleistet werden. Eine Haftung für evtl. auftretende Schäden wird resultierend daraus grundsätzlich ausgeschlossen.

Die Haftung für vertragliche Pflichtverletzungen sowie aus Delikt ist auf Vorsatz und grobe Fahrlässigkeit sowie den typischerweise entstehenden Schaden beschränkt. Dies gilt nicht bei der Verletzung von Leib, Leben und Gesundheit und Ansprüchen wegen der Verletzung von Kardinalpflichten. Insoweit haftet WiTCOM für jeden Grad des Verschuldens. Soweit es um Schäden geht, die nicht aus der Verletzung von Leib, Leben und Gesundheit resultieren, haftet WiTCOM aber nur für den typischerweise entstehenden Schaden.

Die Haftung für mittelbare Schäden und Mangelfolgeschäden, wie z.B. entgangenen Gewinn oder mangelnden wirtschaftlichen Erfolg, ist ausgeschlossen. Die vorstehenden Haftungsbeschränkungen gelten entsprechend für Mitarbeiter und Erfüllungsgehilfen der WiTCOM.

9. DATENSCHUTZ

WiTCOM verpflichtet sich, die Vorgaben des Telekommunikationsgesetzes (TKG), des Teledienstegesetzes (TDG) und des Teledienstedatenschutzgesetzes (TDDSG) zu beachten, sowie das Fernmeldegeheimnis zu wahren.

WiTCOM verpflichtet sich, ihre Mitarbeiter auf das Datengeheimnis zu verpflichten, sie insbesondere zuvor über die Pflichten aus dem Bundesdatenschutzgesetz (BDSG) und sonstiger Datenschutzvorschriften zu belehren, sowie einen IT-Sicherheitsbeauftragten zu benennen.

WiTCOM verpflichtet sich, die aus dem Projekt bekannt werdenden Daten des Kunden, insbesondere die personenbezogenen Daten im Sinne des BDSG, ausschließlich nur für die Erfüllung der Zwecke dieses Vertrages zu verwenden, das Datengeheimnis zu wahren und die eigenen Mitarbeiter entsprechend zu verpflichten. Diese Verpflichtung gilt umgekehrt in gleichem Maß für den Kunden.

WiTCOM verpflichtet sich, die erforderlichen technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes zu ergreifen und aufrechtzuerhalten sowie dem Kunden bei Bedarf und auf Anforderung nachzuweisen.

Es wird klargestellt, dass im datenschutzrechtlichen Sinne der „Herr der Daten“ der Kunde bleibt. Insoweit liegt nach dem Willen der Parteien eine privilegierte Datenverarbeitung im Auftrag gemäß § 11 BDSG 2001 vor. Infolgedessen ist zwar WiTCOM während der Laufzeit der projektbezogenen Einzelverträge zur Verarbeitung und Verwendung der Daten des Endkunden berechtigt, jedoch nur im Rahmen der Geschäftsbesorgung aus den jeweiligen projektbezogenen Einzelverträgen.

Ansonsten bleibt der Kunde auch hinsichtlich des Eigentums an diesen Daten Alleinberechtigter, so dass er berechtigt ist, jederzeit über WiTCOM die Herausgabe seiner sämtlichen, eventuell vorhandenen Daten zu verlangen. Für diesen Fall steht WiTCOM kein Zurückbehaltungsrecht zu. Entsteht mit dem Herausgabeverlangen ein nicht unerheblicher zusätzlicher Aufwand, kann WiTCOM den so entstehenden Aufwand nach den Stundensätzen der Preisliste berechnen.

WiTCOM ist berechtigt, einen Unterlieferanten mit der Bereitstellung von Teilen dieses Dienstes zu beauftragen. In diesem Fall verpflichtet WiTCOM sich, in seinem Vertragsverhältnis mit dem Kunden die vorstehenden Vereinbarungen zum Datenschutz weiterzugeben und sämtliche schriftlich zu erteilende fachliche Weisungen des Endkunden unverzüglich und ohne Änderung an den Unterlieferanten weiterzuleiten.

10. EIGENTUM

WiTCOM bleibt Eigentümerin der für die Vertragslaufzeit mietweise überlassenen Firewall Hardware. Die für die Laufzeit gemieteten Systeme unterliegen den jeweiligen Lizenzbestimmungen des Herstellers. Bei Kündigung des Vertrages ist die Firewall Hardware in der Originalkonfiguration an WiTCOM zu übergeben. Der Kunde haftet für jede von ihm oder von Dritten, für die er einzustehen hat, verschuldete Beschädigung der mietweise überlassenen Hardware.