Pro Net Managed Security

LEISTUNGSBESCHREIBUNG

1. Allgemeines

1.1 AGB

Für alle in Anspruch genommenen Dienstleistungen und Produkte gelten die Allgemeinen Geschäftsbedingungen, im Folgenden AGB genannt, der NetAachen GmbH, im Folgenden NetAachen genannt.

Im Falle von Widersprüchen gehen jedoch die nachfolgenden Bestimmungen vor.

1.2 Gegenstand und Bezüge

Die folgenden Ausführungen beschreiben das Produktbündel „Pro Net Managed Security (MS)" mit seinen zugeordneten Produkten und im Zusammenhang stehenden aktuell gültigen Auskünften und Störungsbeseitigungen.

Alle Leistungsmerkmale der Produkte, die fortfolgend aufgeführt werden, sind ausschließlich für diese Angebote gültig. Kein Merkmal ist auf andere Produkte, Merkmale oder Produktbündel übertragbar.

NetAachen behält sich im Zuge technischer Neuerungen und Weiterentwicklungen vor, Merkmale oder Produkte durch bessere oder gleichwertige, für den Kunden kostenfrei, zu ersetzen.

1.3 Dokumentation

Für die Dienstleistung und die genutzten Systeme stellt NetAachen nach eigener Wahl dem Kunden eine Nutzerdokumentation in elektronischer und/oder gedruckter Form zur Verfügung. Die Nutzerdokumentation bezieht sich auf die Installation und Konfiguration beigestellter NetAachen-eigener Systeme sowie zur Installation und Konfiguration kundeneigener Systeme in Verbindung mit NetAachen Leistungen.

1.4 Löschung von Daten

Umgehend nach vollständiger Beendigung des Vertragsverhältnisses zwischen dem Kunden und der NetAachen werden alle Daten, welche in Bezug zu dem Produkt stehen oder durch den Betrieb des Produktes entstanden sind, gelöscht.

Dies gilt auch für Daten des Kunden, die an Vertragspartner der NetAachen weitergegeben wurden.

1.5 Abnahme

Nach Beendigung aller zum Produkt zugehörigen Arbeitsschritte wird der Kunde über die Vollendung der Installation informiert.

Die Benachrichtigung erfolgt in Textform oder in Form von Internet Mail und fordert den Kunden zur Abnahme der Installation auf.

Ist innerhalb von 10 Werktagen nach Aufforderung zur Abnahme keine Reklamation von Seiten des Kunden bei der NetAachen eingegangen, die eine erhebliche Beeinträchtigung oder Fehlfunktion der Dienstleistung oder des Systems zeigt, so wird dies als stillschweigende Abnahme verstanden.

Im übrigen gelten die Regelungen der Ziff. 4.1 der AGB hinsichtlich Prüfung der vertraglichen Leistung und Mängelanzeige.

2 Managed Security Services

2.1 Bringing Into Service

2.1.1 Anforderungen

Es werden alle Anforderungen des Kunden im Dialog mit einem Techniker der NetAachen aufgenommen und mit der technischen Machbarkeit der ausgewählten Komponenten abgeglichen.

Alle notwendigen Informationen zur vertragsgemäßen Installation müssen der NetAachen auf Anfrage bereitgestellt werden.

Können wesentliche Voraussetzungen in dieser Phase nicht erfüllt werden, so können beide Vertragspartner aus dem bereits bestehenden Vertrag austreten.

Für den Vertragspartner entstehen die Kosten für die in Stunden geleisteten Aufwendungen während der Aufnahme der Anforderungsdefinition.

Die Anforderungen können in einem Workshop gemeinsam mit dem Vertragspartner erstellt werden. Die Kosten für den Workshop werden individuell veranschlagt.

2.1.2 Konfiguration

Die mit der Anforderungsdefinition ermittelten Regeln, Parameter und Komponenten werden durch NetAachen in einen betriebsfähigen Zustand gebracht.

2.1.3 Penetrationstest

Die installierten Komponenten werden einem Penetrationstest unterzogen. Dieser Test stellt sicher, dass die beauftragten Komponenten richtig und sicher installiert wurden.

Der Penetrationstest entspricht im Wesentlichen den einzelnen Tests des Security Check.

2.1.4 Auslieferung

Alle Komponenten werden dem Vertragspartner auf dem Postweg zugestellt. Soll von dieser Regelung abgewichen werden, so werden die Kosten für den Transport gesondert berechnet.

2.1.5 Installation

Die Installation der ausgelieferten Komponenten und Software wird von einem Mitarbeiter des Vertragspartners durchgeführt.

Auf Wunsch wird ein Servicetechniker zur Verfügung gestellt, welcher fernmündlich die Installation begleitet.

Die Installation durch einen Mitarbeiter des Vertragspartners bezieht sich ausschließlich auf den physikalischen Anschluss der gelieferten Komponenten und/oder auf das menügeführte Installieren von Software auf einem Client.

Alle weiteren Konfigurations- und Installationsschritte werden per Fernadministration durchgeführt.

Soll die Installation der Hardware und/oder Software vor Ort von einem Servicetechniker der NetAachen durchgeführt werden, so sind Reisekosten und alle weiteren Kosten, welche von der Ferninstallation abweichen, vom Vertragspartner zu übernehmen.

2.1.6 Abnahme

Der Vertragspartner erhält ein Testprotokoll sowie einen Installationsbericht über die vertraglich vereinbarte Konfiguration, welche durch die Anforderungsdefinition vereinbart wurde.

Vor der Abnahme wird ein Termin mit einem Servicetechniker der NetAachen vereinbart. Die Abnahme erfolgt unter Einbeziehung eines Mitarbeiters des Vertragspartners.

Es können mehrere Abnahmetermine vereinbart werden.

Der Vertragspartner hat während der Abnahme zu prüfen, ob alle Systeme erwartungsgemäß reagieren und arbeiten.

Sollten Störungen auftreten, welche durch falsche oder fehlende Regeln in der Firewall, im Content Filter oder im VPN verursacht werden, so werden diese innerhalb eines Zeitraums von 20 Werktagen kostenfrei behoben.

2.2 Firewall

Die Firewall arbeitet als Filter zwischen Internet und dem Organisationsnetzwerk des Vertragspartners. Die Firewall verfügt über ein Regelwerk, welches die Filtereigenschaften gemäß der Security-Policy und den Netz- und Systemvoraussetzungen des Vertragspartners abbildet.

Das Regelwerk definiert die Zugriffsmöglichkeiten auf Ressourcen vom Organisationsnetzwerk zum Internet und vom Internet auf Ressourcen des Organisationsnetzwerkes.

Der Aufbau gewährleistet den ausschließlichen Transport von Daten durch die Firewall. Ein Transfer von Daten über einen anderen Kanal ist nicht möglich.

Die Filter- und Transportregeln beziehen sich auf die OSI-Schichten 2 und 3 (IP/ICMP,TCP/UDP) und können bei Bedarf angepasst werden. Die Firewall arbeitet zum Transport der Datenpakete ausschließlich mit den Networklayer 3 Protokollen IP, ICMP und den Transportlayer 4 Protokollen TCP und UDP. Zum Transport anderer Protokolle muss eine IP-Encapsulation eingesetzt werden. Siehe hierzu auch Virtual Private Network.

Mögliche Angriffe, welche sich auf IP/ICMP (Netzwerklayer) oder TCP/UDP (Transportlayer) beziehen, werden innerhalb der Firewall erkannt und abgewehrt. Dies gilt für Angriffe auf die Firewall und die zu schützenden Netzwerke. Angriffe aus dem Organisationsnetzwerk auf die Firewall, sowie Angriffe aus dem Organisationsnetzwerk auf andere Netzwerke, welche über die Firewall erreicht werden, werden erkannt und abgewehrt.

Der IP-Router, welcher der Verbindung zum Internet dient, befindet sich aus Sicht des Organisationsnetzes im Internet und vor der Firewall. Somit ist ein Schutz des Routers vor Angriffen nicht gegeben.

Die Firewall bietet keinen Schutz vor Viren oder anderem schädlichem Code (Malicious Code), welcher auf den OSI Layern 5 und 6 verbreitet wird. Siehe hierzu auch Content Filter.

Datentransfers, welche nicht durch die Firewall transportiert werden, entziehen sich der Kontrolle durch die Firewall. Der Vertragspartner muss sicherstellen, dass keine andere Internetverbindung existiert, welche die Firewall umgeht, wie z.B. Modems mit Anbindung an andere Netzwerke oder Wireless-LANs.

2.2.1 Schnittstellen

Die Firewall verfügt über mindestens 2 physikalische Layer-2-Schnittstellen, welche als Ethernet (IEEE802.3, 10/100baseTx) ausgeführt sind.

Der Betrieb von einer oder mehreren DMZ setzt ein Modell voraus, welches über mindestens 3 Ethernet Schnittstellen verfügt.

Andere Layer 2 Protokolle als Ethernet werden nicht unterstützt. Die Anbindung von Netzen, welche über andere Netzzugangsprotokolle eingebunden werden sollen, erfolgt über Medienkonverter oder Router. Diese Geräte sind nicht Bestandteil der Firewall und müssen separat beauftragt werden.

Folgende Tabelle gibt Aufschluss über die verwendeten Schnittstellen je Modell und der maximalen Bandbreite bezogen auf alle Interfaces.

Produkt	Bandbreite	Schnittstelle	DMZ
NetScreen-5GT	20 MBit/s	10/100baseTx	nein
NetScreen-25	100 MBit/s	10/100baseTx	ja (2)

Beim Einsatz anderer Modelle als den hier aufgeführten gelten die entsprechenden Schnittstellenparameter des jeweilig eingesetzten Systems.

2.2.2 Filter

Gemäß der Security-Policy des Vertragspartners werden Filterregeln für die Firewall konfiguriert.

Durch die Firewall werden die IP-Netze kontrolliert, welche über die Layer-2-Schnittstellen der Firewall IP-Pakete transportieren.

Das Regelwerk des Filtermechanismus arbeitet auf der Ebene von IP-Netzen, IP-Nummern, ICMP Typen, TCP/UDP Ports und TCP/UDP Port Bereichen.

Die Regeln können für eingehende und ausgehende Datenpakete definiert werden.

Ein von der Tageszeit abhängiges Regelwerk ist konfigurierbar.

Das Regelwerk ist so aufgebaut, dass ein Datenpaket von einer Startadresse zu einer Zieladresse abgelehnt oder durchgelassen wird. Eine Ablehnung erfolgt explizit (Reject), indem ein ICMP Reject an den Absender gesendet wird oder ohne Rückmeldung an den Absender (Silent Deny). Die Anzahl der Regeln ist je Firewall auf 100 Stück begrenzt

2.2.3 Überwachung

Die Firewall arbeitet mit einer permanenten Intrusion Detection, welche Angriffsversuche erkennt, protokolliert und je nach Stärke des Angriffs die Administration informiert.

2.2.4 NAT/PAT

An der Layer 2 Schnittstelle, welche die Verbindung zum Internet darstellt, wird bei Bedarf eine IP-Network Adresstranslation (NAT) durchgeführt.

Die Adresstranslation kann für eingehende und ausgehende Verbindungen konfiguriert werden.

Es steht statische und dynamische NAT zur Verfügung.

Die dynamische NAT wird durchgeführt, wenn es sich bei den IP-Nummern im Organisationsnetz des Vertragspartners um private IP-Netze nach RFC-1918 handelt oder die IP-Netze aus dem offiziellen Adressraum des Internets stammen aber einem AS zugeordnet sind, welches nicht dem Vertragspartner gehört und kein AS der NetAachen ist.

Die statische NAT wird verwendet, wenn externe IP-Adressen auf interne IP-Adressen abgebildet werden müssen, um einen Zugriff auf organisationsinterne Ressourcen zu ermöglichen.

Bei statischer NAT ist eine Abbildung von externer Adresse mit beliebigem Port auf eine interne Adresse mit definiertem Port möglich (Port Adress Translation).

2.2.5 DMZ

Die demilitarisierte Zone (DMZ) ist ein kostenpflichtiger optionaler Service und steht nur bei entsprechend gekennzeichneten Produkten zur Verfügung. Die Kosten werden je eingesetztem Interface erhoben, welches als DMZ eingesetzt wird.

Die DMZ wird zum Betrieb von Diensten verwendet, welche sowohl aus dem Organisationsnetz als auch aus dem Internet erreichbar sein sollen.

Durch das Auslagern von Diensten in die DMZ werden diese Dienste außerhalb des Netzwerkes der Organisation betrieben und somit von den internen Netzen des Vertragspartners physikalisch und logisch getrennt, befinden sich aber weiterhin im Schutzbereich der Firewall.

Typische Dienste, welche in einer DMZ platziert werden, sind E-Mail-Server oder -Router, HTTP-Server, DNS-Server, Proxy-Server und RA-Server.

In der DMZ können offizielle und private Netze koexistieren. Dies setzt voraus, dass die eingesetzten IP-Endgeräte in der DMZ ebenfalls mit mehreren unterschiedlichen IP-Nummern und IP-Netzen je NIC arbeiten können.

Das Layer 2 Netzwerk in der DMZ ist als IEEE802.3 10/100 baseT ausgelegt.

2.2.6 Traffic-Shaping

Das Traffic-Shaping ist ein kostenpflichtiger optionaler Service, welcher von der Firewall zur Verfügung gestellt wird.

Durch das Traffic-Shaping wird ausgehender und eingehender Datenverkehr nach IP-Netzen und TCP/UDP Ports in der Bandbreite begrenzt und priorisiert.

2.3 IP VPN

Das Produkt Virtual Private Network (VPN) verbindet private IP-basierte Netzwerke über öffentliche IP-Netzwerke mit Hilfe von VPN Gateways, welche in der Regel in der Firewall implementiert sind.

Das hierzu verwendete Verfahren wird auch als IP-Tunneling oder IP-IP Encapsulation bezeichnet.

Die Daten werden vor dem Verlassen des Netzwerks des Vertragspartners in dem VPN Gateway verschlüsselt und an das adressierte VPN Gateway übergeben.

Die Adressierung innerhalb des VPN wird durch die VPN Gateways vorgegeben. Das Routing zwischen den Gateways wird von der IP-Infrastruktur übernommen, welche die VPN Gateways miteinander verbindet.

Das VPN Gateway stellt sicher, dass die Daten nur an autorisierte Knoten des VPN zugestellt werden. Das adressierte VPN Gateway entschlüsselt die Datenpakete und sendet diese an den Empfänger in den adressierten Teil des VPN.

Für den Aufbau der Verbindungen wird IPSec verwendet. Es findet keine End-to-End Verschlüsselung statt. Die Daten werden im Netzwerk des Vertragspartners weiterhin unverschlüsselt übertragen.

Der Transport der Daten findet auf Layer 3 des OSI-Modells statt.

2.3.1 VPN Gateways

Das VPN Gateway ist als Teil der Software in der Firewall implementiert. Die Anzahl der maximal möglichen VPN Tunnel ist von der eingesetzten Hard- und/oder Software abhängig und kann durch NetAachen nicht beeinflusst werden.

Die Schlüssellänge, welche zur Verschlüsselung der IP-Datenpakete verwendet wird, ist von der eingesetzten Hard- und Software des Anbieters abhängig. Heute werden Schlüssel mit einer Länge von 128 Bit eingesetzt.

Zusätzliche Tunnel können über eine weitere Firewall bereitgestellt werden, welche dann ausschließlich als VPN Gateway eingesetzt wird.

2.3.2 VPN Clients

VPN Clients sind ausschließlich als Software ausgelegt, welche vom Anbieter der Firewall oder einem Drittanbieter bereitgestellt werden. Die VPN Software wird auf einem Client installiert.

Die installierte Clientsoftware ist nicht für alle Betriebssysteme und Versionen von Betriebssystemen verfügbar. Die benötigten Versionen für die zum Einsatz kommenden Betriebssysteme sind mit der Technik der NetAachen abzustimmen.

NetAachen hat keinerlei Einfluss auf die Verfügbarkeit der Software auf verschiedenen Betriebssystemen und deren Versionsständen.

Die Authentifikation der Benutzer kann auf Benutzer- oder Systemebene erfolgen. Die Authentifikation wird von der Firewall durchgeführt. Soll auf vorhandene Authentifikationsmethoden und Protokolle zugegriffen werden, so ist dies dringend in die Anforderungen mit aufzunehmen.

Die Anzahl der konfigurierbaren VPN User ist je Firewall auf 25 Stück begrenzt. Größere Anzahlen sind in Ausnahmefällen nach Absprache möglich.

Die Anzahl der gleichzeitig einwählbaren VPN User ist gerätespezifisch von der Anzahl der maximal möglichen VPN Tunnel abhängig.

2.3.3 Routing

Der Transport der IP-Pakete zwischen den VPN Gateways und VPN Clients erfolgt über öffentliche IP-Backbones.

Auf den Transport der Daten außerhalb des IP-Backbones der NetAachen hat NetAachen keinerlei Einfluss. Nichterreichbarkeit, hohe Latenzzeiten oder Störungen beim Transport der IP-Daten fallen in die Verantwortung des IP-Backbone Betreibers, an den ein VPN Gateway oder VPN Client angebunden ist.

Bei Transportproblemen innerhalb des IP-Backbones der NetAachen werden die SLA zwischen NetAachen und dem Vertragspartner wirksam.

2.3.4 Encapsulation

Die IP-Datenpakete des Vertragspartners werden innerhalb der Firewall verschlüsselt und an das VPN Gateway oder den VPN Client adressiert, welcher Daten angefordert hat oder an welchen die Daten adressiert werden.

Durch das Verpacken von IP-Datenpaketen in IP-Datenpakete wird der Protokollanteil des Datentransfers verdoppelt und die maximal zur Verfügung stehende Nettobandbreite entsprechend belastet.

Die Latenzzeit wird durch den Vorgang der Encapsulation und des Verschlüsselns geringfügig erhöht.

Die Kosten für den zusätzlich anfallenden Datentransfer aufgrund des erhöhten Protokollaufwandes gehen zu Lasten des Vertragspartners.

2.3.5 Quality of Service

Das IP-Protokoll verfügt in der aktuell eingesetzten Version 4 über QoS Merkmale welche jedoch nicht ausgewertet werden. Eine gesicherte Bandbreite sowie gesicherte Paketlaufzeiten sind derzeit nicht realisierbar, insbesondere dann nicht, wenn die Daten über IP-Backbones übertragen werden, die nicht in den Verwaltungsbereich der NetAachen fallen.

2.4 Content Filter

Der Content Filter arbeitet als Scanner zwischen Internet und dem Organisationsnetzwerk des Vertragspartners. Der Content Filter verfügt über eine Mustererkennung, welche bekannte schädliche Inhalte und deren Derivate erkennt.

Als schädlich erkannte Inhalte werden aus dem Datenstrom isoliert und gelangen nicht auf das Zielsystem, welches den Datenstrom angefordert hat.

Es wird dringend empfohlen, den Content Filter in der DMZ einer Firewall zu platzieren.

Der Content Filter arbeitet als Proxy- bzw. Store-and-Forward Server. Der Nutzer kann nur durch entsprechende Konfiguration eines Routers oder einer Firewall zur Nutzung gezwungen werden. Wird der Content Filter umgangen, können schädigende Inhalte auf das Zielsystem gelangen, welches den Datenstrom angefordert hat.

Der Content Filter arbeitet auf den OSI Layern 5 und 6 ausschließlich für die Dienste, welche im Folgenden beschrieben sind. Content Filter für weitere Dienste können bei Bedarf und Herstellerverfügbarkeit kostenpflichtig nachgerüstet werden.

Dienste, bei denen die Datenübertragung, deren Inhalte oder Teile von deren Inhalten verschlüsselt sind, entziehen sich der Mustererkennung.

Der Content Filter ersetzt keinen Virenprüfer auf Client Systemen. Viren oder andere schädliche Programme können auch auf austauschbaren Datenträgern vorhanden sein.

2.4.1 Schnittstellen

Der Content Filter verfügt über eine physikalische Layer 2 Schnittstelle, welche als Ethernet (IEEE802.3, 10/100baseTx) ausgeführt ist.

Andere Layer 2 Protokolle als Ethernet werden nicht unterstützt.

2.4.2 HTTP/FTP

Verbindungen aus dem Netzwerk des Vertragspartners werden an den HTTP/FTP Proxy gerichtet oder durch eine Firewall an diesen umgeleitet.

Der Content Filter nimmt die Anfragen des Clients entgegen und leitet diese an die durch den URL (Uniform Ressource Locator) des Client vorgegebene Ressource im Internet weiter.

Der Datenstrom des angefragten URL wird durch einen Prozess im Content Filter verarbeitet und nach schädlichen Inhalten untersucht.

Schädliche Inhalte werden beim HTTP aus dem Datenstrom isoliert und durch eine Warnmeldung ersetzt.

Beim FTP wird die Kommunikation bei der Erkennung von schädlichen Inhalten abgebrochen.

Nach dem Erkennen schädlicher Inhalte wird der Vorgang protokolliert und die Administration verständigt.

Inhalte, welche archiviert und/oder komprimiert sind, werden zuerst entpackt und dann auf schädliche Inhalte untersucht.

Datenströme, welche clientseitig verschlüsselt werden, können nicht untersucht werden.

Unbekannte und unerwünschte Inhalte bzw. URL können gesperrt werden.

2.4.3 SMTP

Der Transport von E-Mails über den Content Filter findet ausschließlich über SMTP statt. Der Content Filter arbeitet als SMTP-Router, welcher eine empfangene E-Mail zwischenspeichert, auf schädliche Inhalte überprüft und dann an das adressierte Zielsystem weiterleitet.

Dies gilt für eingehende wie für ausgehende E-Mails.

Der Content Filter arbeitet nicht als E-Mail-Server. E-Mails werden vom SMTP-Prozess auf dem Content Filter nach der Überprüfung an den E-Mail-Server des Vertragspartners zugestellt.

Schädliche Inhalte werden isoliert und durch einen Warnhinweis in der E-Mail ersetzt.

Eine Filterung nach unerwünschten oder unbekannten Inhalten ist ebenfalls möglich.

Archivierte oder komprimierte Inhalte werden zunächst entpackt und dann auf schädliche Inhalte untersucht.

Verschlüsselte Inhalte, welche clientseitig ver- und entschlüsselt werden, können nicht untersucht werden.

2.5 Betrieb

Der Betrieb aller Dienste der Pro Net Managed Security ist ein Fullservice. Kosten für Hardwareaustausch bei Defekt, Software-Upgrades, Security-Patches sowie 24 x 7 Überwachung sind in den monatlichen Betriebskosten enthalten.

2.5.1 Reporting

Angriffe, ab einer vereinbarten Intensität, auf die durch NetAachen betriebene Installation, werden unverzüglich dem Vertragspartner auf einem vorher vereinbarten Kanal zur Anzeige gebracht.

Die während des Betriebs gesammelten Ereignisse werden über einen Zeitraum von 3 Monaten gesichert und anschließend gelöscht. Eine Archivierung findet durch NetAachen nicht statt.

Auf Wunsch werden dem Vertragspartner Auswertungen kostenpflichtig zur Verfügung gestellt. Der maximale Auswertungszeitraum kann hierbei maximal 3 Monate betragen.

2.5.2 Updates

Updates werden zeitnah eingespielt, sobald der Hersteller der eingesetzten Komponente solche zur Verfügung stellt. Die NetAachen hat keinerlei Einfluss auf die Bereitstellung von Updates durch einen Hersteller.

2.5.3 Change Management

Änderungen am Regelwerk der Firewall oder des Content Filter werden von NetAachen bei Bedarf durchgeführt. Eine Änderung darf nur von autorisierten Personen, welche der NetAachen bekannt sein müssen, beauftragt werden. Die Änderungsanfrage bedarf der Schriftform.

Das Hinzufügen von VPN-Verbindungen oder Änderungen der bestehenden Verbindungen sind gesondert zu beauftragen und fallen nicht unter den Support der Pro Net Managed Security.

NetAachen behält sich vor, eine Änderung auf Sinnhaftigkeit zu überprüfen und gegebenenfalls weitere Änderungsberechtigte des Vertragspartners über die Änderung in Kenntnis zu setzen und um Bestätigung der Änderung zu ersuchen.

Die Änderungen beziehen sich ausschließlich auf bestehende Netze und System des Vertragspartners zum Zeitpunkt der Inbetriebnahme.

Weitere, während der Betriebsphase hinzugefügte Komponenten sind nicht durch den Vertrag abgedeckt und werden durch einmalige Aufwendungen abgegolten.

Alle weiteren Änderungen, welche sich auf die hinzugefügten Komponenten beziehen, werden in den normalen Betrieb übernommen. Weitere Änderungen, welche sich auf später hinzugefügte Systeme oder Netze beziehen, sind durch die MSS abgedeckt.

2.5.4 Sicherheitstrennung

Erfolgt ein Angriff auf die Installation des Vertragspartners, welche durch die NetAachen betrieben wird und durch die aktuellen Sicherheitseinstellungen nicht abgefangen werden kann, behält sich die NetAachen vor, die Anbindung an das Internet physikalisch zu trennen, indem die Firewall oder der Router ausgeschaltet wird. Ein Einschalten ist dann nur noch durch Betätigen des Netzschalters möglich.

Solches Eingreifen belastet die Verfügbarkeit anderer durch NetAachen bereitgestellter Dienste nicht.

2.5.5 Service Level

2.5.5.1 SLA Bereitstellung

Die Bereitstellung einer vorbereiteten Umgebung zur Installation von Produkten der MSS erfolgt spätestens 20 Arbeitstage nach Unterzeichnung des Kundenauftrags, sofern keine Sonderlösungen beauftragt wurden, welche nicht Bestandteil der Leistungsbeschreibung der MSS sind.

Bei Überschreitung der Bereitstellung einer vorbereiteten Umgebung durch die NetAachen werden folgende prozentuale Erstattungen vom im Auftrag festgehaltenen Installationspreis vereinbart:

Überschreitung in Werktagen	Erstattung der Installationskosten
Bis 2 Tage	10%
Bis 5 Tage	20%
Bis 10 Tage	40%
> 10 Tage	50%

2.5.5.2 SLA Änderungen

Änderungen am Regelwerk der Firewall sowie allen weiteren Komponenten der Installation, welche durch die Leistungsbeschreibung der MSS abgedeckt sind, werden innerhalb von 2 Werktagen nach Beauftragung durch den Vertragspartner von NetAachen eingepflegt.

Bei Überschreitung der Installationszeit wird NetAachen folgende prozentuale Erstattungen vom im Auftrag festgehaltenen monatlichen Grundpreis rückerstatten:

Überschreitung in Werktagen	Erstattung der Installationskosten
Bis 1 Tag	10%
Bis 3 Tage	25%
Bis 5 Tage	50%
> 5 Tage	100%

2.5.5.3 SLA Verfügbarkeit

Die Verfügbarkeit bezieht sich auf die Verfügbarkeit aller Produkte der MSS.

Die Verfügbarkeit für die Produkt der MSS wird mit 98,5% pro Monat angegeben.

Bei Unterschreitung der angegebenen Verfügbarkeit der MSS werden dem Kunden folgende prozentuale Erstattungen pro Monat vom monatlichen Auftragswert erlassen:

Unterschreitung in %	Erstattung der monatlichen Kosten
Bis 0,25%	10%
Bis 0,50%	25%
Bis 0,75%	50%
> 0,75%	75%

2.6 Security Check

Auf Anfrage und ausdrückliche Erlaubnis führt NetAachen einen Security Check auf angegebene IP-Adressen oder IP-Netze und Dienste des Vertragspartners durch.

Es werden automatisierte und manuelle Angriffe auf die gewünschten Netzwerke oder Systeme simuliert.

Der Vertragspartner muss hierbei versichern, dass es sich um IP-Adressen handelt, welche seinem Verwaltungsbereich zugeordnet sind oder von einem ISP überlassen wurden.

Die angegriffenen Systeme werden nicht wirklich physikalisch oder logisch beschädigt, noch werden daraus gewonnene Informationen an Dritte weitergegeben oder veräußert.

Ein unkontrolliertes Verhalten, sowie Fehlfunktion und dauerhafte Schäden lassen sich dennoch nicht ausschließen. Die Kosten, welche durch eine solche Schädigung entstehen, übernimmt der Vertragspartner.

2.6.1 Firewall

Die Firewall des Vertragspartners wird von einem System der NetAachen angegriffen. Es wird versucht, Sicherheitslücken in der Firewall zu finden und die Sicherheitsmechanismen der Firewall auszuschalten oder zu umgehen.

2.6.2 Privates Netzwerk

Das interne Netzwerk des Vertragspartners wird von einem System der NetAachen angegriffen. Es wird versucht, in das Kundennetzwerk einzudringen, um Informationen über Sicherheitslücken auszuspionieren, welche das weitere Vordringen ermöglichen oder begünstigen.

2.6.3 DMZ

Das DMZ Netzwerk des Vertragspartners wird von einem System der NetAachen angegriffen. Es wird versucht, in die DMZ einzudringen, um Informationen über Sicherheitslücken auszuspionieren, welche das weitere Vordringen ermöglichen oder begünstigen.

2.6.4 Server

Von einem System der NetAachen wird ein Server des Vertragspartners angegriffen. Es wird versucht, Sicherheitslücken in den Diensten der freigeschalteten Ports ausfindig zu machen.

Der gesamte TCP/UDP Adressbereich des Servers wird auf Ports untersucht, welche eine Angriffsoberfläche liefern.

3 Tarifierung

3.1 Allgemeines

Grundlage für alle Preise ist die zur Vertragsunterzeichnung gültige Preisliste. Gesonderte Tarife oder Rabatte sind schriftlich im Kundenauftrag festzuhalten und als besondere Regelung zu kennzeichnen.

Die Tarife und Konditionen werden in den Preislisten näher erläutert.

3.1.1 Kosten

Dem Kunden entstehen in Zusammenhang mit dem Produkt und den erbrachten Dienstleistungen einmalige und monatliche Kosten. Die Höhe des monatlichen Entgelts, welches an NetAachen bezüglich der erbrachten Leistungen zu entrichten ist, wird im jeweiligen Kundenauftrag festgehalten.

3.1.2 Optionale Dienste

Alle optionalen Dienste erfordern einen Kundenauftrag. Alle optionalen Dienste werden separat auf der Rechnung ausgewiesen.

3.2 Vertragslaufzeit und Kündigung

Der Vertrag wird auf unbestimmte Zeit geschlossen.

Die Mindestvertragslaufzeit im Rahmen des Vertrages in Auftrag gegebener Dienstleistungen, Produkte oder Produktgruppen ist im jeweiligen Kundenauftrag geregelt und festgelegt.

Der Vertrag ist für beide Vertragsparteien erstmals mit einer Frist von sechs Wochen zum Ende des Quartals, in dem die Mindestvertragslaufzeit endet, kündbar. Nach Ablauf der Mindestvertragslaufzeit oder wenn keine Mindestvertragslaufzeit vereinbart ist, ist der Vertrag mit einer Frist von sechs Wochen zum Quartalsende kündbar. Die Kündigung muss schriftlich erfolgen.

Nach Beendigung des Vertragsverhältnisses obliegt dem Kunden die unverzügliche ordnungsgemäße Bereitstellung der von NetAachen leihweise überlassenen System-Technik und sonstiger Komponenten. Zur Abholung des Eigentums von NetAachen wird ein Termin vereinbart. Bei Verlust oder im Schadensfall wird dem Kunden der Wiederbeschaffungspreis für die System-Technik und sonstige Komponenten in Rechnung gestellt. Die Anfahrtkosten werden in Rechnung gestellt, wenn trotz vereinbartem Termin der Kunde zur Abholung des NetAachen-Eigentums nicht anzutreffen war und daher eine erneute Abholung erfolgt.

3.3 Rechnungsstellung

Der Kunde erhält seine monatliche Rechnung postalisch. NetAachen ermöglicht es dem Kunden auf Wunsch, die Abrechnung per Online-Service abzurufen. Entscheidet sich der Kunde für diese Möglichkeit, wird dem Kunden keine schriftliche Abrechnung mehr zugestellt.

4 Service und Support

4.1 Störung

Ergänzend zu den Regelungen der Ziff. 4.1 der AGB hinsichtlich Prüfung der vertraglichen Leistung und Mängelanzeige gilt für die Störung folgendes:

Als Störung werden alle Zustände bezeichnet, bei denen ein System oder ein Dienst nicht über die vertraglich vereinbarten Schnittstellen erreichbar ist oder nicht die vom Kunden erwarteten Ergebnisse in einer normalen Antwortzeit liefert.

Ist die Erreichbarkeit eines Systems oder eines Dienstes durch Störungen in Systemen, Komponenten oder Diensten des Kunden begründet, fällt dieses nicht in den Verantwortungsbereich der NetAachen und es handelt sich somit nicht um eine Störung seitens der NetAachen.

Jeder Kunde ist gehalten, die Symptome einer Störung möglichst genau zu beschreiben.

Hat der Kunde die Störung zu vertreten oder liegt eine vom Kunden gemeldete Störung nicht vor, ist NetAachen gemäß Ziff. 4.1 der AGB berechtigt, dem Kunden die durch die Fehlersuche, Mängelbeseitigung bzw. Entstörung entstandenen Kosten in Rechnung zu stellen.

Als Störung des ordentlichen Betriebs gelten alle in den Leistungsbeschreibungen von Produkten beschriebenen Störungen, die in einem Maße schädlich sein können, dass diese den Betrieb weiterer Systeme so nachhaltig stören, dass ein den anderen Kunden garantierter Betrieb nicht mehr möglich ist. Dies bezieht sich auf alle von der NetAachen betriebenen Systeme, Komponenten und Dienstleistungen.

Verursacht eine vom Kunden beigestellte Komponente eine betriebsgefährdende Störung, so kann diese Komponente, ohne vor-

herige Rücksprache mit dem Kunden gehalten zu haben, in dem Sinne abgestellt werden, dass diese keine weiteren Störungen des ordentlichen Betriebs mehr verursachen kann.

Werden NetAachen Störungen von Internet-Diensten durch Kunden eines anderen Providers bekannt (z.B. durch Spamming, Mail-Bombing, Denial-of-Service-Attacken etc.), so kann NetAachen die Übermittlung von Daten zu Kunden dieses Providers vorübergehend unterbrechen oder einschränken.

4.1.1 Servicebereitschaft

Die Hotline der Servicebereitschaft ist 24 Stunden an 7 Tagen pro Woche besetzt. Die Servicebereitschaft nimmt Störmeldungen entgegen, qualifiziert diese und leitet die Meldungen an Fachpersonal weiter.

Die Servicebereitschaft führt selbst keine Entstörung durch, noch leistet diese irgendwelche Beratungsleistungen zu Produkten, Dienstleistungen oder Diensten.

Sie erreichen die Service-Hotline unter der Telefonnummer 0800-2222-111.

4.1.2 Störmeldung

Die Meldung einer Störung bei der Störungsannahme erfolgt fernmündlich oder in Schriftform. Die Störungsannahme nimmt jegliche Störmeldung erst nach positiver Vertragsprüfung entgegen. Kann dem Kunden kein gültiger Vertrag zugewiesen werden, der ihn zur Störungsmeldung berechtigt, so wird die Störung nicht angenommen. Störmeldungen können weiterhin maschinell automatisiert durch Überwachungssysteme erfolgen. Bei Annahme der Störung erhält der Kunde eine Trouble-Ticket-Nummer. Diese Nummer gilt als Referenznummer für die weitere Kommunikation betreffend der Störmeldung. Die Hotline ist unter der dem Produkt zugeordneten Service-Nummer (Ziff. 4.1.1) zu erreichen, wie unter Servicebereitschaft angegeben.

4.1.3 Störungsdauer

Eine Störung beginnt mit der Meldung der Störung durch den Kunden oder einer maschinell automatisiert ausgelösten Störmeldung. Eine Störung endet mit der Meldung der Entstörung durch die NetAachen, es sei denn, dass der Kunde gemäß Ziffer 4.1.5 fristgerecht und zu Recht mitteilt, dass die Entstörung nicht erfolgreich war.

Ist es nicht möglich, eine Entstörung an den Kunden zu melden, so gilt der dokumentierte Versuch der Entstörungsmeldung als Meldung zur Entstörung.

Für Rückerstattungen wird die Störungsdauer zugrunde gelegt.

Die Höhe der Rückerstattung ist von Produkt, SLA und gegebenenfalls einem zusätzlichem Service-Level-Vertrag abhängig.

4.1.4 Entstörzeiten

Entstörzeiten sind Montag bis Freitag von 8–18 Uhr.

Falls erforderlich, vereinbart NetAachen mit dem Kunden einen Termin für den Besuch eines Servicetechnikers.

Ist für die angebotenen Dienste und Systeme diese Entstörzeit nicht akzeptabel, kann durch Abschluss eines gesonderten SLA-Vertrags die Entstörzeit den Bedürfnissen des Kunden angepasst werden.

4.1.5 Entstörung und Wiederherstellungszeit

Der Kunde wird über den Status seiner Störungsmeldung und den Fortschritt der Entstörung von der Störungsstelle in nicht definierten zeitlichen Abständen informiert.

Der Kunde wird nach der Entstörung aufgefordert, die Entstörung zu bekunden. Ist der Kunde nicht erreichbar oder erfolgt nach mehrmaliger Aufforderung keine negative Meldung bezüglich der Entstörung, so wird nach 10 Tagen die Störmeldung geschlossen und von Seiten der NetAachen davon ausgegangen, dass eine Entstörung im Sinne des Kunden erfolgt ist. Des Weiteren gilt eine Entstörung als erfolgreich, wenn der Kunde nach der Entstörung schriftlich oder fernmündlich eine Entstörung bekundet.

Die Wiederherstellungszeit kann in Fällen von höherer Gewalt überschritten werden. Die Wiederherstellungszeit kann im Einzelfall, nach Absprache, vertraglich gesondert geregelt werden.

Die Störung wird innerhalb der Wiederherstellungszeit zumindest soweit beseitigt, dass der Anschluss (ggf. übergangsweise mit Qualitätseinschränkungen) wieder genutzt werden kann oder alternative Lösungen in Anspruch genommen werden können.

4.2 Support

Für die Störungsannahme bietet NetAachen eine gebührenfrei Hotline an: 0241-413413-0. Diese Rufnummer ist 24 Stunden an 7 Tagen pro Woche erreichbar.

Für den Internetsupport stellt NetAachen eine gebührenpflichtige Hotline bereit: 0900-1222230 (1,19 EUR/Minute inkl. gesetzl. MwSt. aus dem deutschen Festnetz).

Der Support beschränkt sich auf MS-Windows-Betriebssysteme ab Windows 2000 und wird nur in Zusammenhang mit den von NetAachen angebotenen Leistungen erbracht.

Die Rufnummer ist Montag bis Freitag von 8–18 Uhr erreichbar.

Support-Leistungen welche im Rahmen des Telefon-Supports nicht erbracht werden können, werden nach Aufwand abgerechnet. Es gelten die Geschäftsbedingungen für Service-Leistungen der NetAachen, sowie die darin enthaltenen Preise.

4.3 Wartung

Die Wartung von Systemen, welche zum Betrieb notwendig sind, werden azyklisch durchgeführt. Über anstehende Wartungen, welche zum Betrieb notwendige Komponenten betrifft, wird der Kunde 2 Wochen im Voraus informiert.

Sofern wartungsbedingte Unterbrechungen nicht häufiger als 1 mal pro Quartal auftreten und nicht länger als eine Stunde anhalten, gelten diese Unterbrechungen nicht als Störung.

4.4 Spezieller SLA-Vertrag

Sollten die aufgeführten SLA und Betriebsvereinbarungen den Ansprüchen des Kunden nicht genügen, so wird zwischen dem Kunden und der NetAachen ein spezieller SLA-Vertrag geschlossen, welcher den Bedürfnissen des Kunden gerecht wird.

Bei Abschluss eines solchen SLA-Vertrags verlieren die aufgeführten Vereinbarungen, welche mit SLA gekennzeichnet sind, ihre Gültigkeit und werden durch den speziellen SLA-Vertrag ersetzt. Alle weiteren Punkte dieser Leistungsbeschreibung bleiben davon unberührt.