

Leistungsbeschreibung VT Security [basic], [advanced], [professional]

versatel

V100 608/0112/01. Änderungen vorbehalten.
Gültig ab 01/2012 – Seite 1/3

1 Einleitung

Die Versatel-Gruppe in Deutschland (im nachfolgenden Versatel genannt) bietet dem Kunden professionelle und einfach konfigurierbare Firewall-Lösung zum Schutz des Kunden-IP-Netzwerkes (LAN) vor unberechtigten Zugriffen aus dem öffentlichen Internet an. Die Firewall kann zum Aufbau von Virtuell Privaten Netzwerken (VPN) über das öffentliche Internet genutzt werden. Die Firewall wird zwischen das kundenseitige LAN und dem öffentlichen Internet eingefügt und bietet zahlreiche Funktionen, um unerwünschten Verkehr zwischen dem Internet und dem LAN zu unterbinden. Zusätzlich bietet die Firewall Möglichkeiten zum Schutz des LANs vor aktiven Angriffen. Als weiteres Leistungsmerkmal kann mit der Firewall eine vom LAN getrennte demilitarisierte Zone (DMZ) zum Betrieb von Internetservern, wie E-Mail-, Web- und DNS- Server aufgebaut werden. Das VPN Gateway erlaubt es dem Kunden über das öffentliche Internet ein VPN zur Vernetzung seiner LANs aufzubauen und z.B. Mitarbeitern über einen VPN Client Fernzugriff auf das Firmennetzwerk zu ermöglichen. Das Produkt VT security bietet Standardleistungen sowie gegen gesonderte Vergütung zu beauftragende zusätzliche Leistungen an.

2 Standardleistungen

VT security bietet im Rahmen der technischen Möglichkeiten und der mit dem Kunden getroffenen Vereinbarungen Leistungsmerkmale zum Schutz von Kunden-Netzwerken vor unberechtigtem Zugriff. Die Firewall besteht aus mehreren aktivierbaren Modulen. Sie wird zwischen den Internetzugang des Kunden und das zu schützende Kundennetz eingefügt. Versatel stellt dem Kunden die erforderliche Hard- und Software für die Dauer des Vertrages bereit und konfiguriert die VT security gemäß der Vorgaben durch den Kunden. Voraussetzung für die Nutzung von VT security ist eine Anbindung an das öffentliche Internet. Der Internetzugang ist nicht Bestandteil des Produktes und kann bei Versatel gegen ein gesondertes Entgelt beauftragt werden. Folgende Standardleistungen sind bei VT security enthalten:

- Modul Network Security mit dem Dienst Firewall
- Definition von Netzwerkobjekten
- Gemeinsame Erstellung eines Regelwerkes (First-Audit)
- Einrichtung eines benutzerdefinierten Regelwerkes
- Einrichtung einer DMZ sofern gewünscht
- Konfiguration verschiedener Proxy-Dienste
- Einrichtung eines DHCP-Servers sofern gewünscht
- Einrichtung einer x-DSL Backup-Anbindung sofern kundenseitig vorhanden

2.1 Produktvarianten/&- module

Versatel bietet dem Kunden 5 unterschiedliche Hardware-Ausbaustufen an, die sich in der Leistungsfähigkeit unterscheiden. Folgende Produktvarianten &- module werden angeboten:

- VT security [basic, 10, 50, 250, 500, 1000]
- VT security [advanced, 10, 50, 250, 500, 1000]
- VT security [professional, 10, 50, 250, 500, 1000]

Die Zahlen 10, 50, 250, 500, 1000 innerhalb des Produktnamens stellen einen groben Richtwert der möglichen User dar. Ab der Version VT security [50 bis 1000] sind die Anzahl der Userlizenzen softwaretechnisch unlimitiert, werden jedoch durch die jeweils eingesetzte Hardware und deren maximaler CPU-Performance auf die genannten Richtwerte begrenzt. Bei Aktivierung der optional zubuchbaren Module Mail- und/oder Websecurity kann sich die maximale Anzahl der zu verwaltenden User durch erhöhte Prozessorlast verringern.

2.2 Konfiguration

Die VT security wird von Versatel, gemäß der im Konfigurationsdatenblatt festgelegten Regeln, konfiguriert. Aufgrund des vom Kunden festgelegten Regelwerkes, sowie der beauftragten Konfiguration für das System, kann es zu Beeinflussung der Datenströme kommen. Versatel nimmt zusammen mit einem Mitarbeiter des Kunden, die Konfigurationsanforderungen auf und hält diese in einem beidseitig gegenzuzeichnendem Konfigurationsdatenblatt fest. Hierzu vereinbart Versatel mit dem Kunden einen Vor-Ort-Termin. Kundenseitig sind hierfür alle, für die Konfiguration nötigen Parameter bereitzuhalten. Sind vom Kunden weitere Termine zur Aufnahme der Konfigurationsanforderung erwünscht, werden diese in der jeweiligen Höhe der einmaligen Setupgebühr berechnet.

2.3 Installation

Die Installation, Inbetriebnahme und die Wartung der VT security erfolgt standardmäßig durch einen Versatel-Techniker oder durch einen von Versatel be-

auftragten Servicepartner. Versatel liefert die beauftragte Hard- und Software und überlässt sie dem Kunden für die Dauer der Vertragslaufzeit. Die Installation umfasst keine Verkabelungsarbeiten an Inhouse-Netzen. Es werden keine Netzwerkkabel zum Anschluss an das System bereitgestellt. Voraussetzung für die Installation des VT Security Produktes ist die Bereitstellung eines funktionierenden Uplinks (z.B. zum Internet).

2.4 Betrieb

Der Betrieb der VT security umfasst insbesondere folgende Leistungen:

- Versatel führt Updates durch und installiert Patches auf den zur Verfügung gestellten Firewalls. Dazu ist Versatel oder ein durch Versatel beauftragter Servicepartner, falls erforderlich, zur Außerbetriebnahme der Systeme berechtigt. Bei kritischen Updates oder Patches erfolgt - unabhängig vom abgeschlossenen Servicelevel - keine Kundeninformation. Sollte die Installation einer höherwertigen Version nicht möglich sein, weil die vorhandene Hardware nicht ausreichend dimensioniert ist, kann die VT security nicht auf die neue Version aktualisiert werden. Auf Wunsch stellt Versatel dem Kunden in diesem Fall die notwendige Hardware kostenpflichtig zur Verfügung.
- Service Level Agreements gemäß Punkt 4 dieser Leistungsbeschreibung

2.5 Konfigurations- und Regeländerungen

Versatel führt im Rahmen einer Kundenanforderung folgende kostenlose Konfigurationsänderungen (Changes) durch:

- Einrichten und Ändern von Regeln, Rechten und Netzwerkobjekten, beispielsweise Benutzergruppen und Netzwerkdienste
- Anpassungen des IP- Routings nach Erfordernissen des Kunden
- Anpassung der Firewall bei der Einrichtung eines VPN

Regel- und Konfigurationsänderungen können nur per Auftragsformular beauftragt werden. Das Auftragsformular muss von den berechtigten Personen des Kunden unterschrieben und an Versatel gesendet werden. Änderungen werden von Versatel innerhalb des Servicezeitraums von Montag bis Freitag in den Zeiten von 08:00 bis 16:00 durchgeführt und bearbeitet. Die Umsetzung erfolgt in der Regel werktags innerhalb von 24 Stunden spätestens innerhalb von 3 Arbeitstagen nach Auftragseingang und Auftragsklarheit. Die Bearbeitungsfrist wird freitags ab 16 Uhr, samstags, sonntags und feiertags bis zum nächsten Werktag (Montag bis Freitag) ausgesetzt. In allen Produktvarianten sind 10 Changes pro Monat kostenfrei enthalten. Sollten mehr als 10 Changes pro Monat beauftragt werden, ist jede weitere Change gesondert zu vergüten. Die Kosten je Change ergeben sich aus der jeweils im Zeitpunkt des Vertragschlusses oder nach einer Preisänderung gültigen Preisliste. Nicht in Anspruch genommene Changes können nicht in den Folgemonat übertragen werden.

2.6 Schnittstellen

Die Firewalls verfügen über mindestens 3 Ethernet-Schnittstellen 10/100baseT gemäß IEEE802.3 zum Anschluss der LANs, des öffentlichen Internets und zum Betrieb einer demilitarisierten Zone (DMZ). Die Produkte bieten modulunabhängig folgende Anzahl an Schnittstellen:

- VT security [10]: 3 x 10/100baseT
- VT security [50]: 3 x 10/100baseT
- VT security [250]: 8 x 10/100baseT
- VT security [500]: 4 x 10/100baseT + 4 x 1000baseT
- VT security [1000]: 6 x 1000baseT + 2 x Gigabit SFP

2.7 DMZ

Die DMZ wird zum Betrieb von Systemen und Diensten auf Kundenseite verwendet, die sowohl aus dem Internet, als auch aus dem LAN erreichbar sein sollen. Die in der DMZ aufgestellten Systeme können durch die Firewall gegen Zugriffe aus dem LAN und dem Internet abgeschirmt werden. Durch diese Trennung kann z. B. der Zugriff auf öffentlich erreichbare Dienste gestattet und gleichzeitig das interne Netz (LAN) vor unberechtigten Zugriffen geschützt werden. Systeme die in einer DMZ aufgebaut werden sind beispielsweise E-Mail-Server und Webserver.

2.8 Endgerät bei VT security

Versatel stellt dem Kunden ein Firewall-System und ein Anschlusskabel für die Spannungsversorgung zur Verfügung. Das überlassene System verbleibt im Eigentum der Versatel und muss nach Vertragsende zurück gegeben werden. Erfolgt keine Rückgabe des Systems innerhalb von vier Wochen nach Ver-

Leistungsbeschreibung VT Security [basic], [advanced], [professional]

versatel

V100 608/0112/01. Änderungen vorbehalten.
Gültig ab 01/2012 – Seite 2/3

tragsende, so ist Versatel berechtigt, das System zum aktuellen Widerbeschaffungswert dem Kunden in Rechnung zu stellen.

2.8.1 Aufstellungsort des Endgerätes

Während der Nutzung des Produktes VT security hat der Kunde folgende Parameter bei der Aufstellung des Endgerätes einzuhalten:

- Vermeidung von direkter Sonneneinstrahlung
- Wärmeeinwirkung durch Heizkörper oder andere wärmeentwickelnde Geräte sind zu unterbinden
- Sicherung des Systems mit geeigneten technischen Einrichtungen gegen Blitzschlag (sind nicht im Lieferumfang enthalten)
- Evtl. Bereitstellung der notwendigen Klimatisierung zur Einhaltung der empfohlenen Umgebungsbedingungen:
Raumtemperatur: 0°C bis 40°C
Luftfeuchtigkeit: 10% bis 90%
Stromversorgung: 230 VAC, 50-60Hz
Max. Leistungsaufnahme: 60 W
180 W (VT security [firewall plus 250])

3 Security Module

Je nach Produktausprägung sind in der Leistung verschiedene Module enthalten, die nachfolgend beschrieben werden.

3.1 VT security [basic]

Die Dienste des Produkts VT security [basic] beinhalten die Grundfunktionen wie unter 3.1.1 und 3.1.2 beschrieben.

3.1.1 Firewall (Network Security)

Die Firewall überwacht ein- und ausgehende Datenpakete. Sie kontrolliert auf IP-Ebene sowohl wichtige Paket-Header als auch übliche Applikationsdaten (Payload), um unerwünschte Kommunikation erkennen und unterbinden zu können. Um bestimmten Benutzergruppen für einen definierten Zeitraum Zugriff auf Netzwerke und Server zu geben, lassen sich Paket-filter-Regeln für spezifische Zeitabschnitte festlegen. Datenverkehr, der nicht durch die Firewall transportiert wird, entzieht sich der Kontrolle durch die Firewall. Der Kunde muss sicherstellen das keine sonstigen Internetverbindungen wie z.B. Modemverbindungen ins Internet aufgebaut werden.

3.1.2 VPN Gateway

Für den Aufbau sicherer Kommunikationstunnel über das öffentliche Internet stellt das VPN Gateway eine Reihe von Verschlüsselungssystemen bereit. Die VT security unterstützt eine Vielzahl von VPN-Protokollen wie IPSec, L2TP over IPSec und PPTP.

3.2 VT security [advanced]

Im Produkt VT security [advanced] sind die Security Module des Produktes VT security [basic] enthalten und als Auswahloption, ist das Modul Email-Security oder Web-Security enthalten, das im folgenden beschrieben wird.

3.2.1 Modul „E-Mail-Security“

3.2.1.1 Virenerkennung für E-mail

Virus Protection for E-Mail kann Viren im E-Mail-Datenverkehr erkennen, wobei ein- und ausgehenden E-Mail-Nachrichten, sowie die E-Mail-Anhänge (SMTP und POP3) gescannt werden. Wird ein Virus festgestellt, so wird die infizierte E-Mail entsprechend nach Kundenwunsch abgewiesen oder in Quarantäne verschoben. Die VT security unterstützt mehrere Filtermethoden und nutzt eine Datenbank mit üblicherweise mehr als 100.000 Virenpatterns, die eine hoch effiziente Trefferquote sicherstellt. Die Virenerkennung beschränkt sich auf die bei der VT security eingesetzten Virensclannern bekannten Viren und Dateiformate. VT security installiert automatisch Updates der Virendefinitionen. Das Modul gewährleistet nur die bei Virensclannern übliche Trefferquote, und ersetzt nicht die üblichen Netz- und Client basiesernden Virensclanner.

3.2.1.2 Spam Protection

Spam Protection kann unerwünschte E-Mails erkennen und markieren. Durch den Einsatz verschiedener Erkennungsmechanismen ist es möglich, eine hohe

Trefferquote zur Erkennung unerwünschter E-Mails, wie z.B. störende Werbung zu ermöglichen. Die leistungsfähige Identifizierung von Spam-E-Mails erfolgt durch:

- Überprüfung des Absenders
- Realtime Blackhole Lists
- Analyse des Headers
- Heuristische Analyse des Inhalts
- Überprüfung des SPF-Eintrags
- URL scanning
- Greylisting
- BATV Reverse Path Signing
- Whitelists
- Blacklist

3.2.1.3 Phishing Protection

Phishing-Mails täuschen offiziell wirkende Nachrichten, wie z. B. von Finanzinstitutionen, Webplattformen und anderen Quellen vor, um Benutzer zur Preisgabe vertraulicher Informationen zu verleiten. Die Phishing Protection nutzt mehrere Mechanismen, um Phishing-Mails erkennen zu können:

- Textvergleich mit bekannten Phishing E-Mails
- Blockieren verdächtiger Links (im Zusammenspiel mit Content Filtering)
- Blockieren typischer Phishing-Signaturen

3.2.2 Modul „Web Security“

Im Produkt VT security [advanced] als Auswahloption, und im VT security [professional] generell, ist das Modul Web Security enthalten, das im folgenden beschrieben wird.

3.2.2.1 Spyware Protection

Die VT security kann sowohl Infektionsversuche mit Spyware, Adware sowie anderen unerwünschten Programmen aus dem Internet unterbinden und die Preisgabe vertraulicher Informationen durch bereits infizierte Systeme vermeiden.

3.2.2.2 Virus Protection for Web

Virus Protection for Web kann Viren in Download-Dateien und web-basierten E-Mails erkennen und blocken. Dafür werden HTTP-Daten und per Browser gestarteten FTP-Downloads gescannt und überprüft. Die Virenerkennung beschränkt sich auf die bei der VT security eingesetzten Virensclannern bekannten Viren und Dateiformate. Versatel installiert regelmäßig Updates der eingesetzten Virensclanner. Das Modul gewährleistet nur die bei Virensclannern übliche Trefferquote, und ersetzt nicht die üblichen Netz- und Client basierenden Virensclanner.

3.2.2.3 Content Filtering

Das Content-Filtering überwacht und kontrolliert den Zugriff auf Webseiten. Eine automatische Analyse von Schlüsselwörtern, Bildinhalten und Textzusammenhängen ordnet URL-Seiten nach insgesamt 60 Kategorien, die individuell gefiltert werden können.

3.3 VT security [professional]

Im Produkt VT security [professional] sind die Security Module des Produktes VT security [basic] enthalten und beide unter 3.2 VT security [advanced] beschriebenen Module E-Mail Security und Web Security enthalten.

3.4 Optionale Leistungen

3.4.1 VPN Secure Zugang

Gegen gesonderte Beauftragung und Vergütung bietet Versatel dem Kunden einen VPN-Secure-Zugang für Mitarbeiter auf Clients wie z.B. Laptops an. Der VPN-Secure-Zugang ermöglicht die IPSec-verschlüsselte Anbindung von Mitarbeitern über das öffentliche Internet an das Kundennetzwerk.

3.4.2 Backup-Anbindung

Gegen gesonderte Beauftragung und Vergütung bietet Versatel dem Kunden die Einrichtung einer Backup-Anbindung. Die Backup-Anbindung der VT security ermöglicht es dem Kunden, im Fall einer Störung der Internetanbindung, eine zusätzliche Einwahlmöglichkeit über eine Backupleitung ins Internet aufzubauen. In Abhängigkeit der realisierten Backup-Möglichkeit können Dienste, die eine feste

Leistungsbeschreibung VT Security [basic], [advanced], [professional]

versatel

V100 608/0112/01. Änderungen vorbehalten.
Gültig ab 01/2012 – Seite 3/3

IP-Adresse erfordern, eingeschränkt nutzbar sein. Bei Nutzung dieser Möglichkeit muss vom Kunden die Backleitung auf eigene Kosten zur Verfügung gestellt werden. Als Backleitung können sowohl eine Internet-Einwahl als auch eine zweite permanente Internetanbindung genutzt werden. Dieser Dienst ist nur unter bestimmten Voraussetzungen möglich, und kann nicht garantiert werden.

3.4.3 Weitere Leistungen

Versatel erbringt jeweils nach Vereinbarung im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten gegen gesondertes Entgelt folgende zusätzliche Leistungen:

- Abbau und Transport und Wiederinbetriebnahme der VT security an einen anderen Installationsort.
- Kundenindividuelle Leistungen, die Versatel nach Vereinbarung für den Kunden erbringt.

4 Service

Versatel beseitigt Störungen ihrer technischen Einrichtungen im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten in zwei unterschiedlichen Service Level Agreements (SLA): Standard und Profi security, die im folgenden beschrieben werden:

4.1 Standard

Der Service Level „Standard“ ist die Standardleistung bei dem Produkt VT security.

4.1.1 Störungsannahme

Versatel nimmt die Störungen täglich von 0.00 bis 24.00 unter den Servicenummern entgegen und erfasst sie in einem Trouble-Ticket-System. Die Rufnummern der Störungshotline entnehmen Sie bitte Ihrer Auftragsbestätigung. Die durchschnittliche Reaktionszeit beträgt:

- Bei Eingang der Störungsmeldung Montag-Freitag 08.00 Uhr-20.00 Uhr durchschnittlich 4 Stunden
- Bei Eingang der Störungsmeldung Montag-Freitag 20.00 Uhr-08.00 Uhr durchschnittlich 8 Stunden
- Bei Eingang der Störungsmeldung Samstag, Sonntag und an Feiertagen beginnt die Reaktionszeit um nächsten Werktag (Montag-Freitag) um 08.00 Uhr und beträgt durchschnittlich 4 Stunden.

4.1.2 Entstörung

Die Entstörung erfolgt während der Servicebereitschaft, werktags (Montag –Freitag) von 08.00 Uhr bis 18.00 Uhr durchschnittlich innerhalb von 24 Stunden nach Eingang der Störungsmeldung. Die Entstörfrist wird freitags ab 18 Uhr, samstags, sonntags und feiertags bis zum folgenden Werktag 8.00 Uhr ausgesetzt.

4.1.3 Dienstverfügbarkeit

Verfügbarkeitsaussagen sind auf den Standort bezogen und werden auf Jahresbasis ermittelt. Die Dauer einer Störung bemisst sich nach dem Zeitraum der zwischen der Benachrichtigung von Versatel durch den Kunden über die Störung und Beseitigung der Störung liegt. Die Verfügbarkeit beträgt 98 % im Jahresmittel. Folgende Ausfallzeiten werden in der Verfügbarkeitsrechnung nicht berücksichtigt:

Fehler, die im Verantwortungsbereich des Kunden liegen unvermeidliche Unterbrechungen aufgrund von Änderungswünschen des Kunden, Ausfälle bedingt durch höhere Gewalt, Kunde wünscht ausdrücklich keine Störungsbehebung, Anlageräumlichkeiten des Kunden sind für die Störungsbehebung vor Ort nicht zugänglich, aufgrund geplanter oder gegenseitig vereinbarter Unterbrechungen infolge Wartungsarbeiten von Versatel (Mo-So: 00:00 Uhr bis 06:00 Uhr sowie nach Bedarf) oder des Kunden, aufgrund von Störungen durch unbefugte Eingriffe des Kunden oder von Drittpersonen an den Ausrüstungen der Netzbetreiber, aufgrund von Störungen an den Hausinstallationen (z. B. Inhouse-Verkabelung), Stromversorgungsanlagen oder an Kundenausrüstungen, aufgrund der Einspielung von Updates und Patches.

4.2 Profi

Der Service Level „Profi security“ wird als kostenpflichtige optionale Leistung bei dem Produkt VT security angeboten. Der Servicelevel Profi (SLA Profi) setzt

ein Hochverfügbarkeits-System (HA-Modus) voraus. Das Hochverfügbarkeits-System wird durch die Verbindung zweier identischer Hardware-Systeme durch einen vom Kunden zu stellenden Switch mit Patchkabel hergestellt. Die Beauftragung des Service Level „Profi security“ erfordert daher die Bestellung eines zusätzlichen kostenpflichtigen Hardware-Systems in der Variante [basic] in gleicher Größe des beauftragten Produktes, ohne Mail- und Websecurity. Die Kosten für das zusätzliche Hardware-System und den Service Level „Profi security“ sind der jeweils bei Vertragsschluss oder nach einer Preisänderung gültigen Preisliste zu entnehmen.

4.2.1 Störungsannahme

Versatel nimmt die Störungen täglich von 0.00 Uhr bis 24.00 Uhr unter den Servicenummern entgegen und erfasst sie in einem Trouble-Ticket-System. Die Rufnummern der Störungshotline entnehmen Sie bitte Ihrer Auftragsbestätigung.

Die durchschnittliche Reaktionszeit beträgt:

- Bei Eingang der Störungsmeldung Montag-Freitag 08.00 Uhr-20.00 Uhr durchschnittlich 1 Stunde
- Bei Eingang der Störungsmeldung Montag-Freitag 20.00 Uhr-08.00 Uhr sowie Samstags, Sonntags und an Feiertagen durchschnittlich 2 Stunden.

4.2.2 Entstörung

Die Entstörung erfolgt, vorbehaltlich der nachfolgenden Ausnahme, während der Servicebereitschaft, täglich von 0.00 Uhr bis 24.00 Uhr durchschnittlich innerhalb von 8 Stunden ab Eingang der Störungsmeldung.

Bei dem, im SLA Profi erforderlichen HA-Modus, wird eine identische Hardware neben die aktive gesetzt. Fällt eine der beiden Systeme aus, übernimmt die verbleibende Hardware den kompletten Dienst. Dieser Fall wird nicht als Störung angesehen. Versatel stellt innerhalb von 48 Stunden nach Eingang der Fehlermeldung den HA-Modus wieder her. Es entsteht keinerlei Einschränkung der Funktionalität. Fallen beide Systeme aus, gelten die o.g. Entstörzeiten.

Versatel teilt nach technischen und betrieblichen Möglichkeiten auf Wunsch des Kunden innerhalb von 2 Stunden nach Eingang der Störungsmeldung ein erstes Zwischenergebnis zum Status der gemeldeten Störung mit.

4.2.3 Dienstverfügbarkeit

Verfügbarkeitsaussagen sind auf den Standort bezogen und werden auf Jahresbasis ermittelt. Die Dauer einer Störung bemisst sich nach dem Zeitraum der zwischen der Benachrichtigung von Versatel durch den Kunden über die Störung und Beseitigung der Störung liegt. Die Verfügbarkeit beträgt 99,6 %. Folgende Ausfallzeiten werden in der Verfügbarkeitsrechnung nicht berücksichtigt:

Fehler die im Verantwortungsbereich des Kunden liegen, unvermeidliche Unterbrechungen aufgrund von Änderungswünschen des Kunden, Ausfällen bedingt durch höhere Gewalt, Kunde wünscht ausdrücklich keine Störungsbehebung vor Ort, Anlageräumlichkeiten des Kunden sind für die Störungsbehebung vor Ort nicht zugänglich, aufgrund geplanter oder gegenseitig vereinbarter Unterbrechungen infolge Wartungsarbeiten von Versatel (Mo.-So.: 00.00 Uhr bis 06.00 Uhr, sowie nach Bedarf) oder des Kunden, aufgrund von Störungen durch unbefugte Eingriffe des Kunden oder von Drittpersonen an den Ausrüstungen der Netzbetreiber, aufgrund von Störungen an den Hausinstallationen (z.B. Inhouse-Verkabelung), Stromversorgungsanlagen oder an Kundenausrüstungen, aufgrund der Einspielung von Updates und Patches. Über geplante Wartungsfenster mit einer Unterbrechung von mehr als 10 Minuten wird der Kunde mindestens 5 Arbeitstage vor Unterbrechung informiert; über das Installieren von kritischen Updates / Patches erfolgt keine separate Kundeninformation.