

1. Übersicht

Das Colt Internet Access Services-Portfolio besteht aus einer Reihe von Colt Services. Sie können diese Services kombinieren, um eine spezifische Lösung zusammenzustellen, oder ein Business Pack bestellen, das vordefinierte Services enthält.

Das Colt Internet Access Services-Portfolio beinhaltet die folgenden Services:

- Colt IP Access
- Colt Managed Dedicated Firewall
- Colt Router-based Firewall
- Colt IP Domain
- Colt IP Mail
- Colt IP Web
- Colt IP Voice Line
- Colt VoIP Access
- Colt Conferencing
- Colt IN Services
- Colt Fax Divert on DDI
- Colt Fax2Mail
- Colt IP Guardian
- Ausfallsicherheit Sprache
- Ausfallsicherheit Daten
- Ausfallsicherheit Sprache & Daten
- Colt Managed Business E-Mail
- Colt Managed E-Mail Security
- Colt Managed E-Mail Archiving
- Colt Managed Virtual Firewall
- Colt Workforce Mobility
- Colt Managed Web Security

Hinweis: Das Auftragsformular für diesen Service ist so aufgebaut, dass Sie nur Produkte und Produktmerkmale auswählen können, die auch miteinander kombinierbar sind.

2. Leistungsbestandteile und Optionen des Service

IP-Zugriff

Übersicht

Colt IP Access bietet einen dedizierten, permanenten Zugang zum öffentlichen Internet sowie eine Reihe von Optionen, wie z. B. verschiedene Zugangsleitungen, DNS, CPE Router und SMTP Relay. Zudem sind diverse Sicherheits- und Kommunikationsoptionen verfügbar.

Technologieplattform

Colt IP Access-Standorte können direkt an die im Besitz von Colt befindliche und selbst gemanagte Glasfaserinfrastruktur angebunden werden. In den städtischen und Langstreckenbereichen unseres Netzes sind zudem ausfallsichere Leitungen erhältlich. Diese gewährleisten während eines Ausfalls die Bereitstellung einer alternativen Strecke auf dem Ring.

Netzwerkzugang

Es gibt zwei Möglichkeiten, Colt IP Access für Ihren Standort bereitzustellen:

- On-Net bei durchgängiger Verwendung des im Besitz von Colt befindlichen Glasfaserkabels für Standorte, die direkt an unser Netzwerk angeschlossen sind, oder
- Off-Net bei Verwendung einer Leitung eines Drittanbieters (Mietleitungen) oder unserer SDSL-Infrastruktur oder der xDSL-Infrastruktur eines Partners

Wenn Colt die Verbindung zwischen Ihrem Standort und dem Colt Netzwerk kontrolliert, wird dieser Service entweder als geteilter oder ungeteilter Service, wie unten erläutert, bereitgestellt. Bei einem geteilten Service wird die Kapazität der Zugangsleitung mit anderen Benutzern geteilt.

Colt Fibre	Ungeteilt
Colt SDSL	Ungeteilt
Drittanbieter	Ungeteilt
Premium DSL	Ungeteilt
Business/Standard DSL	Geteilt

Colt IP Access Services werden während der Geschäftszeiten installiert. Die Geschäftszeiten sind von Montag bis Freitag zwischen 8.30 und 17.30 Uhr Ortszeit, allgemeine oder gesetzliche Feiertage ausgenommen. Wenn Sie eine Installation Ihres Services außerhalb der Geschäftszeiten wünschen, fallen dafür unter Umständen zusätzliche Installationsgebühren an.

Funktionen

Die folgenden Funktionen gehören zum Standardumfang des Colt IP Access Service:

Vom Provider bezogene IP-Adressen	Ein Bereich mit festen, dedizierten vom Provider bezogenen IP-Adressen wird bereitgestellt
Vom Provider unabhängige IP-Adressen	Sie können vom Provider unabhängige IP-Adressen mit den meisten

CCP Colt Internet Access Services – Service-Beschreibung

IP-Adressen	Zugangstechnologien verwenden
IP Domain	Eine IP Domain ist enthalten
Online Performance Reporting	Im Rahmen des IP Access Service werden auch Online Reports für die Service-Leistung und das Service Management bereitgestellt
Abrechnung	Colt bietet feste oder nutzungsabhängige Abrechnungsoptionen für IP-Bandbreitennutzung
Class of Service (COS)	Wir bieten Ihnen bis zu drei COS, die es Ihnen ermöglichen, geschäfts- oder zeitkritischen Datenverkehr (wie Sprach- und Videoanwendungen) bei Überlastung zu priorisieren.

Optionen

Die folgenden Optionen können abhängig von der jeweiligen Implementierung verfügbar sein.

Gemanagter CPE Router	Im Rahmen des Services kann Colt optional auch den Router an Ihrem Standort bereitstellen, installieren, konfigurieren, managen und warten. Gemäß neuester Technologie-Entwicklungen können wir nach eigenem Ermessen virtuelle CPEs anstatt eines physischen Geräts an Ihrem Standort installieren. In beiden Fällen ist kein eigener CPE Router und keine Layer-3 Routing-Funktion erforderlich. Wenn Sie die Option Managed CPE Router nicht auswählen, müssen Sie einen eigenen CPE Router oder eine Layer-3 Routing-Funktion bereitstellen.
Ausfallsicherheit durch Dual Access	Im Rahmen des Services kann Colt optional auch den Router an Ihrem Standort bereitstellen, installieren, konfigurieren, managen und warten. Zudem kann ein ausfallsicherer Zugang über einen weiteren ISP bereitgestellt werden.
Ausfallsichere Optionen für Sprache	Wenn IP Access mit einem Voice Service genutzt wird, sind verschiedene Optionen im Hinblick auf die Ausfallsicherheit für Sprache verfügbar: Ausfallsicherheit für Sprache Umleitung von eingehenden Anrufen – nur VoIP Access Ausfallsicherheit für Sprache und Daten
Einwahl- und DSL Backup	Die primäre Zugangsleitung kann mit einer ISDN-Einwahlverbindung oder einer separaten DSL-Leitung zu Backup-Zwecken geschützt werden.
NAT (Network Address Translation)	Sie haben die Wahl zwischen 'NAT' und 'Kein NAT'
DHCP (Dynamic Host)	Wir können DHCP Services bereitstellen

Configuration Protocol)	
Anzeige der Router-Konfiguration und Event Viewer	Schreibgeschützter Zugriff auf Router-Konfigurationsinformationen ist über eine sichere Website möglich
Schreibgeschützter SNMP-Zugang	Bietet Transparenz für den optionalen gemanagten CPE Router, der die IP-Zugangsleitung an Ihrem Standort abschließt
BGP-4 (Border Gateway Protocol-4) Feed	Für die meisten Zugangstechnologien kann ein BGP-4 Feed mit einigen oder allen Internet Routes bereitgestellt werden. Der BGP Feed verbraucht selbst immer wieder Bandbreite auf der Zugangsleitung
SMTP Mail Relay und Backup	SMTP Mail Relay und SMTP Mail Backup Services sind verfügbar
Colt Speedy Surf und Ausfallsicherheit für Daten	Bietet ein von Colt konfiguriertes CPE, das nichtkritischen Datenverkehr über eine alternative DSL-Verbindung sendet. Sie sind dafür verantwortlich, die alternative DSL-Verbindung und das zugehörige CPE zur Verfügung zu stellen, das eine Verbindung zum Colt CPE herstellt. Die LAN IP-Adresse des CPE, das Ihre alternative DSL-Verbindung unterstützt, muss auf Ihrem Bestellformular angegeben werden. Sie müssen alle Hosts in Ihrem LAN konfigurieren, um die Colt CPE LAN IP-Adresse als Standard-Gateway einzurichten. Das Colt CPE wird dann den als nicht kritisch definierten Datenverkehr zwischen Webbrowsern intelligent auf die LAN IP-Adresse umleiten, die Sie angegeben haben. So werden nur geschäftskritische Daten über die Colt SDSL-Verbindung gesendet. Sie sind weiterhin dafür verantwortlich, Ihre alternative DSL-Verbindung zu managen und deren effektive Funktionsweise sicherzustellen. Wir können diese Funktion bei Bedarf deaktivieren, wenn Ihre alternative Verbindung ausfällt, wir werden jedoch keine Fehlerbehebung durchführen oder Konfigurationsunterstützung für Ihre alternative Verbindung leisten.

Wir haben ein Upgrade für unseren Internet Service durchgeführt, um das IPv6-Protokoll zu unterstützen. Wenn Sie sich entscheiden, dieses neue Protokoll zu verwenden, haben Sie die Möglichkeit, es entweder exklusiv zu verwenden oder in Kombination mit dem bestehenden IPv4-Protokoll. Die Verwendung von IPv4 und IPv6 für dieselbe Leitung wird als "Dual-Stack" Service bezeichnet. Bitte

CCP Colt Internet Access Services – Service-Beschreibung

beachten Sie, dass bestimmte Funktionen und Optionen möglicherweise unter IPv6 nicht unterstützt werden (unabhängig davon, ob es exklusiv oder mit einem „Dual-Stack“ Service verwendet wird). Weitere Informationen und mögliche Antworten auf Ihre Fragen finden Sie im Service-Handbuch.

Colt Router-based Firewall

Dieser Service bietet Firewall-Funktionen wie dynamische Paketfilterung nach IP-Adresse und Port-Nummern, Network IP Address Translation und Überwachung des geschützten Netzwerks. Grundlegende Protokollierung wird ebenso unterstützt wie die Konfigurierung einer weniger vertrauenswürdigen Zone (DMZ – demilitarisierte Zone), in der die Server traditionell angeordnet sind.

Router-based Firewall ist ein vollständig gemanagter Service, der Folgendes umfasst:

- Hardware-Reparaturen
- Software Updates
- Erweiterungen und Änderungen
- Reaktion auf sicherheitsrelevante Ereignisse
- Protokolldatei-Speicherung
- Sicherheitsfunktionen und Adressierung

Colt Router-based Firewall bietet Konfigurationsoptionen für eine Zugangskontrollliste (ACL) und reflexive ACLs.

Die Verbindung für das Firewall Management ist über IP Sec in-band.

Zugangskontrolllisten bieten grundlegende Fähigkeiten zum Filtern des Datenverkehrs. Wir konfigurieren die Paketfilter auf der Grundlage Ihrer Kriterien. Sie können festlegen, welche Pakete weitergeleitet und welche Pakete an der Schnittstelle verworfen werden sollen – und zwar auf Grundlage der Informationen zur Vermittlungsschicht jedes einzelnen Pakets.

Reflexive ACLs ermöglichen es, IP-Pakete auf der Grundlage der Informationen zum Sitzungsstatus zu filtern. Die Setup-Pakete für ausgehende Verbindungen (zum Internet) lösen die dynamische Erstellung einer Paketfilterungsregel für den entsprechenden eingehenden Verkehr (in das Netzwerk des Kunden) aus. So kann der Antwortverkehr für bestimmte Anwendungen nur dann in das Kundennetzwerk eintreten, wenn dieser Antwortverkehr als Antwort auf eine von einem Benutzer innerhalb des Kundennetzwerks ausgelöste Verbindung erzeugt wird. Auf diese Weise können Sie für den Anwendungsverkehr für jede Richtung ein unterschiedliches Verhalten vorsehen.

Statisches und dynamisches Network Address Translation (NAT) wird unterstützt.

Sie können über ein sicheres Portal auf die Log-Datei zugreifen und auf der Basis eines rollenden Acht-Tage-Zeitraums Ereignisdaten für die vergangenen acht Tage abrufen. Diese Daten können auch als CSV-Datei (Comma Separated Variable) heruntergeladen werden.

Bei jeglichen Problemen, die durch die in der Log-Datei enthaltenen Informationen erkannt werden, sollte der

Prozess zu Service-Änderungen genutzt werden, um sicherheitsbezogene Maßnahmen auszulösen.

Colt Managed Dedicated Firewall

Dieser Service umfasst einen dedizierten, vom Router abgetrennten Firewall Service. Indem die Firewall-Funktionen mit speziell hierfür ausgelegter Hardware-Plattform und sicherheitsspezifischem Betriebssystem getrennt gehalten werden, wird eine höhere Leistungsfähigkeit erreicht.

Die Firewall befindet sich an Ihrem Standort und wird von uns installiert und per Remote-Zugriff gemanagt und gemäß den von Ihnen festgelegten Sicherheitsrichtlinien (Security Policy) und Ihren Firewall-Regelsätzen konfiguriert.

Colt Managed Dedicated Firewall (MDF) ist in vier verschiedenen Varianten erhältlich, um den verschiedenen Anforderungen an Service- und Netzwerkleistung gerecht zu werden.

Colt Managed Dedicated Firewall umfasst alle Leistungsmerkmale, die mit Services Router-based Firewall verfügbar sind. Darüber hinaus ist eine Konfiguration mit hoher Verfügbarkeit für erweiterte Ausfallsicherheit erhältlich, und die Firewall kann die bei Bedarf von Ihnen eingerichteten VLANs (Virtual LANs) erkennen (bei der Variante Entry Level (Eingangsstufe) nicht verfügbar).

Mit Ausnahme der Eingangsstufe werden alle Varianten der Colt Managed Dedicated Firewall proaktiv überwacht. Wir überwachen eine Reihe von Parametern Ihres Services, einschließlich Geräte-Verfügbarkeit, Netzwerk-Durchsatz, CPU- oder Speicherauslastung. Für jeden Parameter setzen wir einen Warnungsschwellenwert fest. Wenn dieser Schwellenwert überschritten wird, untersuchen wir die Ursache und informieren Sie über die laufenden Maßnahmen.

Webbasiertes Reporting wird bereitgestellt und beinhaltet die Einzelheiten zu den genutzten Sicherheitsrichtlinien, zur Firewall-Leistung und zu Aktivitäts-Statistiken sowie eine Event-Darstellung mit konfigurierbaren Reporting-Intervallen.

Optionen

Colt Managed Dedicated Firewall kann mit folgenden optionalen Deep Inspection-Funktionalitäten als kostenpflichtige Zusatzleistung zur Verfügung gestellt werden:

Signaturbasierter Intrusion Schutz: Erkennt und blockiert Verkehr in der Transportschicht basierend auf einer Datenbank mit Verkehrsprofilen und auffälligen Mustern, die auf einen Angriff hindeuten (Deep Inspection Signaturen) Die Deep Inspection-Funktionalität, die auf der MDF-Plattform verfügbar ist, wird durch die Anzahl der Signaturen in der Datenbank begrenzt und bietet deshalb nicht den umfassenden Schutz eines speziellen, eigenständigen Angriffsschutzsystems.

Colt Managed Virtual Firewall

Dieser Service bietet Firewall-Funktionen wie statusbehaftete Paketfilterung nach IP-Adresse und Port-Nummern, Network IP Address Translation und Überwachung des geschützten Netzwerks sowie grundlegende Protokollierung.

CCP Colt Internet Access Services – Service-Beschreibung

Managed Virtual Firewall ist ein vollständig gemanagter Service, der über eine gemeinsame, von Colt gemanagte und gehostete Infrastruktur angeboten wird. Wir stellen für Sie auf der gemeinsamen Hardware-Plattform eine einzelne Virtual Firewall-Instanz bereit. Diese wird mithilfe von Virtualisierungstechnologie auf der gleichen Plattform von anderen Kunden-Firewall-Instanzen getrennt betrieben. Da es sich hier um eine gemeinsame Plattform handelt, obliegt Colt die Verantwortlichkeit für alle mit Hardware in Verbindung stehenden Angelegenheiten. Der Service umfasst folgende Standardfunktionen:

- Umsetzung einer von Ihnen genehmigten Firewall-Richtlinie
- Protokolldatei-Speicherung
- Sicherheitsfunktionen und Adressierung

Statisches und dynamisches Network Address Translation (NAT) wird unterstützt.

Sie können über ein sicheres Portal auf die Log-Datei zugreifen und auf der Basis eines rollenden 30-Tage-Zeitraums Ereignisdaten für die vergangenen acht Tage abrufen. Diese Daten können auch als CSV-Datei (Comma Separated Variable) heruntergeladen werden. Sie finden die URL für das sichere Portal in Ihrem Begrüßungs-Kit.

Optional:

Bei jeglichen Problemen, die durch die in der Log-Datei enthaltenen Informationen erkannt werden, sollte der Prozess zu Service-Änderungen genutzt werden, um sicherheitsbezogene Maßnahmen auszulösen.

Sie selbst müssen die Protokolldaten prüfen und entscheiden, ob weitere Maßnahmen zu treffen sind. Jede weitere von Ihnen angeforderte Änderung oder Adaption wird von uns in Rechnung gestellt, sollte sie nicht in den Umfang der oben genannten Standardfunktionen fallen.

Regeln, die für alle Firewall-Arten gelten

Es wird vorausgesetzt, dass Sie bereits über Sicherheitsrichtlinien verfügen, in denen die Sicherheitsparameter festgelegt sind, auf deren Basis die Konfiguration Ihrer Colt Router-based, Managed Virtual oder Managed Dedicated Firewall durchgeführt wird. Sie sind für die Sicherheitsrichtlinien und den implementierten Firewall-Regelsatz verantwortlich und müssen sicherstellen, dass diese Richtlinien Ihren Sicherheitsanforderungen entsprechen. (Der Firewall-Regelsatz ist die technische Implementierung der relevanten Parameter, die in den Sicherheitsrichtlinien definiert werden).

In der Folge sind Sie für jegliche Beeinträchtigungen (einschließlich jeglicher Angriffe von außen) verantwortlich, die auf die Sicherheitsrichtlinien oder den Regelsatz zurückzuführen sind, die Sie für die Implementierung bereitgestellt haben. Die von uns für die Wiederherstellung Ihrer Services benötigte Zeit und der entstandene Aufwand können zusätzliche Kosten verursachen.

Sie sind für die Konfiguration des VLANs an Ihrem Standort verantwortlich.

Colt IP Domain

Wir können in Ihrem Auftrag einen Domännennamen registrieren lassen, sofern dieser verfügbar ist. Es können zwei Arten von Domännennamen registriert werden:

- Länderspezifische Domänenerweiterungen (beispielsweise: .de, .fr und .it)
- Generische Top Level Domains (beispielsweise: .com, .org, .net)

Der IP Domain Registrierungs-Service umfasst:

- Erste Registrierung Ihrer Domäne
- Stetige Verwaltung Ihrer Domäne - es können Gebühren anfallen

Wir bieten mit dem IP Access Service die kostenfreie Registrierung eines (1) Domännennamens. Dieser Domänenname beschränkt sich auf:

- eine länderspezifische Domänenerweiterung für ein Colt Land, das über eine Erweiterung verfügt; oder
- eine der folgenden generischen Top Level Domains: com, org, net, biz, info, mobi, eu, asia

Colt IP Mail

Colt IP Mail bietet individuelle Postfächer an.

- Kann mit den meisten E-Mail-Clients zusammenarbeiten
- Bereitstellung einer Webmail-Schnittstelle
- Einschließlich Administratorschnittstelle zum Management der Endbenutzer
- Bereitstellung von Spam- und Virus-Filtern

Colt IP Webpace

Der Colt IP Webpace-Service stellt Ihnen die Tools zur Verfügung, die Sie für die Erstellung und Pflege Ihrer eigenen Webseite benötigen.

- Tausende von direkt nutzbaren Vorlagen und Bildern
- Verschiedene Assistenten, die Ihnen bei der Erstellung Ihrer Webseite helfen
- Unterstützung aller wichtigen Anwendungen und Datenbanken zur Erstellung von Webseiten

Colt Workforce Mobility

Workforce Mobility bietet Endbenutzern die Möglichkeit, sich über eine sichere Internetverbindung mit Ihrem Unternehmensnetzwerk zu verbinden. Der Zugriff auf das Internet für Endbenutzer kann entweder von Ihnen oder von Colt über einen Drittanbieter bereitgestellt werden.

Wenn Colt den Internetanschluss bereitstellt, können sich Ihre Endbenutzer in Großbritannien über ein globales Wi-Fi, einen drahtgebundenen Dial-in-Zugriff oder einen optionalen 3G-Wireless-Zugriff mit Ihrem Unternehmensnetzwerk verbinden und Ihre bestehende Breitband-Internetverbindung mithilfe der bereitgestellten Client Software nutzen.

CCP Colt Internet Access Services – Service-Beschreibung

Für die Sicherung der Benutzer-Internetverbindung sind folgende Verschlüsselungsmethoden verfügbar:

- Secured Socket Layer-Verschlüsselung (SSL) mit verschiedenen Benutzerzugriffsrollen
- IPsec-Verschlüsselung mit einem VPN-Softwareclient

Es bestehen folgende Möglichkeiten zur Authentifizierung von Benutzerzugangs-Anfragen:

- Unsere Authentifizierungssysteme und unser Online-Portal
- Ihre eigenen Authentifizierungssysteme (in diesem Fall leitet Colt alle Zugangs-Anfragen an Ihre Server weiter)

Sie müssen den gesamten Endbenutzer-Support für die als Teil des Workforce Mobility Service gelieferte Hardware und Software bereitstellen. Unser Service und die dazugehörige Service-Gewährleistung stehen nur Ihrer Technikabteilung zur Verfügung. Wir bieten keinen Direkt-Support für Ihre Endbenutzer.

Colt Managed Web Security

Colt Managed Web Security bietet einen mehrstufigen Schutz für die ein- und ausgehende E-Mail-Kommunikation in Ihrem Unternehmen. Damit wird Ihr Unternehmen einerseits vor einer Vielzahl an Sicherheitsbedrohungen beim Datenverkehr im Internet geschützt. Andererseits ermöglicht dies die Durchsetzung von Webinhalt-Richtlinien in Ihrer Benutzergemeinschaft, um unangemessene Internetnutzung zu verhindern.

Der Service muss für alle Internetbenutzer in Ihrem Unternehmen eingerichtet werden, da der gesamte Internetverkehr im Rahmen des Service über die Colt Managed Web Security-Plattform umgeleitet wird.

Pflichten des Kunden

Sie sind für Folgendes verantwortlich:

- Einrichten der Benutzerkonten über das Managed Web Security-Verwaltungsportal. Sie finden die URL für das sichere Portal in Ihrem Begrüßungs-Kit.
- Entsprechende Konfiguration der Endnutzer-PCs und -Laptops, um sowohl die Durchführung des Service als auch die Behebung von Problemen nach der Installation zu ermöglichen

Standardleistungsbestandteile

Anti-Viren- & Anti-Spyware-Programme – Der Service bietet Signaturen und dynamische Gegenmaßnahmen zum Schutz vor einer großen Bandbreite an Spyware und Viren

Moderner Schutz vor Bedrohungen – Blockade bekannter Bedrohungen der nächsten Generation, beispielsweise bösartiger aktiver Inhalte, Botnets, Cross-Site Scripting (XSS), Phishing, sowie Blockade neuer Bedrohungen, sobald diese bekannt werden

URL-Filter – Filtern von Web-Inhalten anhand festgelegter Kriterien. Sie können unterschiedliche Browsing-Richtlinien für unterschiedliche Benutzergruppen festlegen

Web 2.0-Kontrolle – Festlegen und Umsetzen einer Richtlinie in Bezug auf den Zugriff auf Web 2.0-Ressourcen wie Facebook und deren Nutzung

Service-Varianten

Die jeweiligen Standardleistungsbestandteile hängen von der Service-Variante ab, die Sie auf Ihrem Auftragsformular ausgewählt haben. Sie müssen eine Service-Variante für alle Benutzer auswählen. In der folgenden Tabelle findet sich eine Übersicht über die Funktionen, die bei jeder Variante inbegriffen sind:

Funktionen	Filtering Suite	Protection Suite	Control Suite
Antiviren- & Anti-Spyware-Programme	enthalten	enthalten	Enthalten
Moderner Schutz vor Bedrohungen	Nicht enthalten	Enthalten	Enthalten
URL-Filter	Enthalten	Nicht Enthalten	Enthalten
Web 2.0-Kontrolle	Nicht enthalten	Nicht enthalten	Enthalten

Colt IP Voice Line

IP Voice Line ist ein Telefonie-Service, der PRI- oder BRI-Anschlüsse nach dem ETSI-Standard für Ihre alte TDM PBX bereitstellt und den Sprachverkehr über das Colt IP-Netzwerk überträgt. Dieser Service ist für den Anschluss von PBX-Anlagen und Key-switches ausgelegt. Ein Anschluss von Endbenutzergeräten, wie ISDN-Telefongeräten, ist nicht vorgesehen.

Am Kundenstandort wird ein Integrated Access Device (IAD) installiert, um eine Konvertierung zwischen BRI/PRI-Sprachschnittstellen und IP zu ermöglichen. Wir bieten einen umfassenden Support für IAD.

Um die Nutzung der SDSL-Zugangsleitung oder der Zugangsleitung des Colt Fibre Services zu optimieren, komprimiert VoIP bei der Verbindung zwischen der Serviceschnittstelle und dem Colt PSTN Gateway die Sprachdaten pro aktivem Kanal auf ca. 25 Kbit/s bis 32 Kbit/s (ohne Pausenunterdrückung) einschließlich IP-Paket-Overheads.

Die Bandbreite für den Sprachverkehr hat Vorrang, allerdings wird die Gesamtbandbreite dynamisch so zugewiesen, dass der IP-Datenverkehr die gesamte Zugangsbandbreite nutzen kann, wenn keine Anrufe erfolgen.

Funktionen

Unterstützte Kommunikationsmerkmale	Voice- und Faxübertragung
CLIP	CLIP (Calling Line Identification Presentation) ermöglicht die Anzeige der

CCP Colt Internet Access Services – Service-Beschreibung

	Rufnummer des Anrufers (sofern freigeschaltet) in einem Format, das Rückrufe gestattet
CLIR	CLIR (Calling Line Identification Restriction) unterdrückt die Anzeige der Rufnummer des Anrufers für den Angerufenen. Die CLIR-Funktion kann für einzelne oder alle ausgehenden Anrufe aktiviert werden
DDI	DDI (Direct Dialling In) ermöglicht dem Anrufer, direkt bei einer Nebenstelle anzurufen, ohne eine Vermittlung nutzen zu müssen
DTMF	Unterstützung von DTMF (Dual Tone Multi Frequency)-Tönen nach RFC2833 und H.245 (Alphanumeric Type)
Fax	Beachten Sie, dass bei Faxübertragungen, die über IP gesendet werden, Paketverluste und Störungen auftreten können. Der Verlust eines Pakets kann im schlimmsten Fall zur Folge haben, dass das gesamte Fax nicht gesendet wird
Trägerarten	Sprache: Unterstützung von G.729a Codecs. Fax (analog): Unterstützung von ITU T.38 Fax-Relay.
Rufnummern	Wir stellen Ihnen mit dem Service eigene DDI-Nummern bereit. In der Regel handelt es sich hierbei um geografisch gebundene Nummern; hierbei ist jedoch zu beachten, dass besonders gefragte lokale Rufnummern bereits vergeben sein können
Anrufersperre nur Deutschland und Schweiz	Wir bieten Ihnen die Möglichkeit, den Benutzerzugang zu bestimmten Premium Rate-Nummern zu beschränken

Colt VoIP Access

Colt VoIP Access verbindet Ihre IP PBX-Anlage über ein umfassendes IP-Netzwerk mit dem öffentlichen Telefonnetz (PSTN). Mit Colt VoIP Access können Sie Ihre IP PBX den

neuesten Branchenstandards entsprechend für eingehende und ausgehende VoIP-Anrufe nutzen. Der Service umfasst einen PSTN-Telefonnummernbereich. Sie benötigen weder unternehmenseigene Gateways noch separate TDM-Zugangsleitungen.

Der Service unterstützt die VoIP-Signalisierung zwischen Ihrer IP-Telefonanlage und unserem Netzwerk über SIP (Session Initiation Protocol).

- Im Vergleich zu DSL-basierten Verbindungen liegt die Mindestanforderung für ungeteilte physikalische Zugänge (Contention Ratio 2:1) bei einer Bandbreite von 256 kbit/s und mehr.
- Sie müssen sicherstellen, dass ausreichend Zugangsbandbreite zur Verfügung stehen, um vorhersehbare hohe Anrufvolumen bewältigen zu können. Wir empfehlen Ihnen, nicht mehr als 50 % der Ihnen zur Verfügung stehenden Bandbreite für Sprachanrufe zu nutzen, da sich dies bei hohen Anrufvolumen auf die Sprachqualität auswirken kann.
- Sie müssen Ihre IP PBX Anlage so konfigurieren, dass das vollständige Nummernformat gesendet werden kann. Voraussetzung hierfür ist, dass der Standard des Landes erfüllt wird, in dem sich Ihre IP PBX Anlage befindet.
- Um ein korrektes Anruf-Routing zu Notrufdiensten zu ermöglichen, müssen Sie dafür sorgen, dass die beim Angerufenen angezeigte Rufnummer (CLI = Calling Line Identity) dem Ortsnetzkennzahlbereich entspricht, von dem der Ruf abgesetzt wird, und die angezeigte CLI eine Ihnen zur Nutzung zugeteilte Rufnummer ist.

Die Bandbreite für den Sprachverkehr hat Vorrang, allerdings wird die Gesamtbandbreite dynamisch so zugewiesen, dass der IP-Datenverkehr die gesamte Zugangsbandbreite nutzen kann, wenn keine Anrufe erfolgen.

Funktionen

Unterstützte Kommunikationsmerkmale	Voice- und Faxübertragung
CLIP	CLIP (Calling Line Identification Presentation) ermöglicht die Anzeige der Rufnummer des Anrufers (sofern freigeschaltet) in einem Format, das Rückrufe gestattet
CLIR	CLIR (Calling Line Identification Restriction) unterdrückt die Anzeige der Rufnummer des Anrufers für den Angerufenen. Die CLIR-Funktion kann für einzelne oder alle ausgehenden Anrufe aktiviert werden
DDI	DDI (Direct Dialling In) ermöglicht dem Anrufer, direkt bei einer Nebenstelle

	anzurufen, ohne eine Vermittlung nutzen zu müssen
DTMF	Unterstützung von DTMF (Dual Tone Multi Frequency)-Tönen nach RFC2833 und H.245 (Alphanumeric Type)
Fax	Beachten Sie, dass bei Faxübertragungen, die über IP gesendet werden, Paketverluste und Störungen auftreten können. Der Verlust eines Pakets kann im schlimmsten Fall zur Folge haben, dass das gesamte Fax nicht gesendet wird
Signalisierungsprotokolle	Unterstützung von SIP (RFC2361). Übertragung von Multimedia-Daten mit RTP (RFC 1889)
Trägerarten	Sprache: Unterstützung von G.711 (unkomprimiert) und G.729a Codecs. Fax (analog): Unterstützung von ITU T.38 Fax-Relay. Nicht unterstützt werden: uneingeschränkte Daten („Unrestricted Data“/URD), Sub Rate-Optionen und Datenkanäle mit 64 Kbit/s
IP-Adressierung	Öffentliche Adressierung wird unterstützt. Bitte beachten Sie, dass u. U. bestimmte Adressbereiche nicht zur Nutzung zur Verfügung stehen
NAT Traversal	Wir bieten Ihnen NAT (Network Address Translation) Traversal-Unterstützung an
Rufnummern	Wir stellen Ihnen mit dem Service eigene DDI-Nummern bereit. In der Regel handelt es sich hierbei um geografisch gebundene Nummern; hierbei ist jedoch zu beachten, dass besonders gefragte lokale Rufnummern bereits vergeben sein können
Anruf Sperre nur Deutschland und Schweiz	Wir bieten Ihnen die Möglichkeit, den Benutzerzugang zu bestimmten Premium Rate-Nummern zu beschränken

Colt Conferencing

Colt Conferencing ermöglicht Konferenzen und Zusammenarbeit über eine einzige Schnittstelle mithilfe eines Webbrowsers und eines Telefons. Der Service ist vollständig automatisiert und steht rund um die Uhr zur Verfügung. Eine Reservierung oder die Einbeziehung eines Betreibers ist nicht erforderlich.

Colt Conferencing wird in folgenden Ländern angeboten: Belgien, Dänemark, Deutschland, Frankreich, Großbritannien, Irland, Italien, Niederlande, Österreich, Schweden und Schweiz. Konferenzteilnehmer können sich von jedem Standort aus zuschalten, an dem ihnen ein Telefon und ein Internetzugang zur Verfügung stehen.

Pro Konferenz können sich bis zu 125 Teilnehmer für eine beliebige Dauer einwählen. Die Reservierung von Leitungen oder vorherige Festlegung der Gesprächsdauer ist nicht erforderlich.

Sicherheit

Über eine Konferenzraumnummer und eine PIN erhält der Colt Konferenzleiter Zugriff auf die Web- und Sprachfunktion seines Konferenzraums. Eingeladene Teilnehmer benötigen lediglich die Konferenznummer, um an einer Konferenz teilnehmen zu können.

Colt Conferencing bietet dem Konferenzleiter folgende Möglichkeiten:

- Kennwortschutz für Konferenzen
- Sperrung eines Konferenzraums, um das Einwählen weiterer Teilnehmer zu verhindern
- Ausschluss unerwünschter Teilnehmer

Der webbasierte Teil des Colt Conferencing Services verwendet eine SSL-Verschlüsselung.

Während einer Konferenz

Folgende Leistungsmerkmale stehen dem Konferenzleiter während einer Konferenz zur Verfügung:

Leiten und Steuern der Konferenz	Erkennen, wer sich zur Konferenz eingewählt hat Anwählen von Teilnehmern unabhängig von deren Standort Stummschalten (Mute-Modus) von Teilnehmern Aufteilen von Teilnehmern in private Unterkonferenzen, die zu einem späteren Zeitpunkt wieder zur Hauptkonferenz hinzugeschaltet werden können
Während einer Audio-Konferenz	Sicherheits-Management Sperrungen und Öffnen eines Konferenzwartebereichs für die Teilnehmer bis zum Konferenzbeginn Stummschalten/Deaktivieren der Stummschaltung von einzelnen Teilnehmern oder einer Gruppe Anwählen von Teilnehmern Generieren und Managen von

CCP Colt Internet Access Services – Service-Beschreibung

	Unterkonferenzen Ausschließen von Teilnehmern Einrichten akustischer Benachrichtigungssignale Ein- und Auswahl von Teilnehmern Aufzeichnen und Wiedergeben der Konferenz
Während einer Webkonferenz	Nutzen des Präsentations- oder Vollbildmodus Gemeinsame Nutzung von Anwendungen Übertragung von Dateien Einsatz von Whiteboards Durchführung von Web-Touren Nutzung der Chat-Funktion Nutzung von Emoticons während der Präsentation Durchführung von Frage- und Antwort-Sitzungen Durchführung von Abstimmungen und Umfragen Anzeige des Status der Internetverbindung Nutzung von Konferenzmanagement-Tools Zeitweiliges Einbeziehen von Mitpräsentatoren Einbindung von Konференzeinladungen in Ihr E-Mail-Adressbuch Einsehen und Managen der Teilnehmerliste Zugriff auf detailliertes Reporting Nutzung verschiedener Sicherheitsebenen für Inhalt, Netzwerk, Zugang, Streaming Management der Einbindung von Medien

PSTN-Leitung, die direkt mit Ihrem Faxgerät verbunden ist. Eingehende Anrufe für die Faxnummer werden automatisch zur PSTN-Leitung geroutet

Es liegt in Ihrer Verantwortlichkeit, die PSTN-Leitung für den Anschluss Ihres Faxgerätes zu bestellen und über das Auftragsformular die PSTN-Nummern und die Nummern, die Sie umleiten möchten, mitzuteilen.

Colt Fax2Mail

Colt Fax2Mail ermöglicht Ihren Endbenutzern das Senden und Empfangen von Faxen direkt auf dem Desktop. Somit werden Faxgeräte nicht mehr benötigt.

Sie erhalten ein Administratorkonto und Zugang zu einem speziellen Web-Portal, wo Ihr Administrator Endbenutzerkonten erstellen kann - entweder mit neuen Rufnummern oder wiederverwendeten Rufnummern aus Ihrem bestehenden Rufnummernbereich.

Colt Fax2Mail ist im Rahmen diverser Preset-Pakete verfügbar, die sowohl Endbenutzerkonten als auch eine festgelegte Anzahl an eingehenden und ausgehenden Faxseiten pro Monat umfassen. Sollten Sie diese Anzahl überschreiten, behält sich Colt das Recht vor, jede weitere Faxsendung je nach Faxziel mit den in der Preisliste angegebenen Gebühren in Rechnung zu stellen. Bitte beachten Sie, dass Sie mit dem Colt Fax2Mail-Dienst keine Faxe zu Premium-Rate oder Freephone-Nummern senden können.

	Max. Anzahl dedizierter Faxnummern	Max. Anzahl der Seiten, die gesendet werden können	Max. Anzahl der Seiten, die empfangen werden können
Paket A	10	50	50
Paket B	10	100	100
Paket C	10	200	200
Paket D	50	250	250
Paket E	50	500	500
Paket F	50	1000	1000
Paket G	1	100	100

Colt IN-Services

Die Colt Intelligent Network (IN) Services bieten die folgenden beiden Services.

Colt Freephone

Unter diesen Rufnummern eingehende Anrufe sind für den Anrufer kostenlos, sodass Sie die gesamten Kosten des Anrufs tragen.

Colt Shared Cost

Die Kosten eines Anrufs werden zwischen Ihnen und dem Anrufer aufgeteilt. Bei dieser Variante besteht für Sie die Möglichkeit einer Beteiligung an den Anruferumsätzen, abhängig vom gewählten Anruferarif.

Colt IN nutzt "Routing Manager Easy", ein webbasiertes Tool für die Anwendung von Routing-Plänen für Kunden.

Colt Fax Divert on DDI

Der Colt Fax Divert on DDI-Service ermöglicht Ihnen die Weiterleitung Ihrer Faxnummern(n) an eine bestimmte

Colt IP Guardian

Colt IP Guardian bietet erweiterten Schutz vor DDoS-Angriffen (Distributed Denial of Service).

Wenn ein DDoS-Angriff so kritisch ist, dass die Integrität des Colt IP/MPLS-Netzwerks bedroht ist und andere Colt Kunden beeinträchtigt werden könnten, wird Colt den gesamten an Ihre angegriffene IP-Adresse gerichteten Datenverkehr verwerfen, um die Integrität des Colt Netzwerks aufrechtzuerhalten (Black Holing).

Für Kunden, die zusätzlich zu Colt über andere Anbieter angeschlossen sind (mehrfach vernetzte Kunden): Wenn der Verkehr auf dem Netzwerk eines anderen Anbieters aufgrund eines gegen den Kunden gerichteten Angriffes auf das Colt

CCP Colt Internet Access Services – Service-Beschreibung

IP/MPLS-Netzwerk umgeleitet wird, ist Colt berechtigt, alle BGP-Sitzungen, die an den Kunden weitergeleitet werden, zu verwerfen, um das Colt IP/MMPLS-Netzwerk zu schützen.

Colt IP Guardian ist in drei Varianten verfügbar:

- **Continuous (Fortlaufend):** Dies ist die Standardvariante des Services, die ständige und automatische Angriffsverminderung bietet. Sie können den Colt Helpdesk kontaktieren, um den Mitigationsvorgang manuell zu stoppen oder zu ändern. Der Datenverkehr wird jedoch immer automatisch umgeleitet, sobald eine Anomalie erkannt wird.
- **On-Demand** – diese Service-Variante ist im Prinzip wie die Continuous-Variante, sie ermöglicht es Ihnen jedoch auch, Mitigationen über das Colt Portal manuell zu aktivieren und deaktivieren. Standardmäßig ist dies mit demselben automatischen Schutz gekoppelt wie bei der Continuous-Variante. Sie haben jedoch die Möglichkeit, diesen automatischen Schutz auszuschalten, sodass Mitigationen nur dann eingesetzt werden, wenn Sie diese manuell starten. Benachrichtigungen werden per E-Mail versandt. Bitte beachten Sie, dass Mitigationen nicht kontinuierlich ausgeführt werden dürfen. Sie sollten nur dann eine Mitigation starten, wenn Sie fest davon überzeugt sind, dass Sie angegriffen werden, und sollten sie stoppen, wenn Sie glauben, dass der Angriff vorüber ist. Colt behält sich das Recht vor, den Service entweder einzustellen oder die Gebühren anzupassen, wenn diese Regel nicht befolgt wird. Sie müssen Mitigationen über das Colt Portal aktivieren und deaktivieren, das ebenfalls verwendet werden sollte, um den Fortschritt bestehender Mitigationen nachzuverfolgen.
- **Notfallimplementierung:** Colt IP Access-Kunden, die noch keine der oben erwähnten Continuous (Fortlaufend) oder On-Demand-Varianten erworben haben, können uns kontaktieren, um eine Notfallimplementierung des Services anzufordern, wenn ein Angriff gerade geschieht oder unmittelbar bevorsteht. Dieser Service wird für einen bestimmten Zeitraum zur Verfügung gestellt und ist, wie auf dem Bestellformular für die Implementierung angegeben, gebührenpflichtig. Da dieser Service für Notfälle bereitgestellt wird, sind keine Langzeitanalysen Ihrer regulären Verkehrsmuster enthalten. Dadurch besteht hier ein höheres Risiko von falschen Positiven als bei den Continuous (Fortlaufend) oder On-Demand-Standard-Services.

Colt Managed Business E-Mail

Colt Managed Business E-Mail ist ein gemanagter Messaging- und Kollaborationsservice, der über eine von mehreren Kunden gemeinsam genutzte, hochverfügbare, von uns gehostete Microsoft Exchange 2003-Plattform bereitgestellt wird.

Dieser Service beinhaltet den Colt Managed Email Security-Service.

Folgende Plattformen werden bereitgestellt und unterstützt:

Microsoft Exchange	Microsoft Exchange 2003
E-Mail Clients	Outlook 2003
	Outlook Express
Mobile Geräte	Windows Mobile 5.0/6.0
	BlackBerry (v4.0 oder höher)

Pflichten des Kunden

Sie sind für Folgendes verantwortlich:

- Die Ersteinrichtung und laufende Verwaltung der Postfächer und Daten der Benutzer sowie Verteilerlisten mithilfe der von uns bereitgestellten Verwaltungs-Software. Jede von Ihnen durchgeführte substantielle Änderung am Service, die den Speicherplatzbedarf über den im Bestellformular angegebenen Platz hinaus erweitert, führt zu zusätzlichen Kosten, die Ihnen in Rechnung gestellt werden
- Installation und Verwaltung des Outlook Software Clients auf den PCs der Benutzer
- First Line Support für Benutzer – wir unterstützen nur den (die) von Ihnen angegebenen Administrator(en)
- Die Service-Kontinuität der gesamten Kunden-Hardware, aller Software Clients und des Internetzugangs, sofern nicht von uns bereitgestellt
- Verweisen der DNS MX-Datensätze auf die Colt Managed E-Mail Security-Plattform
- Die Migration von einer früher benutzten E-Mail-Plattform auf den Colt Managed Business E-Mail-Service
- Zurücksetzen von Kennwörtern, Neuzuweisung von Postfächern, Änderung der Speicherkontingente
- Einschränken des Port 25-Verkehrs (SMTP) auf der Firewall oder dem Mailserver, so dass nur E-Mail-Nachrichten von Colt akzeptiert werden
- Konfiguration der E-Mail-Richtlinienregeln für den Content-Filter
- Erstellen von Regeln für den Schutz vor Spam und Einrichten von E-Mail-Benachrichtigungen für Benutzer über verdächtige Spam-Nachrichten im Quarantäneordner
- Sicherstellen, dass Benutzer keine Aktivitäten ausführen, die die entsprechenden Nutzungsbestimmungen der Colt Acceptable Use-Richtlinien verletzen (verfügbar unter www.colt.net)

Standardleistungsbestandteile

Die folgenden Postfach-Optionen stehen zur Verfügung:

- Lite Mailbox (100 MB, nur mit Outlook Web Access)
- Standard-Mailbox (250 MB, MAPI Access)
- Standard-Mailbox mit BlackBerry (250 MB, MAPI Access)

CCP Colt Internet Access Services – Service-Beschreibung

- Power-Mailbox (500 MB, MAPI Access)
- Power-Mailbox mit BlackBerry (500 MB, MAPI Access)
- Super User (1 GB, MAPI Access)
- Super User mit BlackBerry (1 GB, MAPI Access)
- Kundenspezifische Mailbox (mit 1 GB+ Speicher, MAPI Access)
- Kundenspezifische Mailbox mit BlackBerry (mit 1 GB+ Speicher, MAPI Access)

Jeder Benutzer von Managed Business E-Mail hat Zugriff auf folgende E-Mail-Leistungsmerkmale:

- Versenden und Empfangen von E-Mail-Nachrichten über einen Client
- Zugriff auf E-Mail-Nachrichten über einen Browser (Outlook Web Access)
- Zugriff auf Kontakte, Kalender, Aufgaben und Ordner
- Schutz vor Spam und Viren aus E-Mails

Zusätzliche Funktionen für die Colt Managed Business E-Mail-Versionen Standard Mailbox, Power Mailbox und Super User:

- Zugriff auf eine internationale Adressenliste (Global Address List, GAL) über den Browser
- Zugriff auf E-Mail-Nachrichten über ein mobiles Endgerät mit Outlook Web Access. Die Bereitstellung des mobilen Endgerätes sowie der Abschluss eines entsprechenden Mobilfunkvertrages obliegt Ihnen. Unterstützte Geräte: Windows Mobile 5.0/6.0-Geräte und BlackBerry-Geräte mit Software-Version 4.0 oder höher. BlackBerry-Geräte müssen in der Lage sein mit BlackBerry Services, die von einem dritten Anbieter bereitgestellt werden, zu arbeiten.
- Gemeinsamer Zugriff auf Kontaktdaten
- Gemeinsamer Zugriff auf persönliche Kalender
- Gemeinsamer Zugriff auf Aufgaben
- Gemeinsamer Zugriff auf öffentliche und persönliche Ordner
- Vollfunktionfähige Version von Microsoft Outlook 2003 (kann von uns gestellt werden, die Nutzungsrechte sind im Managed Business E-Mail-Service enthalten)
- Vollständige Client-Funktionalität offline über Offline Store (OST) und Personal Store (PST)

Software-Lizenzierung

Im Service-Umfang inbegriffen sind:

Lizenzierung der Microsoft® Exchange Server-Plattform

Ihre Dienstanbieter-Zugriffslizenzen (SALs)

Ihre E-Mail-Antiviren-Lizenzen

Ihre Anti Spam-Lizenzen

Unterstützung Ihrer Microsoft®-Lizenzierung innerhalb des Colt E-Mail-Services

Unterstützung der Anti-Viren-Lizenzen

Unterstützung der Anti Spam-Lizenzen

Unterstützte Protokolle

Colt Managed Business E-Mail unterstützt folgende E-Mail-Übertragungsprotokolle:

- Outlook Web Access (nur HTTPS)
- Outlook Mobile Access (nur HTTPS)
- Simple Mail Transfer Protocol (SMTP)
- Post Office Protocol (POP3)
- Internet Message Access Protocol 4 (IMAP4)

POP3 und IMAP4 werden nur über eine sichere Secure Socket Layer (SSL)-Verbindung unterstützt.

E-Mail Storage und Backup

E-Mail-Nachrichten werden täglich gesichert, damit wir beschädigte Postfächer wiederherstellen können. Die Wiederherstellung von gelöschten E-Mail-Nachrichten oder Anhängen auf Ihre Anforderung ist nicht Bestandteil des Services.

Sicherheit und Überwachung

Ein zweistufiger Anti-Viren-Schutz schützt sowohl die Schnittstelle des Systems nach außen (d. h. das Gateway) als auch die E-Mail-Postfächer. Colt Managed Business E-Mail scannt alle ein- und ausgehenden E-Mail-Nachrichten auf bekannte Viren. Darüber hinaus wird der gesamte interne E-Mail-Verkehr mithilfe eines separaten Anti-Viren-Filters nach Viren durchsucht.

Colt Managed Business E-Mail bietet außerdem standardmäßig für alle Postfach-Optionen mit dem Colt Managed E-Mail Security Service einen Anti-Spam-Schutz

Die gesamte Kommunikation zwischen der Managed Business E-Mail Service-Plattform und dem Client des Benutzers erfolgt über eine verschlüsselte Verbindung.

Colt Managed E-Mail Security

Colt Managed E-Mail Security bietet einen mehrstufigen Schutz für die ein- und ausgehende E-Mail-Kommunikation in Ihrem Unternehmen gegen:

- Viren
- Spam
- Phishing
- E-Mail-Richtlinien-Verletzungen

Der Service ist mit Colt Managed Business E-Mail oder als unabhängiger Service verfügbar.

Mit dem Service können mehrere Domänen geschützt werden. Der Service muss für alle aktiven Postfächer innerhalb der jeweiligen Domäne erworben werden.

Fällt der unternehmenseigene E-Mail Server aus oder wird die Verbindung des Servers zum Internet unterbrochen, stellt

CCP Colt Internet Access Services – Service-Beschreibung

der Colt Managed E-Mail Security Service alle eingehenden Nachrichten während des Ausfalls in eine Warteschlange und übermittelt sie, sobald der Server wieder verfügbar ist.

Zudem kann Ihr Administrator benutzerdefinierte Regeln erstellen, um die Einhaltung der E-Mail-Richtlinien des Unternehmens zu gewährleisten.

Colt Managed E-Mail Security wird über das Internet bereitgestellt und erfordert keine spezielle Hardware oder Software.

Colt Managed E-Mail Security unterstützt alle bekannten E-Mail-Plattformen.

Der Service wird durch eine einfache Änderung des MX-Datensatzes aktiviert, wobei der eingehende Port 25-Verkehr (SMTP) eingeschränkt wird: Die Firewall bzw. der E-Mail Server sollte nur E-Mails von Colt akzeptieren.

Managed E-Mail Security kann im Zusammenhang mit jeder Version von Microsoft Windows, die Internet Explorer 7.0 unterstützt, eingesetzt werden.

Pflichten des Kunden

Sie sind für Folgendes verantwortlich:

- Einrichten der Benutzerkonten über die Verwaltungs-Software
- Unterbrechungsfreier Betrieb Ihrer Hardware, Software Clients und Ihres Internetzugangs
- Verweisen der DNS MX-Datensätze auf die Colt Managed E-Mail Security-Plattform
- Einschränken des Port 25-Verkehrs (SMTP) auf der Firewall oder dem Mailserver, so dass nur E-Mail-Nachrichten von Colt akzeptiert werden
- Erstellen von E-Mail-Richtlinienregeln für den Content-Filter
- Erstellen von Regeln für den Schutz vor Spam und Einrichten von E-Mail-Benachrichtigungen für Benutzer über verdächtige Spam-Nachrichten im Quarantäneordner
- Zudem ist Folgendes untersagt:
- Einrichten des E-Mail Servers als Open-Relay- oder Open-Proxy-Server
- Versenden von Massen-E-Mail-Nachrichten bzw. unerwünschten E-Mail-Nachrichten
- Ausführen von anderen Aktivitäten, die die entsprechenden Nutzungsbestimmungen der Colt Acceptable Use-Richtlinien verletzen (verfügbar unter www.colt.net)

Standardleistungsbestandteile

Im Einzelnen bietet der Service folgende Funktionen:

- Multi Engine-Virenschutz für ein- und ausgehende E-Mail-Nachrichten
- Mehrstufiger Spam-Schutz

- Content- und Richtlinienfilter für ein- und ausgehende E-Mail-Nachrichten
- Zwischenspeicherung der E-Mails über einen Zeitraum von 5 Tagen bei Nichtverfügbarkeit Ihres E-Mail-Servers (Warteschlange für eingehende E-Mail-Nachrichten)

Virenschutz wird definiert als Erkennen und Blockieren bekannter Viren durch Filter zur Verhinderung einer Infektion. „Viren“ werden im Allgemeinen als Malware definiert, zu der Viren, Würmer und Trojaner zählen.

Eine Klassifizierung von Malware finden Sie unter

http://www.microsoft.com/technet/security/topics/serversecurity/avdind_2.msp

- Ein Virus wird als bekannt angesehen, wenn ein Viren-Scanner über eine entsprechende Signatur zur Erkennung des Virus verfügt und die Erkennungsfunktion über das Service-Netzwerk verfügbar ist
- Ein Virus muss eine nicht beabsichtigte Infektion verursachen
- Der Virus muss vom Virenfilter des Service gescannt worden sein
- Wenn wir dem Kunden eine E-Mail übermitteln, die mit einem bekannten Virus infiziert ist, informiert Colt den Kunden und ermittelt und entfernt mit ihm gemeinsam den Virus

Der Service bietet keinen Schutz vor:

- Formen von E-Mail-Missbrauch, die nicht als Malware, Adware und Spyware klassifiziert sind
- Beschädigten, fehlerhaften, unvollständigen oder inaktiven Viren, die in Unzustellbarkeitsmeldungen, Benachrichtigungen oder unzustellbaren E-Mail-Nachrichten enthalten sind

Der Colt Managed E-Mail Security Service verwendet mindestens drei verschiedene Antiviren-Engines und kann bei einer erhöhten Virenbedrohung weitere Engines hinzuziehen.

Colt Managed E-Mail Security bietet einen mehrstufigen Schutz vor Spam-Nachrichten.

Zunächst überprüft der Service die eingehenden Verbindungen und blockiert E-Mails von bekannten Spammern. Die Verbindungen werden anhand von Reputationsdatenbanken analysiert, wobei auch eine IP-basierte Authentifizierung erfolgt.

In einem zweiten Schritt überprüfen mehrere Spam-Filter-Engines, die von einem Team aus Antispam-Experten (rund um die Uhr verfügbar) gesteuert werden, die eingehenden Nachrichten, um zwischen Spam und erwünschten E-Mails zu unterscheiden. E-Mail-Nachrichten werden nach bekannten Fingerprints durchsucht und anhand von Spam-Erkennungsregeln bewertet. Verdächtige E-Mails werden in einen Quarantäneordner verschoben, auf den ein von Ihnen benannter Administrator zugreifen kann. Den Endbenutzern können zudem E-Mail Benachrichtigungen über im Quarantäneordner abgelegte E-Mails zugesendet werden.

CCP Colt Internet Access Services – Service-Beschreibung

Der Service kann so konfiguriert werden, dass Endbenutzer Zugriff auf Quarantäneordner erhalten.

Administratoren können mit dem Colt Managed E-Mail Security-Service unternehmensspezifische E-Mail-Richtlinien durchsetzen. Mithilfe eines Tools zur intuitiven Erstellung von Richtlinienregeln können Administratoren Richtlinienregeln für E-Mail-Nachrichten einrichten und managen, die auf einer Vielzahl von Nachrichtenattributen wie z. B. Quell-IP, Absender, Empfänger, Nachrichtengröße, Dateianhang oder Zeichenfolgen im Betreff oder im Nachrichtentext der E-Mail basieren.

Bei einem Ausfall des unternehmenseigenen E-Mail-Servers oder der Internetverbindung stellt der Colt Managed E-Mail Security-Service alle eingehenden E-Mail-Nachrichten für maximal fünf Tage in eine Warteschlange. Sobald der E-Mail Service wieder verfügbar ist, werden alle Nachrichten in der Warteschlange automatisch an ihre Empfänger übertragen.

Ihr Administrator kann den Colt Managed E-Mail Security-Service über ein webbasiertes Portal managen, z. B. Einstellungen für Ihre E-Mail-Domänen vornehmen und bearbeiten. Das Portal bietet zudem eine Vielzahl von Informationen:

- Top-Spam-Empfänger
- Top-Viren-Empfänger
- Prozentsatz der als Spam gekennzeichneten eingehenden E-Mail-Nachrichten
- Gesamtaufkommen der E-Mail-Nachrichten

Die Benachrichtigung von Benutzern über E-Mails im Spam-Quarantäneordner kann in den Sprachen Deutsch, Englisch, Französisch, Holländisch, Italienisch, Portugiesisch oder Spanisch erfolgen.

Colt Managed E-Mail Archiving

Colt Managed E-Mail Archiving ermöglicht die Archivierung der gesamten eingehenden, ausgehenden und internen E-Mail-Kommunikation.

Dieser Service beinhaltet den Colt Managed Email Security-Service.

Der Service ist mit Colt Managed Business E-Mail oder als unabhängiger Service verfügbar.

Colt Managed E-Mail Archiving ist für die folgenden Plattformen verfügbar:

- Microsoft Exchange Enterprise 2003 SP2+

Beim Austausch von E-Mail-Nachrichten über Microsoft Exchange Server 2007 oder 2010 durchsucht der Service diese auf Viren und Spam. Anschließend wird eine Kopie jeder Nachricht in einem sicheren Online-Nachrichtenarchiv erfasst und gespeichert. Alle gespeicherten Nachrichten erhalten einen Zeitstempel, und eine eindeutige Seriennummer.

Der Zugriff auf archivierte Nachrichten erfolgt über eine sichere webbasierte Benutzeroberfläche. Durch umfassende Textindexierung kann das Archiv äußerst flexibel durchsucht werden. Gespeicherte Nachrichten können nach Kopfzeile, Betreffzeile, Nachrichtentext und nach mehr als 200 Typen

von Anhängen durchsucht werden. Sobald Nachrichten gefunden wurden, können diese gekennzeichnet, exportiert, wiederhergestellt und über SMTP weitergeleitet werden.

Pflichten des Kunden

Sie sind für Folgendes verantwortlich:

- Aktivieren der Journaling-Funktion auf Ihren Exchange Server (wenn Sie Colt Managed Business E-Mail nutzen, müssen Sie möglicherweise Ihre Firewall-Richtlinien anpassen.)
- Einrichten der Benutzerkonten über die Verwaltungs-Software
- Unterbrechungsfreier Betrieb Ihrer Hardware, Ihrer Software Clients und Ihres Internetzugangs
- Verweisen der DNS MX-Datensätze auf die Colt Managed E-Mail Archiving-Plattform
- Einschränkung des Port 25-Verkehrs (SMTP) auf der Firewall oder dem E-Mail Server, sodass nur E-Mail-Nachrichten von Colt akzeptiert werden (nur relevant wenn Sie nicht Colt Managed Business E-Mail nutzen)
- Einhaltung aller Pflichten des Kunden, die in der Service-Beschreibung für Colt Managed E-Mail Security angegeben sind

Standardleistungsbestandteile

Nachrichten werden auf Spam, Viren und Verstöße gegen unternehmenseigene E-Mail-Richtlinien geprüft, bevor sie für die Archivierung erfasst werden. So wird sichergestellt, dass unerwünschte Nachrichten nicht im Archiv gespeichert werden.

Der Service stellt einen sicheren Online-Nachrichtenspeicher bereit, mit dem archivierte Nachrichten sofort wiederhergestellt, abgerufen und extrahiert werden können. So kann Ihr Unternehmen wichtige Voraussetzungen für die Einhaltung gesetzlicher Bestimmungen erfüllen.

Der Service bietet vollständigen webbasierten Zugriff auf E-Mail-Nachrichten, sodass Ihre Benutzer auf ein Backup E-Mail-System zurückgreifen können, wenn auf die Hauptplattform nicht zugegriffen werden kann.

Benutzerberechtigungen

Mithilfe vordefinierter Richtlinien kann Ihr Administrator oder der für die Einhaltung von Richtlinien verantwortliche Mitarbeiter Berechtigungen für Benutzer im System festlegen, die mit den Berechtigungen innerhalb des Unternehmens vergleichbar sind.

Dazu zählen:

- Für die Einhaltung von Richtlinien verantwortlicher Mitarbeiter
- Technischer Administrator
- Personalleiter
- Sicherheitsleiter

CCP Colt Internet Access Services – Service-Beschreibung

Darüber hinaus können mithilfe benutzerdefinierter Richtlinien flexible Zugriffsberechtigungen eingerichtet werden.

E-Mail-Filterung

Dieser Service beinhaltet alle Leistungsmerkmale und Vorteile des Colt Managed E-Mail Security-Service. Siehe Beschreibung für diesen Service.

Domännennamen

Die folgenden Bestimmungen gelten im Zusammenhang mit den von Ihnen für die Nutzung im Rahmen von Colt Managed Business E-Mail, Colt Managed E-Mail Security und Colt Managed E-Mail Archiving angegebenen Domännennamen.

Sie sind dafür verantwortlich sicherzustellen, dass die im Auftragsformular angegebenen Domännennamen Ihnen gehören bzw. Sie die Lizenz haben, diese zu nutzen. Sie sind für alle für diese Domänen anfallenden Zahlungen oder Gebühren verantwortlich.

Sie stellen Colt von jeglichen Forderungen, Kosten, Klagen und/oder Verlusten in Verbindung mit Forderungen durch Dritte frei, die angeben, dass die Nutzung des Domännennamens bzw. der Domännennamen ihre Rechte am geistigen Eigentum verletzt.

Die Services werden nur für die Domänen bereitgestellt, die Sie im Auftragsformular auflisten.

CCP Colt IP Access Service Description

3. Business-Pakete

Zusätzlich zu den oben genannten, im Internet Access Service-Portfolio angebotenen Produkten können Colt-Kunden eines der folgenden Business Packs auswählen:

- Colt Business Access Pack
- Colt Business Messaging Pack
- Colt Business Security Pack

Ein Business Pack besteht aus mehreren vorkonfigurierten Funktionalitäten. Jedes dieser Business Packs ist für vier verschiedene Standortgrößen erhältlich.

Die gewählte Größe wird verwendet, um die Konfiguration des Packs zu bestimmen, z. B. die enthaltene IP Access-Bandbreite.

Die vier Standortgrößen sind:

- Zweigstelle - der Kunde muss bereits eine der anderen Standortgrößen gewählt haben bzw. wählen, bevor die Standortgrößenoption Zweigstelle gewählt werden kann
- Kleiner Standort
- Großer Standort
- Sehr großer Standort

In den folgenden Tabellen sind die inbegriffenen Produkte und ihre Erstkonfiguration aufgeführt.

Übersicht Business Packs

Business Access Pack

Standortgröße	Zweigstelle	Kleiner Standort	Großer Standort	Sehr großer Standort
Bandbreite (IP Access)	1 Mbit/s	2 Mbit/s	4 Mbit/s	10 Mbit/s (EoSDH/EFM)
Entweder IP Voice Line (TDM-basiert)	2 bis 4 BRI	4, 6 oder 8 BRI ½ PRI, 1 PRI	8 BRI 1 PRI	1 bis 2 PRI
oder VoIP Access (IP PBX-Konnektivität)	Die genaue Anzahl der zulässigen Anrufe hängt vom gewählten Zugangsverfahren und der CODEC-Kompression ab			
IP Mail (Anz. der Konten)	0	25	50	75
IP Web (Instanzen)	1	1	1	1
IP Domain (Instanzen)	1	1	1	1

Business Messaging Pack

Standortgröße	Zweigstelle	Kleiner Standort	Großer Standort	Sehr großer Standort
Bandbreite (IP Access)	1 Mbit/s	2 Mbit/s	4 Mbit/s	10 Mbit/s (EoSDH/EFM)
Managed Business E-Mail (Anz. der Konten)	0	20 Super-Accounts 1 PDA-Lizenz	40 Super-Accounts 2 PDA-Lizenzen	50 Super-Accounts 2 PDA-Lizenzen
Managed E-Mail Security (Instanzen)	0	1	1	1
IP Web (Instanzen)	1	1	1	1
IP Domain (Instanzen)	1	1	1	1

Business Security Pack

CCP Colt Internet Access Services – Service-Beschreibung

Standortgröße	Zweigstelle	Kleiner Standort	Großer Standort	Sehr großer Standort
Bandbreite (IP Access)	1 Mbit/s	2 Mbit/s	4 Mbit/s	10 Mbit/s (EoSDH/EFM)
Router-based Firewall	1	1	1	1
Managed E-Mail Security (Instanzen)	1	1	1	1
IP Web (Instanzen)	1	1	1	1
IP Domain (Instanzen)	1	1	1	1

Colt-Kunden können nur ein Pack pro Standortauftrag bestellen, wobei jedoch in Bezug auf die Zusatzoptionen bzw. auf zusätzliche Instanzen des inbegriffenen Services, die bezogen werden können, keine Beschränkung besteht. Es gibt allerdings technische Einschränkungen, die für einige Packs gelten können, so wird z. B. beim Business Access Pack keine nutzungsabhängige Abrechnung unterstützt. Weitere Einzelheiten zu Service-Einschränkungen sind im externen Service-Handbuch aufgeführt.