VITHOS

Januar 2012

IT-Dienstleistungen

Infrastruktur-Netzwerke-Security-Monitoring-Administration

Frisch ans Werk

- die Vithos-Frühjahresputz–Aktionen -

Rent-an-Admin

Schließen Sie offene Projekte und ewige Baustellen oder verringern Sie die Kosten von neuen Projekten.

Egal ob Helpdesk-Aufgaben, Umstrukturierungen, offene Projekte oder neue Anforderungen. Trotz niedrigen Ressourcen und geringem Budget.

Mit dem Rent-an-Admin-Paket haben Sie die Möglichkeit für 495.- € pro Manntag Ihr Budget zu schonen, offenen Task abzuschließen und neue Projekte anzugehen.

Die Mindestabnahmemenge beträgt 5 Manntage und sind individuell in einem 12 monatigem Zeitraum abrufbar.

IN DIESEM HEFT

THEMEN IN DIESER AUSGABE

- Offene Baustellen schnell und günstig schließen!
- Neue Preisstruktur bei der Vithos
- Alte Sorgen & neue Herausforderungen: *Mit uns und unseren Partnern lösen Sie Ihre Probleme!*

Neue Preisstruktur 2012

Um unsere Preisstruktur für unsere Kunden noch transparenter zu gestallten und um größere Projekte besser kalkulieren zu können, haben wir die verschiedenen Tarife (Security/ Admin/ Techniker) abgeschafft und einen einheitlichen Tagessatz eingeführt. Dieser beträgt 680,00 € netto pro Manntag.

Non-Profit, Governance und Healthcare Einrichtungen bekommen einen ermäßigten Tagessatz von 560,00 €netto/ pro Manntag.

Mit dem Rent-an-Admin-Paket haben Sie die Möglichkeit für 495.- € pro Manntag Ihr Budget zu schonen, offenen Task abzuschließen und neue Projekte anzugehen.

“Non-Profit, Governance und Healthcare Einrichtungen bekommen einen ermäßigten Tagessatz von 560,00 €netto/ pro Manntag.“

MDaemon

- Flexibilität durch POP, IMAP, SMTP, und DomainPOP-Diensten
- Integration von iPhone, Android, Windows Mobile, Symbian,,Blackberry, Palm
- ActiveSync und SyncML Unterstützung
- integrierter BlackBerry Server
- volle Outlook Unterstützung
- sichere InstantMessaging Applikation
- absolute Sicherheit durch Relay Controls, IP-Abschirmung, SMTP-Authentifikation, Reverse Look-UP etc.
- umfassende Kollaboration: Email, Kalender, Kontakte, Aufgaben, Notizen, Journale
- einfache Administration

www.altn.de

Einer für alles:
Der MDaemon– Groupwareserver von Alt-N
Teure MS-Exchange Migration? Nicht mit uns...

Sie müssen Ihren MS-Exchange auf die aktuelle Version migrieren? Warum nicht die doppelte Funktionalität und bei halbem Preis? Unser Endspurt-Paket„MDaemon 50“ gewährleistet Ihnen einen vollständigen Exchange-Ersatz mit vielen integrierten Mehrwerten! Wie zum Beispiel einen BlackBerry Enterprise Server.

MDaemon Messaging Server ist ein schneller, wirtschaftlich vorteilhafter und sicherer E-Mail- und Groupware-Server und gehört heute mit über 87.000 Installationen, weit mehr als 4,4 Millionen Nutzern und monatlich rund einer Milliarde an verarbeiteten E-Mails zu den beliebtesten Mailservern überhaupt.

Unser Jahres-Endspurt-Paket „MDaemon 50“ umfasst die„schlüsselfertige“ Installation des MDaemon-Mailservers für 50 Benutzer, den Outlook-Connector, Premium-Support des Herstellers, Aktualisierungsgarantie für alle Module und Features für 12 Monate, und, und, und…
Paket-Festpreis: 1.999 .- €

Unser Jahres-Endspurt-Paket „MDaemon 100“ umfasst die „schlüsselfertige“ Installation des MDaemon-Mailservers für 100 Benutzer, den Outlook-Connector, Premium-Support des Herstellers, Aktualisierungsgarantie für alle Module und Features für 12 Monate, und, und, und…
Paket-Festpreis: 2.500 .- €

Sophos Endpoint Protection 10

Complete Security inklusive Verschlüsselung, Web-Schutz und Patch-Analyse

Bei uns erhalten Sie alles, was Sie benötigen, um mit nur einer Konsole und einem Agenten Malware Einhalt zu gebieten und Ihre Daten zu schützen. Und das unabhängig vom Betriebssystem!

Die Complete Security Technologie von Sophos ist schnell, effektiv und schützt Ihre Benutzer unabhängig vom Standort.

Dank einfacher Installation, Bedienung und Verwaltung sparen Sie außerdem Zeit und Geld.

Sie erhalten alle Leistungen in einer Lizenz, gemeinsam mit unbegrenztem 24-Stunden-Support, kostenfreien Sicherheits-Updates, Software-Upgrades, Heimnutzung uvm., ohne Ihr Budget zu überlasten.

Umfassender, vielfach ausgezeichneter Computerschutz

Umfassender Datenschutz

Vereinfachte, zentrale Verwaltung

Zuverlässige Performance und bewährter Support

Software-Komponenten

Enterprise Console
Eine einzige automatisierte Konsole für Windows, Mac, Linux, UNIX und virtuelle Plattformen. Installiert und verwaltet Viren- und Client Firewall-Schutz, Intrusion Prevention, Web- Schutz auf Endpoint-Ebene, Patch-Analyse, Verschlüsselung, Data, Device und Application Control sowie Endpoint- Analyse und -Kontrolle von zentraler Stelle.

Endpoint Security (Anti-Virus, HIPS, Device Control, Application Control, DLP)
Ein zentraler Endpoint-Agent für Windows. Erkennt Viren, Spyware, Adware, Rootkits sowie verdächtige Dateien und Verhaltensweisen. Die Übertragung sensibler Daten an Orte außerhalb des Netzwerks wird überwacht und schädliche bzw. unangemessene Websites werden blockiert. Der Agent kontrolliert auch die Verwendung von Wechselmedien und nicht zugelassenen Anwendungen auf zahlreichen Plattformen.

Client Firewall
Zentral verwaltete Client-Firewall, speziell für Unternehmensumgebungen konzipiert. Blockiert Würmer, stoppt Hacker-Angriffe und wehrt unbefugte Zugriffe ab.

NAC
Network Access Control (NAC) analysiert verwaltete, unverwaltete und nicht zugelassene Computer, erkennt Konfigurationsprobleme (z.B. veralteten Virenschutz oder deaktivierte Firewall) und nimmt Korrekturen vor, bevor Zugriff gewährt wird.

Mobile Security
Schützt Windows Mobile-Smartphones und PDAs vor Viren und Spyware.

Anti-Virus
Schützt Windows, Mac, Linux, UNIX, NetWare, NetApp, EMC und OpenVMS vor Viren.

Sophos PureMessage für Microsoft Exchange
Schützt Microsoft Exchange-Server vor Viren und Spam.

Sophos für SharePoint
Stellt Virenschutz für Microsoft SharePoint-Server, Kennwort- und Computer-Wiederherstellungstools bereit.

Sophos Data Protection Add-On
Verschlüsselt Festplatten vollständig und stellt Funktionen zur Pre-Boot-Authentisierung sowie umfassende Tools zur Wiederherstellung von Kennwörtern und Systemen bereit.

Sophos Patch Assessment Add-On
Scannt und Identifiziert Computer, denen kritische Patches fehlen, zur Behebung von Bedrohungen, die beliebte Sicherheitslücken ausnutzen.

Sophos Endpoint Web Protection Add-On
Setzt Internet-Richtlinien zur Blockierung unangemessener Websites durch.

SOPHOS ENDPOINT 10

Identifiziert neue Bedrohungen, bereinigt diese und reduziert False Positives durch Einsatz unseres praktischen Host Intrusion Prevention -Systems (HIPS).

Scannt über den Endpoint-Agenten auf Internet-Malware und filtert unangemessene Websites. So erhalten Sie standortunabhängigen Web-Schutz und reduzieren gleichzeitig Ihre Kosten für Sicherungsmaßnahmen am Internet-Gateway.

Scannt mittels Patch-Analyse auf kritische Patches, mit denen gefährliche Bedrohungen behoben werden können, und spielt diese mit Bevorzugung ein.

Scannt nur Dateien, die sich verändert haben und überwacht die CPU-Beanspruchung Ihrer Benutzer, damit unsere Scans keine unnötigen Ressourcen beanspruchen und Ihre Benutzer ungestört arbeiten können.

Stellt sicher, dass alle mit Ihrem Netzwerk verbundenen Computer Ihre Sicherheitsrichtlinien erfüllen.

Realisiert dank integrierter und vollständiger Festplattenverschlüsselung eine schnellere Initial- Verschlüsselung und eine um 30 % schnellere laufende Verschlüsselung. So erhalten Ihre Benutzer schneller Zugriff auf benötigte Daten.

Sophos gestaltet das Auffinden von Computern und die Bereitstellung des Virenschutzes kinderleicht. Sie haben sogar die Wahl zwischen unterschiedlichen Methoden, einschl. Active Directory-Integration.

Über ein zentrales Dashboard erhalten Sie Einsicht in den Status des Endpoint-Schutzes, Ereignisse und Maßnahmen auf allen unterstützten Plattformen.

Nach einmaliger Richtlinienerstellung können Richtlinien zahlreichen Gruppen zugeordnet werden.

Dank Active Directory-Synchronisierung werden neue Computer in Ihrem Netzwerk automatisch geschützt.

Die gezielte Desinfektion von Computern ist über unsere zentrale Konsole im Handumdrehen erledigt.

Mittels rollenbasierter Administration können Verantwortlichkeiten für Maßnahmen wie z.B. Infektionsbereinigungen aufgeteilt und delegieönrt werden.

Durch die Konfiguration und Zeitsteuerung von Reports stehen Informationen dann bereit, wenn sie benötigt werden.

Funktionen und Vorteile

Einfache Implementierung.
Nachdem die Bereitstellung und Konfiguration lassen sich Routing, Implementierung und Integration mehrerer WXA-Appliances im Netzwerk unkompliziert realisieren.

Verbesserte Sicherheit.
Die SonicWALL Reassembly-Free Deep Packet Inspection™-Technologie bietet eine zusätzliche Sicherheitsschicht, da der gesamte Datenverkehr auf Bedrohungen geprüft wird, bevor er an die WAN-Beschleunigungs-appliance gesendet wird.

Protokoll-Optimierung.
Latenzen und Chattiness durch leistungsschwache Protokolle und ineffiziente Anwendungskommunikation werden reduziert. Benutzer, die über das WAN auf Unternehmens-Ressourcen zugreifen, profitieren so von einer LANähnlichen Anwendungsperformance.

Byte- und File-Caching.
Senkt den Bandbreitenverbrauch um mehrere Größenordnungen. Auf diese Weise lassen sich bestehende WAN-Links länger nutzen, während gleichzeitig die Benutzererfahrung verbessert wird.

Niedrigere Total TCO (Cost of Ownership).
Dank einer effizienteren Nutzung und besseren Auslastung der verfügbaren WAN-Bandbreite sind keine teuren und unnötigen WAN-Upgrades erforderlich.

Datenkompression.
Sorgt für eine höhere Performance und niedrigere Latenz im WAN.
Windows File Sharing (WFS)-Beschleunigung.

Verkürzt die Antwortzeiten und reduziert das Datenaufkommen beim Herunterladen oder Aufrufen von Dateien auf einem gemeinsam genutzten Laufwerk.

Visualisierung.
Liefert eine Echtzeit-Darstellung der Performance-Steigerung durch die WANBeschleunigung im Netzwerk

SonicWALL WXA WAN Accelerator

- WAN- und Latenzzeiten– Optimierung-

Viele IT-Manager kaufen Bandbreite oder erweiterte Services hinzu, um die WAN (Wide Area Network)-Performance in ihrem Unternehmen zu steigern. Dafür gibt es jetzt eine clevere Alternative:

Statt die Bandbreite immer weiter aufzustocken, können Sie mit SonicWALL Ihre bestehende WAN-Bandbreite optimieren und gleichzeitig Ihre Netzwerksicherheitslösung aufrüsten.

SonicWALL WXA WAN Acceleration Enabler reduzieren die Latenzzeiten von Anwendungen und optimieren in kleinen und mittleren Unternehmen mit Niederlassungen und Außenstellen die Bandbreitennutzung.

Die Appliances reduzieren den Datenverkehr um bis zu 95 Prozent. Deswegen haben Anwender auch schnelleren Zugriff auf geschäftskritische Anwendungen und können somit weit produktiver arbeiten.

- **Einfache Implementierung**
- **Verbesserte Sicherheit**
- **Protokoll-Optimierung**
- **Byte- und File-Caching**
- **Niedrigere TCO**
- **Datenkompression**
- **Windows File Sharing (WFS)-Beschleunigung**
- **Visualisierung**

GFI MailArchiver™ – die führende KMU-Lösung zur E-Mail-Archivierung

Reibungslose Geschäftsabläufe sind auch in kleinen und mittleren Unternehmen ohne die Korrespondenz per E-Mail nicht mehr denkbar. Diese hohe Abhängigkeit hat jedoch Nachteile, wie wachsende Speicheranforderungen bei begrenzten Kapazitäten, regelmäßig erforderliche Backups, problematische PST-Dateien, Schwierigkeiten beim Abruf älterer E-Mails oder auch strenge gesetzliche Compliance und eDiscovery-Vorgaben. All diese Herausforderungen müssen effektiv bewältigt werden, andernfalls drohen schwerwiegende Konsequenzen.

Mit GFI MailArchiver zur Archivierung und Verwaltung der über Microsoft Exchange Server laufenden E-Mail-Kommunikation lassen sich erforderliche Aufgaben zentral lösen. Die führende Lösung zur Langzeitsicherung von E-Mails in KMU ist bereits bei über 10.000 Kunden weltweit im Einsatz. Administratoren können sämtliche elektronische Firmenkorrespondenz in Einklang mit der wachsenden Anzahl an Archivierungsvorschriften (E-Mail-Compliance und eDiscovery) dauerhaft sichern und effizient verwalten – jetzt auch mit GDPdU-zertifizierter Unterstützung für steuerrelevante E-Mail-Korrespondenz. GFI MailArchiver sorgt außerdem für eine bedeutende Entlastung des Exchange- Servers und eine weitaus geringere Abhängigkeit von PST-Dateien.
Neben ihrer leichten Installation und einem überaus geringen Administrationsaufwand überzeugt die Lösung nicht zuletzt auch mit marktweit niedrigsten Preisen.

Sophos Mobile Control

Datenschutz, Richtlinien-Compliance und Device Control für Mobile Devices

Ab sofort können Ihre Mitarbeiter alle Mobiltechnologien im vollen Umfang nutzen, ohne die Sicherheit ihrer Unternehmensdaten zu beeinträchtigen. Mit Over-the-Air- Kontrolle und einem Self-Service-Portal, das den Schutz von Mobiles Devices für jeden zur einfachen Angelegenheit macht, unterstützen wir Sie bei der Sicherung, Überwachung und Kontrolle Ihrer Netzwerkgeräte.

- Schützt iPhone, iPad, Android und Windows Mobile Devices.
- Ermöglicht über seine zentrale Web-Konsole das Enforcement einheitlicher Richtlinien.
- Kontrolliert, welche Smartphones und Tablet-Geräte Zugriff auf Unternehmens -E-Mails erhalten.
- Sperrt Geräte und löscht gespeicherte Daten bei Bedarf remote, um Datenverlusten vorzubeugen und eine lückenlose Compliance sicherzustellen.
- Gibt Usern die Möglichkeit, Geräte über ein Self-Service-Portal zu registrieren und zu schützen.
- Erleichtert die Verwaltung, Bereitstellung und Deinstallation von Anwendungen über eine zentrale Konsole.

Professionelles und zentral managebares WLAN

Aruba ist Hersteller von integrierten Systemen, die es dem Anwender ermöglichen Wireless LAN Dienste, kombiniert mit optimaler User-Mobility als auch mit höchster Sicherheit, über das vorhandene Firmennetzwerk zu realisieren. Aruba Networks bietet Lösungen für die Entwicklung einer sicheren benutzerzentrierten Mobilitätsinfrastruktur in Ihrem Unternehmen. Alle Mitarbeiter erhalten sicheren Zugang zum Unternehmensnetzwerk – über Kabel- und Drahtlosverbindungen.

ArubaOS Basis Software-Module:
WLAN Switching and RF Management, Policy Management, Automatic Radio Management, Authentication, Encryption, User Services, Mobility Services, Intrusion Detection

Um die Basismerkmale von ArubaOS zu erweitern, werden Software-Module für zusätzliche Funktionalitäten angeboten:

VOICE SERVICES bietet Voice over WiFi mit Fast-Roaming von Funkzelle zu Funkzelle, Gespräche werden nicht unterbrochen bzw. gestört. Quality of Service (QoS) ist jederzeit gewährleistet.
POLICY ENFORCEMENT FIREWALL ermöglicht userbasierten Netzzugang und Priorisierung von Applikationen. Die Policy kann auf Basis von Userrollen- und Authorisierungslevels zentral definiert werden. Diese Policy begleitet die Benutzer auch während eines Umzuges im Unternehmensnetzwerk.
WIRELESS INTRUSION PROTECTION schützt Sie vor böswilligen Angriffen auf drahtlose Netzwerke und macht Sie unverwundbar gegen nicht autorisierte AccessPoints und Clients.
REMOTE ACCESS POINT erweitert das Unternehmensnetzwerk auf kleinere Zweigniederlassungen und SoHo-Offices, die einen festen Internetanschluss haben. Die Remote-APSoftware verbindet sich mit dem zentralen Aruba-Controller und gestattet nahtlosen Zugang von zu Hause, aus einem Hotelzimmer oder einer anderen Außenstelle mit Gewährleistung der identischen Securitypolicies.
VPN SERVER dehnt das mobile Unternehmensnetzwerk auf größere Zweigniederlassungen und / oder einzelne Benutzer über das allgemeine Internet aus.
EXTERNAL SERVICES INTERFACE enthält Steuer- und Managementschnittstellen, um Third-Party-Applikationen, Zusatz-Software-Module und Dienstleistungen in Aruba nahtlos zu integrieren.
XSEC bietet den Federal Information Processing Standard (FIPS) 140-2140-2, der beispielsweise zur Verschlüsselung hochsicherer Regierungsnetze verwendet wird.
ARUBA AP 124/125 – 802.11A/N + B/G/N WLAN ACCESS POINT sind leistungsstarke 802.11n (3x3) MIMO, Doppelradio (gleichzeitig 802.11a/n + b/g/n) Indoor AccessPoints mit Datenraten von bis zu 600Mbps. Diese multifunktionalen Funkzellen bieten drahtlosen LAN-Zugang, Luftüberwachung und drahtloses Erkennen von Eindringlingen und Verhindern von Angriffen über das gesamte WLANSpektrum mit 2.4-2.5GHz und 5GHz

SOPHOS MOBILE CONTROL

Daten sichern und Vorschriften lückenlos einhalten

- Schützt vertrauliche Daten, indem Mobile Devices konsistent und sicher konfiguriert werden, einschl. Kennwort-Richtlinien und Bildschirmsperre.
- Ermöglicht es Administratoren oder Benutzern, Geräte remote zu sperren und Daten in wenigen Sekunden zu löschen, wenn ein Mobile Device gestohlen wird oder verloren geht.
- Kontrolliert den Zugriff auf Unternehmens-E-Mails über Exchange ActiveSync Proxy, damit nur richtlinienkonforme Geräte Zugriff auf den E-Mail-Server erhalten.
- Steuert den Einsatz bestimmter Funktionen und Apps (z.B. Spiele oder Bluetooth), welche die Produktivität beeinträchtigen, Datenverluste hervorrufen oder Compliance- Verletzungen verursachen könnten.
- Erfasst und meldet den Datenverkehr von Geräten (z.B. über WiFi, 3G oder Roaming).

iPhone, iPad, Android und Windows Mobile mühelos verwalten

- Sie können Sicherheitsfunktionen auf Geräten aktivieren. So erhalten nur richtlinienkonforme Systeme Zugriffe auf die E-Mail-Server im Unternehmen.
- IT-Administratoren können alle unterstützten Smartphones und Tablet PCs über eine zentrale webbasierte Konsole verwalten – unabhängig von Betriebssystem, Dienstanbieter, Netzwerk oder Gerätestandort.
- Setup und Konfiguration werden Over-the-Air bereitgestellt. Geräte können daher zu jeder Zeit und von jede Standort aus problemlos kontrolliert werden.

Zeitsparende Mobile Security

- Dank des Self-Service-Portals können User Routine-Aufgaben selbst übernehmen, neue Geräte aktivieren und gestohlene Geräte sperren oder löschen.
- Übersichtliche Bestandslisten sämtlicher registrierter Geräte, Konfigurationseinstellungen, Seriennummern, Modellnummern und Hardwaredaten sind im Handumdrehen einsehbar.
- User können Anwendungen auf Geräten verwalten und vorkonfigurierte Anwendungen Over-the- Air bereitstellen. Zudem können Anwendungen auf die gleiche Weise deinstalliert werden.

Astaro All-in-One Internet Security

Die mehrfach preisgekrönte Sicherheitlösung Astaro Security Gateway schützt heute mehr als 100.000 Netze vor Viren, Spam und Hackern, die täglich die Sicherheit von Firmennetzwerken bedrohen.

Unabhängig davon, ob Sie sehr kleine Büros mit bis zu 10 Anwendern zu einem günstigen Preis sichern möchten oder auf der Suche nach maximaler Performance und Zuverlässigkeit in anspruchsvollsten Umgebungen für bis zu einige tausend Anwender sind – Sie profitieren in jedem Fall von den gleichen umfassenden Sicherheitsfunktionen, die unter einer benutzerfreundlichen browserbasierten Oberfläche zusammengefasst sind.

Der Astaro-Unterschied

Nur Astaro Appliances gibt es gleich dreimal: Als Hardware, Software und Virtual Appliance– damit wird die Integration in bestehende Infrastrukturen noch einfacher.

Keiner ist schneller: Mit dem „Astaro 10-Minuten-Setup" gelingt jede Installation im Handumdrehen.

Keiner ist flexibler: Die Astaro „One-Click-Clustering"-Technologie ermöglicht skalierbare Performance und Ausfallsicherheit mit bis zu zehn Cluster-Knoten.

Bereits 47.000 Kunden schützen ihre Netzwerke mit einer Astaro Appliance

Astaro Network Security schützt gegen ausgefeilte Arten von Würmern, Trojanern und Exploits, die mit einer Firewall alleine nicht mehr abzuwehren sind. Zu den Funktionen gehören ein konfigurierbares Intrusion-Protection-System ebenso wie Flood Protection gegen Denial-of-Service-Angriffe und umfassende IPsec- und SSL-Tunnel-Mechanismen zur Erstellung flexibler Site-to-Site- und Remote- Access-VPN-Verbindungen zwischen Büros und mobilen Mitarbeitern.

Astaro Mail Security stellt sicher, dass Missbrauch von E-Mails für Spam, Viren und Verletzungen der Privatsphäre die täglichen Geschäftsabläufe nicht beeinträchtigt. Mithilfe dieser Anwendung werden erwünschte Nachrichten ordnungsgemäß zugestellt und die Mitarbeiter finden, was sie brauchen, ohne mit schädlichen Inhalten konfrontiert zu werden.

Astaro Web Security schützt Ihre Mitarbeiter vor Risiken und ermöglicht es Ihnen, Bedingungen festzulegen, wann und wo Ihre Mitarbeiter Zeit online verbringen dürfen. Spyware und Viren werden gestoppt, bevor sie ins Netzwerk gelangen und Schaden verursachen können. Alle Informationen werden in detaillierten Berichten gesammelt und angeordnet, die Ihnen aufzeigen, wie wirksam Ihre Sicherheitsrichtlinien sind und welche Anpassungen unter Umständen erforderlich sind.

Astaro Web Application Security schützt Ihre Webserver und Applikationen wie Outlook Web Access (OWA) vor ausgefeilten Angriffsmethoden wie SQL Injection und Cross Site Scripting (XSS), die Hacker einsetzen, um Zugriff auf vertrauliche Informationen wie Kreditkartendaten, Sozialversicherungsnummern und andere persönliche Daten zu erlangen. Die Lösung unterstützt Sie zudem hinsichtlich Compliance-Anforderungen, wenn eine Web-Application-Firewall gefordert wird.

Astaro Wireless Security ist ein neuer Ansatz, der den Betrieb sicherer und zuverlässiger WLANs wesentlich vereinfacht. Mit den kostengünstigen und konfigurationslosen Access Points und dem integrierten Wireless Controller im Astaro Security Gateway ist die Einrichtung von WLAN-Lösungen für kleine und mittlere Unternehmen so einfach wie nie zuvor.

Astaro RED (Remote Ethernet Device) ist der einfachste und kostengünstigste Weg, Ihre Außenstellen zu sichern. Die Konfiguration erfolgt zentral über ein Astaro Security Gateway in Ihrem Hauptsitz und wird automatisch an alle Astaro RED-Appliances übertragen. Indem es den gesamten Datenverkehr an das zentrale Astaro Security Gateway weiterleitet, bietet Astaro RED auch für die kleinsten Remote oder Home Offices umfassende UTM-Sicherheit. Im Gegensatz zu anderen Security Appliances bietet Astaro RED nicht nur mehr Sicherheit, sondern reduziert auch die Total Cost of Ownership um 80%, da im entfernten Office weder technische Fertigkeiten noch laufende Wartung benötigt werden.

Der Einsatz der **Astaro Access Points** AP 10 und AP 30 ist der einfachste und kostengünstigste Weg, Ihre WLANs zu sichern. Das Management findet dabei zentral über ein Astaro Security Gateway statt, das als WLAN-Controller dient. Die Astaro Access Points selbst erfordern keine Konfiguration. Das bedeutet, dass die Steuerfunktionen in den Access Points auf ein Minimum reduziert sind und stattdessen im WLAN-Controller zentralisiert wurden. Dieser Ansatz verringert die Total Cost of Ownership eines Wireless LAN erheblich, da weniger teure Upgrades benötigt werden und einfache Migrationspfade für zukünftige Technologien zur Verfügung stehen.

In vielen Unternehmen benötigen mobile Mitarbeiter und Heimarbeiter jederzeit und von jedem Standort aus Fernzugriff auf die Daten des Unternehmensnetzwerks. Die Einrichtung dieser Clients auf den einzelnen PCs wird verwaltungstechnisch aber häufig zu einer großen Belastung. **Astaro VPN Clients** bieten für alle Arten von Netzwerkumgebungen und Betriebssystemen mit minimalem Verwaltungsaufwand flexiblen Fernzugriff.

Das **Astaro Command Center** ist eine zentrale Managementanwendung, die Benutzern die Möglichkeit bietet, über ein einziges Login auf alle Astaro Security Gateways zuzugreifen. Sofortig verfügbare Hardwareberichte und Informationen zu aktuellen Sicherheitstrends machen aus der Überwachung und Verwaltung aller Geräte einen effizienten und effektiven Prozess. Mit ein paar einfachen Schritt können IPSec-VPN-Tunnel eingerichtet und Richtlinien auf viele Installationen angewendet werden.

VITHOS

Mehr Informationen? Kein Problem!

Selbstverständlich schicken wir Ihnen mehr Informationen zu Technologien oder Themen, die Sie interessieren.

Wir freuen uns auf Ihre Anfragen!

Ihre Ansprechpartner

Beratung und Vertrieb:

Oliver Thehos

Tel: 0231-5322 1207

Mail: thehos@vithos.de

Beratung und Technik:

Marco Ossig

Tel: 0231-5322 1206

Mail: ossig@vithos.de

Vithos Consulting

Ginsterstraße 6
44225 Dortmund

Telefon: 0231-5322 1200
Telefax: 0231-5322-1201
E-Mail: kontakt@vithos.de

Barracuda Backup Service

Lokale festplattenbasierte Datensicherung und Deduplizierung

Der Barracuda Backup Service stellt eine vollständige und dabei kostengünstige Backup-Lösung für Ihre Daten bereit. Der Barracuda Backup Server sorgt dabei für eine lückenlose lokale Datensicherung und nimmt zudem eine standortferne Replizierung dieser Daten vor. Dieses Hybrid-Konzept vereint das Beste aus zwei Welten – lokale Datensicherungen über eine bestimmte Appliance – für überzeugende Leistung und rasche Wiederherstellungszeiten – sowie eine Datensicherung gegen Komplettverlust durch unseren abgesicherten Cloud Storage bei Barracuda Networks. Die Deduplizierung der Daten erfolgt inline und blockweise, um den üblicherweise erforderlichen Speicherplatz um das 20- bis 50-Fache zu reduzieren. Zugleich vermindern sich die Anforderungen an Backup-Zeiten und Bandbreite.

Leistungsstarke Komplettlösung

Entwickelt für Unternehmen verschiedener Größe mit unterschiedlichen Anforderungen, bewahrt der Barracuda Backup Server eine lokale Kopie der Daten auf und nimmt eine effektive Übertragung dieser Daten an einen standortfernen Speicherort vor, ohne dabei aber die Server im Produktionsbetrieb zusätzlich zu belasten. Der Barracuda Cloud Storage Service wird von Barracuda Central überwacht und verwaltet. Dabei wird eine zuverlässige und sichere Offsite-Speicherung geschäftskritischer Daten bei einer Notfallwiederherstellung gewährleistet. Die Supporttechniker von Barracuda Networks sind täglich rund um die Uhr erreichbar und leisten Nothilfe bei der Wiederherstellung im Falle eines Systemausfalls oder eines umfassenden Datenverlusts.

Die Windows-Software Barracuda Backup Agent, die kostenfrei im Barracuda Backup Service enthalten ist, sorgt für ein lückenloses natives Backup der Daten aus Microsoft Exchange Server, Microsoft SQL Server, des Windows-Systemstatus, sämtlicher Windows-Systemdateien sowie Microsoft Hyper-V-Hosts. Neben der Datensicherung durch den Backup Agent lassen sich mit dem Barracuda Backup Server die Daten unmittelbar über Netzwerkdateifreigaben unter Verwendung von Industriestandardprotokollen sichern. Für eine granulare und bequeme Wiederherstellung von E Mail-Nachrichten und Postfächern kann mit der Sicherungsfunktion auf Nachrichtenebene eine direkte Verbindung mit Microsoft Exchange und Novell GroupWise hergestellt werden.

Benutzerfreundlich und einfach in der Wartung

Die webbasierte Benutzeroberfläche des Barracuda Backup Service erleichtert das Management der Datensicherungen sowie die Durchführung von Datenwiederherstellungen über mehrere Barracuda Backup Server hinweg, an einem oder mehreren Standorten. Die webbasierte Benutzeroberfläche bietet Zugriff und Kontrolle auf bzw. über Einstellungen, Berichte, Wiederherstellungen, Statistiken und Kontoinformationen und es können über eine einzige Schnittstelle mehrere Barracuda Backup Server und Cloud Storage Service- Pläne verwaltet werden. Des weiteren erhält der Kunde eine automatische Warnmeldung, sobald Faktoren erkannt werden, die die Datensicherung negativ beeinflussen.

CLOUD STORAGE SERVICE

Der Barracuda Backup Service kann mit dem Barracuda Cloud Storage Service bereitgestellt werden, um die Anforderungen an Offsite-Backups und Notfallwiederherstellungen zu erfüllen. Die marktführende Cloud Storage ist skalierbar und erschwinglich. Dank moderner Daten-Deduplizierungs- und Kompressionsverfahren werden im Vergleich zu herkömmlichen Backup-Methoden in der Regel 20-50-fache Speichereinsparungen erzielt.