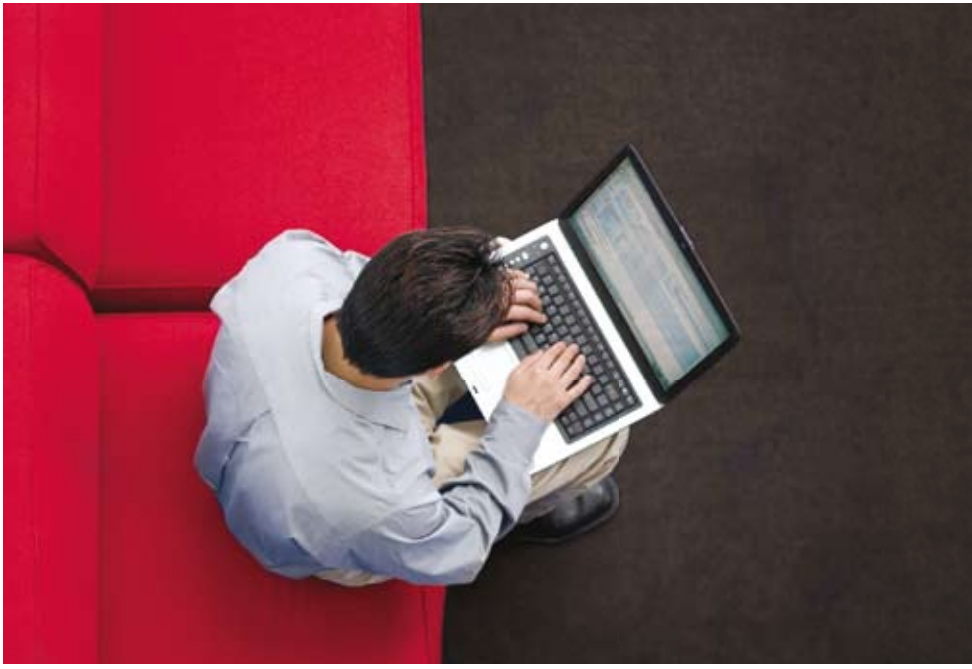
Beveiliging voor ondernemers



Cisco One

Inleiding

Voor u ligt een boekje over netwerkbeveiliging. Beveiliging is één van de meest urgente problemen in het bedrijfsleven. Uit onderzoek blijkt dat 64% van de middelgrote en kleine bedrijven in hoge mate afhankelijk is van ICT en Internet, maar dat 80% geen gestructureerd beveiligingsbeleid heeft. In dit boekje kunt u lezen hoe u de beveiliging van uw bedrijf wél gestructureerd kunt aanpakken.

Beveiliging voor ondernemers

Cisco Self Defending Netwerk
Aan de hand van een groeiscenario laten wij u zien welke stappen u moet nemen als uw bedrijf nieuwe diensten gaat ontwikkelen waarbij u intensiever gebruik gaat maken van Internet. U leest hoe een Cisco Self Defending Netwerk is opgebouwd en welke producten zich het best lenen voor uw specifieke situatie en bedrijfsomvang. In het laatste deel leest u meer over de Cisco MKB Business Partner services en aantrekkelijke financieringsopties.

Cisco helpt mensen en bedrijven om op een slimmere, veiligere en efficiëntere manier te werken. Door uw problemen centraal te stellen, zijn wij in staat technologie te ontwikkelen die uw bedrijf verder helpt. Wij kijken altijd eerst naar uw bedrijfsbehoeften en bepalen aan de hand daarvan welke technologie zich het best leent om hieraan te beantwoorden. Specifiek daarom heeft Cisco een Smart Business Communications aanpak ontwikkeld, een stappenplan dat u helpt bij het realiseren van vier belangrijke bedrijfsdoelstellingen: verhogen van de productiviteit, verlagen van de kosten, beter reageren op de klant en beveiligen van uw bedrijfskritische informatie.

Inhoud

Groeiende beveiligingsrisico's

Informatiebeveiliging: is de grootste uitdaging voor het MKB. Uit onderzoek blijkt dat informatiebeveiliging de grootste uitdaging is waarmee ondernemingen tot 250 medewerkers mee geconfronteerd worden. Tegenwoordig heeft vrijwel iedere onderneming een vaste breedbandverbinding, waardoor het bedrijf continu blootstaat aan bedreigingen zoals virussen, wormen en andere netwerkindringers. We noemen hier een aantal aspecten die invloed hebben op de beveiligingsmaatregelen die u zou moeten nemen.

Webapplicatie

Webapplicaties zijn sterk in opkomst: steeds meer bedrijven maken daar gebruik van voor het onderhouden van relaties of voor het uitvoeren van transacties. Dit stelt echter specifieke eisen aan de beveiliging, niet alleen van de applicatie, maar van uw gehele ICT-omgeving.

Online software

Hosted diensten worden steeds populairder. Daarbij kunt u software afnemen als online dienst, vergelijkbaar met internetbankieren. Met name boekhoudsoftware en klantenbeheersystemen worden volop op deze wijze aangeboden. Dat betekent dat bedrijfskritische informatie zoals financiële gegevens en klantinformatie op een server bij de dienstverlener wordt opgeslagen en via internet toegankelijk is voor alle medewerkers met een gebruikersnaam en wachtwoord. Zonder goede beveiliging kunnen die gegevens gemakkelijk op straat komen te liggen.

Mobiel werken

De risico's nemen tevens toe doordat medewerkers steeds vaker mobiel werken. Ze nemen hun bedrijfslaptop mee naar huis. Het netwerk thuis is vaak niet of matig beveiligd. De draadloze verbinding

staat vaak wagenwijd open, met alle risico's van dien voor de bedrijfskritische informatie die zich op de laptop bevindt. De toegenomen populariteit van mobiel werken betekent ook dat zakenrelaties een verloren kwartiertje graag willen benutten om bij u op kantoor de laptop even aan te zetten om hun e-mail te checken. U weet niet welke virussen, wormen of spyware op deze manier uw bedrijfsnetwerk binnenkomen. Dit soort geavanceerde bedreigingen vraagt om een geavanceerde beveiliging.

Spam

Een ander groot risico is spam. Niet alleen komt er zoveel ongevraagde mail binnen dat medewerkers gemakkelijk een belangrijk mailtje over het hoofd zien, ook worden uw servers onnodig belast. Spamfilters kunnen gelukkig steeds beter filteren, maar het is niet de bedoeling dat een spamfilter goede berichten tegenhoudt. Spamfilters moeten de juiste berichten tegenhouden. Daarnaast leidt spam mensen ook vaak naar webcontent met spyware en andere malware wat een bijkomend risico is.

Wet- en regelgeving

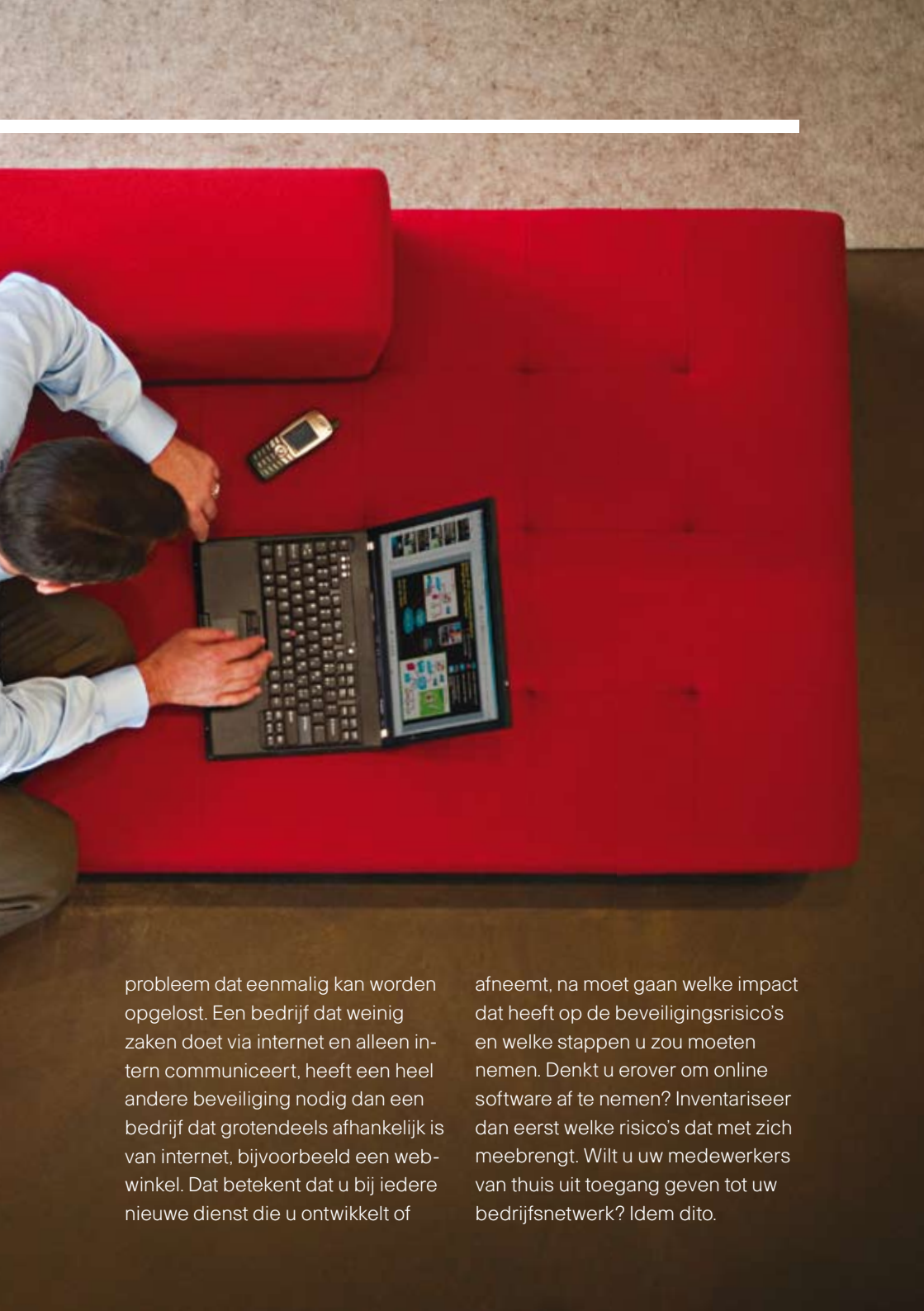
De steeds veranderende bedreigingen voor de beveiliging, zowel van binnen als van buiten het bedrijfsnetwerk, kunnen ernstige gevolgen hebben voor de bedrijfsactiviteiten en daarmee voor de winstgevendheid en klanttevredenheid. Daarnaast moet u voldoen aan nieuwe regels en wetten ter bescherming van persoonsgegevens en beveiliging van elektronische transacties, die enerzijds door de EU worden opgelegd en anderzijds door de Nederlandse overheid. Een voorbeeld hiervan is de Payment Card Industry (PCI) Data Beveiliging Standard, die geldt voor alle bedrijven die met creditcardtransacties te maken hebben.

Kosten

Als er wordt ingebroken op een netwerk brengt dat zowel zichtbare als onzichtbare kosten met zich mee. De meeste inbreuken op de beveiliging, zoals een virus op een PC, veroorzaken relatief weinig schade. De kosten die ermee gemoeid zijn, zijn vooral de tijd om het virus van de geïnfecteerde systemen te verwijderen en de daarmee gepaard gaande verloren werktijd omdat een werknemer moet wachten totdat zijn computer is schoongemaakt. Ernstiger wordt het wanneer het gehele netwerk dermate geïnfecteerd raakt dat het uitvalt. In dat geval is er niet alleen sprake van verloren werktijd, maar ook van gemiste orders, weggelopen klanten en een verslechterde reputatie. De grootste schade als gevolg van slechte beveiliging ontstaat vaak bij diefstal of uitlekken van gegevens. Als uw klantenbestand op straat komt te liggen, is de kans groot dat dit de publiciteit haalt, met alle imagoschade van dien, om nog maar niet te spreken over de kans op een rechtszaak die klanten tegen u kunnen aanspannen. Bij een retailketen die e-mailadressen van klanten verzamelt om ze regelmatig een mailing te kunnen sturen, zal de schade van het uitlekken van gegevens meevallen, bij een incassobureau of accountantskantoor is het vertrouwen dat klanten hebben natuurlijk volledig weg.

Hoe het ook kan

Cisco Self Defending Netwerk
Niemand kan voorspellen wat de toekomst in petto heeft. Wel is duidelijk dat hoe meer onze economie afhankelijk wordt van computernetwerken, hoe interessanter deze netwerken worden voor criminelen, spammers en andere niet gewenste gasten. De beste verdediging is er één die zich gemakkelijk aanpast aan toekomstige bedreigingen en die niet te duur is. Beveiliging is geen



probleem dat eenmalig kan worden opgelost. Een bedrijf dat weinig zaken doet via internet en alleen intern communiceert, heeft een heel andere beveiliging nodig dan een bedrijf dat grotendeels afhankelijk is van internet, bijvoorbeeld een webwinkel. Dat betekent dat u bij iedere nieuwe dienst die u ontwikkelt of afneemt, na moet gaan welke impact dat heeft op de beveiligingsrisico's en welke stappen u zou moeten nemen. Denkt u erover om online software af te nemen? Inventariseer dan eerst welke risico's dat met zich meebrengt. Wilt u uw medewerkers van thuis uit toegang geven tot uw bedrijfsnetwerk? Idem dito.

Uw netwerk vormt een essentieel onderdeel van uw IT-beveiliging, alles in uw bedrijf is er op aangesloten: PC´s, servers, applicaties, telefonie en uw data. Ten eerste moet uw netwerk vooral zelf goed beveiligd zijn, misbruik moet worden voorkomen. Alle door Cisco geleverde producten bieden beveiligingsmogelijkheden om inbraak op het netwerk te voorkomen. U kunt hierbij bijvoorbeeld denken aan toegangsbeveiliging voor beheer of versleuteling van beheersgegevens. Om te zorgen dat u niets vergeet bieden we in de beheersapplicaties de mogelijkheid om een door Cisco aanbevolen en geteste standaard beveiligingsconfiguratie te gebruiken.

Daarnaast kan uw netwerk een belangrijke rol spelen in de beveiliging van de aangesloten systemen, software en data. Elke door Cisco geleverde netwerkcomponent biedt hiervoor mogelijkheden, zoals firewalls geïntegreerd in routers en toegangscontrole geïntegreerd in switches. Niet voor niets noemen we dit geïntegreerde beveiliging. En daarbij werken deze systemen ook goed samen. Dit wordt ook wel samenwerkende beveiliging genoemd. Daarnaast kunt u met de Cisco beveiligingsaanpak ook nieuwe vormen van inbraak herkennen. Dit noemen wij het aanpassend vermogen.

De drie elementen: geïntegreerde beveiliging, samenwerking en aanpassend vermogen vormen samen het Cisco Self-Defending Netwerk.

De onderdelen van een Cisco Self Defending Netwerk

De stappen die u dient te nemen om uw eigen bedrijf te beveiligen, zijn uiteraard geheel afhankelijk van uw situatie, dat wil zeggen de manier waarop u zaken doet. Een webwinkel loopt tegen andere problemen aan dan een bedrijf dat buiten e-mail nauwelijks gebruikmaakt van internet. Ook zijn de toekomstplannen belangrijk om in overweging te nemen. Toch zijn er een aantal standaardstappen te definiëren. Cisco werkt samen met locale MKB Select Partners die u kunnen helpen bij onderstaand stappenplan.

Stap 1. Inventariseren

Test je eigen vaardigheden en kennis en die van medewerkers/ collega's en bepaal of er hulp nodig is. Ga na welke informatie en apparatuur, inclusief hardware en software beschermd moet worden. Bepaal met welke bedreigingen en risico's het bedrijf te maken kan krijgen en welke maatregelen reeds getroffen zijn. Maak een prioriteitenlijst van zaken die beveiligd moeten worden.

Stap 2. Plannen

Schrijf procedures over hoe bedreigingen voorkomen en opgespoord kunnen worden, en hoe erop gereageerd moet worden. Maak ook in de organisatie duidelijk wie verantwoordelijk is voor het uitvoeren en controleren van deze procedures. Stel een tijdschema op voor de implementatie. Zorg ook voor afspraken en regels voor werknemers over hoe zij om moeten gaan met bedrijfscomputers en -netwerk, Internet, e-mail enzovoort.

Voer de plannen uit en introduceer het beleid. Communiceer over de voortgang naar de werknemers en biedt hen waar nodig ook trainingen aan.

Stap 4. Controleren
Controleer regelmatig of de procedures en afspraken worden gevolgd en of bijsturing nodig is. Wanneer er veranderingen optreden in personeel, hardware of software kan het namelijk noodzakelijk zijn plannen aan te passen.

Stap 5. Herhalen
Een incident kan een reden zijn om de plannen en procedures te herzien. Maar het kan nooit kwaad om op geregelde tijdstippen (bijvoorbeeld jaarlijks) de plannen en procedures te evalueren en waar nodig aan te passen. Blijf de mogelijke bedreigingen inventariseren om de beveiliging optimaal te houden.

Smart Business Communications aanpak
Een beveiligde IT-omgeving maakt het mogelijk dat de bedrijfsdoelstellingen worden gehaald en dat is waar het uiteindelijk om draait. Om de IT-plannen af te stemmen op de prioriteiten van uw bedrijf, biedt Cisco de Smart Business Communications aanpak: een geïntegreerd bedrijfs- en technologieplan dat ervoor zorgt dat de IT-omgeving meegroeit met uw bedrijf en dat de beveiliging ervan is afgestemd op de situatie. Om groeiende ondernemingen door elke ontwikkelingsfase te leiden - beginfase, groeifase en geoptimaliseerde fase - biedt de Cisco Smart Business Communications aanpak een benadering die bestaat uit drie fases. In de eerste fase wordt de Secure Network Foundation gelegd: een basisbeveiliging die voldoende is voor bedrijven die buiten e-mail nauwelijks gebruikmaken van het Internet en die een uitstekende basis biedt om in een later stadium beveiligingsfuncties aan toe te voegen. In de tweede fase ontstaan nieuwe risico's doordat medewerkers bijvoorbeeld ook thuis toegang willen tot het bedrijfsnetwerk en doordat klanten via Internet bestellingen bij u plaatsen. De maatregelen in deze fase zijn daarop

afgestemd. In de derde fase is Internet een belangrijke levensader van uw bedrijf. U past uw netwerk daarop aan door het zo in te richten dat het zichzelf kan verdedigen. Daarnaast gaat u uw applicaties en data via het web ontsluiten. Cisco noemt dit een Self Defending Netwerk.

Cisco Self Defending Netwerk
Het Cisco Self Defending Netwerk is een geavanceerde beveiligingsoplossing waarmee uiterst betrouwbare, zichzelf verdedigende netwerken worden gebouwd. De beveiliging is voor een groot deel ingebouwd in de al aanwezige netwerkcomponenten, zoals routers en switches. Door deze geïntegreerde benadering bent u er niet alleen zeker van dat uw netwerk op alle onderdelen is beveiligd, het vergemakkelijkt ook nog eens de installatie, onderhoud en beheer. Een Self Defending Netwerk is in staat zichzelf aan te passen aan nieuwe omstandigheden. Het kan bijvoorbeeld zelf nieuwe verdedigingsmechanismen ontwikkelen. Daardoor bent u minder afhankelijk van uw systeembeheerder of Cisco MKB Business Partner.

Onderdelen geïntegreerde beveiligingsstrategie
Het Cisco Self Defending Netwerk bestaat uit verschillende onderdelen.

Threat management
Threat management is erop gericht om bedreigingen buiten uw netwerk te houden.

- Firewall: Firewalls scheiden netwerken die een afwijkend beveiligingsbeleid hebben. Bijvoorbeeld het Internet en uw eigen interne netwerk of uw (virtuele) netwerk voor telefonie en uw (virtuele) netwerk voor data. Firewalls inspecteren het verkeer dat van de ene zone naar de andere zone wil en laten alleen dat verkeer door wat voldoet aan de vooraf gestelde regels (policy). Firewalls zijn dus vergelijkbaar met bewakers bij de deur.
  Ze voeren toegangscontrole uit en voorkomen daarmee dat ongewenst verkeer geen toegang heeft.

- Cisco Intrusion Prevention System: Intrusion Preventie ofwel inbraakbeveiliging wordt gebruikt om het verkeer dat de firewall door laat verder te inspecteren om mogelijke kwaadaardigheden op te sporen en

uit te schakelen. Vergelijk deze functie met camerabewaking in een gebouw, mensen (verkeer) zijn door de bewaker (firewall) binnengelaten, maar eenmaal binnen gaan ze zich kwaadaardig (intrusions) gedragen. Een Intrusion Prevention System (IPS) maakt gebruik van zogenaamde signatures om kwaadaardig gedrag op te sporen en kent net als firewalls een policy. Wat doet de IPS met dit verkeer als er een inbraak wordt gedetecteerd? Om het u gemakkelijk te maken rust Cisco haar Intrusion Prevention Systems uit met een policy die voor veel bedrijven in het MKB een goede bescherming biedt.

- **Web security:** Web security is een verzamelnaam voor een aantal functionaliteiten die ervoor zorgen dat u veilig en in lijn met het beveiligingsbeleid kunt internetten. Websites, ook van respectabele bedrijven, kunnen gecompromitteerd zijn en zonder dat u het weet malware installeren op uw PC of uw gegevens stelen. Ook kunt u opgelicht worden door valse websites die zich voordoen als een website van een ander bedrijf (phishing). URL filtering is een van de web security maatregelen die Cisco biedt. URL filtering zorgt ervoor dat u alleen naar die sites kunt die in geoorloofde categorieën vallen. Content security bekijkt het webverkeer en inspecteert het onder andere op bekende malware, maar kan ook specifieke bestandstypes tegenhouden.

- **E-mail security:** Bij e-mail security denkt u uiteraard direct aan antispam. De hoeveelheden spam groeien nog steeds en spammers blijven nieuwe manieren zoeken om u te bereiken. Een e-mail security gateway zorgt ervoor dat uw e-mailserver en uw gebruikers niet meer worden belast met spam. E-mail security gateways worden continue geüpdate om ervoor te zorgen dat de juiste berichten worden aangemerkt als spam. Daarnaast kunnen e-mail security gateways ervoor zorgen dat het e-mail beveiligingsbeleid wordt nageleefd en malware in e-mails wordt geblokkeerd.

Vulnerability management

Vulnerability management is erop gericht om zwakheden in uw netwerk, servers en desktops op te sporen en te verhelpen.

- **Network Admission Control:** Network Admission Control (NAC) controleert of PC´s die toegang willen hebben tot het netwerk voldoen aan het gestelde beveiligingsbeleid. Het zorgt er dus voor dat uw gebruikers volledig ´bij´ zijn en dat er geen achterstallig onderhoud is. U kunt NAC ook inzetten om mensen van buitenaf toegang tot uw netwerk te geven door gebruik te maken van de optie gastgebruik.

- **Cisco Security Agent:** Cisco Security Agent (CSA) is een compleet beveiligingspakket voor servers en PC´s. CSA geeft u bescherming tegen bekende en onbekende dreigingen. CSA zorgt er dus voor dat u ook beschermt bent, als u nog niet de laatste patches heeft toegepast. Daardoor kunt u patchen op het moment dat u het wil, wat weer kosten bespaart en zorgt voor extra stabiliteit.

- **Smartcare:** Smartcare is een service van Cisco. Het is een service die u in staat stelt uw netwerk veilig en efficiënt te houden. Smartcare geeft u via een dashboard inzicht in uw netwerkprestaties. Potentiële problemen, zoals zwakheden in uw netwerkconfiguratie en software, worden tijdig duidelijk en kunnen proactief worden opgelost. Smartcare spoort die zwakheden op, en geeft aanwijzigen hoe u ze snel kunt oplossen.

- **Identity and Acces management:** Identity and Access management richt zich op het veilig toegankelijk maken van uw netwerk. Door toenemende mobiliteit is dit een onderdeel waar u direct voordelen mee kan boeken voor uw bedrijf door applicaties en data toegankelijk te maken van buitenaf.

- **Virtual Private Networks voor mobiel werken:** Door middel van Virtual Private Networks (VPN) kunnen medewerkers veilig met elkaar en met het kantoor communiceren, zelfs wanneer ze dat via het openbare internet doen. Gebruikersverificatie zorgt ervoor dat alleen bevoegde gebruikers toegang krijgen tot het netwerk. Encryptie garandeert dat de gegevens onleesbaar zijn voor iedereen die de VPN-communicatie via het openbare netwerk probeert te onderscheppen.

Indien gewenst kunnen medewerkers gebruik maken van Web VPN (SSL VPN), een VPN oplossing waarbij de browser de VPN software is op uw PC. U hoeft dus geen software te installeren op de PC. Via de web browser hebben medewerkers na controle van hun inloggegevens toegang tot een portaal. Via dit portaal kunt u alle applicaties beschikbaar stellen die normaliter alleen binnen het bedrijf gebruikt kunnen worden. Wilt u voorkomen dat medewerkers met onveilige PC´s toegang krijgen, dan kunt u gebruik maken van de Cisco Secure Desktop. De Cisco Secure Desktop test de PC voordat het portaal wordt opengesteld. Met Cisco Secure desktop kunt u er ook voor zorgen dat gegevens zoals cookies, browsergeschiedenis, tijdelijke bestanden en gedownloade content niet worden achtergelaten als de web VPN-verbinding wordt verbroken.

- **Virtual Private Networks voor bedrijfsvestigingen:** Indien uw bedrijf meerdere vestigingen heeft, kunt u deze heel eenvoudig met elkaar verbinden door middel van VPN. VPN-verbindingen kunnen ook ingericht worden gebruikmakend van het Internet. Quality of Service zorgt ervoor dat tijdsgevoelige applicaties zoals telefonie prima samen met andere applicaties zoals webbrowsing van één verbinding gebruik kunnen maken.

- **Toegangscontrole voor uw interne netwerk:** Steeds meer bedrijven huren mensen in op tijdelijke basis, of maken gebruik maken van outsourcing of outtasking. Daarnaast neemt het gebruik van draadloze netwerken toe. Twee belangrijke redenen om vragen te stellen bij de beveiliging van het interne netwerk. Wat voor toegang wilt u verlenen aan inhuurkrachten, adviseurs of gasten? Op welke voorwaarden? Welke risico´s brengen 'externen' met zich mee? U beheert tenslotte niet hun PC. Met de oplossingen van Cisco kunt u de toegangscontrole van het interne netwerk zelf regelen en beheren.

Voorbeelden Cisco beveiligingsoplossingen

In dit hoofdstuk vindt u een aantal voorbeelden van de Cisco beveiligingsoplossingen. Voor de juiste oplossing voor uw bedrijf raden we u aan om contact op te nemen met een Cisco MKB Business Partner.

ASA5500 Series - De oplossing om thuis, onderweg en op kantoor veilig draadloos te werken

MKB-bedrijven tot 50 medewerkers

Voor een bedrijf tot 50 medewerkers heeft Cisco de ASA5505 ontwikkeld met de volgende functies:

- Netwerkinfrastructuur: 8 LAN poorten waarvan twee met power over ethernet.
- Firewall met diepgaande inspectie voor bijvoorbeeld instant messaging (doorvoer tot 150 Mb/s).
- Mogelijkheid voor uitbreiding van functies met behulp van secure services module kaarten zoals: Intrusion Prevention Service (IPS): om kwaadaardig verkeer, inclusief wormen en netwerk virussen te detecteren en stoppen voordat ze uw netwerk kunnen beïnvloeden.
- VPN remote access server om gebruikers via Internet een veilige verbinding op te laten zetten naar het interne netwerk. Voor zowel IPsec VPN´s als Web VPN (SSL VPN), doorvoer tot 100 Mb/s.
- VPN site-to-site om VPN's op te zetten tussen verschillende vestigingen, doorvoer tot 100 Mb/s.
- Toekomstige mogelijkheid voor uitbreiding van functies.
- Geïntegreerd beheer voor alle beveiligingsfuncties. Hiermee kan de ASA5505 eenvoudig worden ingesteld. Tevens kan nauwlettend worden bekeken welke beveiligingrisico´s zich voordoen.

Tot 10 gebruikers

ASA5505 firewall en VPN	
ASA5505-BUN-K9	ASA 5505 oplossing met SW, 10 gebruikers, 8 poorten, 3DES/AES
ASA5505-SEC-PL	ASA 5505 SEC. Plus Lic. met HA. DMZ VLAN trunk, meerdere aansluitingen
	Optioneel: alleen nodig voor support van DMZ zone, VLAN's en ISP backup
ASA5500-SSL-10	ASA 5500 SSL VPN 10 User License
	Optioneel: standaard licentie gaat tot 2 SSL VPN sessies, deze licentie breidt dat uit tot 10

Tot 50 gebruikers

ASA5505 firewall en VPN	
ASA5505-50-BUN-K9	ASA 5505 oplossing met SW, 50 gebruikers, 8 poorten, 3DES/AES
ASA5505-SEC-PL	ASA 5505 SEC. Plus Lic. met HA. DMZ VLAN trunk, meerdere aansluitingen
	Optioneel: alleen nodig voor support van DMZ zone, VLAN's en ISP backup
ASA5500-SSL25-K9	ASA 5505 VPN Editie met 25 SSL gebruikers, 50 Fire Wall gebruikers, 3DES/AES
	Optioneel: standaard licentie gaat tot 2 SSL VPN sessies, deze licentie breidt dat uit tot 25

Ongelimiteerd aantal gebruikers

ASA5505 firewall en VPN	
ASA5505-UL-BUN-K9	ASA 5505 oplossing met SW, ongelimiteerd aantal gebruikers, 8 poorten, 3DES/AES
ASA5505-SEC-PL	ASA 5505 SEC. Plus Lic. met HA. DMZ VLAN trunk, meerdere aansluitingen
	Optioneel: alleen nodig voor support van DMZ zone, VLAN's en ISP backup
ASA5500-SSL-25-K9	ASA 5505 VPN Editie w/25 SSL Users, 50 Fire Wall gebruikers, 3DES/AES
	Optioneel: standaard licentie gaat tot 2 SSL VPN sessies, deze licentie breidt dat uit tot 25

MKB-bedrijven tussen de 50 en 250 medewerkers

Voor een bedrijf tussen de 50 en 250 medewerkers heeft Cisco de ASA5510 ontwikkeld. Deze herbergt de volgende functies:

- Netwerkinfrastructuur: 4 LAN poorten waarop switches kunnen worden aangesloten.
- Firewall met diepgaande inspectie voor bijvoorbeeld instant messaging (doorvoer tot 300 Mb/s).
- VPN remote access server om gebruikers via Internet een veilige verbinding op te laten zetten naar het interne netwerk. Voor zowel IPsec VPN´s als Web VPN (SSL VPN), doorvoer tot 170 Mb/s.
- VPN site-to-site om VPN´s op te zetten tussen verschillende vestigingen, doorvoer tot 170 Mb/s.
- Mogelijkheid voor uitbreiding van functies met behulp van secure services module kaarten zoals:
  Intrusion Prevention Service (IPS): om kwaadaardig verkeer, inclusief wormen en netwerk virussen te detecteren en stoppen voordat ze uw netwerk kunnen beïnvloeden.
  Anti-X beveiling: biedt anti-virus, anti-spyware, anti-spam, URL filtering en scanning van pagina´s.
- Geïntegreerd beheer voor alle beveiligingsfuncties. Hiermee kan de ASA5510 eenvoudig worden ingesteld. Tevens kan nauwlettend worden bekeken welke beveiligingsrisico's zich voordoen.

Optie 1: Voor meer dan 50 gebruikers

ASA5510 Fire Wall en VPN	
ASA5510-BUN-K9	ASA 5510 oplossing met SW, 3FE, 3DES/AES
ASA5510-SEC-PL	ASA 5510 Security Plus Licentie w/ A/S HA, meer VLANs + aansluitingen
	Optioneel: voor support van hoge beschikbaarheid, 5 10/100 ethernet poorten
ASA5510-SSL50-K9	ASA 5510 VPN Editie met 50 SSL. Gebruikerslicentie, 3DES/AES
	Optioneel: standaard licentie gaat tot 2 SSL VPN sessies, deze licentie breidt dat uit tot 50

Optie 2: Voor meer dan 50 gebruikers

ASA5510 Fire Wall en VPN en Anti-X module	
ASA5510-CSC10-K9	ASA 5510 oplossing met CSC10, SW, 50 gebruikers AV/Spy, 1 jaar registratie
ASA5510-SEC-PL	ASA 5510 Security Plus Licentie met A/S HA, meer VLANs + aansluitingen
	Optioneel: voor ondersteuning van hoge beschikbaarheid, 5 10/100 ethernet poorten, aantal vlans wordt verhoogd van 50 naar 100
ASA5510-SSL50-K9	ASA 5510 VPN Editie met 50 SSL. Gebruikerslicentie, 3DES/AES
	Optioneel: standaard licentie gaat tot 2 SSL VPN sessies, deze licentie breidt dan uit tot 50
ASA-CSC10-PLUS	ASA 5500 CSC SSM10 Plus Lic. (Spam/URL/Phish, 1Yr Subscript)
	Optioneel: Anti-X module ondersteunt standaard anti-virus en anti-spyware, dit breidt de mogelijkheden uit met anti-spam, anti-phishins. Content filtering
ASA-CSC10-USR-100	ASA 5500 Content Security SSM-10 100 Gebruikerslicentie
	Optioneel: Anti-X module ondersteunt standaard 50 actieve gebruikers en uitbreiding tot 100

Optie 3: Voor meer dan 50 gebruikers

ASA5510 Fire Wall en VPN en IPS module	
ASA5510-AIP-K9	ASA 5510, oplossing met AIP-SSM-10, SW, 3FE, 3DES/AES
ASA5510-SEC-PL	ASA 5510 Security Plus Licentie met A/S, HA, meer VLANs + aansluitingen
	Optioneel: voor ondersteuning van hoge beschikbaarheid, 5 10/100 ethernet poorten, aantal vlans wordt verhoogd van 50 naar 100
ASA5510-SSL50-K9	ASA 5510 VPN Editie met 50 SSL. Gebruikerslicentie, 3DES/AES
	Optioneel: standaard licentie gaat tot 2 SSL VPN sessies, deze licentie breidt dan uit tot 50
ASA-CSC10-PLUS	ASA 5500 CSC SSM10 Plus Lic. (Spam/URL/Phish, 1 jaar registratie)
	Optioneel: Anti-X module ondersteunt standaard anti-virus en anti-spyware, dit breidt de mogelijkheden uit met anti-spam, anti-phishins. Content filtering
ASA-CSC10-USR-100	ASA 5500 Content Security SSM-10 100. Gebruikerslicentie
	Optioneel: Anti-X module ondersteunt standaard 50 actieve gebruikers en uitbreiding tot 100

SA500 Series - De veilige draadloze oplossing voor kleine ondernemingen

De SA500 Series; een All-in-one Security oplossing specifiek voor het MKB segment. De Cisco SA 500 Series Security Appliances bieden veelomvattende gateway security functionaliteit: Firewalling, VPN, en optioneel web en email security mogelijkhedencapabilities.

De Cisco SA500 helpt de productiviteit te verhogen middels enerzijds nauwkeurige controle van web access, spam emails, phising attack, en andere mogelijke bedreigingen. En anderszijds door het besparen op IT resources tijdens viruseliminatie en systeem clean activiteiten.

Met de SA 500 kunt u met een gerust hart nieuwe zakelijke applicaties invoeren zonder bloot te komen staan aan security-kwetsbaarheden.

Mobiele werknemers en zakenpartners kunnen op een veilige manier connecteren met uw bedrijfsnetwerk gebruikmakend van (IPsec) of Secure Sockets Layer (SSL) VPN services.

De Cisco SA 500 Series Security oplossingen beschermen de totale netwerkinfrastructuur, zodat u zich geen zorgen meer hoeft te maken over de laatste security bedreigingen en met een gerust hart weer kunt doen waar u goed in bent: ondernemen.

Cisco SA 520 Series Security Appliances

	Artikelnummer	SA520-K9
Firewall	Statful pakketinspectie doorvoercapaciteit	200 Mbps
	Unified Threat Management (UMT) doorvoercapaciteit	200 Mbps
	Verbindingen	15,000
	Rules	100
	Schema's	●
VPN	3DES/AES VPN doorvoercapaciteit	65 Mbps
	IPsec VPN tunnels	50 max
	SLL VPN tunnels	inclusief 2 seats; licentie is verplicht om te upgraden naar max 25 seats
	Dead peer waarneming	●
	IPsec NAT traversal	●
	NetBIOS broadcast over VPN	●
Trend Micro ProectLink Gateway	URL Filtering	80+ categorieën
	beveiliging tegen bedreigingen van het web	●
	Antispam beveiliging	●
	Viruspatronen	Meer dan 3 miljoen
	Spyware patronen	Meer dan 420 miljoen

	Artikelnummer	SA520-K9
Draadloos	802.1 1b/g/n	○
	2 x 3 multiple input, multiple output (MIMO)	○
	2.4 GHz	○
	Wi-Fi Multimedia quality of service	○
	Unscheduled automatic power save delivery	○
	MAC filtering	○
	WEP, Wi-Fi Protected Access Pre-Shared Key	○
	Basic service set identifier (BSSID)	○
	Ability to dynamically or manually adjust transmit power	○
	Wi-Fi Protected Setup (WPS)	○
Overig	Routing	Statisch RIPv1.v2
	VLAN's	16
	IPsec/Point-to-Point Tunneling Protecol	●
	Message digest	MD5/SHA1/SHA2
	Encryptie	DES/3DES/AES
	Gebruikersdatabase	100
	Dynamische DNS (DDNS)	●
	Load balancing	●
	Geintegreerde en geautomatiseerde failover en failback	Ja, middels optionele poort voor dual WAN
	VeriSign VIP support	●
	Fysieke Interfaces	Alle ethernetpoorten 10BASE-T, 100BASE-TX, 1000BASE-T mogelijk 4 LAN poorten, 1 WAN poort, 1 optionele poort voor gebruik als LAN, WAN of DMZ 1 USB 2.0 poort, 1 Power switch

○ Niet aanwezig ● Aanwezig

Cisco SA 520W Series Security Appliances

	Artikelnummer	SA520-K9
Firewall	Statful pakketinspectie doorvoercapaciteit	200 Mbps
	Unified Threat Management (UMT) doorvoercapaciteit	200 Mbps
	Verbindingen	15,000
	Rules	100
	Schema's	●
VPN	3DES/AES VPN doorvoercapaciteit	65 Mbps
	IPsec VPN tunnels	50 max
	SLL VPN tunnels	inclusief 2 seats; licentie is verplicht om te upgraden naar max 25 seats
	Dead peer waarneming	●
	IPsec NAT traversal	●
	NetBIOS broadcast over VPN	●
Trend Micro ProectLink Gateway	URL Filtering	80+ categorieën
	beveiliging tegen bedreigingen van het web	●
	Antispam beveiliging	●
	Viruspatronen	Meer dan 3 miljoen
	Spyware patronen	Meer dan 420 miljoen

	Artikelnummer	SA520-K9
Draadloos	802.1 1b/g/n	●
	2 x 3 multiple input, multiple output (MIMO)	●
	2.4 GHz	●
	Wi-Fi Multimedia quality of service	●
	Unscheduled automatic power save delivery	●
	MAC filtering	●
	WEP, Wi-Fi Protected Access Pre-Shared Key	●
	Basic service set identifier (BSSID)	●
	Ability to dynamically or manually adjust transmit power	●
	Wi-Fi Protected Setup (WPS)	●
Overig	Routing	Statisch RIPv1.v2
	VLAN's	16
	IPsec/Point-to-Point Tunneling Protecol	●
	Message digest	MD5/SHA1/SHA2
	Encryptie	DES/3DES/AES
	Gebruikersdatabase	100
	Dynamische DNS (DDNS)	●
	Load balancing	●
	Geintegreerde en geautomatiseerde failover en failback	Ja, middels optionele poort voor dual WAN
	VeriSign VIP support	●
	Fysieke Interfaces	Alle ethernetpoorten 10Base-T, 100BASE-TX, 1000BASE-T mogelijk 4 LAN poorten, 1 WAN poort 1 optionele poort voor gebruik als LAN, WAN of DMZ, 1 USB 2.0 poort, 1 Power switch 3 externe antennes

○ Niet aanwezig ● Aanwezig

Cisco SA 540 Series Security Appliances

	Artikelnummer	SA520-K9
Firewall	Statful pakketinspectie doorvoercapaciteit	200 Mbps
	Unified Threat Management (UMT) doorvoercapaciteit	200 Mbps
	Verbindingen	15,000
	Rules	100
	Schema's	●
VPN	3DES/AES VPN doorvoercapaciteit	85 Mbps
	IPsec VPN tunnels	100 max
	SLL VPN tunnels	inclusief 50 seats (max)
	Dead peer waarneming	●
	IPsec NAT traversal	●
	NetBIOS broadcast over VPN	●
Trend Micro ProectLink Gateway	URL Filtering	80+ categorieën
	beveiliging tegen bedreigingen van het web	●
	Antispam beveiliging	●
	Viruspatronen	Meer dan 3 miljoen
	Spyware patronen	Meer dan 420 miljoen

	Artikelnummer	SA520-K9
Draadloos	802.1 1b/g/n	○
	2 x 3 multiple input, multiple output (MIMO)	○
	2.4 GHz	○
	Wi-Fi Multimedia quality of service	○
	Unscheduled automatic power save delivery	○
	MAC filtering	○
	WEP, Wi-Fi Protected Access Pre-Shared Key	○
	Basic service set identifier (BSSID)	○
	Ability to dynamically or manually adjust transmit power	○
	Wi-Fi Protected Setup (WPS)	○
Overig	Routing	Statisch RIPv1.v2
	VLAN's	16
	IPsec/Point-to-Point Tunneling Protecol	●
	Message digest	MD5/SHA1/SHA2
	Encryptie	DES/3DES/AES
	Gebruikersdatabase	100
	Dynamische DNS (DDNS)	●
	Load balancing	●
	Geintegreerde en geautomatiseerde failover en failback	Ja, middels optionele poort voor dual WAN
	VeriSign VIP support	●
	Fysieke Interfaces	Alle ethernetpoorten 10Base-T, 100BASE-TX, 1000BASE-T mogelijk 8 LAN poorten, 1 WAN poort 1 optionele poort voor gebruik als LAN, WAN of DMZ, 1 USB 2.0 poort, 1 Power switch

○ Niet aanwezig ● Aanwezig

Cisco Spam & Virus Blocker - De Anti Spam en Virus oplossing die spam en virussen stopt voordat zij uw computer bereiken!
De Cisco Spam & Virus Blocker is geschikt voor bedrijven van 50 tot 250 gebruikers. Deze intelligente beveiligingsoplossing voorkomt spam in uw zakelijke e-mail, vereist een minimum aan beheer en wordt ondersteund door SenderBase, een netwerkdatabase waarin e-mailbedreigingen worden bijgehouden.

Deze eenvoudig te gebruiken toepassing biedt bescherming tegen spam, virussen en phishing, en is speciaal voor kleine bedrijven ontworpen. Andere antispamtoepassingen vereisen tijdrovend handmatig beheer voor optimale effectiviteit en kunnen het niet opnemen tegen deze oplossing van Cisco.

Voordelen
- Bescherm uw bedrijf tegen gevaarlijke e-mailbedreigingen
- Verhoog de productiviteit van uw werknemers door spam te elimineren
- Verkort de benodigde tijd voor het beheer van toepassingen tegen spam en e-mailbedreigingen
- Verhoog de prestaties van uw netwerk, servers en pc's door ongewenste e-mail te blokkeren
- Verklein uw risico op een spam- of virusaanval die via uw netwerk wordt verspreid

productspecificaties

Functie	Specificatie
Protocollen	· DNS · SSL/Transport Layer Security (TLS) · Network Address Translation (NAT) poorttoewijzing · Simple Mail Transfer Protocol (SMTP) · HTTP, HTTPS · FTP · Simple Network Management Protocol (SNMP) · Network Time Protocol (NTP) · Secure Shell (SSH) · Lightweight Directory Access Protocol (LDAP) · Remote Procedure Call (RPC) · Telnet · TCP/IP

Functie	Specificatie
Harde schijf	2 x 80 GB 2,5 inch 7,2 k seriële ATA (SATA)
Processor	Intel Celeron 440
Connectiviteit	Ethernet; dual embedded Gigabit netwerkinterfacekaarten (NIC's)
Geheugen	2 GB
Betrouwbaarheid en beschikbaarheid	Mean time between failures (MTBF): 74.000 uur
Netwerkbeheer	Toegankelijk via HTTP en HTTPS; opdrachtregelinterface toegankelijk via SSH en Telnet
Netwerkinterface (of programmeer-interface enz.)	Toegankelijk via HTTP en HTTPS; opdrachtregelinterface toegankelijk via SSH en Telnet
Ondersteunde talen	GUI: Engels Documentatie: Engels, Frans, Italiaans, Duits, Spaans, Chinees en Japans
Afmetingen (HxBxD)	1U-rek: 16,1 inch diepte, Gewicht: 6,62 kg (zonder rails)
Voeding	345 W
Temperatuurbereik	Bedrijfstemperatuur: 10 tot 35 °C Opslagtemperatuur: -40 tot 65 °C
Goedkeuringen en compliantie	· UL t/m UL 60950-1 · UL t/m CAN/CSA C22.2 nr. 60950-1 · TUV/GS t/m EN 60950-1 · CB t/m IEC 60950-1 met alle afwijkingen per land · CE-markering Certificaten voor elektromagnetische compatibiliteit: · FCC deel 15 klasse A · EN 55022 klasse A (CISPR22) · EN 55024 (CISPR24) · VCCI klasse A · AS/NZS CISPR22 klasse A · MIC · EMC-vereisten China · GOST
Compatibiliteit mailserver	Te integreren met alle mailservers (Exchange, Notes, Domino enz.)

Cisco Software en Support-abbonement

Bij de eerste aankoop van de Cisco Spam & Virus Blocker-oplossing zijn de hardware, software, licenties voor 50, 100 of 250 gebruikers en één of drie jaar Cisco Software and Support-abonnement inbegrepen. Het is niet noodzakelijk ondersteuning en abonnement afzonderlijk te verkopen voor deze oplossing.

Artikelnummer Aantal gebruikers Aantal jaren support en software

Artikelnummer	Aantal gebruikers	Aantal jaren support en software
BLKR-SVB-50U-1Y	50	1
BLKR-SVB-50U-3Y	50	3
BLKR-SVB-100U-1Y	100	1
BLKR-SVB-100U-3Y	100	3
BLKR-SVB-250U-1Y	250	1
BLKR-SVB-250U-3Y	250	3

Een 'Cisco Software en Support Abonnement is vereist om de Cisco Spam & Virus Blocker up-todate te houden. Verlengingen na het verlopen van het eerste termijn verloopt via de volgende service-product-ID's (SKU's) voor een periode van één of meer jaren.

Gebundelde oplossing - verlenging

Artikelnummer	Aantal gebruikers
CON-BLK-BLKR50U	SW + Supp Subscr NBD Blocker 50 gebruikers
CON-BLK-BLKR100U	SW + Supp Subscr NBD Blocker 100 gebruikers
CON-BLK-BLKR250U	SW + Supp Subscr NBD Blocker 250 gebruikers

Onze dienstverlening aan u

Cisco MKB Business Partners

Cisco werkt samen met een lokaal netwerk van 250 MKB Business Partners. Het doel van onze MKB Business Partners is om u een zo goed mogelijke dienstverlening te bieden. Van nuttige trainingen tot betrouwbare en waardevolle ondersteuning. De partners van Cisco zijn specialisten die precies weten hoe ze het beste uit uw netwerkinfrastructuur kunnen halen op het gebied van Routing & Switching, Unified Communications, draadloze netwerken en beveiliging. Daarnaast hebben zij diepgaande kennis en expertise op het gebied van ontwerp, implementatie, service en onderhoud. Ze kunnen u helpen om uw infrastructuur zo op te zetten dat deze perfect past bij de specifieke eisen die uw bedrijf daaraan stelt. Zodat u uw doel kunt bereiken.

Cisco Services: SMARTnet & MKB Support Assistent

Cisco biedt twee services: SMARTnet en MKB Support Assistent. SMARTnet staat voor Software Maintenance Advance Replacement en Technical assistence. Dit betekent dat in geval apparatuur stuk gaat, deze de volgende werkdag wordt vervangen. U profiteert van voortdurende software updates en upgrades. Vanuit het Technical Assistance Centre in Brussel verlenen wij 24 uur per dag online support aan klanten met een een SMARTnet-contract. Onze MKB Select Partners kunnen u meer vertellen over de voorwaarden. De Cisco MKB Support Assistent is een gemakkelijk te gebruiken en voordelig programma dat ondersteuning biedt bij de meest voorkomende problemen en dat ervoor zorgt dat het netwerk beschikbaar en veilig blijft. Het geeft tijdig aan waar problemen zijn opgetreden, hoe die kunnen worden opgelost en wanneer er een nieuw onderdeel moet worden besteld.

De Cisco MKB Support Assistent Portal is een beveiligde online verzameling van hulpmiddelen waarmee klanten wachtwoorden kunnen herstellen, ondersteuningsdocumentatie kunnen raadplegen, het netwerk kunnen controleren, software patches kunnen downloaden en cases kunnen openen wanneer dat nodig is.

Cisco financieringsoplossingen

U kunt uw bedrijf al snel laten profiteren van de nieuwste technologie van Cisco dankzij de Cisco Capital EasyLease financieringsregelingen die eenvoudige, duidelijke betaalbare financiering bieden. Hiermee houdt u de druk op uw budget laag houdt en maakt u contanct geld vrij. De belangrijkste voordelen van een financieringsoplossing van Cisco Capital EasyLease zijn:

- Behouden van kapitaal. Voorspelbare en beheersbare betalingen helpen om de liquiditeit te verbeteren en kredietlijnen open te houden.
- Vermijden van technologische veroudering. Er kan een technologische upgrade-optie in de leaseovereenkomst worden ingebouwd. Daardoor kunt u op een gegeven moment tijdens de leaseperiode upgraden naar de nieuwste technologie.
- Maximale flexibiliteit. Laat u bij de keuze en implementatie van een oplossing leiden door uw bedrijfsbehoeften en niet door mogelijke budgettaire restricties. Dat zorgt ervoor dat uw technologie nieuw blijft en gelijke tred houdt met de gebruiksbehoeften.

Meer informatie

Bezoek onze website voor meer informatie over de financiering van uw technologiebehoeften met Cisco Capital: www.cisco.nl/mkb

rotl/6488/05.09