

Cisco Meraki en Connect Secure Meraki

CBG Connect B.V.

Bollenmarkt 8i

1681 PJ Zwaagdijk-Oost

0228 56 60 70



Excellence



1. Cisco Meraki Security
2. Meraki Security MX64
3. Meraki Security MX84
4. Het Cisco Talos Team beschermt
5. Connect Secure Meraki
6. Scheidingspunt van de dienst
7. CBG Connect als security partner

“Verklein de mogelijkheid van een datalek aanzienlijk, door uw netwerk en digitale bestanden te beveiligen met professionele beveiligingsoplossingen, zoals de Cisco Meraki Securityoplossing.”

Cisco Meraki Security

We slaan met zijn allen steeds meer data op in databases. Wanneer we onze gegevens bij een bedrijf achterlaten, gaan we er dan ook vanuit dat deze gegevens goed beveiligd worden. Helaas is dit in de praktijk lang niet altijd het geval. En met toenemende dreiging van hackers en DDOS-aanvallen zou dit eigenlijk wel moeten. Daarom heeft de overheid per 1 januari 2016 de wet meldplicht datalekken ingesteld. Deze wet stelt dat ernstige datalekken bij bedrijven verplicht gemeld moeten worden bij de Autoriteit Persoonsgegevens.

Het is mogelijk om een datalek aanzienlijk te verkleinen door het bedrijfsnetwerk en de digitale bestanden te beveiligen met professionele beveiligingsoplossingen zoals de Cisco Meraki Securityoplossing. De Meraki Securityoplossing bestaat uit een hardwarecomponent met daarbij een licentie waardoor u toegang krijgt tot alle mogelijke beveiligingsopties van Cisco Meraki Security. De Cisco Meraki Securityoplossing wordt beheerd via een Cloudportaal. Via deze omgeving kunnen alle instellingen aangepast worden.

De Cloudportaal is uitgebreid ingericht om de beveiliging van het netwerk op diverse fronten in te stellen. Tevens is de Cloudportal uitgerust met verschillende diagnostische functies die een overzicht geven van alle informatie omtrent het netwerk. Uniek is ook het feit dat mogelijke malware gebeurtenissen onderzocht worden door de onderzoekers van het Talos Team. Mocht er toch sprake zijn van gedownloade malware dan komt hiervan een melding in de Cloudportal en wordt het systeem ook meteen geupdate en dus intelligenter gemaakt. Zo worden toekomstige downloads van de bewuste malware tegen gehouden.

Als u een Meraki Securityproduct aanschaft dan heeft u op dat product een levenslange garantie. Het feit dat Cisco deze levenslange garantie afgeeft zegt eigenlijk al voldoende over het product.

Cisco Meraki Security MX64

Ideale firewall voor kleinzakelijke omgevingen

De Meraki Security MX64 is voor kleinzakelijke omgevingen de ideale firewall, is geschikt voor maximaal 50 gebruikers en heeft een doorvoersnelheid van 250 Mbps. Deze firewall beschermt uw netwerk uitstekend tegen schadelijke data. De firewall maakt gebruik van Stateful Packet Inspection, wat inhoudt dat elk "pakketje" data afzonderlijk bekeken wordt. Kans op virussen of andere schadelijke bestanden is hierdoor minimaal.

Met dit apparaat van Cisco zet u maximaal 25 VPN-tunnels op. Een VPN-tunnel gebruikt u om vanaf welke locatie dan ook veilig een verbinding op te zetten met het bedrijfsnetwerk. Dit bevordert flexwerken en maakt het mogelijk om altijd bij belangrijke documenten te kunnen wanneer u niet op kantoor kunt zijn.

Let op voor het gebruik van een Cisco Meraki Firewall heeft u een Cloud Management Advanced Security Licentie nodig.

EIGENSCHAPPEN CISCO MX64

- + Ideale firewall voor klein zakelijk gebruik
- + Geschikt voor maximaal 50 gebruikers
- + Doorvoersnelheid: 250 Mbps
- + 5 x Gigabit LAN-poorten
- + 3G/4G failover via USB-modem
- + Maximaal 25 VPN Tunnels
- + Beheer via de Cloud
- + Iedere 3 minuten een update vanuit Cisco

Uitgebreide security in één product

Identity based Firewall

Wijst automatisch firewall- en verkeersvormgevingsregels, VLAN-tags en bandbreedte-limieten toe om het juiste beleid voor elke gebruikersklasse af te dwingen.

Intrusion Prevention

Bescherm kritieke netwerkbronnen tegen de nieuwste beveiligingsrisico's en kwetsbaarheden. Vanuit Cisco wordt iedere 3 minuten automatisch een update verzonden voor continue bescherming

Content Filtering

Blokkeer ongewenste webcontent in meer dan 70 categorieën en benut cloud-lookups om miljarden URL's te filteren.

Advanced Malware Protection

Bescherm uw netwerk tegen malware met behulp van de nieuwste bedreigingsinformatie en identificeer voorheen onbekende schadelijke bestanden met retrospectieve detectie.

Application Visibility & Control

Identificeer welke applicaties worden gebruikt, en prioriteer kritieke apps terwijl u recreatieve apps beperkt.

Centralized Management

Producten van Cisco Meraki zijn vanaf de basis opgebouwd voor cloudbeheer. Er wordt gebruik gemaakt van Cloudlicenties waardoor real-time web gebaseerde diagnostiek, monitoring, rapportage en nog veel meer mogelijk is.

Cisco Meraki Security MX84

Ideale firewall voor middelgrote zakelijke omgevingen

De Meraki Security MX84 is voor middelgrote zakelijke omgevingen de ideale firewall, is geschikt voor maximaal 200 gebruikers en heeft een doorvoersnelheid van 500 Mbps. Deze firewall beschermd uw netwerk uitstekend tegen schadelijke data. De firewall maakt gebruik van Stateful Packet Inspection, wat inhoudt dat elk "pakketje" data afzonderlijk bekeken wordt. Kans op virussen of andere schadelijke bestanden is hierdoor minimaal.

Met dit apparaat van Cisco zet u maximaal 100 VPN-tunnels op. Een VPN-tunnel gebruikt u om vanaf welke locatie dan ook veilig een verbinding op te zetten met het bedrijfsnetwerk. Dit bevordert flexwerken en maakt het mogelijk om altijd bij belangrijke documenten te kunnen wanneer u niet op kantoor kunt zijn.

Let op voor het gebruik van een Cisco Meraki Firewall heeft u een Cloud Management Advanced Security Licentie nodig.

EIGENSCHAPPEN CISCO MX84

- + Ideale firewall voor middelgrote zakelijk omgeving
- + Geschikt voor maximaal 200 gebruikers
- + Doorvoersnelheid: 500 Mbps
- + 2 x Gigabit Wan, 8 x Gigabit LAN-poorten, 2 x SFP
- + 3G/4G failover via USB-modem
- + Maximaal 100 VPN Tunnels
- + Beheer via de Cloud
- + Iedere 3 minuten een update vanuit Cisco

Uitgebreide security in één product

Identity based Firewall

Wijst automatisch firewall- en verkeersvormgevingsregels, VLAN-tags en bandbreedte-limieten toe om het juiste beleid voor elke gebruikersklasse af te dwingen.

Intrusion Prevention

Bescherm kritieke netwerkbronnen tegen de nieuwste beveiligingsrisico's en kwetsbaarheden. Vanuit Cisco wordt iedere 3 minuten automatisch een update verzonden voor continue bescherming

Content Filtering

Blokkeer ongewenste webcontent in meer dan 70 categorieën en benut cloud-lookups om miljarden URL's te filteren.

Advanced Malware Protection

Bescherm uw netwerk tegen malware met behulp van de nieuwste bedreigingsinformatie en identificeer voorheen onbekende schadelijke bestanden met retrospectieve detectie.

Application Visibility & Control

Identificeer welke applicaties worden gebruikt, en prioriteer kritieke apps terwijl u recreatieve apps beperkt.

Centralized Management

Producten van Cisco Meraki zijn vanaf de basis opgebouwd voor cloudbeheer. Er wordt gebruik gemaakt van Cloudlicenties waardoor real-time web gebaseerde diagnostiek, monitoring, rapportage en nog veel meer mogelijk is.

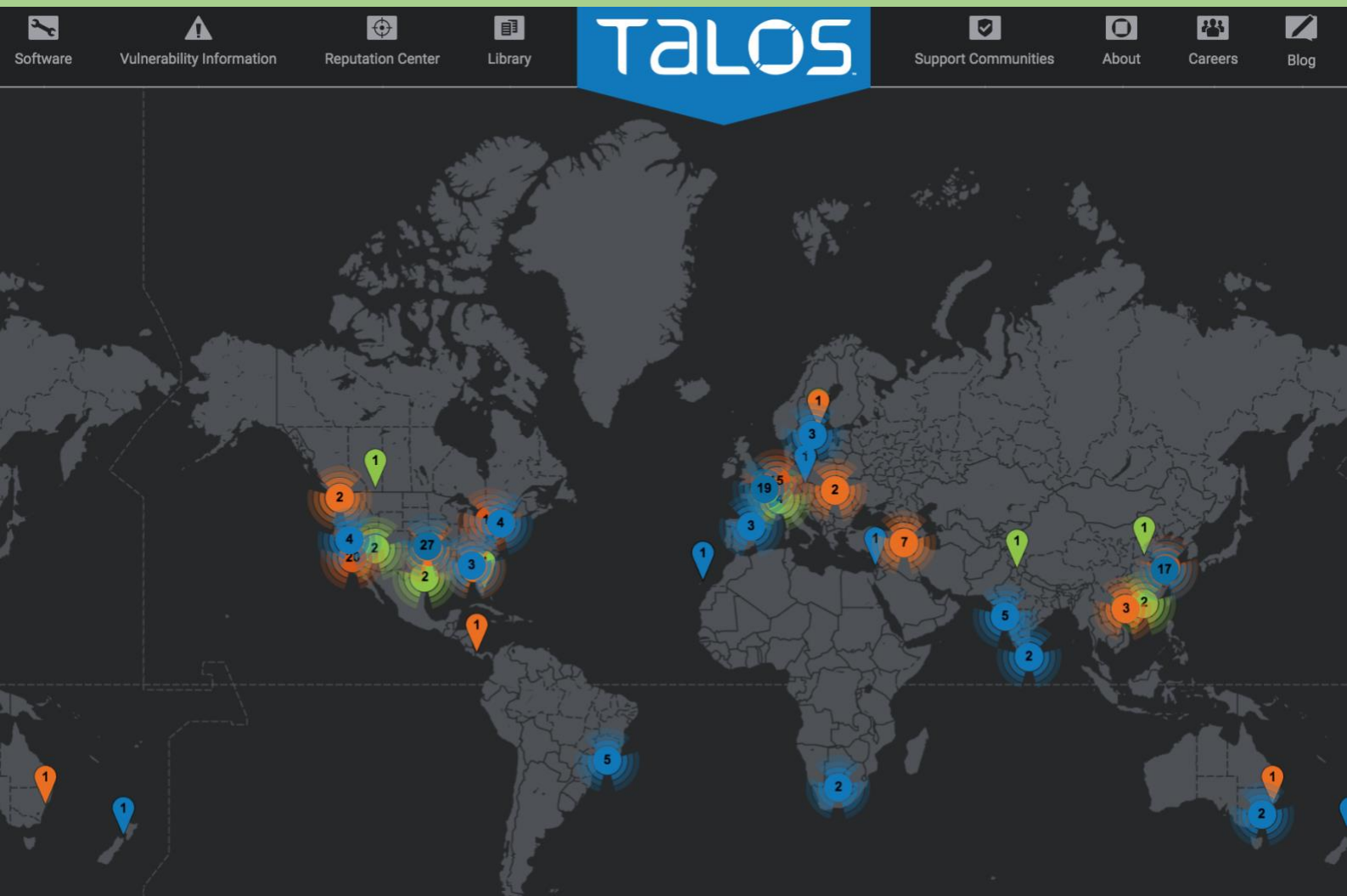
Het Cisco Talos Team biedt bescherming

Het Talos team biedt bescherming tegen aanvallen en malware. Zodra er een mogelijke dreiging is dan worden de gegevens doorgestuurd naar het Talos Team. Als zij na beoordeling van de gegevens menen dat er sprake is van malware, dan wordt deze informatie teruggekoppeld via de MSP Cloudportaal. De Meraki oplossing wordt onmiddellijk intelligent gemaakt met de teruggezonden info. Het is wel nodig om het bedrijfsnetwerk te onderzoeken waar eventuele malware terecht gekomen is.

Het Talos Team beschermt de mensen, gegevens en infrastructuur van uw organisatie. De onderzoekers, datawetenschappers en ingenieurs verzamelen informatie over bestaande en zich ontwikkelende bedreigingen. Het Talos Team bestaat uit 250+ fulltime dreigingsrechercheurs.

Talos analyseert elke dag zo'n 1,5 miljoen keer malware en helpt jaarlijks 7,2 biljoen aanvallen te stoppen. Om dit te doen, onderhoudt Talos het grootste dreigingsdetectienetwerk ter wereld, waarbij gebruik wordt gemaakt van geavanceerde detectie- en preventietechnieken die zijn ontworpen om de nieuwste trends in hackactiviteiten, inbraakpogingen, malware en kwetsbaarheden te ontdekken, te beoordelen en erop te reageren. Er kan live meegekeken worden, op de Talos website, waar op dat moment de grootste dreigingen zijn.

<https://talosintelligence.com>



Connect Secure Meraki

Wij bieden onze klanten de mogelijkheid om een Connect Secure dienst af te nemen, voor die onderdelen van de interne ICT-oplossing, die voor de ondernemer moeten voldoen aan de gestelde verwachting. Als ondernemer wilt u kunnen rekenen op een optimale beschikbaarheid van veiligheid van het bedrijfsnetwerk.

Met Connect Secure Meraki neemt u een service gerichte dienst af, waarbij u voor een vast bedrag per maand een overeengekomen pakket van dienstverlening ontvangt op de door u bij CBG Connect aangeschafte Cisco Meraki Securityoplossing.

Voordelen van Connect Secure Meraki

- Opname van klantsituatie in de Managed Service Providers Cloudportaal
- Duidelijk afspraken door Service Level Agreement
- Standaard monitoren van dagelijkse meldingen 24 uur per dag 7 dagen per week
- Proactieve controle van basismeldingen tijdens werkdagen en kantooruren 8:30-17:00 uur
- Proactief monitoren van alarmmeldingen volgens Service Level Agreement
- Voorzien van maandrapporten en securityrapporten
- Gratis tijdelijke vervangende oplossing indien hardware defect raakt (hoeft niet direct een volledig vervangende Meraki oplossing te zijn)
- 24 x 7 storingsdienst op de door CBG Connect geleverde internetverbinding
- Recht op storingscode voor meldingen van storingen op internetverbinding buiten kantooruren
- Doormelding van storingen aan provider (internetverbinding)
- Bewaken van de voortgang storingsafhandeling bij provider
- Gratis whitelists van websites na basis content filtering
- Geen kleine facturen bij kleine aanpassing in de Cloudportaal (zie informatie in de dienstbeschrijving Connect Secure Meraki)
- Maandelijks opzegbaar
- Eindklant blijft ten alle tijden hoofd- en eindverantwoordelijke voor de beveiliging van het eigen netwerk
- Er worden geen voorrijkosten en geen arbeidsloon gerekend ingeval van een herinstallatie bij defecte hardware (Tenzij de configuratie van de voorgaande situatie aangepast wordt)

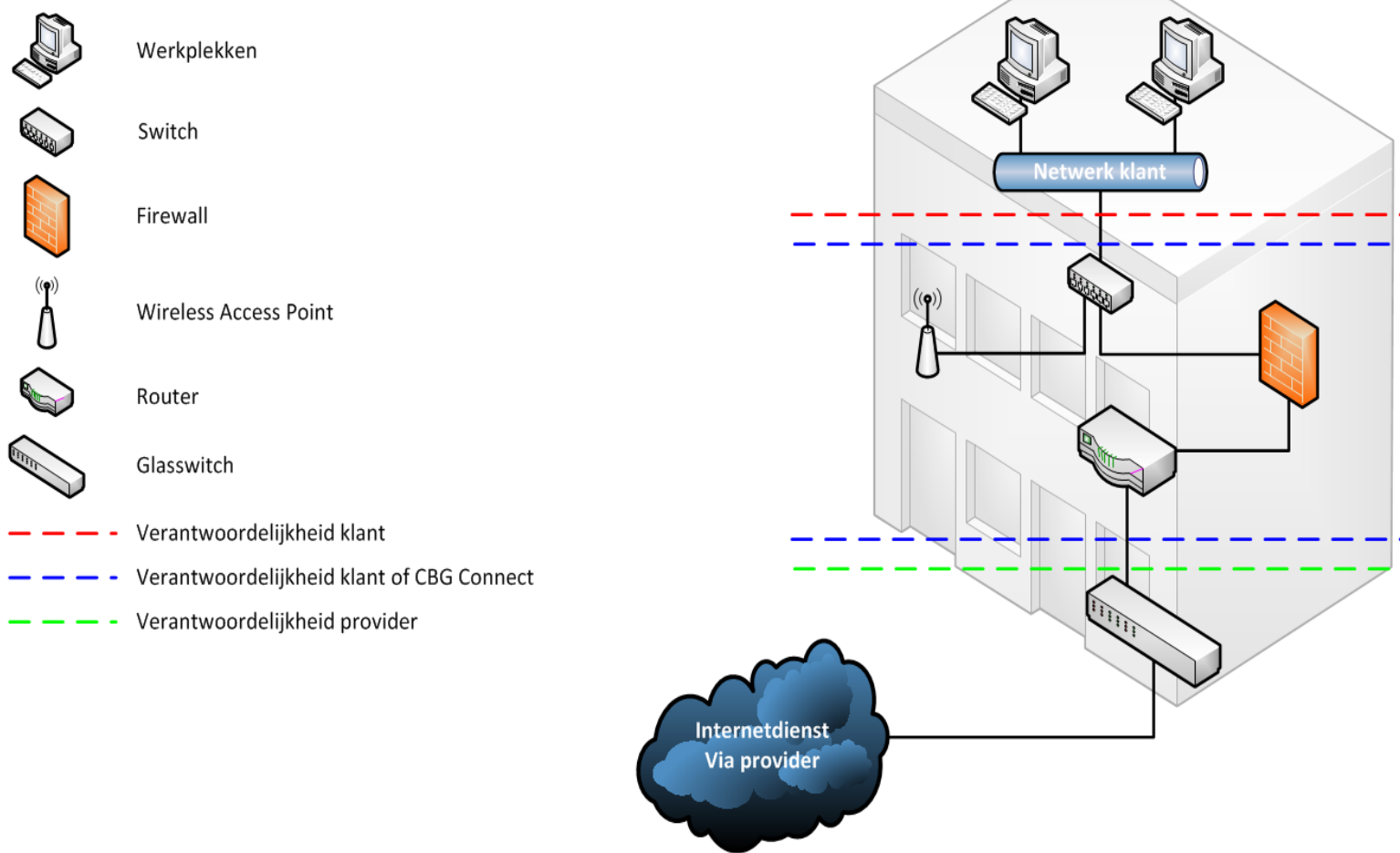


Scheidingspunt van de dienst

In de onderstaande afbeelding is overzichtelijk weergegeven op welke wijze een internetverbinding met een Meraki MX (firewall/router), Meraki MS (switch) en Meraki MR (Wireless Access Point (WiFi)) aangesloten kan worden op uw automatiseringsnetwerk. Met de stippellijnen is visueel weergegeven wie verantwoordelijk en aanspreekpunt is ingeval zich een storing voordoet.

CBG Connect is verantwoordelijk voor de dienst conform de afgegeven Service Voorwaarden. U bent zelf verantwoordelijk voor het aansluiten van uw netwerk en/of uw randapparatuur aan de door CBG Connect geleverde apparatuur en voor een correcte werking van deze aansluiting, tenzij u de installatie van hardware producten heeft uitbesteed aan CBG Connect.

Let op: onderstaande tekening is een voorbeeld tekening en hoeft niet overeen te komen met uw eigen situatie.



CBG Connect als securitypartner

Bij afname van de Connect Secure Meraki dienst wordt de klantsituatie opgenomen in de Managed Service Provider portaal van CBG Connect en machtigt de klant CBG Connect om toegang te hebben tot de klantsituatie.

De machtiging voor toegang tot de klantsituatie in de Managed Service Portaal heeft alleen het doel voor monitoren van meldingen, het kunnen analyseren van gegevens van meldingen, het uitbrengen van een advies aan de klant en het op aanvraag van de klant doorvoeren van wijzigingen.

Meldingen vanuit Meraki worden gedaan via een e-mailbericht. De klant machtigt CBG Connect voor het ontvangen van deze emailberichten en voor het opslaan van deze berichten in het belang van het kunnen uitvoeren van de monitoringwerkzaamheden.

CBG Connect heeft nimmer de intentie om diepgaand inzicht te krijgen in gebruik van het klantnetwerk tenzij zij hier, van de klant, schriftelijk opdracht voor krijgt.

CBG zal de resultaten van de monitoring tot zich nemen en een advies uitbrengen aan de klant. De klant is hoofd- en eindverantwoordelijke en kan desgewenst een advies naast zich neerleggen. CBG Connect zal alleen bij een schriftelijk akkoord, op een uitgebracht advies, werkzaamheden verrichten aan de klant situatie. Wij attenderen u er op dat alle adviezen gearhiveerd worden, dus ook de adviezen die niet tot een opdracht hebben geleid.

Beveiliging is nooit waterdicht

Enig realisme met betrekking tot netwerk security is dus gepast. Een besmetting met ransomware of het binnen halen van malware is nooit volledig uitgesloten. Een waterdichte beveiliging moet ook niet het streven zijn. Het gaat erom dat uw organisatie het risico op infectie verkleint en zo goed mogelijk voorbereid is als het onverhoopt toch misgaat. Zo beperkt u de impact en bent u snel weer operationeel.

Wilt u meer informatie ontvangen over Cisco Meraki Security of wilt u een vrijblijvende offerte ontvangen, dan kunt u contact op nemen met één van onze accountmanagers. Zij helpen u graag bij het maken van een juiste keuze voor een securityoplossing die past bij uw organisatie.

CBG Connect verbindt zich alleen aan organisaties die A-Kwaliteit producten en diensten leveren.

CBG Connect is:

- KPN Excellence Business Partner
- Partner Cisco
- Microsoft Partner

CBG Connect levert o.a.

- Connectiviteit KPN ÉÉN
- VoIP KPN ÉÉN
- Mobiel KPN ÉÉN
- Microsoft 365
- Cisco Meraki Securityoplossingen
- CBG Connect servicediensten Connect Secure
- Netwerkbeheer
- Overige IT-ondersteuning



“De integrale aanpak van beveiliging is een samenhang van de drie assen mensen, processen en technologie en de samenhang van deze 3 processen, bepaalt het succes van de bescherming van uw organisatie”



CBG Connect

Bollenmarkt 8i

1681 PJ Zwaagdijk-Oost

www.cbgconnect.nl

Algemeen telefoonnummer 0228 56 60 70

Team Verkoop: optie 2

Directie:

Johan Schotanus en Manuel Jamin