



Grieppandemiepakket telewerken





inhoudsopgave

1.	Inleiding	4
1.1.	Achtergrond	4
1.2.	Doelstelling	4
1.3.	Beperkingen	4
2.	Gebruikerservaring	5
2.1.	Aanloggen met SMS Tokens	5
2.2.	Telewerkportaal – direct in het hoofdmenu	5
3.	Oplossing	6
3.1.	Basis is secure SSLVPN Appliance	6
3.2.	Beveiliging is succesfactor voor telewerken	6
3.3.	Grafische vormgeving in huisstijl	7
3.4.	Modellen en specificaties	7
3.5.	Sterke authenticatie met SMS tokens	8
	Appendix: Bedrijfsprofiel Motiv	10

inleiding

1.1. Achtergrond

Met de terugkomst van de eerste groep vakantiegangers is ook de dreiging van verspreiding van de Mexicaanse griep op de werkvloer verhoogd. Volgens cijfers van het RIVM is de kans groot dat een aantal jongeren die vakantie aan het vieren zijn, onder meer aan de Spaanse kust, terug komt met Mexicaanse griep. Bovendien zijn werkgevers krachtens de Arbo-wet verantwoordelijk voor het nemen van passende maatregelen om zo een veilige en gezonde werkplek voor hun werknemers te garanderen. Dit geldt ook wanneer er sprake is van een grieppandemie. Omdat dit moeilijk zal zijn, zullen veel werknemers ervoor kiezen niet naar hun werk gaan. Dat recht hebben ze volgens de Arbo-wet. Daarom verwacht de overheid dat het aantal medewerkers dat als gevolg van de Mexicaanse griep niet op de werkvloer zal verschijnen op kan lopen tot 50% van het hele werknemersbestand.

Het telewerkpakket dat Motiv aanbiedt is gebaseerd op appliances van Juniper Networks. De SSLVPN-appliance wordt voorzien van een speciale pandemielicentie die kan worden geactiveerd bij een uitbraak binnen kantoor. Vanaf dat moment kunnen tot duizend gebruikers gelijktijdig telewerken via internet. Doordat er geen speciale cliëntsoftware nodig is kunnen werknemers via internet vanaf elke standaard PC of notebook werken. Het telewerkpakket zorgt ervoor dat werknemers die als gevolg van de verspreiding van het Influenza A virus (H1N1, of Mexicaanse griep) thuis moeten of

willen blijven, actief blijven voor de organisatie. Thuisblijvers worden thuiswerkers.

1.2. Doelstelling

De doelstelling is verspreiding van de Mexicaanse griep binnen kantoor zo veel mogelijk te beperken. Dit kan onder andere worden bereikt om snel en effectief thuiswerken aan te bieden. Onze oplossing wordt in zeer korte doorlooptijd geïmplementeerd en bestaat uit de volgende onderdelen:

- Levering van centrale VPN-appliance plus licenties en eventueel uitgebreid met de pandemielicentie;
- Levering van SMS token software plus een SMS-bundel of een SMS interface de ict-afdeling zelf Sms'jes kan versturen;
- Installatie en configuratie van het pakket;
- Onderhoudspakket met een service contract.

1.3. Beperkingen

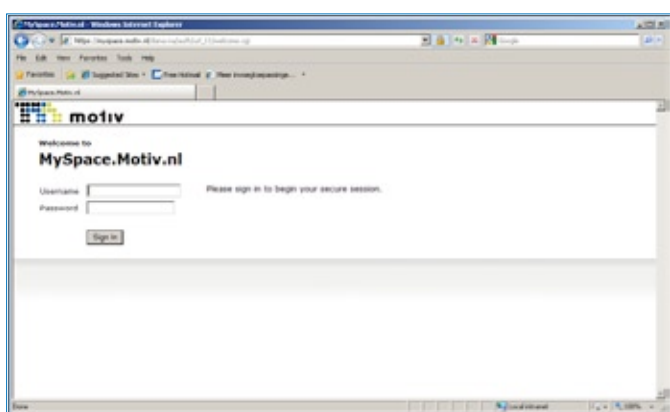
De telewerkvoorziening werkt met standaard Pc's met Microsoft Windows, Macintosh en LINUX. Wel is het zo dat de gebruiker (zelf) een PC thuis tot zijn/haar beschikking moet hebben. Voor het gebruik van SMS tokens is het gebruik van een mobiele telefoon noodzakelijk.



Gebruikerservaring

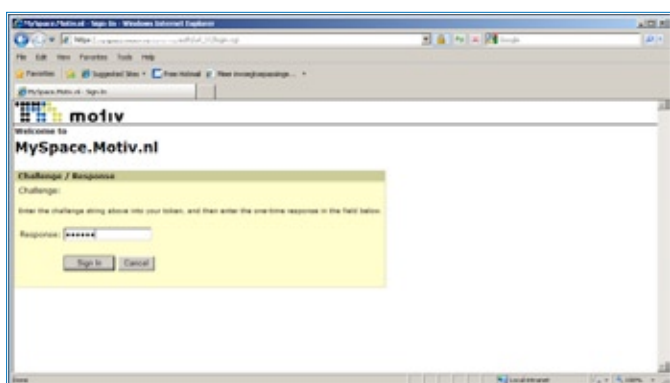
2.1. Aanloggen met SMS Tokens

Log in met een willekeurige PC met internet. Veilig telewerken is beschikbaar voor Microsoft Windows, Macintosh MAC OS (Safari browser) en Linux. De site is beveiligd met een zogenoemd SSL-certificaat (zichtbaar slotje in de webbrowser). De gebruikersnaam en wachtwoord is dus niet zichtbaar voor derden (lees: hackers).



Figuur 1: inlogscherm voor telewerken via elke webbrowser

Gebruik normale gebruikersnaam en bijbehorend wachtwoord. En klik op Sign in. Vervolgens krijg je binnen een paar seconden een flash Sms'je. In deze SMS staat een code van zes cijfers. Tik deze code over in het scherm.

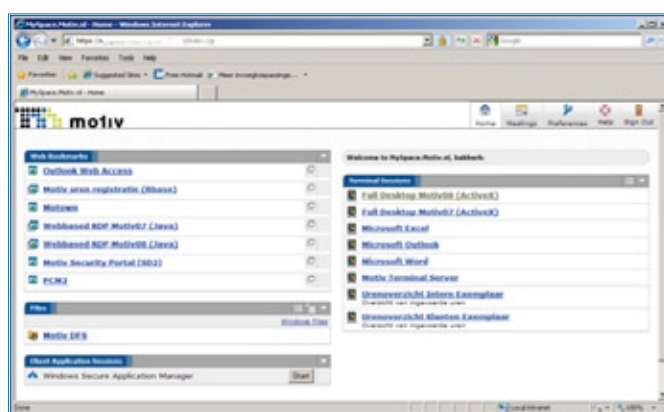


Figuur 2: Sterke authenticatie met SMS token

De gebruiker is nu succesvol aangemeld. Dit is alles.

2.2. Telewerkportaal – direct in het hoofdmenu

Nu verschijnt het hoofdmenu (webpagina) met hyperlinks naar een set van (web)applicaties. Standaard wordt een set van applicaties ondersteund. Voorbeelden zijn Outlook Web Access, intranet, Windows Terminal Server en Citrix. Deze applicaties kunnen we snel beschikbaar stellen via de oplossing voor Motiv telewerken.



Figuur 3: Hoofdmenu voor telewerken via de webbrowser

Standaard worden de volgende applicaties direct vanuit het hoofdmenu ondersteund:

- Alle web based applicaties zoals Outlook Web Access (OWA) en intranet;
- Citrix (via activeX of Java) of Windows Terminal Services (WTS);
- Webapplicaties zoals Oracle Applications en Siebel;
- File sharing via een drive mapping (network connect) of via een webbrowser (met download en upload file).

In veel gevallen worden de standaard webapplicaties zoals OWA direct aangeboden. Voor de overige en standaard kantoorapplicaties (zoals Microsoft Office) geldt dat deze via Citrix of WTS worden aangeboden. Zie ook het screenshot op de vorige pagina.

Oplossing

Motiv Veilig Telewerken is een geïntegreerde totaaloplossing, die werknemers toegang biedt tot toepassingen en bedrijfssystemen via een centraal webportaal. De belangrijkste aspecten die hierbij een rol spelen zijn beveiliging, transparante toegang, passende weergave op basis van uw gebruikte apparatuur (PC, Thin Client, PDA, telefoon) en het personaliseren van informatie op basis van functierollen. De inzet van een transparant portaal heeft verschillende voordelen. Zo zijn uw medewerkers niet langer gebonden aan een vaste werkplek, maar kunnen ze 24 uur per dag overal waar een internetaansluiting is, bedrijfsinformatie ontsluiten. Dat draagt sterk bij aan de flexibiliteit en wendbaarheid van uw organisatie en die van uw medewerkers. Daarnaast hoeft u niet ingrijpend te investeren in aanpassingen aan uw bestaande IT-infrastructuur. Die blijft volledig in tact.

3.1. Basis is secure SSLVPN Appliance

De SSL-VPN security appliance is een veilige, schaalbare en flexibele oplossing voor telewerken. De SSLVPN appliance is een telewerkportaal. De portal is via een versleutelde verbinding (https) via internet bereikbaar.



De belangrijkste eigenschappen van de oplossing zijn hieronder puntsgewijs weergegeven:

- Role based. Op de appliance worden rollen gedefinieerd waar gebruikers aan gekoppeld kunnen worden. Binnen een rol wordt gedefinieerd welke eigenschappen een sessie dient te hebben. Dit geldt zowel voor autorisaties (tot welke resources krijgt een gebruiker toegang), als voor randvoorwaarden waar de gebruikers aan dienen te voldoen (bijvoorbeeld of de client aan bepaalde security eisen voldoet). Binnen het systeem vindt een mapping plaats tussen de gebruikers en de van toepassing zijnde rollen;
- Granulariteit van toegang op basis van rechten en gebruikt platform (security policy);
- In de meeste gevallen kunnen gebruikers bij de SSLVPN-appliance profiteren van single-sign-on. Dat wil zeggen dat zij zich slechts één keer hoeven aan te melden om toegang te krijgen tot alle relevante interne informatiesystemen.
- Gebruikers authenticeren via centrale user directories (bijvoorbeeld LDAP of Active Directory). Het systeem hoeft geen eigen userlijst bij te houden;
- Meerdere portals mogelijk, ieder met een geheel eigen "look and feel";
- Verschillende vormen van toegang voor verschillende gebruikersgroepen huidige en toekomstige, bijvoorbeeld tijdelijke toegang tot een bepaalde applicatie voor derden.
- Ondersteuning diversiteit aan platformen met verschillende typen webbrowsers (Java of ActiveX);
- Ondersteuning aan diverse besturingssystemen. Zo worden bijvoorbeeld Windows, Linux, Mac en Solaris als client ondersteund, maar ook PDA's kunnen toegang verkrijgen tot de diensten;
- Mogelijkheden voor het implementeren van een diepgaande security policy, waarbij lokale data volledig afgeschermd kan worden van de werkplek en versleuteld wordt opgeslagen gedurende de sessie. Na afloop van de sessie wordt deze data definitief verwijderd.

3.2. Beveiliging is succesfactor voor telewerken

Beveiliging is een zeer belangrijke randvoorwaarde voor het telewerken. Zonder beveiliging is niet haalbaar om (interne) informatie over internet te lezen of te verwerken. Onze oplossing biedt een scala aan mogelijkheden voor passende beveiliging.

- De telewerkportaal is gebaseerd op een security appliance van Juniper Networks. Deze appliance is uit zichzelf zeer sterk beschermd tegen aanvallen vanaf internet. De systemen zijn aan

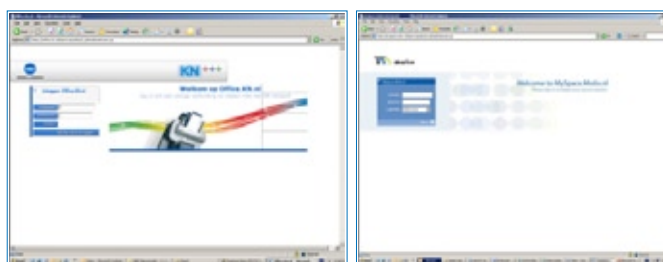
diverse security testen blootgesteld. Voor overheid is er zelfs een speciale versie met EAL-certificering. De appliance is bovendien als absolute marktleider op het gebied van SSLVPN volgens analist Gartner.

- Sterke authenticatie door middel van tokens. Zie tekst en voorbeeld in paragraaf 3.5. Naast de SMS tokens biedt Motiv ook de RSA tokens. Deze digitale sleutels moeten wel worden uitgedeeld aan medewerkers. Het werken met SMS tokens is eenvoudiger, sneller en bovendien goedkoper.
- [Host Security Checker](#)
Preventieve controle van de PC van de gebruiker op beveiligingsinstellingen. Deze optie is alleen zinvol als de PC een PC/notebook van kantoor is.
- [Cache cleaner](#)
Voor Windows-gebaseerde werkplekken biedt Cache Cleaner de mogelijkheid om tijdelijk lokaal opgeslagen data, zoals cookies, temp-files, of applicatie cache, van de PC te verwijderen na een SSL-VPN sessie. Hiermee wordt voorkomen dat bepaalde vertrouwelijke informatie achteraf teruggevonden kan worden op de PC. Tevens voorkomt Cache Cleaner het permanent opslaan van gebruikersnamen, wachtwoorden en andere informatie welke gebruikers in webformulieren invullen.
- [Secure Virtual Workspace \(SVC\)](#)
De Secure Virtual Workspace gaat nog een stuk verder dan Cache Cleaner. Met behulp van de Host Checker functionaliteit kan op Windows gebaseerde werkplekken een zogenaamde Secure Virtual Workspace worden gecreëerd. Dit is een mechanisme wat er voor zorgt dat alle activiteiten van een gebruiker op de portal plaatsvinden in een volledig beschermd gedeelte van de werkplek. Secure Virtual Workspace versleutelt alle informatie die door applicaties naar de harddisk of het Windows register worden geschreven en vernietigt alle informatie over zichzelf en de SSL-VPN sessie bij het afsluiten hiervan. De SSL-VPN omgeving zorgt ervoor dat de Secure Virtual Workspace client wordt gedownload naar de gebruiker op het moment dat deze zich aanmeldt. Deze client creëert een versleuteld virtueel filesystem en een versleutelde virtuele registry op de PC. Voor het draaien van de Secure Virtual Workspace hoeft de gebruiker geen lokale administrator-rechten op de PC te hebben. SVC kent een aantal beperkingen waardoor dit niet voor alle type (web)-applicaties geschikt is.

3.3. Grafische vormgeving in huisstijl

Tegen meerprijs kan Motiv naast alle implementatie en support services ook het ontwerp op maat leveren. Hierbij moet worden de volgende zaken meegenomen in het project:

- Token met eigen design – zie voorbeelden in de kantlijn¹
- Alle inlog- en uitlog pagina's in eigen huisstijl
- Kleurgebruik en basiszaken van het portaal in de eigen huisstijl (voor zover mogelijk in de appliance)



Figuur 4: voorbeelden van custom design van de SSLVPN Portal

3.4. Modellen en specificaties

Juniper kent een drietal SSLVPN appliances voor de zakelijke markt. Het verschil in de modellen zit voornamelijk in de capaciteit van de appliances. Het aantal gelijktijdige gebruikers is hoger bij een groter model.

Functie	2500	4500	6500
Aantal gelijktijdige gebruikers (maximaal)	100	1.000	>10.000
Aantal gelijktijdige gebruikers (minimale/maximaal) (maximaal)	25/100	50/1.000	50/10.000
Griepandemielicentie - optioneel (dertig dagen maximaal aantal gebruikers)	nee	ja (1.000)	ja (10.000)
Maximale virtualisatie (ondersteuning van vlands e.d.)	nee	optie	optie
Basisapplicaties <ul style="list-style-type: none"> • Web (HTML, Java, ActiveX) • Citrix (ICA, Secure Access Gateway) • WTS (RDP) • File shares • Web shares 	ja	ja	ja
Clustering en load balancing	HA	HA	HA/LB

Alle apparatuur wordt geleverd inclusief een set met licenties en inclusief de software modules network connect (transparante netwerkverbindingen over SSL) en secure application manager (beschikbaar stellen van specifieke applicaties). Daarbij kan de apparatuur worden uitgebreid met de speciale pandemielicentie.

¹ Logo of beeldmerk wordt gedrukt in hart van het token (cirkel van 18,5mm x 18,5mm)

3.5. Sterke authenticatie met SMS tokens

Authenticatie is het proces waarbij een applicatie nagaat of een gebruiker daadwerkelijk is wie hij beweert te zijn. Bij authenticatie wordt gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken. Tijdens de authenticatie kan er gebruik worden gemaakt van drie verschillende kenmerken. Deze kenmerken zijn:

- **iets wat je weet** (Bijv. wachtwoord of pincode)
iets wat je weet is bijvoorbeeld een wachtwoord, een Pincode of een geheime zin. Het is de bedoeling dat dit bewijs geheim is, het mag niet uitlekken om diefstal van de identiteit tegen te gaan. Een beroemde geheime zin is "Sesam open U". Een hacker zal proberen de identiteit van iemand over te nemen door een wachtwoord te raden of te kraken. Om die reden wordt in professionele omgevingen dan ook het gebruik van complexe wachtwoorden afgedwongen, die periodiek gewijzigd moeten worden. Als het goed is, moet de kraaktijd van een wachtwoord langer zijn dan de vervaltermijn. **iets wat je bezit** (token, mobiele telefoon)
Dit betekent dat het bewijs van de identiteit wordt geleverd door het gebruikmaken van een fysiek herkenningsteken, dat door of namens het autoriserende systeem werd uitgereikt. Te denken valt aan een 'token' zoals een chipkaart (de smartcard), een USB-sleutel, of een SecureID token. Hierbij wordt vaak gebruik gemaakt van de challenge-response functie: Het autoriserende systeem stelt een vraag en degene die toegang vraagt moet met behulp van het token een passend antwoord geven. Een voorbeeld is een SecureID token van RSA of het versturen van een SMS naar een van te voren opgegeven mobiele telefoon. Dat laatste is bekend bij DigiD (communicatie met de overheid).
- **iets wat je bent** (persoonlijke eigenschap zoals een vingerafdruk).

Beveiligingspecialisten zijn het erover eens dat een combinatie van twee technieken voldoende is voor authenticatie over internet. Specialisten spreken over two-factor authenticatie (ook wel genoemd sterke authenticatie). In de praktijk is dit meestal een pincode of wachtwoord in combinatie met iets wat je hebt (bijv. Flash SMS naar mobiele telefoon).

Onze oplossing is gebaseerd op SMS tokens van SecurEnvoy. De belangrijkste voordelen:

- Krachtige, betaalbare, gebruiksvriendelijke two-factor-authenticatie (gebruikersnaam plus wachtwoord en daarna tokencode via SMS)
- Reductie van helpdeskkosten
- Geen problemen met het wijzigen van het wachtwoord of bewaren van de Pincode



- Geen kosten en tijdsverlies voor distributie, vernieuwing of vervanging van tokens of smartcards
- Geen extra voorzieningen (bijvoorbeeld kaartlezers) nodig
- Geen software op de mobiele telefoon vereist
- Geen vertragingen door het wachten op een passcode
- De passcode is altijd beschikbaar (Preload of Real Time), zelfs als u tijdelijk geen bereik hebt

SecurAccess maakt het mogelijk om vertrouwde personen veilig op het bedrijfsnetwerk te laten inloggen. Problemen met wachtwoord - of



tokenbeheer en social engineeringaanvallen zijn nu definitief verleden tijd. Een elegante oplossing voor een zwaarwegend zakelijk probleem.

SecurAccess is eenvoudig in gebruik. Het gepatenteerde systeem stuurt een passcode van zes cijfers via SMS naar de mobiele telefoon van de gebruiker. Via hun SMS tekstberichten krijgen gebruikers toegang tot de pascode. Door die pascode in te geven, samen met hun UserID en hun Microsoft paswoord, of PIN, krijgen zij toegang tot het telewerkportaal van Juniper Networks. Zodra de passcode is gebruikt, wordt er een nieuwe verstuurd naar de telefoon van de gebruiker, die

de vorige code automatisch vervangt. Ook als een onjuiste pascode werd ingegeven, wordt een nieuwe gestuurd, zodat er steeds een code beschikbaar is. Het bedrijf kan zelf beslissen hoeveel onjuiste Pincodes of passcodes geaccepteerd worden.

De SecurAccess security server wordt rechtstreeks geïntegreerd in de Microsoft Active Directory en andere veelgebruikte directory servers zoals eDirectory. Daardoor is het niet nodig om gebruikers opnieuw te creëren of te synchroniseren in een aparte database. Het systeem kan eenvoudig beheerd worden via de dynamische webpagina's van SecurEnvoy, die veilig en ook op afstand toegankelijk zijn. Zodra het mobiele van een gebruiker in de Active Directory is opgenomen, kan de gebruiker direct aan de slag.

Kenmerken:

- Met dit systeem maakt u van elke mobiele telefoon een SMS-token
- Er zijn geen extra hardware tokens vereist
- Geen kosten voor verdeling van hardware onder eindgebruikers
- Geen problemen met niet-functionerende hardware bij eindgebruikers
- Rechtstreekse integratie in uw bestaande Active Directory, e-Directory, Sun Directory, OpenLdap
- Eenvoudige authenticatiecode van zes cijfers via SMS
- Eenmalige pascodes voorkomen alle bekende paswoord aanvallen
- Flash SMS waarmee een SMS eenmalig op het GSM verschijnt en daarna wordt verwijderd (mits GSM deze functie ondersteund)

De sterke authenticatie werkt met elke mobiele telefoon die Sms'jes kan ontvangen. De oplossing werkt met twee componenten:

- SecurEnvoy SecureAccess server (Windows of Linux). Deze server kan ook op een VMware omgeving worden geplaatst. De server verzorgt de sterke authenticatie. Sterke authenticatie is een combinatie van iets wat een gebruiker weet (wachtwoord) en iets wat de gebruiker heeft (mobiele telefoon waar de SMS op binnenkomt). Sterke authenticatie met SMS tokens wordt door beveiligingsspecialisten en EDP-auditors als noodzakelijk gezien voor beveiliging van telewerken over internet.
- Interface voor versturen van Sms'jes. De Sms'jes kunnen met een speciale SIM-box worden verstuurd (eigen SIM-kaart van bedrijf nodig) of kunnen als dienst (per 1000 Sms'jes) worden afgenomen van SecurEnvoy. Bijbestellen kan de klant zelf doen middels creditcard. De prijs per SMS is in dit geval 10 cent. Motiv kan beide opties direct leveren.

Appendix: Bedrijfsprofiel Motiv

Motiv is sinds 1998 actief als sparringpartner, systems integrator en probleemoplosser voor klanten die zoeken naar innovatieve ICT-oplossingen voor de ondersteuning van hun bedrijfsprocessen. Rode draad in onze activiteiten is de beveiliging van netwerken en gegevens. Of het nu gaat om het optimaal beveiligen van een netwerk of de veilige toegang tot een database, Motiv biedt de juiste oplossing op basis van de in eigen huis opgebouwde expertise. Die combineren we met de geavanceerde producten van toonaangevende leveranciers als Microsoft, Oracle, Juniper Networks en RSA Security.

Sparringpartner - Veel klanten weten wat ze willen en hoe ze het willen, maar schakelen ons toch in om te bepalen of en hoe het beter kan. Zij vertrouwen op onze kennis en expertise op het gebied van databases, netwerken en security en weten dat onze consultants altijd tot het uiterste gaan om creatieve invalshoeken te bedenken bij elke klantvraag.

Probleemoplosser - Uiteraard vragen klanten ons ook gewoon om een concreet probleem op te lossen of een concrete vraag te beantwoorden. En daarbij zoeken we steeds naar onderscheidend vermogen met een creatieve en heldere aanpak.

Systems integrator - De complexiteit van IT-infrastructuren neemt nog met de dag toe. Daarom doen veel klanten een beroep op Motiv bij de integratie van nieuwe technologie in de bestaande omgeving. Zo halen we samen met de klant het uiterste uit alle IT-investeringen.

Probleemoplosser - Uiteraard vragen klanten ons ook gewoon om een concreet probleem op te lossen of een concrete vraag te beantwoorden. En daarbij zoeken we steeds naar onderscheidend vermogen met een creatieve en heldere aanpak.

Transparant

Voor beheer en ondersteuning beschikt Motiv over mogelijkheden voor telefonische ondersteuning, proactief beheer op afstand en bewaking. Uniek is de Service Desk van Motiv, die klanten via het web in een oogopslag alle actuele informatie biedt over apparatuur, wijzigingen, storingen en andere relevante zaken.

Klanten

Motiv is actief in verschillende sectoren en werkt onder meer voor financiële instellingen, telecom- en service providers, lokale en centrale overheden en vele commerciële en dienstverlenende organisaties.





Motiv
Poortdijk 13
NL - 3402 BM IJsselstein

T +31 [0]30 - 68 77 007
F +31 [0]30 - 68 77 006

www.motiv.nl
info@motiv.nl