Wat is een remote werkplek?

Managed Werkplek · https://aucuba.nl/kennisbank/managed-werkplek/wat-is-een-remote-werkplek/

Een remote werkplek is een **digitale werkomgeving** waarmee je vanaf elke locatie toegang hebt tot alle bedrijfsapplicaties, bestanden en systemen die je nodig hebt voor je werk. In plaats van fysiek aanwezig te zijn op kantoor, log je via internet in op een beveiligde omgeving waar je precies dezelfde mogelijkheden hebt als op je werkplek in het bedrijfspand. Dit betekent dat je thuis, onderweg of vanaf een andere locatie productief kunt werken met dezelfde tools en toegang tot bedrijfsinformatie.

Wat is een remote werkplek precies?

Een remote werkplek verschilt fundamenteel van traditioneel kantoorwerk doordat je niet meer gebonden bent aan een vaste locatie. Waar je vroeger naar kantoor moest om bij je bestanden en programma's te komen, heb je nu alles binnen handbereik via een internetverbinding. De technologie achter remote werkplekken maakt gebruik van cloudoplossingen, virtuele desktops en beveiligde netwerkverbindingen.

Het belangrijkste verschil met thuiswerken op je eigen computer is dat een remote werkplek een volledig beheerde omgeving is. Je werkt niet op je persoonlijke apparaat met losse programma's, maar logt in op een professionele werkplek die door de ICT-afdeling of een Managed Service Provider wordt onderhouden. Alle software is up-to-date, back-ups worden automatisch gemaakt en de beveiliging is op orde.

Deze digitale werkplekken maken gebruik van verschillende technologieën zoals Remote Desktop Services, Virtual Desktop Infrastructure (VDI) of Desktop-as-a-Service (DaaS). Voor jou als gebruiker maakt het weinig uit welke technologie erachter zit, het resultaat is hetzelfde: je hebt overal toegang tot een complete werkplek.

Hoe werkt een remote werkplek in de praktijk?

Het werken met een remote werkplek begint met inloggen via een beveiligde verbinding. Je opent een programma of website op je laptop, tablet of zelfs smartphone en voert je gebruikersnaam en wachtwoord in. Vaak wordt dit aangevuld met **twee-factor authenticatie** voor extra beveiliging,

bijvoorbeeld een code op je telefoon.

Na het inloggen zie je je vertrouwde bureaublad verschijnen, compleet met alle programma's die je gewend bent. Of je nu werkt met Office-applicaties, boekhoudprogramma's of specifieke bedrijfssoftware, alles staat klaar zoals je het hebt achtergelaten. Je bestanden staan op dezelfde plek en je kunt direct aan de slag.

De verbinding met de bedrijfsserver loopt via het internet, maar is beveiligd met encryptie. Dit betekent dat al je gegevens versleuteld worden verzonden, net zoals bij internetbankieren. Cloud-diensten spelen vaak een belangrijke rol, waarbij je bestanden en applicaties niet meer op een fysieke server in het bedrijf staan, maar in een professioneel datacenter.

Voor jou als gebruiker voelt het alsof je gewoon achter je bureau op kantoor zit. Het enige verschil is dat de computer waarop je werkt ergens anders staat en je via internet de besturing overneemt.

Wat heb je nodig voor een goed functionerende remote werkplek?

Voor een soepel werkende remote werkplek zijn verschillende componenten nodig, zowel thuis als binnen je bedrijf. De basis begint met een stabiele internetverbinding van minimaal 10 Mbps voor normaal kantoorwerk, maar bij intensief gebruik van video of grote bestanden is meer bandbreedte aan te raden.

Qua hardware heb je een apparaat nodig om mee in te loggen. Dit kan een laptop, desktop, tablet of zelfs een smartphone zijn. Het hoeft geen krachtige computer te zijn, omdat het zware werk op de server gebeurt. Wel belangrijk zijn een goed scherm, comfortabel toetsenbord en muis voor langdurig werken.

Aan de bedrijfskant moet de ICT-infrastructuur op orde zijn. Dit betekent voldoende servercapaciteit, goede netwerkverbindingen en de juiste software-licenties. Ook moet er nagedacht zijn over back-ups, updates en onderhoud van de systemen.

Beveiligingssoftware is onmisbaar voor veilig werken op afstand. Denk aan antivirusprogramma's, firewalls en VPN-software voor een beveiligde verbinding. Deze worden meestal centraal beheerd zodat je er als gebruiker geen omkijken naar hebt.

Waarom kiezen steeds meer MKB-bedrijven voor remote werkplekken?

MKB-bedrijven ontdekken dat remote werkplekken belangrijke voordelen bieden voor hun organisatie. De flexibiliteit voor medewerkers staat vaak bovenaan: zij kunnen werken waar en wanneer het hen uitkomt, wat de werk-privébalans verbetert en reistijd bespaart.

Kostenbesparingen zijn een ander belangrijk argument. Met minder mensen tegelijk op kantoor kun je besparen op kantoorruimte, parkeerplaatsen en facilitaire kosten. Ook de ICT-kosten kunnen lager uitvallen doordat je minder krachtige computers op kantoor nodig hebt en centraal beheer efficiënter is.

Voor de bedrijfscontinuïteit bieden remote werkplekken grote voordelen. Bij calamiteiten zoals extreme weersomstandigheden, stakingen in het openbaar vervoer of zelfs een pandemie, kan het werk gewoon doorgaan. Medewerkers loggen vanuit huis in en de productiviteit blijft op peil.

Ook het aantrekken van talent wordt makkelijker. Je bent niet meer beperkt tot mensen die in de buurt van je kantoor wonen, maar kunt de beste kandidaten aannemen ongeacht waar ze wonen. Dit vergroot je vijver van potentiële medewerkers aanzienlijk.

Hoe beveilig je een remote werkplek tegen digitale dreigingen?

Beveiliging van remote werkplekken vraagt om een andere aanpak dan traditionele kantoorbeveiliging. Een VPN-verbinding (Virtual Private Network) is de basis voor veilige communicatie tussen de thuiswerkplek en het bedrijfsnetwerk. Deze versleutelde tunnel zorgt ervoor dat niemand kan meekijken met je dataverkeer.

Twee-factor authenticatie voegt een extra beveiligingslaag toe. Naast je wachtwoord moet je ook een code invoeren die je op je telefoon ontvangt. Zo voorkom je dat iemand met alleen je wachtwoord toegang krijgt tot bedrijfsgegevens.

Endpoint security beschermt de apparaten waarmee wordt ingelogd. Dit betekent dat elk apparaat moet voldoen aan beveiligingseisen zoals up-to-date antivirussoftware, automatische updates en versleuteling van de harde schijf. Veel bedrijven kiezen ervoor om alleen goedgekeurde apparaten toegang te geven.

Regelmatige updates en back-ups zijn belangrijk voor de continuïteit. Software moet automatisch worden bijgewerkt om beveiligingslekken te dichten, en belangrijke gegevens moeten dagelijks worden geback-upt. Als MSP nemen wij deze zorgen uit handen door proactief te monitoren en onderhouden.

Conclusie: Is een remote werkplek iets voor jouw bedrijf?

Remote werkplekken bieden MKB-bedrijven de mogelijkheid om flexibel, veilig en kostenefficiënt te werken. De technologie is volwassen genoeg om betrouwbaar te functioneren en de voordelen wegen voor veel organisaties op tegen de investeringen. Of het voor jouw bedrijf de juiste keuze is, hangt af van je specifieke situatie, het type werk dat je doet en de wensen van je medewerkers.

Bij Aucuba begrijpen we dat de overstap naar remote werkplekken een grote stap kan zijn. Daarom bieden we persoonlijke ondersteuning bij het opzetten en beheren van digitale werkplekken. We nemen de technische complexiteit uit handen zodat jij je kunt focussen op je core business. Wil je weten wat de mogelijkheden zijn voor jouw organisatie? Neem dan contact met ons op voor een vrijblijvend gesprek over de mogelijkheden.