

Tekst: Jan Martijn Broekhof

Fotografie: Mirjam van Dijk

*Thuiswerken en het zogenaamde mobiel werken heeft de laatste jaren een enorme vlucht genomen. Door de toename van Internetbandbreedte, het fileprobleem en de behoefte aan flexibel werken kiezen werkgevers er steeds vaker voor om het bedrijfsnetwerk open te stellen voor gebruik buiten het pand.*

## Thuiswerken: een beveiligingsrisico?

**D**e voordelen van thuiswerken liggen voor de hand: uit onderzoek blijkt dat thuiswerkers 5 tot 15% productiever zijn dan werknemers op kantoor; er is geen reistijd meer en werknemers zijn meer tevreden. Veel functies laten thuiswerken goed toe, zeker in de zakelijke dienstverlening is het helemaal niet nodig om elke dag naar kantoor te komen. In steeds meer bedrijven wordt thuiswerken dan ook een secundaire arbeidsvoorwaarde.

### Geen wondermiddel

Voor organisaties die veel uren zien weglekken in files en reistijd in het algemeen lijkt thuiswerken de perfecte oplossing. Veel ondernemingen zien echter de consequenties van het niet op kantoor zijn te laat in. Buiten het feit dat het klaarmaken van de organisatie voor thuiswerk een andere aansturing, rapportage en coaching vergt, moet de techniek van de organisatie er ook voor klaargemaakt worden. Even een server toegankelijk maken en wat applicaties online beschikbaar maken is lang niet genoeg. Hieronder worden een aantal risico's beschreven die afgedekt dienen te worden.

### Informatiediefstal derft 6% van de bedrijfswinst

Bij bedrijven die geen fysieke producten leveren of produceren is informatiediefstal een groeiende zorg. Waarschijnlijk is het merendeel van uw medewerkers te vertrouwen, maar toch moet u alert zijn. Uit onderzoek van de ondernemingsorganisaties VNO-NCW, MKB Nederland, het

Openbaar Ministerie (OM) en de Raad van Hoofdd commissarissen blijkt dat de schade door interne criminaliteit gemiddeld zo'n 6% van de bedrijfswinst bedraagt. Wanneer u cruciale bedrijfsinformatie thuis benaderbaar maakt kan uw medewerker die kwaad in de zin heeft rustig zijn gang gaan. Op kantoor is daar minder gelegenheid voor omdat er meer onderling toezicht is.

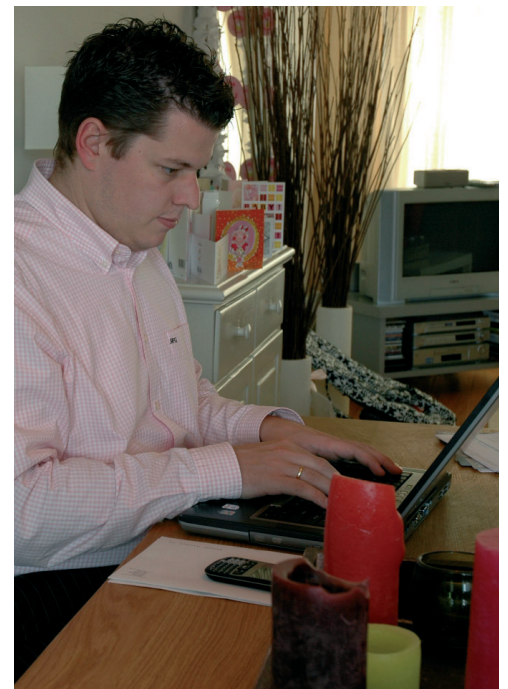
Ook het gebruik van usb-sticks houdt in dat grote hoeveelheden data makkelijk verloren kunnen gaan of gestolen kunnen worden. De afgelopen tijd zijn er voorbeelden genoeg te noemen van bedrijven die in verlegenheid zijn gebracht door het op straat liggen van gegevens over salarissen, creditcards en betalingen.

### Virussen en spam

Een ander punt van zorg is dat u geen zicht heeft op de apparatuur die gebruikt wordt om thuis te werken. Op een laptop van de zaak of een privé computer worden spelletjes, download programma's en allerlei andere "handige" software geïnstalleerd. Binnen uw bedrijfspand kunt u hier makkelijk op controleren, thuis niet. Hierdoor loopt u grote kans dat uw netwerk vervuild wordt met virussen, spyware en spam.

### Back-up

Op kantoor heeft u waarschijnlijk voorzieningen getroffen om van uw bestanden een back-up te maken. Na een brand of diefstal van uw apparatuur kunt u de gegevens eenvoudig weer terughalen. Bestanden die bij uw medewerkers op harde schijven en in privé email-



■ Jan Martijn Broekhof is frequent thuiswerker

boxen staan, zijn door u niet in een back-up mee te nemen.

### De oplossing

Zoals u in dit artikel heeft kunnen lezen heeft thuiswerken een aantal beveiligingsrisico's in zich. Toch is thuiswerken aan te raden: de voordelen zijn legio en door uw IT goed in te richten kunnen alle risico's op een acceptabele manier afgedekt worden. De kans dat één van de risico's bewaarheid wordt hoeft dan nauwelijks serieus genomen te worden.

Er zijn bijvoorbeeld mogelijkheden om uw gegevens centraal op te slaan en toch thuis en onderweg beschikbaar te maken. U kunt uw gegevens blijven opnemen in een back-up en uw bestanden komen niet op usb-sticks en thuis-pc's te staan. Ook plannen van kwaadwillende werknemers kunnen in een vroeg stadium gedwarsboemd worden.

Wilt u een keer een oriënterend gesprek voeren over veilig thuiswerken? Neem dan contact op met Jan Martijn Broekhof of Martijn van der Schaaf.

Computation  
Dakweg 48  
Postbus 430  
3700 AK Zeist  
T 030-6934500  
info@computation.nl  
www.computation.nl