



## De dure consultant de deur uit

Wellicht kijkt u vreemd op, deze term uit de mond van een bureau die ook consultancy verkoopt, te horen. Een toelichting hierop is denk ik op zijn plaats. Specialistische kennis wordt door bedrijven vaak ingehuurd bij hier in gespecialiseerde bureaus. Dit omdat de kennis vaak voor kortere tijd nodig is en deze kennis niet in huis is. Kennis inkopen door middel van het werven van specialisten is vaak duurder dan het tijdelijk inhuren van externe expertise. Tot zover lijkt het allemaal logisch.

In de praktijk gebeurt het echter ook vaak dat herhalende werkzaamheden, die met wat kennisoverdracht ook intern zouden kunnen gebeuren, toch door externen worden uitgevoerd.

Soms zijn hier hele plausibele redenen voor, maar de oorzaak ligt ook vaak bij het feit dat er geen kennisoverdracht plaatsvindt, de organisatie niet leert van de consultant en daardoor volledig afhankelijk blijft van de expertise van het ingehuurde bureau.

Secure Connection wil kennis uitdragen, zodat een organisatie herhalende werkzaamheden zelf kan uitvoeren, al dan niet met wat ondersteuning van een externe partij.

Een methode die wij hanteren om onze kennis uit te dragen is door middel van het maken van kennisobjecten.

In een kennisobject zit alle kennis die nodig is om bijvoorbeeld een risico-analyse of een audit op een organisatie een systeem of een netwerk te houden.

Kennisobjecten bevatten vragenbomen, adviezen, koppeling tussen de resultaten van de vragen en de adviezen in de vorm van mathematische (sub-) objecten en rapportages om de resultaten van de analyse of de audit weer te geven. Via onze StandardGUI zijn de objecten te gebruiken.

Het grote voordeel van deze methode is dat u tegen geringe kosten zelf in staat bent analyses uit te voeren met hooguit wat ondersteuning vanuit Secure Connection. U bespaart een hoop kosten op consultancy en haalt bovendien een stuk kennis in huis.

Consultancy blijft op deze manier betaalbaar en daardoor ook bereikbaar voor de organisatie met wat minder budget voor advies.

Secure Connection wil op deze manier graag kennispartner zijn.

## Thuiswerken

Meer en meer blijkt de thuiswerkplek bijzonder kwetsbaar voor onbevoegde inzage van uw vertrouwelijke bedrijfsinformatie. Het verbieden om thuis te werken aan gevoelige informatie is geen reële optie meer. We willen steeds flexibeler werken. Ook de nog steeds toenemende files brengt veel mensen er toe om één of twee dagen per week thuis of 's avonds bij thuiskomst het werk te doen.

## Kennisobject

Secure Connection heeft het antwoord. Met SCRemote kunt u een veilige thuiswerkplek creëren, rekening houdend met uw specifieke beveiligingsrisico's. SCRemote is een kennisobject waarmee u exact vast kunt stellen welke beveiligingsrisico's u loopt en welke maatregelen u hiertegen moet treffen. De maatregelen gaan tot en met de instellingen in uw browser, emailclient, systeem, router, etc.



Standaard Gui 2-9

## Verschillende thuiswerkconcepten

SCRemote legt u geen concept op, maar kan werken met verschillende thuiswerkconcepten, afgestemd op uw behoefte.

Een concept kan bijvoorbeeld het "thin client" concept zijn, waarbij de thuiswerker geen gegevens op zijn desktop krijgt. Een ander concept is bijvoorbeeld de Laptop van de "zaak", waarbij de thuiswerker zelf geen programmatuur kan installeren of instellingen kan wijzigen.

Welke optie u ook kiest, er zal moeten worden nagedacht over de scheiding zakelijk - privé en hoe te voorkomen dat zakelijke informatie in de privé omgeving terecht komt.

Een en ander is natuurlijk afhankelijk van de gevoeligheid van uw gegevens.

## Hoe werkt SCRemote?

SCRemote werkt volgens het standaard kennis objectprincipe van Secure Connection BV en genereert op basis van de analyse een goed leesbaar rapport waarin alle maatregelen (organisatorisch, fysiek, logisch van algemeen tot detail) overzichtelijk zijn weergegeven evenals de motivatie waarom tot de keuze is gekomen.

SCRemote is ook leverbaar in een extended version. Dit houdt in dat er naast het rapport, tevens de configuratiebestanden uitkomen, waarmee u de thuiswerkplek (

Bijvoorbeeld Windows XP) meteen automatisch kunt configureren. Naast het gemak van de snelheid, kan op deze manier geen fouten worden gemaakt.

## Actueel

### Inbraak Openbaar Ministerie.

Bij het Openbaar Ministerie in Den Haag is in het weekeinde van 19 en 20 februari ingebroken. De inbraak vond plaats bij het functioneel parket. De daders hebben ingebroken in de beveiligde ruimte van het parket waar 'informatie betreffende lopende zaken' is gestolen.

Als of 1 inbraak nog niet voldoende is zijn er uit het landelijk computercentrum van de rechtbanken en het Openbaar Ministerie (OM), het beveiligde pand van ICTRO, 26 januari 22 laptops gestolen.

In een zeer kort tijdsbestek word dezelfde organisatie twee getroffen door een inbraak waarbij informatie is meegenomen.

Toeval of niet dit is voor alle betrokkenen zeer veeleend en kan bij het eventueel verlies van vertrouwelijke informatie verstrekkingevolgen hebben voor alle betrokkenen

Uit bovenstaande stuk blijkt dat slechts IT-technische maatregelen niet afdoende zijn om uw informatie veilig te beschermen. Er zal dus ook op een adequate manier aandacht besteed moeten worden aan de fysieke beveiliging en de hierbij horen de maatregelen. Dit gaat verder dan hang- en sluitwerk en her en der een enkele bewakingscamera.

Secure Connection kan u ook helpen bij het fysieke gedeelte van uw (informatie)beveiliging. Denk hierbij aan het uitvoeren van analyses, advisering of implementatie.

Neem voor meer informatie contact op met één van onze medewerkers (0168-382420) of [info@secon.nl](mailto:info@secon.nl)