# Het Nieuwe Werken of Kwetsbaarheid?

*Het Nieuwe Werken* staat volop in de belangstelling. Maar informatiebeveiligingsaspecten blijven veelal onderbelicht. In dit artikel worden de kwetsbaarheden beschreven en wordt aangegeven hoe de security manager *Het Nieuwe Werken* veilig kan faciliteren zodat er geen sprake is van *De Nieuwe Kwetsbaarheid*. Johri Maat *

Geef 'Het Nieuwe Werken' op als zoekvraag in Google en je hebt zo 4.160.000 resultaten (stand 1 december 2010) te pakken. Onder Het Nieuwe Werken (hierna: HNW) wordt kortweg een andere manier van werken en samenwerken verstaan, ondersteund door de laatste technologieën zoals social media, cloud computingdiensten en mobiele communicatie (smartphones voor spraak, e-mail en video). Kenmerkend is dat medewerkers en organisaties flexibeler omgaan met arbeidstijd en werkomgeving, ook wel tijd- en plaatsonafhankelijk werken genoemd. De medewerkers hebben een steeds grotere vrijheid om te bepalen wanneer de werkzaamheden verricht worden en waar, of dit nu thuis, op het eigen kantoor, op het strand of bij een buitenlands vakantiehuisje is. Men wordt niet meer afgerekend op het aantal uren dat men op kantoor aanwezig is, maar op de productiviteit, de output.
HNW moet deze productiviteit van medewerkers vergroten, mede opdat zij zich prettiger voelen. HNW is hip en menig werkgever wil zich er graag mee afficheren. Het is dan ook een onderwerp dat veel besproken wordt in dagbladen, vak- en carrièretijdschriften, meestal gepaard gaande met afbeeldingen van ontspannen medewerkers die met hun notebook op schoot werken vanaf hun favoriete locatie.

## Betere dienstverlening

Ook voor de (Rijks)overheid is HNW een manier om de dienstverlening te realiseren die burger en politiek tegenwoordig verwachten. Het Regeerakkoord van het Kabinet Rutte spreekt van '*een krachtige, kleine en dienstverlenende overheid, [...] met minder belastinggeld, minder ambtenaren, minder regels en minder bestuurders*'.
Door het toepassen van HNW zijn ambtenaren minder gebonden aan het eigen departement en kunnen daardoor eenvoudiger programmatisch werken en zo sneller inspelen op maatschappelijke vraagstukken. Social media maken het mogelijk om snel opinies te wisselen tussen ambtenaren onderling, maar ook met burgers. HNW biedt ook de mogelijkheid om te bezuinigen op kantoorruimte en reiskosten, er zijn immers minder werkplekken en reisbewegingen nodig.

## *HNW vergroot de kans op het uitlekken van informatie*

# De Nieuwe

Voor een succesvol gebruik van HNW is het wel van belang dat informatiestromen grotendeels gedigitaliseerd worden. Dat dit goed mogelijk is, heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties laten zien; hier is de stukkenstroom al jaren grotendeels gedigitaliseerd. Het zijn hierbij niet alleen beleidsambtenaren die HNW kunnen toepassen, ook dossierbehandelaars kunnen onder bepaalde voorwaarden (tenminste een deel van) hun werkzaamheden flexibeler inrichten. Hierbij valt te denken aan gerechtelijke procedures, asielverzoeken, vergunningafhandelingen en belastingzaken.

## Kwetsbaarheden

HNW brengt natuurlijk niet alleen voordelen met zich mee. Informatie is het werkkapitaal voor de overheid. Doordat informatie letterlijk buiten de reguliere werkomgeving wordt gebracht, neemt het vluchtige karakter van informatie nog meer toe. Dit heeft gevolgen voor informatiebeveiliging, die draait om drie kernbegrippen: beschikbaarheid, integriteit en vertrouwelijkheid.

Kenmerk van HNW is dat opslag, transport en bewerking van data deels plaatsvinden buiten het eigen domein van de organisatie. Als van tevoren onvoldoende is nagedacht over de vraag welke informatie hiervoor in aanmerking komt of wanneer onvoldoende beveiligingsmaatregelen getroffen worden, zijn deze data mogelijk door derde partijen in te zien, te wijzigen of te verwijderen. Als een medewerker bijvoorbeeld zijn werkzaamheden in het buitenland uitvoert, kan het zelfs zijn dat politie, inlichtingen- of veiligheidsdiensten in het land van verblijf deze data vorderen (zie ook de brochure ‘Spionage bij reizen naar het buitenland’ op de website van de AIVD).

Dit heeft gevolgen voor de privacy van de burgers met wier gegevens gewerkt wordt, maar het kan ook tot economische schade voor bedrijven of een bedreiging van de nationale belangen leiden.

## ‘Bring your own’

Een ontwikkeling die verband houdt met HNW, is het principe van ‘*Bring Your Own*’. Steeds meer medewerkers willen het liefst zelf hun middelen zoals smartphone of tablet-pc uitzoeken (hier zit een hoog gadgetgehalte aan) en kunnen hierop data van de organisatie zetten. Hierdoor kan vertrouwelijke informatie buiten de invloedssfeer van de organisatie komen te liggen, wat tot problemen kan leiden bij vertrek van de medewerker of bij interne onderzoeken naar aanleiding van vermoedens van integriteitsschendingen. Dit geldt ook voor het gebruik van gratis e-mailaccounts als hotmail en gmail of het plaatsen van documenten in bijvoorbeeld Google Docs.

HNW vergroot ook op andere manieren de kans op het uitlekken van informatie. Onbewust doordat gewerkt »

wordt met apparatuur die kwetsbaar is voor manipulatie (zoals hacken) of doordat men werkt in een omgeving waar onbevoegden eenvoudig mee kunnen lezen en luisteren (publieke ruimten zoals horeca en openbaar vervoer). Bewust doordat kwaadwillende medewerkers eenvoudig data kunnen ontvreemden uit de organisatie.
Het autoforwarden van berichten van zakelijke e-mailadressen naar privé e-mailadressen als gmail en hotmail is nu al een risico, maar als men buiten de reguliere werkomgeving rechtstreeks bij alle data op de servers kan, is het wel heel eenvoudig deze naar buiten te pompen. Ook als een medewerker onzorgvuldig omgaat met zijn of haar inloggegevens (zoals het delen hiervan met collega's en zelfs gezinsleden), leidt dit tot grote kwetsbaarheden voor de organisatie.

## Werk of privé?

Het eerdergenoemde voordeel van flexibiliteit voor de medewerker betekent ook dat werk en privé steeds meer door elkaar lopen. De psychosociale gevolgen (Wanneer ben je echt vrij? Gaat de privéomgeving er op vooruit als je steeds je e-mail op je smartphone doorneemt?) en het probleem van de meetbaarheid van productiviteit worden hier verder buiten beschouwing gelaten.

De vermenging van werk en privé maakt dat het met HNW tevens steeds onduidelijker wordt of men als privépersoon of als ambtenaar iets doet. Het gebruik van social media als Twitter waarin 'wetenswaardigheden' en opinies gedeeld worden met de 'followers' heeft al tot diverse incidenten geleid, omdat onduidelijk was of de Twitteraar optrad als privépersoon of als ambtenaar en daarmee een organisatiestandpunt uitdroeg. Zeker als een ambtenaar publiekelijk kritisch zou zijn op het eigen beleidsterrein, kan dit gevolgen hebben. De flexibiliteit van HNW mag bovendien niet tot onthechting van de organisatie leiden en er moet voldoende geïnvesteerd worden in het ontwikkelen van de 'politiek-bestuurlijke sensitiviteit' van de ambtenaar.

De belangrijkste kwetsbaarheid lijkt het gedrag van de ambtenaar. Is deze zich voldoende bewust van de verantwoordelijkheid en beperkingen die HNW met zich meebrengen? Want als HNW tot incidenten leidt, zullen media en politiek zich ongetwijfeld verbazen 'hoe dit toch heeft kunnen gebeuren'.

## Meebewegen

Het is aan de organisatie om dit soort kwetsbaarheden naar een acceptabel niveau terug te brengen door HNW veilig te faciliteren. Als een security manager zich steeds opstelt als een '*dr. NO*', diskwalificeert deze zichzelf en zijn vakgebied alleen maar als star en gedateerd. Een goede security manager beweegt mee en vindt manieren om belangen van informatiebeveiliging te waarborgen binnen de ontwikkeling van HNW. Dit kan door het incident gedreven werken los te laten en te werken op basis van risicoanalyses, waarbij onderscheid gemaakt wordt tussen reguliere en kritische bedrijfsprocessen: Wat zijn de belangen, de dreigingen, de kwetsbaarheden, de te nemen maatregelen en het geaccepteerde restrisico? Daar waar sprake is van bijzondere risico's kunnen selectief en doelmatig beperkingen worden opgelegd, zodat HNW een acceptabel restrisico krijgt. Hiertoe zijn technische en organisatorische maatregelen beschikbaar. Op het terrein van de technische maatregelen is al veel ontwikkeld door marktpartijen. Zowel hard- als softwarematige producten zijn in een mobiele variant beschikbaar om dataopslag en -transport op een veilige manier plaats te laten vinden. De gebruikersvriendelijkheid hiervan neemt ook toe, waardoor het gebruik niet meer is voorbehouden aan mensen met specialistische functies die eerst een uitgebreide instructie voor het werken met cryptomiddelen moeten volgen.

Het gedrag van de ambtenaar kan worden beïnvloed door organisatorische maatregelen: duidelijke regels, procedures en het vergroten van het beveiligingsbewustzijn. Een beknopte en eenduidige set van basisnormen in de vorm van een gedragscode of basisreglement zou idealiter vastgesteld moeten worden, zodat er op dat punt geen onduidelijkheid kan zijn.

Met deze kanttekeningen is het heel goed mogelijk om voor de (Rijks)overheid *Het Nieuwe Werken* niet te laten uitmonden in *De Nieuwe Kwetsbaarheid*. Dit is in het voordeel van de (Rijks)overheid als werkgever, de ambtenaar als werknemer en de publieke zaak waar het allemaal voor bedoeld is. «

* *mr. J.H. Maat is werkzaam bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties*

*Als een security manager zich opstelt als een 'dr. NO', diskwalificeert deze zichzelf*


## Samenvatting

- Ook binnen de **(Rijks)overheid** wordt **Het Nieuwe Werken** (HNW) steeds meer omarmd. HNW biedt mogelijkheden om mensen en organisaties flexibeler om te laten gaan met arbeidstijd en werkomgeving.
- HNW kent naast deze voordelen ook **kwetsbaarheden** op het terrein van **informatiebeveiliging**. Security managers dienen daarom op tijd mee te bewegen met de trend van HNW.
- Van belang is dat naast de **technische** maatregelen zoals beveiligde hard- en software, ook geïnvesteerd wordt in **organisatorische** maatregelen.
- Duidelijke regels, procedures en het vergroten van het beveiligingsbewustzijn zijn een **succesfactor** voor HNW. Hiermee zijn de werkgever, de werknemer en de publieke zaak gediend.