

## Ervaringen met mysterieuze gasten.

(Artikel in Security Management, december 2008)

### **TNO Nederland**

TNO is een van de grootste onderzoeksinstituten in Nederland. Tot de klantenkring behoren van oudsher onder andere de Ministeries van Defensie, Binnenlandse Zaken en Koninkrijks relaties (BZK), Buitenlandse Zaken en politiediensten. Daarnaast wordt tegenwoordig ook veel onderzoek gedaan voor tal van andere klanten. Aandachtsgebieden als petrochemie, bodemonderzoek, sociaal verkeersonderzoek, toepassingen van zetmeel, voertuigonderzoek, maritiem onderzoek en algemene industriële onderzoeken komen allemaal voor binnen TNO. De onderzoeken worden door circa 4500 vaste medewerkers en circa 1700 anders aangestelden op 18 vestigingen in Nederland uitgevoerd.

### **Een nieuwe beveiligingsmanager**

In 2007 werd de functie van Beveiligingsmanager / Chief Security Officer vacant door pensioenplannen van de zittende functionaris. Na sollicitatie mocht ik het stokje over nemen. Ik kende een groot deel van de TNO organisatie uit voorgaande werkzaamheden. Zo had ik het deel van TNO dat zich met opdrachten voor het Ministerie van Defensie bezig houdt van zeer dicht bij leren kennen in een eerder functie van IT Security Consultant. Daarnaast was ik in het verleden ook wel eens bij andere onderzoeksinstellingen van TNO om andere aan beveiliging verbonden redenen op bezoek geweest. Ik kende dus de diversiteit en de verschillende zienswijzen op beveiliging die men op verschillende plaatsen binnen TNO heeft. Aangezien het belangrijkste element in beveiliging naar mijn mening de leden van een organisatie is, was ik heel erg geïnteresseerd in de beleving die de medewerkers van TNO hadden van het fenomeen beveiliging. Ik wilde heel graag weten hoe het beveiligingsbewustzijn, beter bekend als security awareness, bij de medewerkers van alle vestigingen van TNO er uit zag.

### **Metten is Weten**

In een wetenschappelijke organisatie als TNO is het credo "metten is weten" een zeer bekend fenomeen. Hierop aansluitend en gebruik makend van mijn ervaringen in het verleden bij andere bedrijven en organisaties wilde ik daarom ook hier de security awareness meten. Dit meten kon ik natuurlijk zelf uitvoeren. Het gevaar van deze benadering was echter dat ik te veel vanuit mijn oude ervaring binnen het Ministerie van Defensie de zaken zou benaderen terwijl grote delen van TNO niets van doen hebben met dit ministerie. Een alternatief zou zijn om enkele security experts van binnen TNO te vragen de zaak te bemeten. Het gevaar dat ik daarin onderkende was dat men wellicht zaken over het hoofd zou zien omdat bepaalde situaties als normaal worden gezien maar waar toch risico's aan kleven. Een derde alternatief was het inhuren van een externe partij om de meting in opdracht uit te voeren. Na overleg met de Raad van Bestuur van TNO werd voor deze laatste optie gekozen.

In het verleden was al eerder naar mogelijkheden voor externe inhuur voor evaluatie van security awareness gekeken. Hierbij was LBVD in Delft onder de aandacht gekomen. Aangezien contacten goed waren werd besloten met LBVD in zee te gaan. Ik wilde daarbij niet het gehele pallet van maatregelen in handen van één partij leggen. Na overleg kwamen we overeen dat leverancier zich

zou concentreren op een uitgebreide meting aan de hand van bezoeken van niet rechthebbenden, zogenaamde “MysteryGuests”, het verzorgen van rapportages van de metingen en het uitvoeren van enkele informatiesessies.

Het lag in de bedoeling een representatief aantal vestigingen van TNO te laten bezoeken door de MysteryGuests. Alle vestigingen laten bezoeken was niet erg zinvol omdat er vestigingen bij zijn die erg klein zijn. Daarnaast speelden budgettaire beperkingen een rol. Van de achttien vestigingen werden uiteindelijk negen vestigingen gekozen om te bezoeken. Hierbij werd binnen elk kennisgebied, voor TNO beter bekend als kerngebied, tenminste één vestiging geselecteerd. Daarnaast werd ook de zogenaamde hoofdvestiging, de formele “zetel van het bestuur” niet vergeten. Iedere vestiging zou met twee bezoeken worden vereerd om “toevalligheden” uit te sluiten. De bezoeken zouden telkens door twee MysteryGuests worden uitgevoerd zodat men beter, zekerder en natuurgetrouwer kon optreden.

## **Afstemming**

Voorafgaande aan de bezoeken van de MysteryGuests werd veel overleg gepleegd. Zo werd een uitgebreid intakegesprek gehouden en geprotocolleerd. In mijn optiek is het zeker aan te bevelen hier duidelijk aandacht aan te besteden. Enerzijds om teleurstellingen te voorkomen en anderzijds om de uitvoerende MysteryGuests legale dekking te geven voor hetgeen zij in opdracht uitvoeren. Het was overigens niet zo dat na het intakegesprek geen verder overleg nodig was. Voorafgaande aan bijna ieder bezoek werd, eventueel telefonisch, contact opgenomen om laatste aanpassingen door te spreken. Na afloop van activiteiten werd steevast een voorlopig mondeling verslag gegeven. In een enkel geval trof het team van MysteryGuests situaties aan waarbij zij van mening waren dat meteen actie nodig was. Door het goede contact kon in dergelijke gevallen meteen gehandeld worden.

## **Verassing!**

Een van de uitgangspunten voor het uitvoeren van een goede MysteryGuest-actie is het element van verrassing. Er moeten zo min mogelijk mensen op de hoogte zijn van het feit dat een bezoek wordt afgelegd. Dit is nodig om te voorkomen dat medewerkers uitsluitend vanwege het feit dat er gemeten wordt, anders gaan ageren. Het is vergelijkbaar met een snelheidsmeting op straat: vliegende brigades geven een meer waarheidsgetrouw beeld dan statische meetopstellingen. Om deze reden was er voor gekozen om in eerste instantie alleen de beveiligingsfunctionaris van de betreffende vestiging in te lichten. Zowel de directie ter plekke als andere lijnmanagers werden bewust niet geïnformeerd. Ik wilde immers weten hoe men zou reageren op onaangekondigde en niet-rechthebbende bezoekers. Het uitgangspunt was dat in geval van een incident altijd de beveiligingsfunctionaris zou worden ingeschakeld. Dit bleek voor een enkeling in de lijn een moeilijk verteerbaar punt. Het kostte lange telefonische sessies om enkele leidinggevenden van het nut en de noodzaak van de stilte voor de storm te overtuigen. Uiteraard had er voor gekozen kunnen worden om leidinggevenden breder te informeren maar of dit de effectiviteit van de meting ten goede was gekomen is te betwijfelen. Ik had er in overleg met de leverancier voor gekozen deze opvang zelf uit te voeren, ondanks dat men de mogelijkheid van mentale coaching door een sociaal psycholoog had aangeboden. Uiteindelijk ben ik blij deze keuze te hebben gemaakt. Immers: ik was verantwoordelijk voor de gekozen meetmethode. Daarnaast gaf deze aanpak meteen de mogelijkheid directe contacten te leggen zonder tussenkomst van ondersteunend personeel van het ingehuurde bedrijf.

## Reacties

De minder open reacties lieten iets langer op zich wachten. Maar na verloop van tijd, zo ongeveer nadat de eerste twee metingen waren uitgevoerd, begon het onderhuids te zoemen in de organisatie. Daadwerkelijk informatie hierover bereikte mij pas later. Het merendeel van de reacties waren neutraal tot positief. Een enkeling voelde zich ook op de werkvloer in de eer aangetast of wilde de noodzaak niet onderkennen. Het belangrijkste was echter dat zelfs al in de periode van de meting de aandacht voor security awareness begon toe te nemen. Zelfs tijdens de meetperiode gingen de deuren al beter op slot. Voorlichting Een heel belangrijk deel van de uit te voeren werkzaamheden waren de voorlichtingsrondes die volgden op de meting. Hiervoor werden alle vestigingen bezocht. Op de negen direct bemeten vestigingen ging ook een van de MysteryGuests mee om de ervaringen te delen. Dit bleek een zeer succesvolle formule. De herkenning bij de medewerkers was niet altijd even duidelijk aan de oppervlakte zichtbaar, maar reacties achteraf lieten zien dat hier veel effect mee is bereikt. Vooral het tonen van filmbeelden die lieten zien hoe makkelijk het kon zijn om toch binnen te komen in een afgeschermd omgeving, spraken erg aan. Over het algemeen genomen waren de medewerkers verbaasd dat er binnen gedrongen kon worden en dat er binnen toch zo veel waardevolle zaken gevonden konden worden. Ook in deze sessies kwam af en toe een verontwaardigde medewerker naar voren. Maar over het algemeen werd onderkend dat beter opletten toch wel nodig was.

Dit was wat primair ook het doel was: oplettendheid vergroten. Om dit eenvoudiger en meer tastbaar te maken werden voor de voorlichtingsronde in samenspel met de eigen afdeling Corporate Communication van TNO een aantal “leefregels” voor security opgezet. Dat draaide vooral om de genoemde oplettendheid onder medewerkers en de bereidheid om, zij het met gepaste vriendelijkheid, actie te nemen of vreemde zaken te melden.

## Aan de bal blijven

Security Awareness is een aandachtspunt dat niet na eenmalig oprakelen erg lang kan blijven liggen. De aandacht moet er bijna constant op worden gevestigd. Anderzijds moet je voorkomen dat men “informatie-moe” wordt. Goede en zich herhalende informatievoorziening kan uiteraard met uiteenlopende middelen. Er zal niet snel opnieuw een MysteryGuest actie komen binnen TNO, onder andere ook omdat er een substantiële investering mee gepaard gaat. De investering is echter zeer zeker lonend geweest. Er zijn nu van tijd tot tijd voorlichtingsactiviteiten bij verschillende fora in het lijnmanagement: MT-vergaderingen, operations overleg, directie-overleg en dergelijke. Verder hebben we het grootste knelpunt als aandachtspunt aangewezen: het volgen van de clean desk policy: geen bijzondere informatie op onbeheerde werkplekken. Hier wordt veel stringenter op toe gezien en gecontroleerd. Dit wordt daarnaast nog gecombineerd met andere communicatiemethoden zoals rapportages, flyers en on-line berichtgeving naar de medewerkers. Een ander punt van aandacht zal duidelijkere identificatie van bezoekers zijn. Hier wordt geprobeerd een combinatie te bewerkstelligen met de activiteiten die TNO moet ondernemen in verband met technische vernieuwingen van het toegangssysteem. En *last but not least* zullen de medewerkers blijvend voorzien worden van kleinere en grotere stukken informatie zoals dit artikel dat ook binnen TNO zal worden verspreid. In deze stukken informatie kunnen ze nog een keer nalezen waarom het een en ander heeft plaats gevonden en waarom het goed is iets dergelijks te doen. Hopelijk blijft daarbij ook de security awareness op een dergelijk peil dat als we een volgende keer mysterieuze gasten aantreffen adequaat kunnen reageren, want ze komen beslist een keer terug, ingehuurd of niet.

## **Conclusie**

Het laten uitvoeren van een MysteryGuest-actie is zeer nuttig gebleken voor TNO. Het heeft een aantal knelpunten aan het daglicht gebracht. Doordat een en ander plaats vond in de vorm van een geregisseerd incident is op verschillende plaatsen een reactie geforceerd. Met name door de voorlichtingsactiviteiten na de meting is het fenomeen security opnieuw, meer en breder gaan leven binnen TNO. De samenwerking met verschillende delen van de organisatie heeft ook een nieuwe impuls gekregen. Directe knelpunten zijn meteen aangepakt en inmiddels opgelost. Uit ervaring weten we echter dat we aan de bal moeten blijven. Voorlopig even niet meer met behulp van mysterieuze gasten maar nu weer met andere middelen. Maar wie weet, over een tijd zal het zeker weer nuttig zijn om dergelijke gasten uit te nodigen om te meten hoe het met security awareness is gesteld.

Rik Ernst  
Beveiligingsmanager TNO Nederland

september 2008