

# Het meten van informatiebeveiligingsbewustzijn

Dr. Ir. Rein de Vries en Ronald Dolfsma CISSP

**Dit artikel richt zich op het meten van informatiebeveiligingsbewustzijn. Allereerst vraagt het zich af of het meten van bewustzijn wel zinvol is, en zo ja, waarom. Na een bevestigend antwoord volgt de vraag wat te meten en op welke wijze. Een drietal pragmatische methodes komt aan bod met hun voor- en nadelen.**

Bewustzijn is een belangrijk aspect van informatiebeveiliging. De inhoudsopgave en index buiten beschouwing gelaten, dan wordt de term maar liefst 28 keer aangehaald in de Code voor Informatiebeveiliging. Bij 18 van de 133 beheersmaatregelen komt het om de hoek kijken. Dat is bij meer dan 13% van de aanbevolen beheersmaatregelen. De conclusie lijkt gerechtigd dat de opstellers zich voldoende bewust zijn van het belang van informatiebeveiligingsbewustzijn voor het bereiken van een gewenst niveau van beveiliging en veiligheid. Althans in ieder geval 'in enige mate', want de ene 'specialist' kan stellen dat het aspect bewustzijn onderbelicht is en nog steeds te weinig aan de orde komt in de code, terwijl de ander kan claimen dat het belang wordt overdreven en andere zaken veel belangrijker zijn. Om maar aan te geven dat zelfs wanneer er een exacte meting kan worden gedaan (het tellen van het aantal keren dat de lettercombinatie 'bewust' voor komt), er een zekere mate van subjectiviteit is.

Tijdens het mini seminar 'Trends in Informatiebeveiliging' van het GvIB op 22 maart 2007 stelde een van de sprekers dat 'bewustwordings-campagnes een marginaal effect hebben'. Hoe weet je zoiets? Zou het gemeten zijn? Slechts 1% (= marginaal) verbetering in plaats van een beoogde 50%? Hoe meet je bewustzijn? Valt bewustzijn überhaupt te meten? (Indien nee, dan is het niet mogelijk de gegeven stelling te formuleren).

Dit artikel doet een drietal methodes voor het meten van informatiebeveiligingsbewustzijn aan de hand. Maar allereerst moet de organisatie bepalen wat precies te meten. Als dat bekend is kunnen organisaties kijken hoe 'dat' te meten. Tenslotte: wat te doen met de uitkomsten? Het doel waarvoor bedrijven de uitkomsten gebruiken stelt eisen aan (de bruikbaarheid van) datgene dat moet worden gemeten. En zo is de cirkel rond en rijst de vraag: waar beginnen? Een eerste stap is bekijken wat een organisatie met de uitkomsten zou willen doen.

## Is meten nuttig?

De Code voor Informatiebeveiliging stelt dat be-

wustzijn in een aantal gevallen een randvoorwaarde is. Het heeft dus nut om bewustzijn te meten om te kijken of aan deze randvoorwaarde is voldaan. Wanneer het bewustzijn onvoldoende is dan schieten de beheersmaatregelen in de uitvoering tekort en zijn de risico's die de beheersmaatregel beoogt af te dekken, niet gemitigeerd. Althans niet volledig, zoals beoogd. Het is tevens prettig om te weten of wel aan de randvoorwaarde is voldaan. Mocht een beheersmaatregel ondanks voldoende bewustzijn niet het beoogde effect hebben, dan zal de oorzaak elders liggen.

[NEYS03] vertaalt security awareness naar de menselijke bijdrage aan het realiseren van een niveau van informatiebeveiliging en maakt daarbij onderscheid tussen een noodzakelijke en een gewenste bijdrage van medewerkers. Indien de bijdrage van medewerkers niet op niveau is zal het noodzakelijke niveau van informatiebeveiliging niet worden gerealiseerd, ook al zijn de technische en organisatorische maatregelen wel op niveau. Beveiligingsbewustzijn is de bepalende factor in de bijdrage die een medewerker levert aan het niveau van informatiebeveiliging en dus is de noodzaak tot inzicht in hoe het zit met beveiligingsbewustzijn in de organisatie evident.

Ook om andere redenen kan het nuttig zijn om een bewustzijnsmeting uit te voeren. Bijvoorbeeld om de accenten van een bewustzijns campagne te bepalen. Het heeft geen zin om tijd en aandacht te besteden aan zaken die reeds op orde zijn. De beschikbare middelen kunnen beter worden besteed aan aspecten die wel aandacht behoeven. Een andere doel is het meten van de effecten van bewustzijns campagnes. Management stelt veelal terecht de kritische vraag wat beveiliging oplevert, wat het bijdraagt aan de organisatie en hoe investeringen worden terugverdiend (ROSI). Het zou mooi zijn om te kunnen aantonen dat een groots opgezette bewustzijns campagne, waar veel in is geïnvesteerd, een substantieel in plaats van een marginaal effect heeft gehad.

Een laatste reden voor het meten van informatiebeveiligingsbewustzijn is dat het voor toekomstig beleid, toekomstige richtlijnen en voorschriften

geen kwaad kan om inzicht te hebben in het bewustzijnsniveau van de medewerkers van de organisatie.

### **Wat wil je wijzer worden?**

Voor het beantwoorden van de vraag wat te meten zijn er definities van security awareness, zie bijvoorbeeld [NEYS03]: security awareness (informatiebeveiligingsbewustzijn) is de mate waarin elke medewerker begrijpt wat het belang van informatiebeveiliging voor de organisatie is en tevens begrijpt welke niveau van informatie-beveiliging voor de organisatie noodzakelijk is en hier tevens naar handelt. Dit is een andere definitie dan een definitie die we elders wel bemerken en overeenkomstig wordt gemeten: security awareness is de mate waarin een persoon (veelal een manager of iemand anders die invloed heeft op het implementeren van beveiligingsmaatregelen) of een organisatie maatregelen heeft getroffen. Hierbij wordt het niet hebben getroffen van maatregelen uitgelegd als een gebrek aan bewustzijn. Hoewel er zeer zeker een verband is tussen geen bewustzijn en daardoor niet adopteren van maatregelen, is dit volgens de auteurs geen bruikbare definitie voor het meten van bewustzijn. Het niet aanwezig zijn van maatregelen is niet altijd terug te voeren op een gebrek aan bewustzijn.

Terug naar de eerst gegeven *definitie*. Verwacht een organisatie van iedere medewerker evenveel begrip van het belang van informatiebeveiliging? Waarschijnlijk niet. De bijdrage van bepaalde medewerkers is belangrijker dan die van anderen. De mate van begrip is afhankelijk van het soort taken dat de medewerker verricht, welke verantwoordelijkheden zij/hij draagt en waartoe zij/hij gemandateerd is. Dit aspect is een belangrijk onderdeel van het meten. Het is belangrijk op de juiste plaatsen te meten en de metingen te wegen, om zuivere conclusies te kunnen trekken. Mag je van iedere medewerker wel verwachten dat zij/hij begrijpt welk niveau van informatiebeveiliging voor de organisatie belangrijk is? De deskundigen zijn het hier vaak zelf al niet over eens, laat staan dat 'normale' medewerkers dit inzicht hebben. Wat belangrijker is, is dat medewerkers het belang van een goed niveau van informatiebeveiliging voor de organisatie onderkennen en onderschrijven, waarbij duidelijk is gecommuniceerd welke normen de organisatie hierbij voor ogen heeft. Denk hierbij aan (gedrags)regels, procedures, regelingen, enzovoorts. Wanneer deze bij de medewerker bekend zijn en zij/hij het belang onderschrijft, mag worden verwacht dat zij/hij er ook naar handelt. De mate waarin dat het geval is is enigszins te meten, op een aantal manieren met elk specifieke voor- en nadelen. De conclusie is dat organisaties alleen situationeel kunnen meten. Bewustzijn laat zich moeilijk generiek meten.

### **Hoe meten?**

Metten moet je goed doen. Bij voorkeur via een meetmethode die eenduidig en objectief is, en het locale of algehele bewustzijnsniveau van een organisatie (onderdeel) eenduidig op een een-dimensionale schaal aangeeft. Andere eisen aan de ideale meetmethode zijn onder meer:

- Het resultaat moet niet (te sterk) afhankelijk zijn van de persoon die de meting uitvoert.
- Extrapolerbaarheid: geldend voor delen van of de gehele organisatie.
- De meting moet met een zelfde nauwkeurigheid op latere tijdstippen als delta-meting kunnen worden herhaald, zodat met een zekere betrouwbaarheid verbetering (of verslechtering) valt te constateren.
- De meting moet toepasbaar en uitvoerbaar zijn. Dit pleit voor een niet al te academische benadering, waarbij binnen een beperking in tijd, middelen en budget resultaten te behalen zijn, die leiden tot het gewenste inzicht cq. score.

Andere selectiecriteria zijn ook denkbaar; zoals afhankelijkheid van een externe partij en het tijdsbestek waarbinnen de meting meetresultaten dient op te leveren. De selectie van een meetmethode hangt ook af van de wensen die er zijn ten aanzien van de meetresultaten. Neemt de organisatie genoegen met een (niet-harde) kwalitatieve uitspraak? Of is bijvoorbeeld een IB-dashboard gewenst? Oftewel moet de meting leiden tot kwantitatieve resultaten? Uiteraard kunnen opdrachtgevers zowel kwalitatieve als kwantitatieve resultaten verlangen. Een ander criterium is dat het meten het doelobject niet (te veel) beïnvloed, immers: wat wordt precies gemeten als het meten wel het resultaat in een te grote mate beïnvloed?<sup>1</sup>

Als beproefde meetmethoden worden nu kort besproken:

1. Fysieke observatie en MysteryGuest
2. Face-to-face interviews
3. Online IB-peilingen

### **Fysieke observatie en MysteryGuest**

Fysieke observatie en MysteryGuest is een van de manieren om informatiebeveiligingsbewustzijn te meten (zie ook [VROU06]). Wetende hoe medewerkers geïnstrueerd zijn, wat de 10 gouden regels zijn en wat er in de gedragscode en handboeken staat, zal een MysteryGuest zich fysiek op locaties door kantoren en gebouwen begeven. Daarbij dient de MysteryGuest op basis van een vooraf opgestelde checklist letten op 'incidenten' die duiden op een tekort aan bewustzijn. Zoals stoelen die toegangs-

- 1 In de praktijk blijkt dat aan een zeker bewustmakend effect niet valt te ontkomen. Vanuit een zuiver academisch perspectief is dit moeilijk te verteren. Voor de organisatie is het echter mooi meegenomen!

deuren tegen de regels in open houden, desktops die niet vergrendeld zijn, waardevolle zaken die op bureaus slingeren (pasjes, PDAs, gevoelige documenten), informatie aanwezig op white-boards en papier bij printers en faxmachines. Dit vergt een scherp oog en een turflijst of een goed geheugen. De foto- of filmcamera is hierbij een uitstekend hulpmiddel.

Een gradatie verder kan de MysteryGuest kijken of zij/hij als vreemdeling wordt aangesproken, of zij/hij zonder geautoriseerd te zijn via vriendelijk vragen tot beveiligde zones wordt toegelaten, of medewerkers toelaten dat de MysteryGuest meekijkt met het intypen van wachtwoorden, de deur openhouden als zij/hij met een paar laptops naar buiten loopt. Deze toevoeging vergt echter verregaande vaardigheden op het gebied van social engineering van degene die de meting uitvoert en deze zijn niet iedereen gegeven. Het resultaat is dus in enige mate en in meer dan één opzicht afhankelijk van de kwaliteiten van de tester.

Voor een bewustzijnsmeting die objectief en nauwkeurig moet zijn en bij herhaling of bij uitvoering door verschillende personen dezelfde resultaten moet opleveren is deze eigenschap niet ideaal. De methode maakt echter de kwetsbaarheid van de organisatie (door een gebrek aan bewustzijn) wel zeer concreet en zichtbaar. Wie slaapt nog lekker wetende dat onbevoegden bij hun organisatie als een 'stille Willie' zo naar binnen kunnen lopen? Dat onbevoegden zich in alle beveiligde zones kunnen begeven en totaal onopgemerkt zich naar buiten kunnen begeven, mogelijk met allerlei bemachtigde zaken? Over deze meetmethode kan verder nog worden opgemerkt dat ze binnen een kort tijdsbestek tot veel resultaat leidt en bij voorkeur dient te worden uitgevoerd door een externe partij, onder meer vanwege blindheid van de eigen organisatie en het (niet) bekend zijn met de onderzoeker.

### Face-to-face interviews

Vraaggesprekken met medewerkers levert veel inzicht op. Zo ook dat het vaak droevig gesteld is met de kennis en het begrip van datgene waarvan ISO17799:2005 vindt dat medewerkers enige kennis en begrip van zouden moeten hebben. Wat dat betreft is de 'beroepsgroep' veelal geneigd het bewustzijnsniveau te hoog in te schatten<sup>2</sup>. Via voorbereide vraaggesprekken is te achterhalen hoe medewerkers tegen informatiebeveiliging aankijken, wat ze er onder verstaan, hoe ze in bepaalde omstandigheden zouden handelen, hoe ver hun kennis van het informatiebeveiligingsbeleid en de daaruit afgeleide regels en richtlijnen van de orga-

2 Ter illustratie: *vercijfering* blijkt voor medewerkers soms al een te moeilijk woord, laat staan *encryptie*. De term *versleuteling* lijkt het meest aan te sluiten op de werksituatie van de doorsnee medewerker maar is nog steeds te moeilijk.

nisatie reikt.

Naast het bepalen van de mate waarin medewerkers zich van aspecten van informatiebeveiliging bewust zijn, kan de interviewer spontaan en interactief inzoomen op zaken die de geïnterviewde te berde brengt en hiervan notitie nemen. Bijvoorbeeld ingesloten informele werk-wijzen die riskant zijn, zoals het gebruik van privé e-mail of USB-sticks voor het uitvoeren van de eigen taak, of onduidelijke taken en bevoegdheden in de organisatie of procedures. De bewerkelijkheid is een groot nadeel van face-to-face interviews. Een 'goed gesprek' duurt al snel één tot anderhalf uur. Daarnaast vergt het uitwerken van gehouden gesprekken aanzienlijke inspanning. Face-to-face interviews lenen zich daardoor meer voor 'smaakbepaling' en toetsing en minder voor grootschalig onderzoek omdat, voor het kunnen doen van een voor de gehele organisatie geldige uitspraak, de benodigde steekproef (te) groot is. Face-to-face interviews zijn zeer geschikt om andere bewustzijnsmetingen te completeren en de kwaliteit van andere metingen te verbeteren. Een voorbeeld hiervan is het napraten over een MysteryGuest-actie die kort daarvoor is gehouden en het evalueren met 'het slachtoffer' hoe zij/hij en haar/zijn omgeving hierop hebben gereageerd. Uit hetgeen de medewerker hierover loslaat valt in kwalitatieve zin e.e.a. te concluderen ten aanzien van bewustzijn. Ook deze meetmethode is sterk afhankelijk van de vaardigheden van de onderzoeker. Daarnaast is ze sterk afhankelijk van de voor de gesprekken geselecteerde personen. Face-to-face interviews worden bij voorkeur door een externe uitgevoerd, zonder aanwezigheid van de opdrachtgever, zodat de geïnterviewde eventuele kritiek vrijelijk kan uiten.

### Online IB-peilingen

Een derde wijze waar de auteurs goede ervaring mee hebben is het meten van bewustzijn via online IB-peilingen. Hierbij wordt een digitale vragenlijst speciaal geprepareerd en 'losgelaten' op alle medewerkers van de organisatie of een bepaalde subgroep. De vragenlijst is via internet of het intranet web-based te beantwoorden en de deelname is al dan niet vrijwillig en/of anoniem.

Om een online IB-peiling tot een acceptabel resultaat te laten leiden hebben diverse zaken aandacht nodig. De vragenlijst is zeer belangrijk, deze moet absoluut goed zijn. Er is maar één gelegenheid om hem op te stellen. Als de meting loopt is de vragenlijst niet meer te wijzigen. De vragenlijst moet dus zeer zorgvuldig worden samen gesteld op basis van datgene waar interesse in is. Het is niet verstandig om te werken met een generieke, alomtoepasbare vragenlijst. Vragen naar zaken die op zich – beroepshalve – interessant zijn, maar niet van toepassing zijn op de werksituatie heeft weinig zin. Let bij het opstellen op de aspecten *kennis*, *attitude* en *gedrag*. Let ook op een goede balans. Een

te eenzijdige vragenlijst geeft een te eenzijdige uitspraak. Enerzijds is het goed om te toetsen of medewerkers bepaalde zaken snappen (en dus bewust zijn van), maar anderzijds is ook relevant wat zij zich in bepaalde omstandigheden zouden doen. In welke vorm moeten de vragen worden gesteld? Hoe multiple choice, open vragen, gebruik van schalen en velden voor vrije invoer te combineren?. Genoeg aspecten om bij stil te staan.

Een ander punt is de wijze van uitnodigen en de responsdoelstelling. Is het de hoogste baas die de uitnodiging tot deelname doet via een 'spam' e-mail, of komt er een melding op het intranet uit naam van de beveiligingscommissie in de hoop dat de medewerkers de melding zien en zullen reageren? Hoe is een responspercentage van bijvoorbeeld minimaal 25% te halen zonder de kwaliteit van de resultaten te beïnvloeden? Een advies: beloon het invullen niet! Voor welke periode zet je de peiling uit? Doe je een pilot? Stuur je herinneringen? Welke enquêtetool ga je gebruiken? Maakt het uiterlijk daarbij uit? (Voor een betere respons heeft het de voorkeur de peiling aan te laten sluiten op de huisstijl) Hoe verwerk je de resultaten? Welke tabel- en grafiekvormen gebruik je? Wat doe je met de feedback die je krijgt via de vrije velden?

Gerust kan worden gesteld dat het houden van een online IB-peiling behoorlijk wat voeten in aarde heeft en dus behoorlijk wat van de uitvoerders vergt. Daar staat echter tegenover dat IB-peilingen een schat aan waardevolle informatie opleveren. Naast de kwantitatieve informatie is er de feedback van medewerkers over zaken die je nooit 'via de wandelgangen' te weet zult komen (wellicht door de anonieme deelname). Organisaties kunnen online IB-peilingen geheel zelfstandig uitvoeren, echter om niet in valkuilen de stappen kan het inschakelen van externe hulp geen kwaad. Reserveer voor een zorgvuldig uitgevoerde peiling 1,5 à 2 maanden.

Om de kwaliteit van de online IB-peiling als meetmethodiek voor het doen van uitspraken inzake het informatiebeveiligingsbewustzijn te verbeteren is door LBVD de samenwerking gezocht met de Faculteit der Sociale Wetenschappen van de Universiteit Leiden (FSW). Dit heeft onder meer geleid tot de onderbouwing van de meting met een model voor het plaatsen en voorspellen van gedrag, een verbeterde wijze van het stellen van vragen en daarmee betere kwantitatieve resultaten en mogelijk-

heden om verbetering te meten.

### **Combinatie van de drie methoden**

Indien de tijd, de middelen en het budget het toelaten, kunnen de bovenstaande meetmethodes ook worden aangewend voor een grote bewustzijnsmeting, om o.m. een kwalitatief betere uitspraak te kunnen doen en via bevestiging een grotere betrouwbaarheid van de resultaten te verkrijgen.

### **Herhaling**

Controleren en bijstelling is onderdeel van de bekende Demming circle. Via herhaalde metingen kan ('dient te') worden geëvalueerd of bewustzijns-campagnes het gewenste positieve resultaat hebben. Behaalde successen moeten breed en goed via de daartoe geëigende wegen worden gecommuniceerd, om te laten zien dat bewustzijns-campagnes niet slechts een marginaal effect hebben, zoals eerder in dit artikel aangehaald. Herhaald meten is niet alleen zinnig om de organisatie te laten zien dat er vooruitgang is geboekt op korte termijn, maar ook waardevol met oog op borging op de lange termijn.

### **Conclusie**

Om uiteenlopende redenen heeft het zin om informatiebeveiligingsbewustzijn te meten. Omdat bewustzijn niet tastbaar is, is het meten lastig. Diverse eisen kunnen worden gesteld aan de te gebruiken meetmethode: uitvoerbaarheid, herhaalbaarheid, eisen t.a.v. de meetresultaten, etc. De meetmethode die aan alle eisen voldoet bestaat niet. Men zal zich moeten behelpen met minder ideale methodes. Hierbij geven de auteurs van-wege het bereik de voorkeur aan de online IB-peiling. De fysieke observatie met social engineering elementen is een goede tweede. Face-to-face interviews kunnen worden ingezet om het plaatje compleet te krijgen, als slagroom op het toetje ...

### **Over de auteurs**

Dr. Ir. Rein de Vries is partner en senior consultant bij LBVD. Ronald Dolfsma CISSP is adviseur informatiebeveiliging bij LBVD.

### **Literatuurverwijzingen**

[NEYS03] IT'ers, regels en security awareness. Afstudeerthesis in het kader van MSIT. Caroline Neys, versie 1.1 (open), april 2003.

[VROU06] De inzet van de mysteryman bij het ministerie van Verkeer en Waterstaat, Wilbert Vrouwenvelder, Informatiebeveiliging nr. 8, dec. 2006.