Bewust veilig?

In een artikel eerder dit jaar is ingegaan op menselijk en organisatorisch falen en het beveiligen ertegen [SPRU10]. In het verlengde hiervan gaat dit artikel dieper in op het fenomeen (informatie)beveiligingsbewustzijn en het verbeteren ervan. Verbetering is niet bij iedereen in de organisatie nodig, maar daar waar het wel nodig is, is het noodzakelijk voor een goede beveiliging.

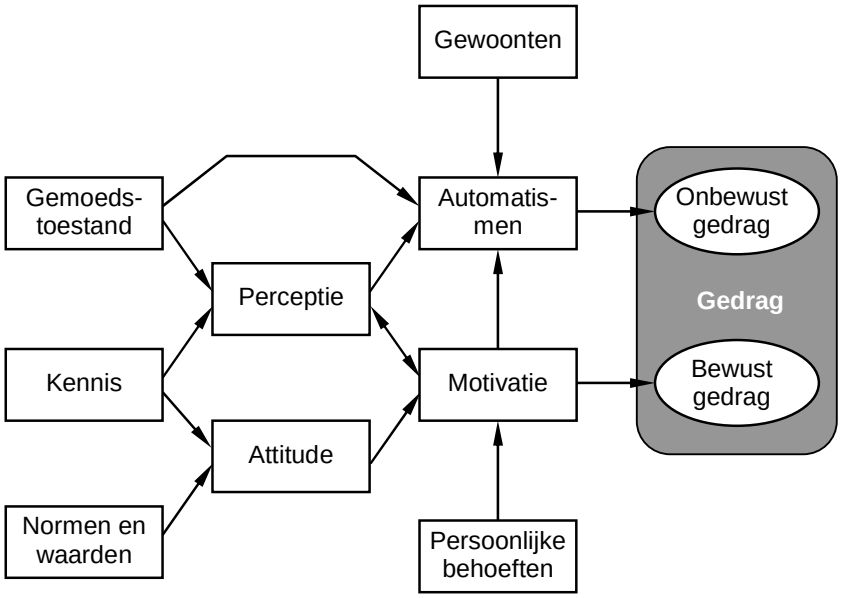
Auteur: **Dr. Marcel E.M. Spruit** is Lector Informatiebeveiliging aan de Haagse Hogeschool en tevens als senior consultant verbonden aan Het Expertise Centrum (HEC).

In een eerder artikel over de menselijke factor werd ingegaan op menselijk en organisatorisch falen [SPRU10]. Daar werd gesteld dat de intrinsieke motivatie voor (informatie)beveiliging – het (informatie)beveiligingsbewustzijn – bij de meeste mensen in een organisatie in orde is. Toch treden in vrijwel elke organisatie regelmatig beveiligingsincidenten op. Eén van de oorzaken hiervan is dat bij een aantal belangrijke spelers binnen de organisatie het beveiligingsbewustzijn nog niet ligt op het niveau dat eigenlijk nodig is. Dit betekent dat het voor deze mensen nodig is om het beveiligingsbewustzijn te verbeteren. Dat is minder eenvoudig dan het klinkt. Eerst moet duidelijk worden wie het betreft en vervolgens moet bepaald worden wat er dan moet gebeuren.

Dit artikel gaat dieper in op het beveiligingsbewustzijn en het verbeteren ervan in een organisatie. Om te beginnen zal ingegaan worden op het fenomeen beveiligingsbewustzijn en de belangrijkste factoren die dit beïnvloeden. Daarna wordt voor ieder van deze factoren bekeken voor wie en hoe dat in de organisatie positief beïnvloed kan worden om zo het beveiligingsbewustzijn te verbeteren.

Beveiligingsbewustzijn

De term ‘beveiligingsbewustzijn’ heeft in de praktijk meerdere betekenissen, maar doelt meestal op het besef van de mate waarin beveiliging nodig is en de daaruit voortvloeiende motivatie om aan de benodigde beveiliging mee te werken. Er is dan sprake van motivatie voor bewust gedrag ten behoeve van de noodzakelijke beveiliging. Figuur 1 geeft weer welke factoren in het algemeen bewust en onbewust gedrag beïnvloeden [BERN05] [OVER05] [ROBB05] [SPRU10]. Iemands motivatie en het daaruit voortvloeiende bewuste gedrag wordt beïnvloed door de perceptie van de omgeving en de daarin benodigde handelingen, de attitude ten opzichte van deze handelingen, en de eventuele beloningen die tegemoet komen aan de persoonlijke behoeften.



Figuur 1: Bewust en onbewust gedrag en de factoren die daarbij een rol spelen.

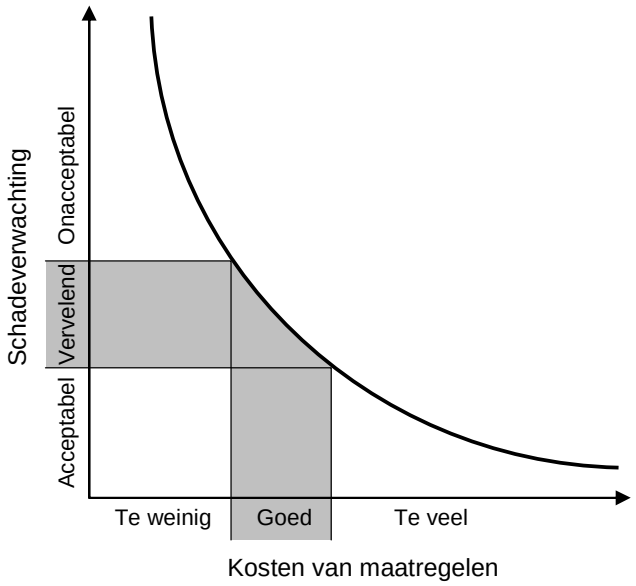
Zowel de perceptie, de attitude als de beloningen kunnen betrekking hebben op risico's en beveiliging en zo het beveiligingsbewustzijn beïnvloeden. Als we de perceptie, de attitude en de beloningen toespitsen op beveiliging dan kunnen we ze als volgt interpreteren:

- De perceptie van de risico's en de daarvoor benodigde beveiligingsmaatregelen. Dit noemen we de *risicoperceptie*.
- De attitude ten opzichte van beveiliging en beveiligingsmaatregelen. Dit noemen we de *beveiligingsattitude*.
- De eventuele *beloningen* (en straffen) die in het kader van de beveiliging gehanteerd worden.

Laten we deze drie factoren eens onder de loep nemen.

Risicoperceptie

De risicoperceptie van iemand geeft die persoon een besef van de risico's die een probleem zijn voor de organisatie, alsmede de maatregelen die nodig zijn om deze risico's adequaat aan te pakken. Het is duidelijk dat te weinig maatregelen treffen onverstandig is. Maar het treffen van te veel of te zware maatregelen is ook onverstandig. Niet alleen is dit vanuit het oogpunt van kosten ongunstig, maar het hindert bovendien de medewerkers onnodig tijdens het uitvoeren van hun werk. In figuur 2 ligt de juiste balans in de gearceerde zone, waar het totale (rest)risico, oftewel de overall schadeverwachting, in een goede verhouding staat tot de kosten die gemoeid zijn met de getroffen beveiligingsmaatregelen.



Figuur 2: De risicocurve.

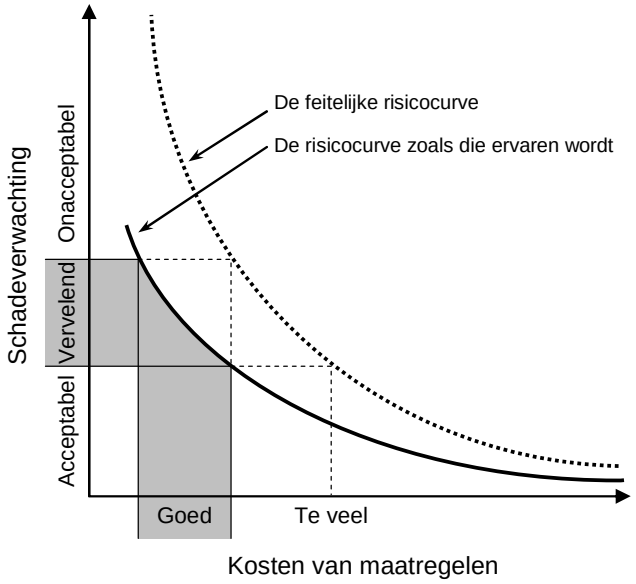
In een organisatie speelt voor de meeste medewerkers beveiliging slechts een bijrol in hun werk. Er spelen altijd wel enkele bedreigingen en deze kunnen tot risico's leiden. In de praktijk blijkt dat de meeste medewerkers bewust of onbewust een tamelijk reëel beeld van de risico's in hun werk hebben, en ook weten welke beveiligingsmaatregelen daarvoor nodig zijn. Aangezien de beveiligingsmaatregelen het primaire werk altijd in enige mate hinderen, zien de medewerkers deze maatregelen als een noodzakelijk kwaad dat gewoon moet gebeuren. Zo snapt bijvoorbeeld vrijwel iedereen dat als hij of zij naar huis gaat de kast met vertrouwelijke gegevens op slot moet en het werkstation uitgelogd moet worden.

Als het werk of de beveiliging in de organisatie significant verandert, bijvoorbeeld bij een reorganisatie of een fusie, dan is het niet ongebruikelijk dat de medewerkers de (gewijzigde) risico's niet goed in kunnen schatten. Dit geldt ook voor medewerkers die door een functieverandering op een voor hen nieuwe positie in de organisatie terechtkomen.

Managers staan in hun dagelijkse werk wat verder af van de risico's op de werkvloer. Als zij vanaf de werkvloer niet goed geïnformeerd worden over deze risico's dan hebben ze daarvan al gauw een vertekend beeld. In de meeste organisaties is dat inderdaad het geval. De communicatie van de werkvloer naar het management over bedreigingen en opgetreden (bijna-)incidenten is zelden goed geregeld, waardoor het management de feitelijke risico's onderschat.

In figuur 3 zien we dat een onderschatting van de risico's de risicocurve naar beneden laat schuiven. Als we ervan uitgaan dat het management goed in kan schatten welke overall schadeverwachting al dan niet acceptabel is (het gearceerde vlak op de verticale as), dan lijkt het of er minder geïnvesteerd hoeft te worden in beveiligingsmaatregelen (het gearceerde vlak op de horizontale as).

In de praktijk valt deze verschuiving nog sterker uit doordat het management verantwoordelijk is voor de financiële zaken, en in het kader van kostenbeheersing minimaal wil investeren in ondersteunende zaken, zoals beveiliging. De verschuiving wordt nog verder versterkt bij managers die zich vooral door de waan van de dag laten leiden. Voor deze laatste groep lijken de risico's namelijk kleiner te zijn, omdat weinig voorkomende bedreigingen niet in de risico-overwegingen meegenomen worden.

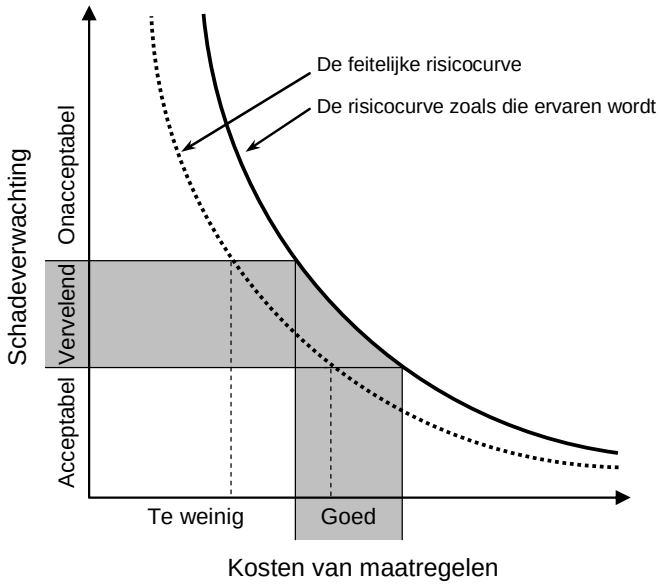


Figuur 3: De risicocurve zoals die ervaren wordt bij onderschatting van de risico's.

Naast de 'gewone' medewerkers en de managers heeft de organisatie ook medewerkers die door hun werk relatief sterk georiënteerd zijn op beveiliging. Het gaat vooral om medewerkers die een functie in de beveiliging hebben, zoals beveiligingsfunctionarissen en privacyfunctionarissen, maar ook medewerkers die een functie hebben waarin beveiliging vanzelfsprekend is, zoals financiële medewerkers, personeelsmedewerkers en ICT-beheerders. Zij worden in hun dagelijkse werk geregeld geconfronteerd met dreigingen en kwetsbaarheden. Zo ziet een ICT-beheerder bijvoorbeeld in de logging van de met internet verbonden systemen dat dagelijks duizenden spamberichten, virussen en hackers binnen willen komen. Deze overvloed aan concrete dreigingen leidt gemakkelijk tot een overschatting van de risico's.

In figuur 4 zien we dat een overschatting van de risico's de risicocurve naar boven laat schuiven. Als we ervan uitgaan dat de beveiligingsgeoriënteerde medewerkers goed in kunnen schatten welke overall schadeverwachting al dan niet acceptabel is, dan lijkt het of er meer in beveiligingsmaatregelen geïnvesteerd moet worden.

In de praktijk valt deze verschuiving nog sterker uit doordat beveiligingsgeoriënteerde medewerkers de aanvaardbaarheid van risico's veelal te laag inschatten. Door onvoldoende inzicht in de primaire processen van de organisatie gaan ze er te gemakkelijk van uit dat middelmatige schades onacceptabel zullen zijn. Beveiligingsgeoriënteerde medewerkers kiezen daarom vaak voor te veel en te zware beveiligingsmaatregelen.



Figuur 4: De risicocurve zoals die ervaren wordt bij overschatting van de risico's.

Nieuwe medewerkers en gewijzigde omstandigheden daargelaten, kunnen we dus constateren dat vooral bij het management en beveiligingsgeoriënteerde medewerkers een gerede kans bestaat dat zij een verkeerde risicoperceptie hebben. Op zich is dit al ongunstig, omdat daardoor te weinig middelen vrijgemaakt worden voor beveiliging en de beschikbare middelen nogal eens terecht komen bij overbodige en te zware maatregelen. In de praktijk is de situatie nog ongunstiger, omdat het management ook leiding geeft aan de beveiligingsgeoriënteerde medewerkers en met hen onder meer over beveiliging moet overleggen. Het ligt voor de hand dat het management en de beveiligingsgeoriënteerde medewerkers ieder vanuit hun eigen (vertekende) werkelijkheid zo'n groot verschil van inzicht hebben dat goed overleg hierdoor gehinderd wordt. Veelal vinden beide 'kampen' dat het andere kamp een volstrekt verkeerd beeld van de realiteit heeft, hetgeen de samenwerking en een goede invulling van beveiliging in de weg staat.

Beveiligingsattitude

De beveiligingsattitude van iemand geeft aan hoe die persoon tegenover beveiliging en beveiligingsmaatregelen staat, oftewel of de betreffende persoon beveiliging en de daarvoor te treffen maatregelen wel of niet nodig vindt.

De meeste medewerkers in een organisatie hebben in principe een neutrale houding ten opzichte van beveiliging: men snapt dat beveiliging nodig is en dat beveiligingsmaatregelen een zekere mate van hinder geven; men wil best aan de beveiliging meewerken, zolang de maatregelen redelijk zijn en anderen er ook aan meewerken.

Dit betekent dat medewerkers bewust of onbewust de redelijkheid van de maatregelen beoordelen door te kijken of de argumentatie voor de getroffen maatregelen logisch is, de maatregelen zelf duidelijk en haalbaar zijn en de zwaarte van de maatregelen klopt met de beoogde doelen. Als mensen maatregelen die ze zelf niet logisch vinden niet

uitgelegd krijgen, of als ze vinden dat bepaalde maatregelen te veel, te zwaar, of niet haalbaar zijn, dan vinden ze die maatregelen niet nodig en werken er niet aan mee.

Daarnaast kijken medewerkers bewust of onbewust hoe anderen in de organisatie met de maatregelen omgaan [BERN05] [OVER05]. Maatregelen die in de organisatie brede steun krijgen, kunnen ook op hun medewerking rekenen. In dit kader telt vooral de mening en de – zichtbare – bijdrage van managers en medewerkers met een bepaalde autoriteit.

Net als de medewerkers hebben de managers in het algemeen ook een positieve grondhouding ten opzichte van beveiliging, zij het dat de meeste managers de inspanning voor ondersteunende zaken, zoals beveiliging, willen minimaliseren. Net als de medewerkers kijken de managers naar de redelijkheid van de beveiligingsmaatregelen en wat anderen ervan vinden. Zij kijken daarvoor echter ook naar externe betrokkenen, zoals adviseurs, auditors, accountants, toezichthouders en klanten. De attitude van de managers wordt dus voor een deel beïnvloed door externen.

Bij beveiligingsgeoriënteerde medewerkers is de positieve houding ten opzichte van beveiliging in principe zeer sterk. Dit komt onder meer doordat deze mensen zelf gekozen hebben voor een beroep waarin beveiliging een belangrijke rol speelt. Zij zijn daardoor relatief veel met beveiliging bezig en verantwoorden dit aan zichzelf door aan beveiliging een groot belang toe te kennen (het opheffen van cognitieve dissonantie [BERN05]). Bij medewerkers die een functie in de beveiliging hebben, zoals beveiligingsfunctionarissen en privacyfunctionarissen, kan hierdoor de focus op beveiliging te sterk worden. Dan kan de situatie ontstaan dat de beveiligingsgeoriënteerde medewerkers zo hard aan de beveiliging trekken dat er te veel en te zwaar beveiligd wordt, waardoor het werk in de organisatie te veel gehinderd wordt en de beveiligingsattitude van de andere medewerkers en het management negatief beïnvloed wordt.

Anderzijds kunnen positief ingestelde beveiligingsgeoriënteerde medewerkers zo vaak bot gevangen hebben bij andere medewerkers en het management, dat ze daardoor gedemotiveerd geraakt zijn. In dit geval slaat de beveiligingsattitude van de betreffende medewerkers om van het ene uiterste naar het andere uiterste. Als een dergelijke demotivatie eenmaal toegeslagen heeft, is daar alleen met veel inspanning nog wat aan te doen [BERN05].

Beloning in het kader van beveiliging

Met beloning in het kader van de beveiliging kunnen mensen zodanig beïnvloed worden dat zij een goede invulling geven aan de beveiliging en de daarvoor benodigde maatregelen. Belonen hoeft niet financieel te zijn, maar kan ook met een schouderklopje, een compliment, het geven van interessante opdrachten, of een betere positie. Belonen van gewenst gedrag werkt in het algemeen effectiever dan het afstraffen van verkeerd gedrag. Belonen van verkeerd gedrag werkt nog effectiever, maar averechts. Dit moet dus te allen tijde voorkomen worden.

Met individuele beloning kan gedrag op individuele basis beïnvloed worden. Met groepsgewijze beloning kan coöperatief gedrag gestimuleerd worden. Voor een goede beveiliging is een optimale mix van individuele en groepsgewijze beloning nodig.

Beloning wordt top-down in de organisatie ingezet. Dit betekent dat medewerkers, ook beveiligingsgeoriënteerde medewerkers, hun beloning van hun managers moeten krijgen. De managers moeten hun beloning krijgen van hogere managers, of van buiten de organisatie, bijvoorbeeld van klanten of toezichthouders.

Het verbeteren van het beveiligingsbewustzijn

Hierboven hebben we gezien dat het beveiligingsbewustzijn wordt beïnvloed door de risicoperceptie, de beveiligingsattitude en beloning. Ieder van deze drie factoren kan aangepakt worden.

Het verbeteren van de risicoperceptie

Zolang het werk en de beveiliging in de organisatie geen significante wijzigingen ondergaan, zullen vooral nieuwe medewerkers, managers en beveiliginggeoriënteerde medewerkers last hebben van een verkeerde risicoperceptie. Het ligt dan ook voor de hand om juist deze groepen te benaderen om hun beeld bij te stellen. Organisatiebrede informatiecampagnes schieten in dit geval hun doel voorbij, omdat daarmee vooral informatie verstrekt wordt aan mensen die dat niet nodig hebben. Bovendien werkt het beter om de doelgroepen doelgroepspecifiek te informeren.

Nieuwe medewerkers moeten geïnformeerd worden over het voor hen nieuwe werk, de daarvoor geldende regels en procedures en de risico's die aan het werk verbonden zijn. Door deze informatie en door het samenwerken met collega's die al langer in het werk meedraaien, komt de risicoperceptie van nieuwe medewerkers al tamelijk snel op een acceptabel niveau.

Bij managers wordt het vertekende beeld vooral veroorzaakt door enerzijds de afstand tot de werkvloer, waardoor zij onvoldoende informatie krijgen over risico's en incidenten, en anderzijds de waan van de dag, waardoor risico's kleiner lijken te zijn. Dit leidt ertoe dat managers de feitelijke risico's onderschatten. Om een beter beeld te krijgen zouden managers effectief gebruik moeten maken van risicoanalyses en een goede registratie van (bijna-)incidenten. Het probleem is echter dat veel managers zich niet bewust zijn van de vele risico's en incidenten en daarom geen risicoanalyses en incidentenregistratie initiëren. Hierdoor ontstaat een vicieuze cirkel, waarin de managers de risico's onderschatten, daarom risicoanalyses en incidentenregistratie onnodig vinden, waardoor de onderschatting van de risico's in stand blijft. Iemand moet deze cirkel doorbreken. Dit moet iemand zijn die het mechanisme achter het ontstaan van de risico-onderschatting kent en daarnaast het vertrouwen van de betrokken managers geniet. Mogelijke gegadigden van binnen de organisatie zijn de CIO, de security manager en medewerkers met een bijzondere autoriteit. Van buiten de organisatie komen bestuur, toezichthouders en auditors in aanmerking. Degene die de managers over deze problematiek kan en wil informeren, zal hier ongevraagd zelf over moeten beginnen, want de managers zullen er niet om vragen.

Bij beveiligingsgeoriënteerde medewerkers ligt de oorzaak van het vertekende beeld vooral bij de nabijheid van bedreigingen en hun betrokkenheid bij het treffen van maatregelen. De veelal grotere afstand tot de primaire processen van de organisatie versterkt de vertekening. Daardoor zijn veel beveiligingsgeoriënteerde medewerkers niet

goed in staat om de voor hen relevante risico's goed in te schatten. Zo is het voor veel ICT-medewerkers bijvoorbeeld een eye-opener als ze horen dat hun collega's, inclusief het management, er niet wakker van liggen als bepaalde niet-vertrouwelijke bedrijfsgegevens op straat komen te liggen.

Om bij de beveiligingsgeoriënteerde medewerkers het gebrek aan inzicht te verbeteren, hebben zij aanvullende kennis nodig over de relatie tussen hun werk en de primaire processen en de te verwachten schadelijke gevolgen van mogelijke beveiligingsincidenten. Ook hier kunnen risicoanalyses en een goede registratie van (bijna-)incidenten helpen. Het is dan natuurlijk wel nodig dat de beveiligingsgeoriënteerde medewerkers bij het uitvoeren van de risicoanalyses betrokken worden en dat vanuit de incidentenregistratie goede rapportages opgesteld worden waarmee niet alleen het management geïnformeerd wordt, maar ook de betrokken beveiliginggeoriënteerde medewerkers. Risicoanalyses en incidentenregistratie worden echter pas gerealiseerd als het management daar opdracht voor geeft, maar als het management in de hierboven genoemde vicieuze cirkel zit, zal zij dit niet uit zichzelf oppakken en is het wachten op de derde, bijvoorbeeld de interne CIO, of een externe auditor, die het noodzakelijke zetje geeft.

We kunnen dus constateren dat voor het verbeteren van de risicoperceptie een aantal acties nodig is (zie tabel 1).

Doelgroep	Actie	Uitvoerder
'Gewone' medewerkers	- Informeren bij significante wijzigingen werk/beveiliging. - Informeren en begeleiden van nieuwe medewerkers.	- Managers/beveiligers. - Managers/beveiligers.
Managers	- Ongevraagd informeren over risico's en incidenten. - Risicoanalyses, incidentenregistratie en -rapportage.	- Vertrouwde derde. - Managers (initiatief), beveiligers (uitvoering).
Beveiligingsgeoriënteerde medewerkers	- Risicoanalyses, incidentenregistratie en -rapportage.	- Managers (initiatief), beveiligers (uitvoering).

Tabel 1: Verbeteracties voor de risicoperceptie.

Het verbeteren van de beveiligingsattitude

De beveiligingsattitude van de meeste medewerker en managers is in principe goed, maar om dat zo te houden moet aan een aantal voorwaarden voldaan worden.

Voor de medewerkers geldt dat duidelijk moet zijn wat de geldende regels en procedures zijn. Als medewerkers zich aan de regels en procedures willen houden, maar deze niet kennen, dan gaat het gemakkelijk fout. Verder moeten zij zien dat de voor hen relevante beveiligingsmaatregelen redelijk zijn, oftewel dat de argumentatie ervoor logisch is, de maatregelen duidelijk en haalbaar zijn en de zwaarte ervan klopt met de beoogde doelen. De getroffen maatregelen moeten brede steun genieten vanuit de organisatie. Vooral het commitment en het goede voorbeeld van het management en anderen met een bijzondere autoriteit telt zwaar. Door de medewerkers te betrekken bij

het selecteren van maatregelen en het kiezen van de implementatiewijze kan hun beveiligingsattitude verder versterkt worden.

Een goede beveiligingsattitude is niet bestand tegen onevenredige uitdagingen. Medewerkers die als 'kat op het spek gebonden' worden, moeten daarom tegen zichzelf beschermd worden om attitudeverschuiving (door opheffen van cognitieve dissonantie [BERN05]) en overtredingen te voorkomen. Dit geldt bijvoorbeeld voor financiële medewerkers, systeembeheerders en magazijnmedewerkers. In dergelijke gevallen zijn extra maatregelen nodig, zoals functiescheiding, supervisie en controle.

Voor de managers geldt ook dat zij de geldende regels en procedures moeten kennen en de voor hen relevante beveiligingsmaatregelen redelijk moeten vinden. Weliswaar zijn ze in principe zelf verantwoordelijk voor de regels, procedures en maatregelen, maar in de praktijk stammen veel regels en procedures nog van hun voorgangers en worden veel maatregelen zonder hun directe invloed getroffen door medewerkers met een beveiligingsfunctie. De redelijkheid van deze maatregelen is dan ook niet zonder meer duidelijk voor de betrokken managers en dit moet daarom aan hen uitgelegd worden. De beveiliging in het algemeen en de beveiligingsmaatregelen in het bijzonder moeten bovendien de steun hebben van anderen die voor de managers belangrijk zijn, zoals hogere managers, adviseurs, auditors, accountants, toezichthouders en klanten. Het verbeteren van deze steun is slechts deels mogelijk en dan nog vooral gestoeld op het verbeteren van hun risicoperceptie.

Managers die zich te sterk richten op hun persoonlijke doelen – financieel of qua carrière – hebben in het algemeen een zwakkere beveiligingsattitude. Als de beveiligingsattitude te zwak is, moet deze bijgestuurd worden door hogere managers, anderen met autoriteit, of externe betrokkenen.

De beveiligingsattitude van de beveiligingsgeoriënteerde medewerkers is in het algemeen zeer positief. Zolang dit niet tot overmatige beveiliging leidt, heeft de organisatie er geen last van en is er geen reden voor actie. Als het wel tot overmatige beveiliging leidt, moet de risicoperceptie van de betrokken medewerkers verbeterd worden. De maatregelen die hiervoor nodig zijn, zijn in de vorige paragraaf besproken.

Als beveiligingsgeoriënteerde medewerkers gedemotiveerd geraakt zijn door gebrek aan support – en mogelijk zelfs tegenwerking – vanuit de organisatie, dan is daar niet veel meer aan te doen. Alsnog de attitude bij de andere medewerkers en het management verbeteren, heeft dan weinig effect meer op de attitude van de beveiligingsgeorienteerde medewerkers. Eigenlijk is job-rotatie dan nog de beste oplossing. Maar dan wel *nadat* de organisatie zich op het punt van beveiligingsattitude verbeterd heeft.

In tabel 2 zijn de verbeteracties ten aanzien van de beveiligingsattitude samengevat.

Doelgroep	Acties	Uitvoerder
'Gewone' medewerkers	- Medewerkers informeren over geldende regels en procedures. - Redelijkheid maatregelen uitleggen. - Commitment aan maatregelen en goede voorbeeld. - Participatie van medewerkers bij selectie en implementatie. - Medewerkers zo nodig tegen zichzelf beschermen.	- Managers/beveiligers. - Beveiligers. - Managers en anderen met autoriteit. - Managers/beveiligers. - Managers/beveiligers.
Managers	- Managers informeren over geldende regels en procedures. - Redelijkheid maatregelen uitleggen. - Commitment aan maatregelen en goede voorbeeld. - Zo nodig te sterke focus op persoonlijke doelen bijsturen.	- Beveiligers. - Beveiligers. - Hogere managers, anderen met autoriteit en externe betrokkenen. - Hogere managers, anderen met autoriteit en externe betrokkenen.
Beveiligingsgeoriënteerde medewerkers	- Bij overmatig enthousiasme risicoperceptie verbeteren. - Bij demotivatie job-rotatie.	- Zie tabel 1 - Managers.

Tabel 2: Verbeteracties voor de beveiligingsattitude.

Het verbeteren van de beloning in het kader van beveiliging

Beloning in het kader van beveiliging kan de motivatie van medewerkers een extra positieve impuls geven. Om effectief met beloning te kunnen werken, moet eerst duidelijk gemaakt worden welk gedrag verwacht wordt en welke beloning daaraan gekoppeld is. Ook moet duidelijk gemaakt worden dat verkeerd gedrag niet tot beloning zal leiden.

Lastige punten bij het werken met beloning zijn het formuleren en communiceren van het gewenste gedrag in het kader van beveiliging, het vinden van de juiste mix van individuele en groepsgewijze beloning en het adequaat en consequent uitvoeren van de beloning.

Omdat beloning top-down in de organisatie ingezet wordt, helpt het vooral om medewerkers te stimuleren. Beloningen voor het management komen deels van buiten de organisatie en zijn vanuit de organisatie moeilijker te beïnvloeden.

Het ligt voor de hand dat beloning van gewenst gedrag in het kader van beveiliging pas gegeven wordt als de managers en externen de inspanning daarvoor waarderen. Daarvoor is het nodig dat de managers en externen een goede risicoperceptie en beveiligingsattitude hebben. Bij veel organisaties is dat nog niet het geval en dan kan het bijvoorbeeld voorkomen dat medewerkers die de (beveiligings)regels en -procedures aan hun laars lappen, beloond worden voor hun productiviteit. Of dat (lagere) managers bonussen krijgen voor resultaten die geboekt worden door onredelijke risico's te

accepteren, of incidenten te verdoezelen. In dergelijke gevallen wordt verkeerd gedrag beloond en dat is fnuikend voor de beveiliging en daarmee voor de organisatie.

Zelfs als de risicoperceptie en de beveiligingsattitude van de managers wel goed zijn, is het tamelijk lastig om verkeerd gedrag nooit te belonen. Beloning kan namelijk allerlei soorten incentives betreffen, van een schouderklopje tot een promotie. Dit betekent dat verscheidene handelingen van managers – bijvoorbeeld het toewijzen van bepaalde taken of projecten – door medewerkers als beloning gezien kunnen worden. Als de 'beloonde' medewerkers zich onder meer op het gebied van beveiliging voorbeeldig hebben gedragen, dan is er weinig aan de hand, maar anders wordt in de ogen van de betrokken medewerkers verkeerd gedrag beloond.

In tabel 3 zijn de verbeteracties ten aanzien van beloning in het kader van beveiliging samengevat.

Doelgroep	Acties	Uitvoerder
'Gewone' en beveiligingsgeoriënteerde medewerkers	- Verwachtingen communiceren, belonen van goed gedrag en niet belonen van verkeerd gedrag.	- Managers.
Managers	- Risicoperceptie en beveiligingsattitude van managers verbeteren. - Verwachtingen communiceren, belonen van goed gedrag en niet belonen van verkeerd gedrag.	- Zie tabel 1 en 2. - Hogere managers en externen (bv. klanten en toezichthouders).

Tabel 3: Verbeteracties ten aanzien van beloning in het kader van beveiliging.

Het meten van verbeteringen

Als een organisatie, al dan niet gestimuleerd door externe betrokkenen, werkt aan het verbeteren van het interne beveiligingsbewustzijn, dan is het nuttig om gerealiseerde verbeteringen zichtbaar te kunnen maken. De twee meest voor de hand liggende indicatoren hiervoor zijn:

- De mate van terugdringen van onacceptabele risico's.
- De afname van het aantal opgetreden beveiligingsincidenten.

De eerste indicator is voor veel organisaties moeilijk te bepalen. Het signaleren en terugdringen van de onacceptabele risico's vergt effectief risicomanagement. Risicomanagement is een complex proces dat lastig te beoordelen is. Een verbetering van dit proces zal in eerste instantie in documentatie zichtbaar worden. Maar 'papier' is geduldig en betere documentatie betekent niet per se dat de onacceptabele risico's ook daadwerkelijk teruggedrongen worden. Het beste kan de organisatie haar risicomanagement zowel voor als na de verbeteringsacties laten beoordelen door een onafhankelijke auditor om zo te bepalen of het risicomanagement verbeterd is en in welke mate dit tot terugdringing van onacceptabele risico's heeft geleid.

De afname van het aantal opgetreden beveiligingsincidenten is in principe goed te bepalen. Om metingen te kunnen doen, heeft de organisatie een goede registratie van (bijna-)incidenten nodig. Deze registratie heeft de organisatie ook nodig voor het verbeteren van het beveiligingsbewustzijn. Een vervelende bijkomstigheid is dat na het op-

zetten van een incidentenregistratie het aantal geconstateerde incidenten eerst toeneemt. Dit komt niet doordat het aantal opgetreden incidenten toeneemt, maar doordat meer incidenten zichtbaar worden. Na een aanvankelijke stijging zou verdere verbetering van het beveiligingsbewustzijn wel tot een daling moeten leiden.

Conclusie

Om tot goede (informatie)beveiliging te komen, is voldoende beveiligingsbewustzijn bij iedereen in de organisatie noodzakelijk. Hoewel het beveiligingsbewustzijn bij veel mensen in orde is, komt het juist bij de voor de beveiliging zo belangrijke managers en beveiligingsgeoriënteerde medewerkers te vaak voor dat het beveiligingsbewustzijn tekort schiet. Niet voor niets gebeuren er regelmatig kleine, maar ook grote, beveiligingsincidenten en lijkt het erop dat de meeste organisaties weinig leren van eerdere incidenten. Hoewel dit deels te verklaren is door de complexiteit van beveiliging en bewustzijn, spelen ook andere zaken een rol, zoals de focus op de waan van de dag en het nastreven van persoonlijke doelen. Bovendien pakken externe betrokkenen, zoals besturen, toezichthouders, auditors en accountants hun verantwoordelijkheid om de risicoperceptie en de beveiligingsattitude van de managers bij te sturen nog te weinig op.

Literatuur

[BERN05] D.A. Bernstein, L.A. Penner, A. Clarke-Stewart en E.J. Roy, *Psychology*. Houghton Mifflin Company, Boston, 2005.
[OVER05] P. Overbeek, E. Roos Lindgreen en M. Spruit, *Informatiebeveiliging onder controle*. Pearson Education, Amsterdam, 2005.
[ROBB05] S.P. Robbins, *Gedrag in organisaties*. Pearson Education, Amsterdam, 2005.
[SPRU10] M. Spruit, *Informatiebeveiliging en bewustzijn*. De EDP-Auditor, nr.1, 2010, pag. 24-27.