

INFORMATIEBEVEILIGING – PEOPLEWARE (1)



Hans Labruyere is directeur en mede-eigenaar van LBVD informatiebeveiligers.
Hij is te bereiken via hans.labruyere@lbvd.nl

In een serie van drie artikelen over informatiebeveiliging en het bewustzijn en onbewustheid van de mens in deze, zet de schrijver een keten methoden uiteen die elkaar in de praktijk kunnen versterken. De keten bestaat globaal gezien uit analyseren, informeren, kanaliseren en toetsen. In dit eerste deel wordt ingegaan op de analyse van de (on)bewustheid.

Informatiebeveiliging. Een breed en lastig onderwerp. Veel organisaties 'hebben al wat', er is technisch een boel gedaan en er zijn allerhande protocollen, regels en convenanten. Toch lukt het maar niet de medewerkers het gewenste gedrag te laten vertonen.

Eenzijds heeft dat met cultuur te maken, of dat nu bedrijfscultuur of cultuur op regionaal of nationaal niveau is. Anderzijds is voornoemde onmacht veelal voornamelijk het gevolg van het feit dat mensen zich gewoon niet bewust zijn. Voorbeeld? Op welke verdieping bevindt u zich nu? Hoeveel verdiepingen zijn er nog boven u? Wel

eens nagedacht over de kans dat het plafond waaronder u nu zit straks gelijk zou kunnen zijn aan de vloer waarop u staat? En wat dat voor uw welzijn betekent? Nee?

Dat dacht ik al. Toch is het niet ondenkbaar. In

Keulen gebeurde vorig jaar maart iets dergelijks. "Maar daar waren ze een tunnel aan het boren", hoor ik u denken. Tjah. Maar dat wisten ze daar ook niet... Het risico werd niet kleiner (of groter) doordat men het risico niet zag.

Een medewerker die onbewust onbekwaam is, is derhalve een lastige

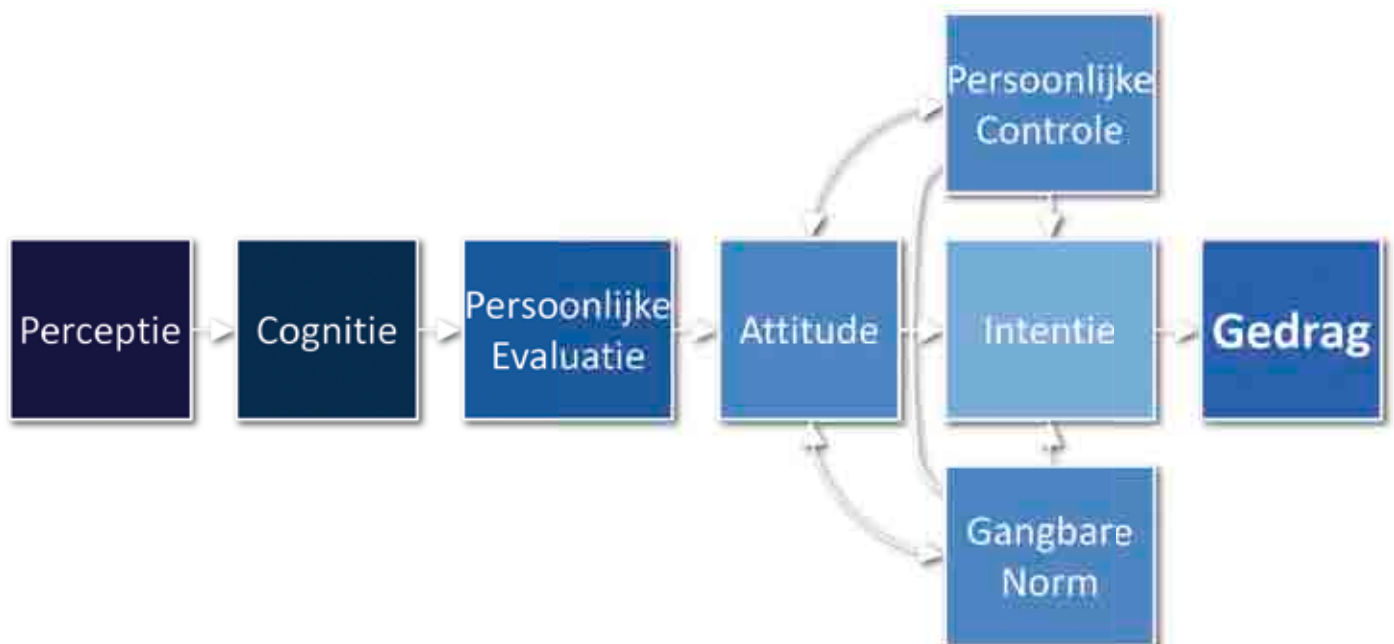
gesprekspartner. Hij hoort je wel, maar luistert niet. Omdat hij denkt al de juiste kant op te gaan. Een deel van de oplossing om te komen tot een meer

volwassen organisatie inzake informatiebeveiliging is het migreren van (de

medewerkers van) die organisatie van onbewust onbekwaam naar bewust onbekwaam.

Onderstaand model is afkomstig uit de sociaal psychologie. Je 'leest' het van rechts naar links:

Het lukt maar niet de medewerkers het gewenste gedrag te laten vertonen



Model: beïnvloeding van gedrag volgens de sociaal psychologie.

1. Gedrag

Wat je wilt is uitvoering van het juiste gedrag. Als je op een sportveld staat en het begint te bliksemen, dan blijf je daar niet staan. Ongeacht het feit dat je 's morgens opstond en niet direct dacht: "Goh, als het vanmiddag gaat bliksemen ga ik niet op een sportveld staan".

Hoe werkt dat nou eigenlijk? Als het gaat bliksemen trek je in je onderbewustzijn een 'laatje open'. In dat laatje zitten allerhande zaken die je in je leven hebt verzameld. Goede raad van je oma, artikelen uit de krant, ervaringen etc. In een split second neem je je beslissing bijna zonder het te weten, en je gaat van het veld af. En by the way, je gaat ook niet onder een boom staan. In dit voorbeeld is uitgegaan van het feit dat er inhoud in dat laatje zit. Informatiebeveiligings-incidenten gebeuren wel, maar wie kan ze herkennen? Wie heeft dit soort info in haar of zijn laatje? Hoe kunnen we als professionals dan het juiste gedrag verwachten bij de medewerkers...? Het gedrag wordt echter sterk beïnvloed door:

2. Intentie

Ofwel, wil ik, of wil ik niet. Vijftig procent van het antwoord is 'ik wil niet'. Maar tegen die tijd is het dan ook een bewust genomen beslissing, al kan niet iedereen alle implicaties altijd overzien. Dit onderdeel wordt beïnvloed door:

3. Attitude

Die mede wordt bepaald door externe factoren als persoonlijke controle en de gangbare norm. Persoonlijke controle is te omschrijven als 'waar heeft je wieg gestaan?' Welke ervaringen heb je van thuis meegekregen? De gangbare norm kan per afdeling, per regio, per bedrijfsproces heel anders zijn. Voor iemand van de receptiebalie heeft een

willekeurige bezoeker een heel ander veiligheidsprofiel dan voor iemand van de tweede verdieping. Voor die medewerker is dit 'gewoon een bezoeker'. Hij is immers voorbij de receptie? Dan zal hij hier wel horen...

Voor iemand van de afdeling ICT is de procedure rondom wachtwoorden logisch en vanzelfsprekend. Personeelsdossiers kun je bij deze afdeling echter nog wel eens op het bureel van de IT-manager vinden. Die periodieke beoordeling moet per slot toch gedaan worden? Voor medewerkers

van HR zijn personeelsdossiers op een bureau (waar je niet direct mee bezig bent) ondenkbaar. Wachtwoordprocedures echter zijn in de praktijk soms zo onwerkbaar, dat de afdelingssecretaresse in de vakantieperiode de usernames van de collegae verzameld. 'Het is zo lastig als er iemand niet is...' Een verschillende kijk dus, op veiligheid, dreiging, realiteit. Niet per se onjuist, maar niet compleet. En die attitude wordt op haar beurt beïnvloed door:

4. Persoonlijke ervaring

Heb je in het verleden iets geleerd? Iets meegemaakt, in de krant gelezen, gehoord of bediscussieerd misschien? Kortom, een eigen interpretatie maakt van het dreigingprofiel voor jou persoonlijk? Want dat is mede een oplossing voor het sturen van (groepen) mensen. Elk individu laten inzien wat hij er zelf beter van wordt. Of minder slecht van wordt. What's in it for me? Maar die ervaring moet je dan ook wel hebben gehad, en ze wordt onder andere opgedaan door:

5. Cognitie

Je leert iets. Door een ervaring, een situatie, een opleiding, breder inzicht.

Die cognitie echter wordt beïnvloed door:

6. Perceptie

Zie je het überhaupt? Een moeder-nijlpaard gaat door voor het meest dodelijke dier op aarde (ze heeft geen natuurlijke vijanden, weegt een paar ton en kan heel hard lopen). Toch heeft zo'n dier een hoge knuffelfactor, en niet iedereen die niet in Afrika is geweest kent deze dreiging. Maar hij is er wel. Een rotje is potentieel gevaarlijk. Toch onderkent niet iedere jongere rond oud en nieuw die dreiging. Maar hij is er wel.

Uit het model kan onder andere worden opgemaakt dat een individu (of een afdeling, of een proces) niet van het blok Perceptie direct naar het blok Gedrag kan worden gebracht. Men moet als individuele medewerker eerst weten (en beseffen) wat de dreiging omvat, waarom dat voor de individu persoonlijk een dreiging kan zijn, hoe te reageren en welke middelen daarvoor nodig zijn. Pas dan wordt besloten óf de gewenste actie (zoals die in de regels staat) wordt aangegaan. En het antwoord kan ook zijn: "Nou neen, nu even niet".

Dat geldt voor de werkvloer, maar natuurlijk ook en onverminderd voor de directiekamer. Ook daar kan men Onbewust Onbekwaam zijn - met verstrekkende gevolgen... Het feit dat men risico's op dat niveau niet 'ziet' kan tot gevolg hebben dat maatregelen niet worden genomen, prioriteiten niet juist (lees: reëel) worden gesteld, en er derhalve risico's worden gelopen. In plaats van genomen. Met onlangs in Keulen catastrofale gevolgen.

Als je op een sportveld staat en het begint te bliksemen, dan blijf je daar niet staan