

**Risicomanagement krijgt
vaste plaats in ITIL**

**Introductie: discussiemodel
voor integrale beveiliging**

Virtualisatie, de ins en outs

Sociale netwerksites onschuldig?

**De menselijke kant van
informatiebeveiliging**

INFORMATIEBEVEILIGING

Het tunen van de menselijke firewall

Drs. Sanne Schaler > Sanne Schaler is werkzaam als sociaal psychologe bij LBVD Consultancy en bereikbaar via sanne.schaler@lbvd.nl. Schaler is fulltime verbonden aan LBVD Informatiebeveiligers als Adviseur Informatiebeveiliging. In 2003 rondde Sanne aan de Universiteit van Amsterdam de studie psychologie af, met als specialisatie sociale psychologie. Na haar studie deed zij verschillende projectmatige en organisatorisch ondersteunende werkervaringen op bij verscheidene organisaties. In 2007 kwam zij terecht bij LBVD Consultancy, waar haar speerpunten de organisatorische en mens-kant van informatiebeveiliging zijn.

In dit artikel worden in vogelvlucht enkele speerpunten uit de cognitieve en sociale psychologie toegelicht die van toepassing zijn op de mens als middel om doelstellingen te bereiken op het gebied van informatiebeveiliging. Welke principes liggen aan inadequaat gedrag ten grondslag en hoe krijg je medewerkers scherper en alerter?

1. De mens als zwakste schakel

Medewerkers maken een organisatie en de onderdelen waaruit een organisatie bestaat. Medewerkers zijn de organisatie. Organisatieonderdelen, zoals ICT en informatiebeveiliging, worden door mensenhanden ontwikkeld, toegepast en gebruikt. Met techniek en beleid kunnen bedreigingen worden bedwongen, echter niet alle. Hoe medewerkers gebruikmaken van techniek en hoe zij invulling geven aan regels en procedures, is mede bepalend voor de veiligheid van een organisatie en de betrouwbaarheid van informatie. De sociale psychologie vindt hier zijn toepassing, aangezien men te maken heeft met menselijk gedrag en de invloed van anderen. Menselijk gedrag wordt beïnvloed door een aantal factoren. Als een organisatie wil dat medewerkers hun gedrag veranderen, is het zaak te weten welke factoren dit zijn en hoe deze factoren hun uitwerking hebben. Met behulp van deze specifieke kennis kunnen gerichte acties ondernomen worden die een effectief, langdurig en duurzaam effect hebben als het gaat om het verkrijgen van adequaat gedrag op het gebied van informatiebeveiliging. Gedragsvorming begint bij het waarnemen van een stukje informatie, ook wel perceptie genoemd. Deze informatie wordt verwerkt en al dan niet opgeslagen in het geheugen. Vervolgens wordt er een mening (attitude) gevormd. Uit deze attitude kan een neiging volgen om iets te gaan doen (gedragsintentie), wat uiteindelijk wel of niet resulteert in gedrag. Deze gedragsfactoren zullen uitgebreid worden

besproken en hun toepassing op het vlak van informatiebeveiliging zal worden toegelicht.

2. Perceptie

Het menselijk redeneren is gebaseerd op wat en hoe we waarnemen, ook wel perceptie genoemd. Perceptie kan gedefinieerd worden als mentale processen waarbij sensorische informatie wordt geselecteerd, georganiseerd en op andere manieren wordt gemanipuleerd door het zenuwstelsel om betekenis te geven aan objecten of gebeurtenissen in de buitenwereld. De mentale processen die bij perceptie komen kijken, zijn onder te verdelen in twee processen: bottom-up en top-down processen. De bottom-up processen, ook wel data-gedreven processen genoemd, registreren en integreren informatie die we met onze zintuigen opdoen. De top-down processen, ook wel concept-gedreven informatie genoemd, maken gebruik van al bestaande kennis om informatie te interpreteren. Wanneer we bijvoorbeeld deze tekst lezen, registreren de bottom-up processen de elementaire kenmerken van de stimuli, namelijk een verzameling van lijnen, kleur, vorm, richting, hoeken, et cetera. We zien dus een hoop zwarte lijntjes die allerlei kanten opstaan met witte vlekken er omheen. De top-down processen zorgen er echter voor, door kennis van objecten en verwachtingen welke objecten waarschijnlijk aanwezig zijn, dat we de zwarte lijntjes niet samen zien met de witte vlekken er omheen, maar als letters gedrukt op een witte achtergrond als zijnde

een pagina uit een tijdschrift. Top-down processen gaan minder automatisch en kosten meer tijd (Treisman & Gormican, 1988).

De Gestalt psychologen pleitten eerder in het begin van de twintigste eeuw voor het automatisch waarnemen van een geïntegreerd geheel in tegenstelling tot het registreren van individuele componenten. Perceptie bestaat volgens de Gestalt-aanhangers niet uit het combineren van aparte elementen, maar is een kwestie van het meteen waarnemen van grote, algehele patronen (Wertheimer, 1923). Daar waar informatie mist, vullen we ontbrekende informatie in zodat een doorlopend patroon en een smnhngnd ghl wrdt gvrmd. Patronen en objecten herkennen we door af te gaan op wat uit ervaring in ons geheugen is opgeslagen. Een onbevoegd persoon in het pand, die qua uiterlijk en gedrag lijkt op andere aanwezigen, past in het gehele plaatje, valt niet op en zal niet snel worden aangesproken omdat wij denken dat diegene er hoort. Wanneer echter tijd wordt genomen om details van deze persoon te bestuderen, zal blijken dat deze persoon niet op zijn plek is.

3. Het geheugen

Informatie die we met onze zintuigen vergaren, verwerken we met onze hersenen in het kortetermijngeheugen en slaan we vervolgens al dan niet op in het langetermijngeheugen. Het hangt af van de cognitieve capaciteit die we toekennen aan het verwerken van informatie of informatie daadwerkelijk terecht komt in het langetermijngeheugen.

“Daar waar informatie mist, vullen we ontbrekende informatie in zodat een doorlopend patroon en een smnhngnd ghl wrdt gvrmd.”

Zo vergroot het herhalen en oefenen van informatie de kans dat informatie wordt opgeslagen in het langetermijngeheugen. Ook het diep over iets nadenken en het (proberen te) begrijpen, het groeperen van informatie tot begrijpelijke brokken, er betekenis aan geven of het visualiseren vergroten de kans dat informatie naar het langetermijngeheugen wordt getransporteerd. Informatie moet genoeg opvallen om überhaupt opgemerkt te worden en bewust te worden verwerkt (Johnston & Dark, 1986; LaBerge, 1995). Interessante, opvallende en leuke informatie zal eerder worden opgemerkt en met meer aandacht worden verwerkt dan neutrale informatie. Ook hangt het af van de interesse en het begrip van een persoon hoeveel aandacht aan een onderwerp wordt besteed. Zolang informatiebeveiliging niet aan de orde wordt gebracht, zullen medewerkers hier geen kennis over vormen en hierover niets opslaan in hun geheugen. Als zich dan bijvoorbeeld een incident voordoet weet niemand hoe te reageren.

4. De vorming van attitude en gedrag

Aandacht speelt een essentiële rol in het Elaboration likelihood model van Petty & Cacioppo (1986). Informatie kan worden verwerkt via de perifere route waarbij sprake is van lage betrokkenheid en weinig cognitieve capaciteit, of via de centrale route waarbij sprake is van hoge betrokkenheid en veel cognitieve capaciteit. Wordt informatie verwerkt via de perifere route, dan zal vertrouwd worden op zogenaamde ‘short cuts’ of heuristieken. Hierbij worden stappen in het informatieverwerkingsproces overgeslagen om snel tot een oplossing te komen. Er wordt vertrouwd op minder betrouwbare en oppervlakkige aspecten van informatie, zoals het aantal positieve of negatieve argumenten of de bron van een argument. De inhoud wordt hierbij niet of nauwelijks overwogen. Er worden vuistregels of ezelsbruggetjes gebruikt die snel, maar meestal een foutief antwoord geven. Wordt informatie echter verwerkt via de

centrale route, dan worden de kwaliteit van argumenten en de voors en tegens zorgvuldig en systematisch afgewogen. Een attitude gebaseerd op informatie verwerkt via de centrale route houdt langer stand dan attitudes gevormd via de perifere route (Eagly & Chaiken, 1993).

In het Model van Gepland Gedrag van Ajzen (1985; 1991) speelt attitude ook een belangrijke rol. In dit model wordt gesteld dat gedrag het resultaat is van de intentie die iemand heeft om bepaald gedrag te vertonen. Bij het vormen van deze intentie worden drie factoren afgewogen; de attitude, wat anderen van dat gedrag vinden (de gangbare norm) en de persoonlijke controle die iemand denkt te hebben om gedrag uit te voeren. De attitude is gebaseerd op persoonlijke overtuigingen en evaluaties van informatie. Hierbij wordt afgevraagd hoe belangrijk een onderwerp is voor de persoon.

Gedrag en attitude kunnen elkaar wederzijds beïnvloeden. Wordt bijvoorbeeld gedrag vertoond dat niet strookt met de attitude, kan de attitude worden aangepast. De mens wil namelijk graag consistent zijn in zijn overtuigingen, woorden en daden. Niet alleen voor zichzelf, maar ook voor anderen. Festinger (1957) liet dit zien in zijn Cognitieve Dissonantie Theorie. In deze theorie wordt gesteld dat wanneer cognitieve elementen niet met elkaar overeenkomen, een conflict wordt ervaren. Dit conflict zorgt voor een negatieve gemoedstoestand die men liever niet wil ervaren. Om dit negatieve gevoel te verminderen, zal een van de cognitieve elementen worden aangepast. Heeft iemand bijvoorbeeld net een dure auto gekocht, zal diegene een (nog sterkere) positieve attitude ontwikkelen tegenover deze auto en de aanschaf ervan. De actie wordt door de persoon als het ware goed gepraat. Eerst wordt gedrag vertoond, dan wordt de attitude gevormd. Bij medewerkers kan adequaat gedrag op het gebied van informatiebeveiliging afgedwongen worden door middel van beloningen en straffen. Medewerkers zullen misschien hun gedrag

aanpassen en daarna hun attitude, echter niet omdat ze het zelf begrijpen en willen, maar omdat het moet. De attitude wordt niet op een constructieve wijze gevormd. Het is echter wenselijk om gemotiveerde medewerkers te hebben die uit zichzelf op basis van hun overtuiging adequaat gedrag vertonen en waar niet continu op gecontroleerd hoeft te worden.

Gedrag wordt dus niet altijd vertoond zoals gepland. Cognitieve processen kunnen zelfs leiden tot ineffectief gedrag, zoals het toch kopen van die veel te dure schoenen of het toch eten van een patatje mét. Ook op het gebied van informatiebeveiliging kunnen medewerkers zich ineffectief gedragen. Het even niet op slot doen van een kast of het niet dragen van een pas zijn hiervan enkele voorbeelden. Mensen zoeken vaak de makkelijkste en snelste manier van werken. Zo ook op mentaal vlak. Als het even kan, wordt niet te diep nagedacht, maar wordt vertrouwd op heuristieken. De mens is van aard een lui wezen. En daar kan misbruik van worden gemaakt.

5. Misbruik van cognitieve processen

Zoals in bovenstaande theorieën is uitgelegd, kost het tijd en moeite om stimuli te onderscheiden, te verwerken en er betekenis aan te geven. Het is makkelijk voor zenders van informatie hierop in te spelen en informatie op een misleidende manier te presenteren. Ook in de informatiebeveiliging worden genoemde psychologische principes ge- en misbruikt. Om toegang te krijgen tot informatie kunnen kwaadwillenden gebruikmaken van social engineering. Hierbij doet men zich voor als een bepaalde persoon die ‘legitieme’ toegang wil hebben tot vertrouwelijke informatie. Er kan bij social engineering gebruik worden gemaakt van stereotypen. Stereotypen zijn beelden die mensen hebben van groepen mensen. Stereotypen kunnen gebaseerd zijn op iemands ras, etniciteit, seksuele geaardheid, nationaliteit, geloof, beroep, uiterlijk of sociale klasse. Mensen worden op basis van een van

“Het herhalen en oefenen van informatie vergroot de kans dat informatie wordt opgeslagen in het langetermijngeheugen.”

deze kenmerken tot een groep ingedeeld en aan iedereen in die groep worden dezelfde, overdreven eigenschappen toegeschreven. Uit stereotypen kunnen bepaalde verwachtingen ten aanzien van gedrag voortvloeien. Deze verwachtingen kunnen zo bekend en universeel worden, dat ze de vorm van ‘sociale regels’ krijgen (Ekman & Friesen, 1969). Zo kennen mensen een bepaalde rol toe aan iemand in een bepaalde situatie. Thuis heeft men bijvoorbeeld een andere rol dan op het werk of op de tennisclub. In verschillende situaties worden verschillende gedragingen verwacht. Stereotypen kunnen bepalen hoe je gedrag interpreteert. Afwijkend gedrag van een man met een oosters uiterlijk en een lange baard op een vliegveld zal eerder als verdacht worden gezien dan hetzelfde gedrag van een westerse vrouw. Van zulke aannames kan misbruik worden gemaakt, zoals bij social engineering wordt gedaan. Iemand doet zich in een bepaalde situatie voor als iemand van een bepaalde groep waardoor bepaalde gedragingen in deze context als ‘normaal’ worden gezien. Er wordt weer vertrouwd op het gehele plaatje dat lijkt te kloppen. Als iemand zich voordoet als politieagent zal minder raar worden opgekeken als naar legitimatie wordt gevraagd dan wanneer een bouwvakker dat doet. En zo zal minder raar worden opgekeken als een bouwvakker uit een rioolput kruipt dan wanneer een secretaresse dat doet. Als mensen vertrouwen op stereotypen, maken ze gebruik van de al eerder genoemde ‘shortcuts’. Men denkt niet diep genoeg na om de werkelijke identiteit van de social engineer te achterhalen, maar men vertrouwt op oppervlakkige informatie zoals uiterlijke kenmerken. Dit gaat immers sneller en makkelijker. Het hele plaatje wordt gezien zonder te letten op specifieke kenmerken waaraan opgemerkt kan worden dat iets toch niet in de haak is.

Niet alleen hoe gedrag wordt geïnterpreteerd, maar ook hoe mensen zich gedragen, kan beïnvloed worden door sociale verwachtingen. Zoals al genoemd,

is wat anderen van jou in een bepaalde situatie verwachten een van de factoren die wordt overwogen in het vormen en uiten van gedrag. Er is dus niet alleen een aantal interne cognitieve factoren binnen de mens die invloed hebben op gedrag, er zijn ook externe factoren; invloeden van buitenaf. De mens is een sociaal wezen en zoekt gezelschap op. We willen graag geaccepteerd worden en ergens ‘bij horen’. We kijken naar het gedrag van anderen en passen ons gedrag wel of niet aan. Zo roept de social engineer een automatische gepaste reactie op bij medewerkers. De druk om te conformeren kan erg hoog zijn, vooral in groepen. Groepsgedrag kan extreme vormen aannemen, zoals vandalistisch gedrag van voetbalsupporters of passieve toeschouwers van een ongeluk. Hoe meer groepsleden hetzelfde gedrag vertonen, hoe groter de druk is om te conformeren (Asch, 1952, 1955). Op het werk vorm je met je collega’s een groep. Hoe meer collega’s bijvoorbeeld geen actie ondernemen als een vreemde door het gebouw loopt, hoe groter de neiging zal zijn dat jij ook niet ingrijpt. Bij deze passiviteit spelen onzekerheid en anonimiteit een rol (Latané & Darley, 1968b). Als men niet helemaal zeker is van wat er van iemand verwacht wordt, zal eerder worden gekeken naar wat anderen doen dan wanneer omstandigheden eenduidig zijn. Zolang een social engineer niet rondloopt in een gestreep pak en een bivakmuts, is het niet geheel duidelijk dat deze persoon kwaad in de zin heeft. Daarnaast vinden mensen het niet prettig de aandacht op zichzelf te richten door als enige naar voren te stappen en verantwoordelijkheid te nemen door in te grijpen.

6. Van theorie naar praktijk

De mens is een rationeel wezen en verzint voor problemen een oplossing. Bepaalde oplossingen zijn echter niet effectief. Mensen willen dingen vaak snel en met zo min mogelijk moeite doen. De automatische piloot waarop men in

sommige gevallen vertrouwt, zorgt niet altijd voor een betrouwbare oplossing. Het hele plaatje dat wordt gezien, klopt niet altijd. Er wordt te weinig aandacht gegeven aan afzonderlijke delen van een object. Informatie wordt niet zorgvuldig afgewogen. Deze processen kosten immers tijd en moeite. Op grond van deze psychologische principes kan een aantal handreikingen worden gegeven om inadequate gedragingen te verbeteren. Net zoals er automatisch adequaat wordt gereageerd, zou er automatisch adequaat moeten worden gereageerd. Om zulke gedragingen aan te leren, is tijd, oefening en aandacht nodig. De eerste stap is medewerkers bewust te laten worden van informatiebeveiliging. Er moet kennis worden verkregen waarmee een positieve attitude kan worden onderbouwd. Medewerkers moeten inzicht krijgen in hun eigen inadequate gedragingen voordat ze hun gedrag willen en zullen veranderen. Om over te gaan tot adequaat gedrag, moeten veel onduidelijkheden worden weggenomen. Er moet bijvoorbeeld duidelijk worden gemaakt wat de individuele verantwoordelijkheid is van de medewerker. Oorzaken van (mogelijke) incidenten moeten worden gezien en er moet duidelijk worden gemaakt hoe bij incidenten gehandeld moet worden. Doordat iedere medewerker weet wat van hem/haar wordt verwacht, zal minder snel gekeken worden naar wat anderen doen en zal zelfstandig adequaat worden gehandeld. De eigen-effectiviteit van de medewerker moet duidelijk worden gemaakt; iedere medewerker kan bijdragen aan het voorkomen van een incident. Hierbij moet worden aangetoond dat informatiebeveiliging de moeite waard is. De afwegingen die medewerkers maken, moeten ertoe leiden dat de baten van informatiebeveiliging groter zijn dan de kosten. Noem persoonlijke consequenties voor de medewerker. Zo kan het gevolg van het niet op slot doen van een deur tot diefstal leiden van een portemonnee of tot een negatieve

**“De mens is van aard een lui wezen.
En daar kan misbruik van
worden gemaakt.”**

evaluatie in een beoordelingsgesprek. Zo wordt informatiebeveiliging een persoonlijke aangelegenheid. Hierdoor zal meer aandacht aan informatiebeveiliging worden gegeven en zal een onderbouwde attitude worden gevormd. Dat is wat de meeste werkgevers willen; gemotiveerde medewerkers die uit zichzelf adequaat gedrag vertonen op het gebied van informatiebeveiliging.

7. Dienstonwikkeling

Nieuwe initiatieven voor bewustwording-programma's zullen moeten uitgaan van deze wens. Zo bestaat een programma van LBVD uit een aantal modules die inhaken op eerder genoemde psychologische principes. Medewerkers leren zelf risicovolle situaties te zien, te begrijpen en adequaat te handelen. Er wordt korte metten gemaakt met onwetendheid en onzekerheid waardoor automatische inadequate handelingen en passiviteit geen rol meer spelen. Er worden verschillende oefeningen aan medewerkers én management voorgelegd waarmee informatiebeveiliging op een constructieve en leuke manier wordt benaderd. De medewerker heeft veel inbreng en dat is ook logisch; want wie staat er het dichtst bij de praktijk en weet wat realistisch en

Ihaalbaar is? Medewerkers en management worden uitgedaagd om over deze en nog meer vragen na te denken en zelf met een antwoord te komen. Met deze persoonlijke benadering raakt iedereen in de organisatie, van boven tot onder, hoog betrokken bij informatiebeveiliging en zal iedereen weten wat te doen en waarom.

Referenties

- Ajzen, I.** (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control: From cognition to behavior* (pp. 11-39). New York: Springer-Verlag.
- Ajzen, I.** (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, 179-211.
- Asch, S. E.** (1952). *Social Psychology*. Englewood Cliffs, NJ: Prentice Hall.
- Asch, S. E.** (1955). Opinions and social pressures. *Scientific American*, 193(5), 31-35.
- Eagly, A. H., & Chaiken, S.** (1993). *The psychology of attitudes*. Orlando, FL: Harcourt Brace Jovanovich.
- Ekman, P., & Friesen, W. V.** (1969). The repertoire of nonverbal behavior: Categories, origins, usage and coding. *Semiotica*, 1, 49-98.
- Festinger, L.** (1957). *A theory of cognitive dissonance*. Stanford, CA: Stanford University Press.
- Frijda, N. H.** (1986). *The emotions*. New York: Cambridge University Press.
- Johnston, W. A., & Dark, V.J.** (1986). Selective attention. *Annual Review of Psychology*, 37, 43-75.
- LaBerge, D.** (1995). *Attentional processing: The brain's art of mindfulness*. Cambridge, MA: Harvard University Press.
- Latané, B., & Darley, J. M.** (1968b). The unresponsive bystander: Why doesn't he help? New York: Appleton-Century Crofts.
- Petty, R. E., & Cacioppo, J. T.** (1986). The elaboration likelihood model of persuasion. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (Vol. 19). New York: Academic Press.
- Treisman, A., & Gormican, S.** (1988). Feature analysis in early vision: Evidence from search asymmetries. *Psychological Review*, 95, 15-48.
- Wertheimer, M.** (1923). *Principles of perceptual organization*. In W. D. Ellis (Ed. & Trans.), *A source-book of Gestalt psychology*. New York: Harcourt Brace.

