Informatiebeveiliging en bewustzijn

Organisatiefouten vaak oorzaak van menselijk falen

Het optreden van beveiligingsincidenten is vaak aanleiding voor het starten van een beveiligingsbewustwordingsprogramma, zonder dat men goed weet hoe zo'n programma opgezet moet worden en of het überhaupt wel zo effectief is. Bovendien worden alle werknemers van een organisatie over één kam geschoren en krijgen één en hetzelfde programma voorgeschoteld. Goed beschouwd is het dan niet zo vreemd dat met dergelijke programma's zo weinig positieve resultaten geboekt worden. Maar kan het beter?

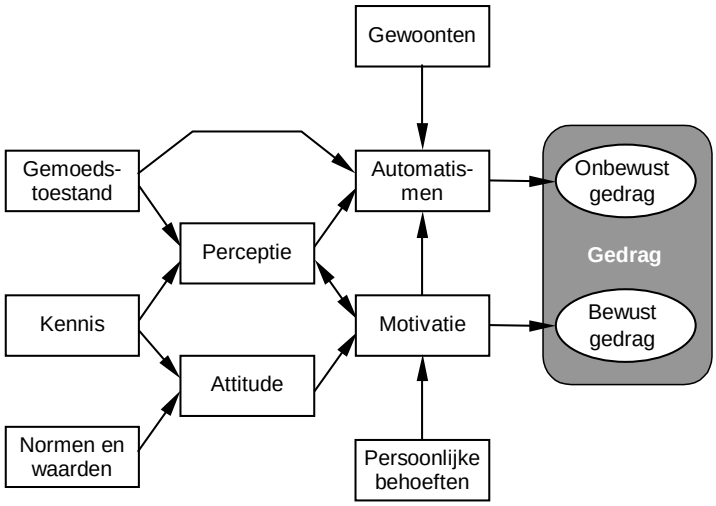
Auteur: **Dr. Marcel E.M. Spruit** is Lector Informatiebeveiliging aan de Haagse Hogeschool en senior-consultant aan Het Expertise Centrum.

Inleiding

Traditioneel leunt informatiebeveiliging sterk op checklisten, risicoanalyses en de daaruit voortvloeiende fysieke en logische beveiligingsmaatregelen. Men gaat er veelal vanuit dat de menselijke factor voldoende wordt afgedekt door het toewijzen van taken en verantwoordelijkheden aan medewerkers. Toch treden er aan de lopende band beveiligingsincidenten op, waarvan het leeuwendeel terug te voeren is op menselijk falen. Als een incident geconstateerd wordt, dan wordt de oplossing in het algemeen gezocht in het nog verder verzwaren van de beveiligingsmaatregelen en het verbeteren van het beveiligingsbewustzijn van de medewerkers. Buiten het feit dat men vaak geen flauw idee heeft hoe het beveiligingsbewustzijn verbeterd zou kunnen worden, is het ook de vraag of een gebrekkig beveiligingsbewustzijn van de medewerkers wel de oorzaak is van al die incidenten. In het algemeen worden andere menselijke en organisatorische aspecten ernstig onderschat. Het is dus hoog tijd om eens wat dieper in te gaan op menselijk gedrag in relatie tot informatiebeveiliging.

Menselijk gedrag en falen

In essentie is het *gedrag* van een persoon alles wat die persoon zegt of doet [Bernstein e.a., 2005; Robbins, 2005]. Figuur 1 laat zien dat gedrag bestaat uit een tweetal componenten, namelijk *onbewust* en *bewust* gedrag [Overbeek e.a., 2005].



Figuur 1: Onbewust en bewust gedrag en de factoren die daarbij een rol spelen.

Onbewust gedrag is gebaseerd op automatismen. Automatismen zijn geactiveerde gewoonten. Het al dan niet activeren van gewoonten wordt beïnvloed door de gemoedstoestand. Daarnaast speelt de perceptie die de persoon van de omgeving heeft een rol: op basis van de waargenomen omgeving zal de 'automatische piloot' bepaalde gewoonten activeren.

Bewust gedrag bestaat uit handelingen die willens en wetens uitgevoerd worden. Hierbij speelt de motivatie, oftewel de wil om iets te doen, een bepalende rol. Op basis van de perceptie van de omgeving en de attitude ten opzichte van de daarin mogelijke handelingen, kan de persoon ervoor kiezen om de desbetreffende handelingen uit te voeren. In dat geval is er sprake van intrinsieke motivatie: de motivatie komt vanuit de persoon zelf, zonder dat er sprake is van beloning. Het kan ook zijn dat de persoon in kwestie de handelingen pas uitvoert als hij ervan overtuigd is dat daar mogelijk profijt uit volgt. In dat geval is er sprake van extrinsieke motivatie: de motivatie ontstaat pas als er sprake is van enigerlei beloning.

Niet alle gedrag is even wenselijk; mensen maken fouten [Reason, 1990; CSI/FBI, 2006]. Zo veel, dat menselijke fouten beschouwd kunnen worden als de belangrijkste bedreiging voor bedrijfsprocessen. De meeste fouten worden onopzettelijk – dus ondanks alle goede wil – gemaakt, door zaken als onoplettendheid, onvoorzichtigheid en onwetendheid [Spruit en Looijen, 1996]. Bovendien is het mogelijk dat men te goeder trouw de geldende regels of voorschriften overtreedt, omdat men – al dan niet terecht – vindt dat deze regels of voorschriften in de betreffende situatie niet van toepassing zijn. Naast alle mensen die te goeder trouw fouten maken, zijn er ook nog mensen die het minder nauw nemen met de algemeen geaccepteerde normen en waarden. De daaruit voortvloeiende misstappen zijn bijvoorbeeld diefstal, fraude, hacking, sabotage, etc.

Om het gedrag van mensen in een organisatie ten aanzien van informatie en de beveiliging daarvan in goede banen te leiden, moet dit gedrag zo nodig bijgestuurd worden. In tegenstelling tot wat veelal gedacht wordt, is de intrinsieke motivatie voor informatiebeveiliging – het beveiligingsbewustzijn – bij de meeste medewerkers in orde, mits de medewerkers ervan overtuigd zijn dat alle te treffen maatregelen redelijk zijn en de onvoorwaardelijke steun van het management hebben [Overbeek e.a., 2005; Robbins, 2005]. Eventuele sturing dient dan ook met name gericht te zijn op de extrinsieke motivatie, oftewel de motivatie die op beloning gebaseerd is.

Verbeterprogramma's die zich richten op het verbeteren van individueel gedrag van medewerkers ten aanzien van informatiebeveiliging, dienen rekening te houden met bovenstaande karakteristieken van menselijk gedrag en falen. Maar men moet ook in het achterhoofd houden dat zulke verbeterprogramma's weinig invloed kunnen uitoefenen op de fouten die ontstaan door gebreken in de organisatie. Toch zijn juist organisatiefouten de oorzaak van een aanzienlijk deel van alle menselijke fouten.

Organisatiefouten

Elke organisatie kent haar onvolkomenheden. Een veel voorkomende fout in organisaties is dat de processen en procedures, alsmede de bijbehorende taken, verantwoordelijkheden en bevoegdheden, niet goed ingevuld zijn. Procedures zijn wellicht ooit goed ingevuld, maar sindsdien vaak jarenlang niet meer geactualiseerd, zodat ze niet meer door de medewerkers gevolgd (kunnen) worden. De kans op fouten neemt daardoor toe. Bovendien zijn informatiebeveiligingstaken nogal eens toegewezen aan medewerkers die daar onvoldoende tijd of kennis voor hebben en daardoor ook sneller fouten maken. Dit soort onvolkomenheden wordt in het algemeen veroorzaakt door onwetendheid of ongemotiveerdheid van het management en beperkt zich meestal niet tot informatiebeveiliging. Als zich in een dergelijke situatie beveiligingsincidenten voordoen, dan hoeft dat geen aanleiding te zijn om het beveiligingsbewustzijn van de medewerkers op te krikken; het volstaat om de focus op het management te richten.

Een ander probleem dat op kan treden – een bijzondere vorm van de hierboven genoemde onwetendheid van het management – is dat de risicoperceptie van het verantwoordelijke management niet juist is. Als dan ook de benodigde risicoanalyses niet, onvolledig, of onjuist uitgevoerd worden, dan leidt dat al gauw tot het nemen van te weinig of wellicht zelfs verkeerde maatregelen. Het is direct duidelijk dat het treffen van te weinig maatregelen leidt tot 'gaten' in de beveiliging. Maar ook het treffen van verkeerde maatregelen vormt een probleem. Als namelijk maatregelen getroffen worden die eigenlijk overbodig of onnodig zwaar zijn, dan kosten ze niet alleen onnodig veel, maar ze tasten ook het cruciale vertrouwen in de andere maatregelen aan; andere maatregelen die wel noodzakelijk zijn. Het treffen van onnodige of te zware maatregelen kan daardoor nog ongunstiger uitpakken, dan het over het hoofd zien van wel benodigde maatregelen.

Een bekend voorbeeld van een onnodig zware maatregel is de verplichting dat gebruikers hun wachtwoord regelmatig (bijvoorbeeld maandelijks) moeten wijzigen. Het nieuwe wachtwoord moet bestaan uit weer een nieuwe onraadbare tekencombinatie, die dus ook nauwelijks te onthouden is en toch nergens opgeschreven mag worden. Zo'n maatregel is in bepaalde situaties zeer nuttig of zelfs noodzakelijk, maar mag niet klakkeloos en ongedifferentieerd voor iedereen binnen de organisatie in dezelfde vorm verplicht gesteld worden. De gebruikers hebben namelijk heel snel door, dat als de regel voor bijvoorbeeld de systeembeheerder en de financieel directeur passend is, die regel dan onnodig zwaar is voor andere medewerkers zoals bijvoorbeeld de magazijnbediende. Het gevolg daarvan is dat veel medewerkers *alle* maatregelen die betrekking hebben op wachtwoorden en aanverwante zaken met een korreltje zout nemen en zonodig overtreden. Maar ook hier geldt dat de medewerkers niet zoveel te verwijten valt. De oplossing moet dan ook gezocht worden in het verbeteren van de beveiligingsmaatregelen en *niet* in het verbeteren van het beveiligingsbewustzijn van de medewerkers.

Maatregelen

Al met al treden door alle menselijke en organisatorische fouten aan de lopende band beveiligingsincidenten op. Kort samengevat liggen de volgende problemen aan de basis van deze incidenten:

- Alle *medewerkers* maken te goeder trouw bij tijd en wijle fouten, onbewust of bewust.
- Sommige *booswichten* binnen en buiten de organisatie nemen het niet zo nauw met normen en waarden.
- Onwetende en ongemotiveerde *managers* veroorzaken organisatiefouten, zoals slechte procedures en verkeerde taaktoewijzing.

Elk van deze problemen heeft betrekking op een andere doelgroep – respectievelijk medewerkers, booswichten en managers – en vraagt om een eigen aanpak. Hieronder wordt per doelgroep kort ingegaan op enkele karakteristieke aspecten van de voor die groep benodigde aanpak. In tabel 1 is dit samengevat.

De medewerkers

De meeste medewerkers zijn normaal gesproken al ingeburgerd in de organisatie waar ze werken en in de functie die ze daar hebben. De intrinsieke motivatie voor informatiebeveiliging is bij deze medewerkers in het algemeen in orde, mits de benodigde maatregelen en procedures redelijk gevonden worden en het management het goede voorbeeld geeft. De intrinsieke motivatie kan extra ondersteuning krijgen door de medewerkers te betrekken bij het selecteren en implementeren van nieuwe maatregelen en procedures. Bovendien helpt het als medewerkers die een zekere autoriteit bezitten, worden overtuigd van de noodzaak van informatiebeveiliging in het algemeen en de specifieke maatregelen in het bijzonder, zodat ze naar hun collega's als 'ambassadeur' van informatiebeveiliging op kunnen treden.

De extrinsieke motivatie van de medewerkers verdient voldoende aandacht. Het is belangrijk om de extrinsieke motivatie op een goede wijze te ondersteunen. Dit betekent dat alleen het gewenste gedrag beloond wordt en elk ongewenst gedrag niet beloond wordt. Tegen dit laatste wordt veelvuldig gezondigd door bijvoorbeeld medewerkers die meer productie 'draaien' ten koste van het volgen van (beveiligings)procedures en richtlijnen te belonen. Dit is fnuikend voor de noodzakelijke motivatie voor informatiebeveiliging. Men moet er bovendien rekening mee te houden dat als men het gewenste gedrag wil belonen, dat men dan nagaat hoe de verhouding tussen 'kosten' en 'opbrengsten' in individuele situaties uitvalt. Slechts als die verhouding voor ieder individu positief uitvalt, dan kan men het gewenste gedrag verwachten.

Voor nieuwe medewerkers komt er een extra probleem bij. Deze medewerkers kennen de organisatie en de daarin geldende procedures en richtlijnen onvoldoende en hebben wellicht minder ervaring met het werk dat ze uit gaan voeren. Nieuwe medewerkers maken daardoor eerder fouten. Deze medewerkers hebben dan ook extra kennis en ervaring nodig. Geschikte hulpmiddelen hiervoor zijn opleiding, training, coaching, etc.

De booswichten

Bij booswichten is het gevoel voor normen en waarden onvoldoende ontwikkeld, of er spelen andere zaken zoals rancune, reorganisatie, overbelasting, of iets dergelijks. In zulke gevallen zijn genuanceerde maatregelen om de motivatie te beïnvloeden onvoldoende en moet grover geschut in stelling gebracht worden. Hierbij valt te denken aan functiescheiding en andere maatregelen om ongewenste activiteiten moeilijk of zelfs onmogelijk te maken.

Extra aandacht moet men schenken aan de functionarissen die omgaan met waardevolle zaken, waarbij misstappen tot grote schade kunnen leiden. Deze functionarissen kunnen namelijk, ondanks hun goede intrinsieke motivatie, toch in de verleiding komen om in de fout te gaan. Hierbij valt te denken aan bijvoorbeeld fraude door een financiële medewerker, afluisteren door een systeembeheerder, of diefstal door een magazijnmedewerker. In alle functies waarbij 'de kat op het spek gebonden wordt', dienen mensen tegen zichzelf beschermd te worden door extra maatregelen zoals functiescheiding, supervisie en controle.

Aan de andere kant kan bij medewerkers de indruk ontstaan zijn dat bepaalde zaken geoorloofd zijn, zoals het voor privégebruik meenemen van kleine zaken uit het magazijn. In dat geval zijn de geldende huisregels niet duidelijk genoeg naar de medewerkers gecommuniceerd. Dit moet dan eerst worden verbeterd. Tevens is een minimale controle op z'n plaats. Daarnaast is het belangrijk dat het management het goede voorbeeld geeft.

De managers

Het management speelt een cruciale rol in de informatiebeveiliging. Zo zet het management het beleid voor informatiebeveiliging uit, draagt het uit naar de medewerkers en ondersteunt en controleert de uitvoering ervan. Het management geeft daarbij zelf het goede voorbeeld. Dit vergt nogal wat van het management: zowel kennis en inzicht op het gebied van informatiebeveiliging, als de motivatie ervoor moeten helemaal in orde zijn. Het spreekt vanzelf dat dit niet gaat lukken bij elke manager in iedere organisatie. Als een manager niet in staat is om informatiebeveiliging goed in te vullen, moet vanuit het hogere management worden aangestuurd op een serieuzere aanpak van informatiebeveiliging. Hierbij kunnen managementcontracten, self-assessments en audits een rol spelen. Als echter het hoogste management van de organisatie informatiebeveiliging niet voldoende serieus neemt, dan komt informatiebeveiliging in de betreffende organisatie niet goed van de grond. Slechts de wetgever en de markt kunnen dan bijsturen, maar dat zal veelal slechts gebeuren als het de spuigaten uitloopt.

Als eventuele ongemotiveerdheid van het management steunt op een verkeerde risicoperceptie, ofwel een verkeerde perceptie van het belang van informatie en de beveiliging ervan, dan kunnen de deskundigen op het gebied van informatiebeveiliging nog een positieve invloed proberen uit te oefenen door goede informatie over risico's en opgetreden beveiligingsincidenten te communiceren naar het management. Voor dit laatste is overigens wel een adequate registratie van incidenten en bijna-incidenten nodig.

Probleem	Doelgroep	Aanpak
Medewerkers maken fouten	Medewerkers	- Redelijkheid van te treffen maatregelen waarborgen en zo nodig uitleggen. - Goede voorbeeld door managers. - Participatie van medewerkers. - Inzetten van 'ambassadeurs'. - Belonen van gewenst gedrag en niet belonen van ongewenst gedrag. - Verhouding kosten/opbrengsten moet in individuele situaties positief uitvallen. - Opleiding, training en coaching van nieuwe medewerkers.
Booswichten nemen het niet zo nauw met normen en waarden	Booswichten	- Functiescheiding en andere maatregelen om ongewenst gedrag te voorkomen. - Extra beveiligingsmaatregelen bij gevoelige functies. - Duidelijk communicatie van de huisregels naar alle medewerkers. - Goede voorbeeld door managers.
Managers veroorzaken organisatiefouten	Management	- Opleiden en trainen van managers. - Afspraken over informatiebeveiliging opnemen in managementcontracten. - Nakomen van afspraken toetsen in self-assessments en audits. - Opzetten van adequate incidenten-registratie en regelmatige rapportage. - Informatie over risico's verschaffen aan het management door deskundigen.

Tabel 1: Voornaamste problemen met betrekking tot menselijk falen en karakteristieke aspecten van de daarvoor benodigde aanpak.

Verbetering van informatiebeveiliging

In veel organisaties is de informatiebeveiliging nog niet in overeenstemming met het hierboven geschetste beeld. Met name het gedrag van managers, de aansturing van medewerkers en de beveiliging tegen booswichten is nog niet goed geregeld. Er is dan een inhaalslag nodig. Als deze inhaalslag goed gebeurt, dan komt dat neer op een meer of minder grote organisatieverandering, met alle consequenties die daaraan verbonden zijn. Daarbij moeten de individuele medewerkers niet uit het oog verloren worden. Het veranderen van de organisatie ten behoeve van een betere informatiebeveiliging valt niet binnen de reikwijdte van dit artikel en wordt hier dan ook niet verder uitgewerkt.

Conclusie

Menselijk falen is de grootste bedreiging voor de bedrijfsprocessen. Daarnaast is het beveiligen tegen menselijk falen vooral mensenwerk. Verschillende maatregelen kunnen ingezet worden om risico's die door menselijk falen veroorzaakt worden, te beperken. Organisatiebrede beveiligingsbewustwordingscampagnes gebaseerd op voorlichting, spelen daarbij geen rol van betekenis. Ze zijn eigenlijk alleen nuttig om plotselinge risico- of organisatieveranderingen onder de aandacht te brengen. Wat wel nodig is, is een verzameling van activiteiten die in dit artikel beschreven zijn; activiteiten die permanent uitgevoerd worden. Het management speelt daarin de hoofdrol, ook al is niet in elke organisatie het management daartoe in staat.

Literatuur

D.A. Bernstein, L.A. Penner, A. Clarke-Stewart en E.J. Roy, *Psychology*. Houghton Mifflin Company, Boston, 2005.

CSI/FBI, *Computer crime and security survey*. Computer Security Institute, 2006.

P. Overbeek, E. Roos Lindgreen en M. Spruit, *Informatiebeveiliging onder controle*. Pearson Education, Amsterdam, 2005.

J. Reason, *Human error*. Cambridge University Press, Cambridge, 1990.

S.P. Robbins, *Gedrag in organisaties*. Pearson Education, Amsterdam, 2005.

M.E.M. Spruit en M. Looijen, *IT security in Dutch practice*. Computers & Security, nr. 2, 1996, pag. 157-170.