6.6 Management en informatiebeveiliging in synergie

In veel organisaties ziet men dat informatiebeveiliging, fysieke beveiliging en fraudemanagement organisatorisch op verschillende afdelingen is belegd. Feit is dat fraudemanagement en management voor informatiebeveiliging een aantal gemeenschappelijke vlakken hebben qua processen, procedures, techniek en borging. Dit artikel belicht de synergie tussen incidentmanagement voor beveiliging en fraudemanagement.

Auteurs: **Ronald Eygendaal CISMP CSS** *is werkzaam als fraudemanager en heeft meer dan tien jaar ervaring in beveiliging en informatiebeveiliging in het bijzonder.*
Ing. Ronald van Erven Msc CISSP *is werkzaam als ICT security officer en heeft tien jaar ervaring in het opzetten van netwerk-, systeembeheer- en in het bijzonder informatiebeveiligingsomgevingen.*
Beide auteurs zijn werkzaam bij een telecommunicatiebedrijf en hebben dit artikel op eigen titel geschreven. Voor reacties: ronaldeygendaal@protectioncompany.com en ronald.vanerven@xs4all.nl.

Inleiding

Onder het motto 'terug naar de tekentafel' zijn de auteurs hun werkzaamheden gaan inventariseren. Waarom terug naar de tekentafel? Beiden hadden elk hun eigen ideeën over het vakgebied en het doel was om 'iets' te maken waarmee de huidige beveiligingsomgeving van hun werkgever verbeterd kon worden en vooral waarmee synergie verkregen kan worden. Overigens is het zo dat dit model kan worden gebruikt voor zowel informatiebeveiliging als voor fysieke beveiliging en uiteraard fraudemanagement.

> Waarom een model gebruiken in informatiebeveiliging? Met modellen kan je ideeën overbrengen. Een model is dan ook geen receptje maar een medium om ideeën of inzichten over te brengen of te verbeteren

Fraudemanagement

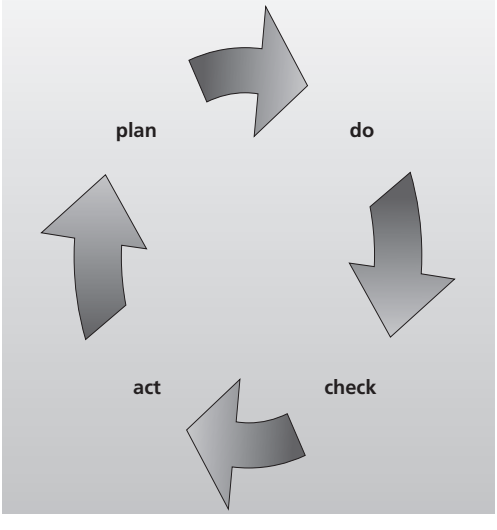
Fraude is een verzamelbegrip waarmee meestal vermogensdelicten zoals oplichting, verduistering en bankbreuk mee worden aangeduid. Taalkundig gezien omschrijft de Dikke van Dale fraude als: 'bedrog bestaande uit vervalsing van administratie of ontduiking van voorschriften.' Deze omschrijving is niet volledig. Ook zonder dat administratieve bescheiden worden vervalst (bijvoorbeeld in geval van 'bankbreuk') kan men frauderen. Toch heeft fraude een aantal kenmerken:

- Bij fraude is er wel altijd sprake van ontduiking of schenden van regels. Dit kunnen regels van het bedrijf zijn, maar ook van de overheid (wet- en regelgeving).
- Door de schending van de regels wordt iets waardevols verkregen.
- Er is altijd sprake van opzet.

Zoals al eerder aangegeven is, is fraude een verzamelbegrip waar vaak diverse verschillende delicten onder kunnen vallen zoals:

- valsheid in geschrifte (artikel 225 WvSr);
- verduistering (artikel 321 WvSr)/diefstal (artikel 310 WvSr);
- telecommunicatiefraude (artikel 326c WvSr)

Het voorkomen van fraude moet worden gezocht in het nemen van beveiligingsmaatregelen. Vooral op dit gebied is door samenwerking dus veel synergie te behalen en zijn er kosten te besparen. De grote vraag is: Hoe passen we fraudemanagement in binnen kwaliteitsmodellen zoals ISO9001 en BS7799?



Figuur 1 PLAN-DO-CHECK-ACT (PDCA).

Met de ISO9001-gedachte en de continue verbetercyclus 'PLAN-DO-CHECK-ACT (PDCA)' in het achterhoofd is men de werkzaamheden gaan inventariseren en structuur gaan aanbrengen.

Werkzaamheden PLAN-fase

Onder de PLAN-fase zijn activiteiten ondergebracht die met het opzetten van beveiligingsmaatregelen en het bestaan van de maatregelen te maken hebben. Hierbij komen de volgende activiteiten aan de orde:

- het doen van risicoanalyses;
- het verkrijgen van een mandaat en budget van de directie om beveiligingsmaatregelen te gaan ontwikkelen;
- het maken van beleid, bijvoorbeeld volgens een standaard als de BS7799;
- het definiëren van de (technische en procedurele) beveiligingsarchitectuur;
- het afhankelijk van de geaccepteerde risico's maatregelen nemen, maar risico's kunnen ook door verzekeringen worden afgekocht;
- en ten slotte moet iedereen aan de wet voldoen; het maken van een inventarisatie van wettelijke verplichtingen en het beleid afstemmen op dit juridische kader is essentieel in de PLAN-fase.

Nog voor dat de DO-fase begint, is het van belang dat de directie twee activiteiten onderneemt:

1. De directie moet het gemaakte beleid, de maatregelen en architectuur aftekenen.
2. De directie moet via een interne mededeling aan alle medewerkers het belang van informatiebeveiliging benadrukken.

Als aan bovenstaande stappen niet wordt voldaan of het is niet de directie die de aftekening en communicatie naar de medewerkers doet, dan kan men zich afvragen of men door moet gaan naar de DO-fase en wat de status is van alle beveiligingsactiviteiten.

Als de PLAN-fase voltooid is, komt men in de DO-fase waarin men het gemaakte beleid en architectuur gaan implementeren en tracht te borgen bijvoorbeeld met behulp van ITIL-processen. Maar ook het trainen van mensen, alle medewerkers bewuster maken van beveiliging, het beleid en de architectuur worden in de DO-fase uitgevoerd.

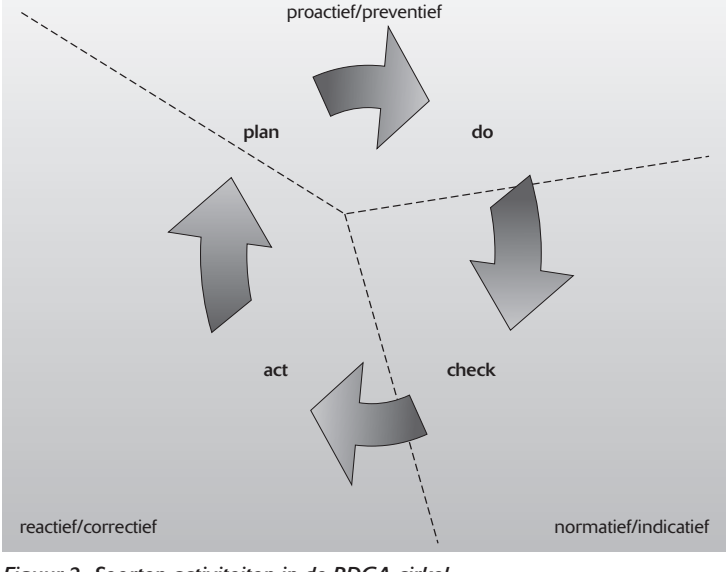
Beveiligingsmaatregelen zijn leuk, maar waar moet een maatregel aan voldoen?

Een beveiligingsmaatregel is opgebouwd uit drie componenten.

1. *Opzet*. Waarom is er besloten om een maatregel te nemen? Welke afwegingen, bijvoorbeeld risicoanalyses, zijn er geweest?
2. *Bestaan*. Wat is de omschrijving of definitie van de maatregel en wie is de eigenaar van de maatregel.
3. *Werking*. Hoe wordt de naleving en effectiviteit van de maatregel gecontroleerd? Wie doet deze controle en naar wie worden de resultaten van de controle gerapporteerd?

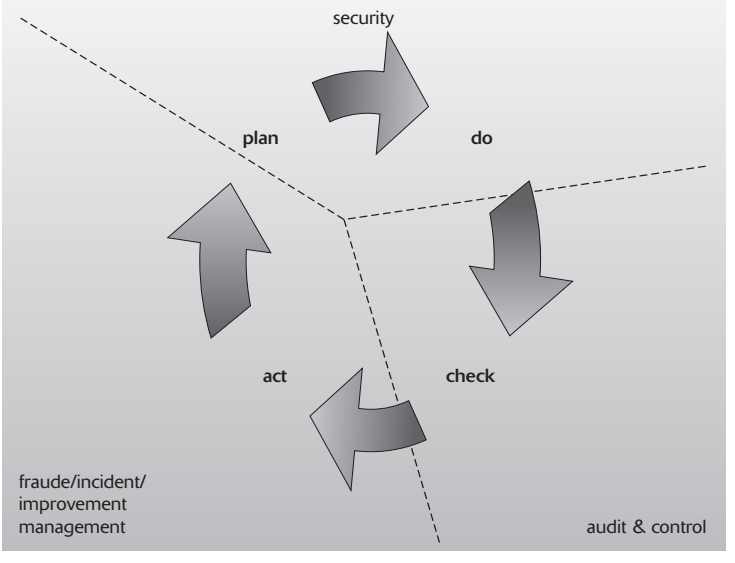
Deze drie componenten moeten helpen om een maatregel *SMART* (*S*pecifiek-*M*eetbaar-*A*anwijsbaar/acceptabel-*R*ealistisch en *T*ijd-gebonden) te maken.

Zodra de DO-fase is afgerond kan men zeggen dat het beleid en alle genomen maatregelen operationeel zijn. Nu komt het neer op beheer van het beleid, de maatregelen en de techniek in de CHECK-fase. Continu meten, testen, rapporteren en het doen van trendanalyses. Centraal staat de vraag: Zijn de genomen maatregelen effectief? Het doen van audits tegen gestelde normen als bijvoorbeeld de BS7799. Twee activiteiten die hier ook gebeuren, zijn bedreigingenanalyses (vulnerability management) met bijvoorbeeld het gebruik van fraudedetectiesystemen of het doen van een antecedentenonderzoek op medewerkers. Dit alles om weer risico's in te kunnen schatten en voorbereid te zijn om incidenten en de schade of impact op de organisatie te minimaliseren.
In de ideale wereld zou het zo zijn dat als de PDC-fase goed is doorlopen er geen activiteiten in de ACT-fase zouden plaatsvinden. Alle incidenten die gebeuren, gebeuren tegen geaccepteerde risico's. Helaas is hier ook nog het onverwachte en die situaties die men vergeten is of misschien een maatregel die toch niet SMART is.
In de ACT-fase is men bezig met het afhandelen van beveiligingsincidenten en fraudegevallen. Alles staat hier in het teken van schadebeperking. Maar de opgedane kennis en ervaring is weer invoer voor de PLAN-fase, want wellicht moet het beleid en de architectuur bijgesteld worden nadat de risico's opnieuw zijn onderzocht en er andere risicoafwegingen zijn gedaan; tijden, situaties, eisen en inzichten veranderen immers. Na het doorlopen van de PDCA-cirkel kan gezegd worden dat men in de PLAN-DO-fase vooral pro-actieve of preventieve activiteiten ontplooit (zie figuur 2). In de CHECK-fase is men aan het meten tegen bijvoorbeeld gestelde SLA's en normen, als de BS7799. Normatieve en indicatieve activiteiten dus.



Figuur 2 Soorten activiteiten in de PDCA-cirkel.

Reageren op incidenten en vervolgens correctieve acties ondernemen vallen in de ACT-fase. Reactief bezig zijn om zo snel mogelijk weer in een 'normale' situatie terug te keren. Correctieve acties betekent niet alleen acties ondernemen om in die normale situatie terug te keren, maar ook eventuele schade verhalen en incidenten evalueren, 'lessons-learned', en kennis door te geven aan de PLAN-fase.
Om dan toch nog een indicatie te hebben over hoe dan beveiligings-management, incidentmanagement en fraudemanagement in de PDCA-cirkel vallen is het denkmodel in figuur 3 gebruikt. Dit model is tot stand gekomen door de hierboven uitgelegde activiteiten inventarisatie.



Figuur 3 Soorten management in de PDCA-cirkel.

Beveiliging is een preventieve activiteit die plaatsvindt in de PLAN-DO-fase. In de CHECK-fase zijn meten en controleren een continue activiteit, met andere woorden 'audit & control'. Fraude-, incident- en verbetermanagement zijn duidelijke activiteiten in de ACT-fase.

Conclusie

Dit model wordt op het ogenblik succesvol in de praktijk gebuikt. En past geheel binnen kwaliteitsmanagement en het beveiligingsmanagementsysteem zoals ISO9001 en BS7799. Dit model kan worden gebuikt om de relatie tussen beveiligingsmanagement en fraudemanagement inzichtelijk te maken. Tot slot moet gezegd worden dat in dit artikel bovenal over informatiebeveiliging wordt gesproken. Maar de PDCA-cirkel is ook toepasbaar voor de fysieke beveiliging.