Continu verbetering in beveiligingsmanagement

Organisaties zien dat informatiebeveiliging, fysieke beveiliging en fraudemanagement vaak organisatorisch op verschillende afdelingen zijn belegd. Feit is dat deze disciplines veel gemeenschappelijk vlakken hebben qua processen, procedures, techniek en borging. In het bijzonder op het gebied van incident- en fraudemanagement.

Door Ronald van Erven en Ronald Eygendaal

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

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 altijd sprake van ontduiking of schenden van regels. Dit kunnen regels van het bedrijf zijn, maar ook van de overheid. Verder wordt er door de schending van de regels altijd iets waardevols verkregen. Tenslotte is er altijd sprake van opzet. Het voorkomen van fraude moet worden gezocht in het nemen van beveiligingsmaatregelen. Vooral op dit gebied is door samenwerking veel synergie te behalen en zijn er kosten te besparen. De grote vraag is hoe fraudemanagement past in kwaliteitsmodellen zoals ISO9001 en BS7799.

Plan-Do-Check-Act

Met de ISO9001-gedachte en de continue verbetercyclus van Plan-Do-Check-Act (PDCA) in het achterhoofd is men de werkzaamheden gaan inventariseren en structuur gaan aanbrengen. Welke werkzaamheden zijn onder PLAN-fase ondergebracht? Onder de PLAN-fase vallen activiteiten die te maken hebben met het opzetten van beveiligingsmaatregelen en het bestaan van de maatregel. Hierbij komen de volgende activiteiten aan de orde:

- risicoanalyses,
- mandaat en budget verkrijgen om beveiligingsmaatregelen te ontwikkelen,
- beleid maken, bijvoorbeeld volgens een standaard als BS7799,
- technische en procedurele beveiligingsarchitectuur definiëren,
- maatregelen nemen afhankelijk van de geaccepteerde risico's hoewel die risico's kunnen ook door verzekeringen kunnen worden afgekocht,
- tenslotte een inventarisatie van wettelijke verplichtingen maken en het beleid afstemmen op dit juridische kader.

Nog voor dat de DO-fase begint, is het van belang dat de directie twee activiteiten onderneemt. De directie moet het ontwikkelde beleid, de maatregelen en architectuur duidelijk ondersteunen. Verder moet de directie via een interne mededeling aan alle medewerkers het belang van informatie beveiliging duidelijk maken. Als aan bovenstaande stappen niet wordt voldaan of wanneer anderen binnen de organisatie verantwoordelijk zijn voor het accorderen en de communicatie richting de medewerkers dan zou de organisatie zich moeten afvragen of men moet doorgaan naar de DO-fase en wat de status van alle beveiligingsactiviteiten is.

Impact

Wanneer de PLAN-fase voltooid is, komt een organisatie in de DO-fase alwaar het gemaakte beleid en de architectuur moet worden geïmplementeerd en geborgd met behulp van bijvoorbeeld ITIL-processen. Maar ook de training en bewustwording van medewerkers op het gebied van de beveiliging, het beleid en de architectuur worden in de DO-fase uitgevoerd. Zodra de DO-fase is afgerond kan een organisatie aangeven 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 bestaande uit het continu meten, testen, rapporteren en het uitvoeren van trendanalyses. Centraal staat de vraag of de genomen maatregelen effectief zijn.

Ing. **Ronald van Erven** *is ICT-security officer, heeft 10 jaar ervaring met de bouw van netwerk-, systeembeheers- en informatiebeveiligingsomgevingen, heeft een complete BS7799-certificatie traject op zijn naam staan en is betrokken geweest bij de opzet van de CISSP-opleiding in Nederland.* **Ronald Eygendaal** *is fraudemanager met ruim 10 jaar ervaring in informatiebeveiliging, is lid van het International Advisory Board van de International Foundation for Protection Officers (IFPO), is Certified Security Supervisor (CSS) en Certificate in Information Security Management Principles (CISMP) (ronald.vanerven @xs4all.nl, ronaldeygendaal@protectioncompany.com)*

Audits tegen gestelde normen zoals de BS7799-norm kunnen worden gebruikt. Twee activiteiten die hier ook gebeuren zijn analyses van bedreigingen in het kader *vulnerability management* en het gebruik van fraudedetectiesystemen of het doen van een antecedentenonderzoeken op medewerkers om risico's te kunnen inschatten en voorbereid te zijn op incidenten en schade en de impact ervan op de organisatie.

In de ideale wereld zou het zo zijn dat als de eerste drie stappen uit de PDCA-fase goed zijn is doorlopen er geen activiteiten in de ACT-fase zouden hoeven plaatsvinden. Alle incidenten die mochten plaatsvinden, gebeuren dan tegen geaccepteerde risico's. In de ACT-fase werkt een organisatie aan het afhandelen van beveiligingsincidenten en fraudegevallen. Alles staat hier in het teken van schadebeperking maar de opgedane kennis en ervaring is weer waardevol voor de PLAN-fase. Want wellicht moet het beleid en de architectuur worden bijgesteld nadat de risico's opnieuw zijn onderzocht en er andere risicoafwegingen zijn gedaan. Tijden, situaties, eisen en inzichten veranderen immers.

De directie moet het ontwikkelde beleid, de maatregelen en architectuur ondersteunen.

Proactief

Na het doorlopen van de PDCA-cirkel kan worden gezegd dat in de PLAN-DO-fase vooral proactieve of preventieve activiteiten zijn ontplooid. De CHECK-fase is gericht op het meten tegen SLA's en normen. Normatieve en Indicatieve activiteiten dus. 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 zijn niet enkel acties om in die normale situatie terug te keren, maar ook eventuele schade te verhalen en incidenten te evalueren en kennis door te geven aan de PLAN-fase. Om dan toch nog een indicatie te hebben van hoe dan beveiligingsmanagement, incidentmanagement en fraudemanagement in de PDCA-cirkel vallen, is het volgende denkmodel gebruikt. Dit model is tot stand gekomen door de voorgaande inventarisatie van activiteiten. Beveiliging is een preventieve activiteit die plaats vindt in de PLAN-DO-fase. In de CHECK-fase zijn meten en controleren een continue activiteit, ofwel *audit & control*. Fraude-, incident- en verbetermanagement zijn duidelijke activiteiten voor de ACT-fase. ■

Conclusies

Het model Plan-Do-Check-Act wordt op het ogenblik succesvol in de praktijk gebruikt ter ondersteuning van informatie-, fysieke en fraudemanagement. Het model past binnen kwaliteitsmanagement- en beveiligingsmanagementsystemen zoals ISO9001 en BS7799. Dit model kan worden gebuikt om de relatie tussen beveiligingsmanagement en fraudemanagement inzichtelijk te maken. Tot slot kan worden geconstateerd dat informatiebeveiliging middels de PDCA-cirkel ook toepasbaar is voor de fysieke beveiliging.