CONTINUE VERBETERING IN INFORMATIE BEVEILIGINGSMANAGEMENT

VAN DE SERIE MODEL DENKEN VOOR (INFORMATIE) BEVEILIGINGSMANAGERS

Ronald Elgendaalen Ronald van Erven

In veel organisaties ziet men dat informatiebeveiliging, fysieke beveiliging en fraudemanagement organisatorisch op verschillende afdelingen is belegd. Feit is dat fraudemanagement en (informatie) beveiligingmanagetnent veel gemeenschappelijke vlakken hebben qua processen, procedures, techniek en borging. In het bijzonder is op het gebied van **beveiliginggsincidennnanagement** en fraudemanagement veel samenwerking, dus synergie te behalen.

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 liet vakgebied en het doel was om `iets' te maken waannee de huidige beveiligingsomgeving van hun werkgever verbeterd kon worden en vooral waar synergie verkregen kan worden. Overigens kan dit model worden gebruikt voor zowel informatiebeveiliging als voor fysieke beveiliging en uiteraard fraudemanagement.

gebruik in u1 b-i.-1
t- ee111"1i;: Rilt 111(x1 llen kuil
idccëu c,v m brengrm l:ro nu l l 1s uar: c~ul:
ge,r ret:cp_je, maar yen ll ie,iiuin om
iLlccén cd 1117i,ln'ei1 o', el te brengen of te
c'erluier,t~.

FRAUDEMANAGEMENT

Fraude is een verzamelbegrip waarmee meestal vermogensdelicten zoals oplichting, verduistering en bankbreuk 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 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)
Verduistering (artikel 321 WvSr)/diefstal (artikel 310 WvSr)
Telecommunicatie fraude (artikel 326(WvSr)

Mogelijkheden tot het voorkomen van fraude moet worden gezocht in liet nemen van

beveiligingsmaatregelen. Vooral op dit gebied is riet samenwerking veel synergie te behalen en zijn er kosten te besparen. De grote vraag is: Hoe passen we fraudemanagement in binnen kwaliteitsmodellen zoals 1509001 en BS7799?

PLAN-DO-CHECK-ACT (PDCA)

Met de IS09001 gedachte en de continue verbetercyclus van PLAN-DO-CHECK-ACT (PDCA) in het achterhoofd is men de werkzaamlieden gaan inventariseren en structuur gaan aanbrengen.

Welke werkzaamheden zijn onder PLAN-fase ondergebracht?

Onder de PLAN-fase zijn activiteiten ondergebracht die met het opzetten var) beveiligingsmaatregelen en het bestaan van de maatregel te snaken 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 rasaken van beleid, bijvoorbeeld volgens een standaard als de BS7799.
Het definiëren van de (technische en procedurele) beveiligingsarchitectuur.
Afhankelijk van de geaccepteerde risico's maatregelen nemen, maar risico's kunnen ook door verzekeringen worden afgekocht.
Het rasaken van een inventarisatie van wettelijke verplichtingen en het beleid afstemmen op dit juridische kader.

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

(1) De directie moet liet gemaakte beleid, de maatregelen en architectuur afrekenen.
(2) De directie moet via een interne mededeling aan alle medewerkers het belang van informatie beveiliging aan de orde stellen.

Als aan bovenstaande stappen niet wordt voldaan, kan men zich afvragen wat de status is van alle beveiligingsactiviteiten en of men door moet gaan naar de DO-fase.

Als de PLAN-fase voltooid is, komt men in de DO-fase, alwaar men het gemaakte beleid gaat implementeren en borgen, bijvoorbeeld met behulp van ITIL processen. Ook het trainen van mensen en alle medewerkers bewuster maken van beveiliging, liet beleid en de architectuur wordt in de DO-fase uitgevoerd.

Beveiligingsmaatregcl er] zijn leuk. ; ii„u waar moet een maatregel a:ui auhiocn=

Een beveiligingsmaatregel is opgebomcd uit drie componenten.

'I) Opzet. \X is er besloten um ecii maatregel te nemen?
Welke afwegingen, bijvoorbeeld risicoanalyses, zrl,! er geweest?
Bestaan. \Wit i, le oinsdi rijving of definitie va: de iuaatregel eii wie is de e g,rLiar pan zie l-
Werking. 1 loc etc ii;ikcin` en eftr.dcitr t s.isi ,(e ma.rtrcgel ~econtrc' leerd-, t,~ie doet deze cuiitrule cii naar wie wr,nlci: de re;ultatcr; "-ar) ~ic controle ge1.1.1' p..t tete, 1.1-

Pezc drie
u!n cel[tri.cin cgcl SIMAiiT {specifiek-
~t urt ri.i r-Aa r.wi?,h,i a r:'.mvrpm b el -
R-di,ti,di e!7 Tij,:gebonden;1 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.

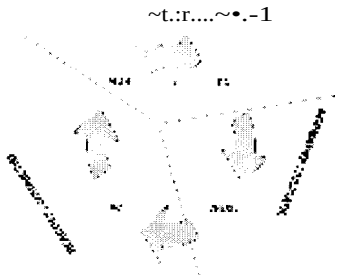
Continu meten, testen, rapporteren en het doen van trendanalyses. Centraal staat de vraag of de genomen maatregelen effectief zijn.

Het doen van audits tegen gestelde nonnen als bijvoorbeeld de BS7799. Twee activiteiten die hier ook plaatsvinden, zijn bedreigingenanalyses (vulnerability management) en bijvoorbeeld het gebruik van fraudedetectiesystemen of het doen van een antecedentenonderzoek op medewerkers. Dit alles wordt gedaan om risico's in te kunnen schatten en voorbereid te zijn om incidenten en de mogelijke 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 vergeet.

In de ACT-fase is men bezig met het afhandelen van beveiligingsincidenten en fraudegevallen. Alles staat in het teken van schadebeperking. De opgedane kennis en ervaring is weer input voor de PLAN-fase. Want wellicht inoet liet beleid en de architectuur bijgesteld worden nadat de risico's opnieuw zijn onderzocht en er andere risicoafwegingen zijn gedaan.

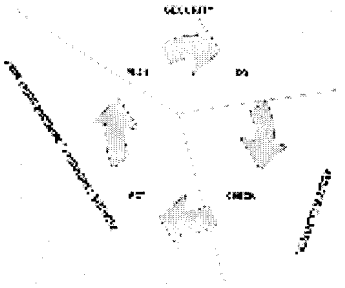
Na het doorlopen van de PDCA-cirkel kan gezegd worden dat men in de PLAN-DO-fase vooral pro-actieve of preventieve activiteiten ontplooit. In de CHECK-fase is enen aan het meten tegen bijvoorbeeld gestelde SLA's en nonnen, als de BS7799. Normatieve en indicatieve activiteiten dus.



Reageren op incidenten en vervolgens correctieve acties ondernemen valt in de ACT-fase. Reactief bezig zijn heeft als doel om zo snel

mogelijk weer in een `normale' situatie terug te keren. Correctieve acties dienen niet alleen om acties te ondernemen om naar normale situatie terug te keren, maar om ook eventuele schade-verhalen en incidenten te evalueren, `lessons-leamed', en kennis door te geven aan de PLAN-fase.

Om een indicatie te hebben over hoe beveiligingsmanagement, incidentmanagement en fraudemanagement in de PDCA cirkel vallen, is het volgende denkmodel gebruikt. Dit model is tot stand gekomen door de hierboven uitgelegde activiteiteninventarisatie.



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 gebruikt en past geheel binnen het kwaliteitsmanagement- en beveiligingsmanagementsysteem zoals IS09001 en BS7799. Dit model kan worden gebruikt 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 I?I)CA-cirkel ook toepasbaar is voor de fysieke beveiliging.

Over de auteurs:

Ronald Ev~en~l.tal CISti'1f zzant lraudematteger eti hert, ?,uit ,laar eMarirtg in beveiliging zit liet bijzonder; i; lid ' aii een I nternational Adri, ,n Board ,n de I nter-n.rtional Foun1latiun kFr froccc[ion Ofti-cer; ,I FI'()). i: certl!ieti Sectuin Super-war CS";l eu Ccr[itictti in Irnfórtnatioti ~Cetrrin `1airtginr,tt Irtnr.hlr; ((l1)M1') '.ra Kt

7ipaii„ ·e(,rn

Int;. Ronald c -1) I?tc.tn M', CISCP i; ~~rrkz:ram ah 1(: I ~cruritt ult;riercn Lee.[l[jaar ervaring in Imt whecucn v:nt pro-werk-, systeet utl,elt,er cai li, l te biizonder informatiebeve lliging,uingee I' lij is E9S77`tt> le„1-aud he, t[een complzte BS-'P) ccrtltictt,e [,-tjee[zijn nct.uti titaan cit is hersokken seleen,[hij de opze[,) , . (hJf ~„ i:a: ii: tiederland. jc kult,- bent berriken cia her e-1nail adres mi:al,l.var1crccn @xs4all.nl

Beide auteurs zijn werkzaam I·ll e communicatiebedrijf en lichhen ttit[jrikel op eigen titel geschreven.