ITIL Security Management

Dr. ir. P.L. Overbeek

Beveiliging en beheer zijn niet te scheiden. Zonder een goed ingericht beheer is beveiliging niet mogelijk. Vice versa is beheer zonder beveiliging niet mogelijk. De nieuwe ITIL-module Security Management brengt beheer en beveiliging samen.

Inleiding

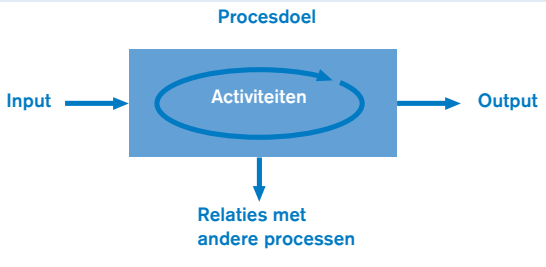
Omdat bedrijven voor hun bedrijfsbelangen steeds meer afhankelijk worden van informatie en informatietechnologie (IT), wordt ook de beveiliging van de informatie en IT steeds belangrijker. In dit artikel wordt uitgelegd hoe beveiliging van, in en door de IT-infrastructuur wordt beheerd, vanuit de optiek van de aanbieder van IT-diensten, ofwel de *service provider*.

De scope van dit artikel is het beheer van de IT-infrastructuur volgens de ITIL-filosofie. ITIL is een procesgerichte benadering voor IT-beheer. Het ITIL-proces Security Management geeft de structurele inpassing van beveiliging in de beheerorganisatie. ITIL Security Management is mede gebaseerd op de Code voor Informatiebeveiliging.

De opbouw van dit artikel is als volgt: allereerst wordt ITIL kort besproken. Vervolgens wordt beschreven hoe de verschillende ITIL-processen moeten worden ingericht om beveiliging en het beveiligingsbeheer mogelijk te maken. Tot slot wordt het proces Security Management zelf beschreven.

ITIL en informatiebeveiliging

De afgelopen decennia is de complexiteit van de IT-infrastructuur belangrijk toegenomen. Juist vanwege die groeiende complexiteit is uniformiteit in het beheer noodzakelijk. ITIL staat voor *Information Technology Infrastructure Library*. ITIL beschrijft processen die uitgevoerd worden voor het beheer van de IT-infrastructuur. *Security Management* is één van de processen van ITIL. Het *Security Management-proces* heeft belangrijke relaties met andere processen, waarvan de belangrijkste in deze paragraaf worden beschreven.



Figuur 1. Procesgerichte benadering.

Opbouw ITIL en Security Management

ITIL gaat geheel uit van een procesmatige benadering van het beheer. Figuur 1 toont hier het model voor. In de processen komt het cyclische karakter van 'management' steeds naar voren: *plan*, *implement*, *evaluate*, *maintenance*. In ITIL wordt het perspectief gekozen van de aanbieder van automatiseringsdiensten (de *service provider*). Deze biedt IT-diensten aan naar de wensen van zijn klanten.

Ieder ITIL-proces bestaat met een zeker doel. Dit doel wordt bereikt door het uitvoeren van een verzameling activiteiten. Deze activiteiten staan niet op zichzelf maar hangen met elkaar samen. Daarom spreken we van een proces. De aansturing van het proces vormt de input, de resultaten van het proces vormen de output. De samenhang met de andere processen wordt beschreven in de relaties.

Voor het proces Security Management is dit model als volgt ingevuld:
Het *doel* van dit proces is tweeledig:
* enerzijds het realiseren van de beveiligingseisen in de verschillende service level agreements (SLA's, de afspraken met de klant) en andere externe vereisten in andere contracten, wetgeving en eventueel intern of extern opgelegd beleid;
* anderzijds het realiseren van een zeker basisniveau aan beveiliging. Dit is nodig om de eigen continuïteit van de beheerorganisatie te waarborgen. Dit is ook nodig om tot vereenvoudiging van het Service Level Management voor informatiebeveiliging te komen. Immers, het beheer van een groot aantal verschillende SLA's is veel complexer dan een beperkt aantal.

De *input*-kant van het proces wordt gevormd door de SLA's met daarin de gespecificeerde beveiligingseisen, eventueel aangevuld met beleidsdocumenten en andere externe vereisten.
De *output* levert verantwoordingsinformatie op met betrekking tot de realisatie van de SLA's, inclusief een rapportage van afwijkingen.

Het proces Security Management heeft *relaties* met de meeste andere ITIL-processen. In de andere ITIL-processen moeten namelijk activiteiten plaatsvinden ten behoeve van beveiliging. Om deze relaties te begrijpen, wordt eerst de lagenstructuur van ITIL besproken.

De driehoek in figuur 2 toont de drie lagen die in ITIL kunnen worden herkend. Iedere laag stelt een abstractieniveau voor. Per laag is een set processen gedefinieerd.

In de bovenste laag wordt de strategie van het beheer uitgestippeld. De processen voor deze strategische laag zijn verzameld in de Managers Set. Voor de informatiebeveiliging is deze set vooral van belang waar het de organisatie van de beheerorganisatie betreft. Dit geldt overigens voor alle processen op dezelfde wijze. Voor deze set zijn dan ook geen specifieke relaties voor Security Management geïdentificeerd.

Figuur 2. Drie lagen in ITIL.

In de middelste laag bevinden zich de tactische processen, verzameld in de Service Delivery Set. Hierin bevinden zich processen die zorgen voor het opstellen van SLA's en die de dienstverlening verzorgen conform de afspraken in deze SLA's. Ook de beveiligingsafspraken worden vastgelegd in de SLA's. Het proces Security Management zelf bevindt zich ook in deze set. Het proces Security Management heeft relaties met de meeste andere processen uit deze set, waaronder:

* Service Level Management;
* Availability Management;
* Capacity Management;
* Contingency planning.

Dan is er ten slotte de operationele laag. De processen in deze laag zijn verzameld in de Service Support Set. De processen binnen de Service Support Set verzorgen het daadwerkelijk operationeel beheer van de IT-middelen zelf. Het proces Security Management is afhankelijk van de processen in deze set omdat deze voorwaardenscheppend zijn. Daarom heeft Security Management relaties met vrijwel alle processen uit deze set, te weten:

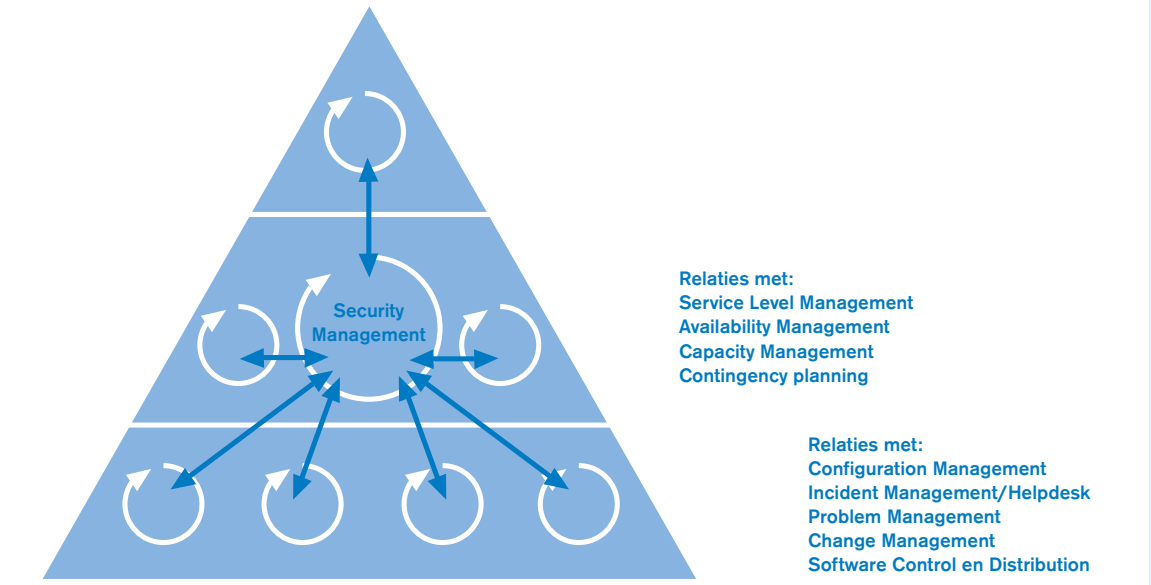
* Configuration Management;
* Incident Management / Helpdesk;
* Problem Management;
* Change Management;
* Software Control en Distribution.

Ieder ITIL-proces heeft een verantwoordelijke manager. Bij Security Management wordt dit de Security Manager genoemd. In kleine beheerorganisaties kunnen meer processen door één functionaris worden gemanaged; in grote organisaties zullen meer personen actief zijn in het Security Management. In het laatste geval is dan doorgaans wel één persoon als de Security Manager aangewezen. De tegenspeler aan de klantkant wordt de (Corporate) Information Security Officer genoemd.

Het proces Security Management heeft, zoals gezegd, relaties met de bovengenoemde ITIL-processen (zie figuur 3). In deze processen moeten namelijk activiteiten plaatsvinden ten behoeve van beveiliging. Deze activiteiten vinden op de gebruikelijke wijze plaats onder verantwoordelijkheid van het betreffende proces en de betreffende manager. Vanuit Security Management worden echter aanwijzingen gegeven aan deze processen met betrekking tot de inrichting van deze beveiligingsgerichte activiteiten. In de praktijk komen afspraken in overleg tussen de Security Manager en de andere procesmanagers tot stand.

De beveiligingsparagraaf in de service level agreement

In de service level agreement (SLA) worden de afspraken met de klant vastgelegd. De SLA is de verantwoordelijkheid van het Service Level Management (SLM, dat bij de behandeling van de Service Delivery Set aan de orde komt). De SLA fungeert als belangrijkste sturingsinformatie voor alle ITIL-processen. Door middel van ver-



Figuur 3. Relaties tussen het proces Security Management en de andere processen.

antwoordingsinformatie wordt rekenschap gegeven over de prestaties van de beheerorganisatie ten opzichte van wat afgesproken is in de SLA. Naast de verantwoordingsinformatie die door de beheerorganisatie wordt aangeleverd, zal de klant doorgaans ook onafhankelijke informatie (laten) verwerven door een EDP-auditor.

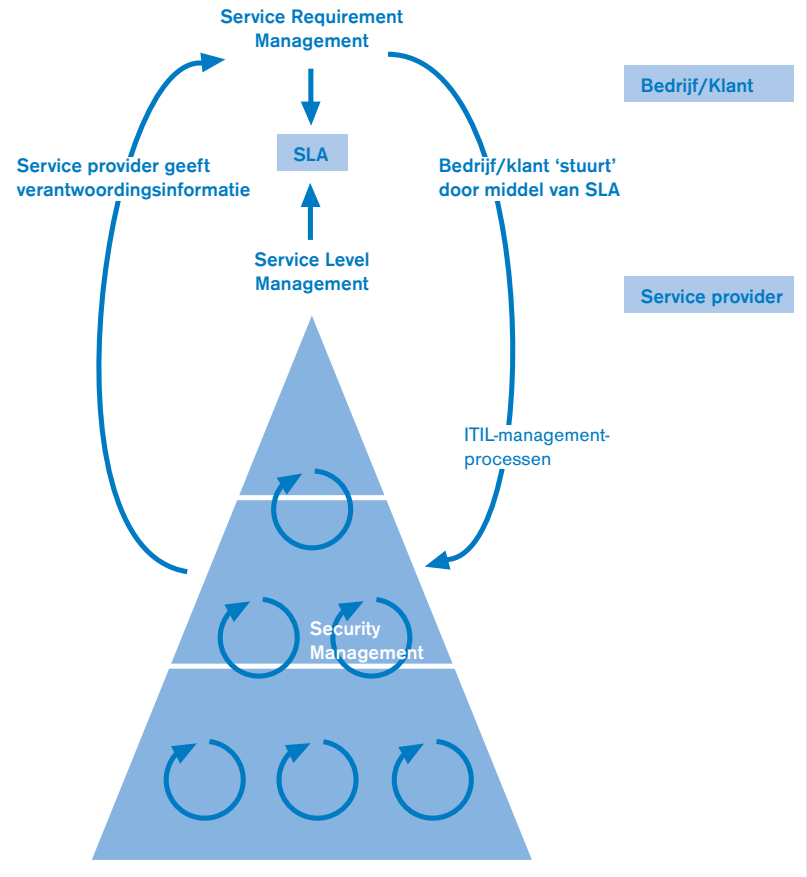
Figuur 5 toont hoe de beveiligingsparagraaf in de SLA totstandkomt. Allereerst dient de klant zelf te bepalen, in abstracte termen, welke beveiligingsbehoefte hij heeft. De klant geeft uitdrukking aan de belangen van zijn bedrijfsprocessen. Deze bedrijfsprocessen zijn afhankelijk van de services van de IT en daarom van de IT-beheerorganisatie. Hoe de servicenemer zijn beveiligingsbehoefte (*Service Level Requirements* voor informatiebeveiliging – niet opgenomen in de figuur) bepaalt, is geen onderdeel van ITIL. Doorgaans zal hij daar echter een vorm van risicoanalyse voor gebruiken. Zo'n analyse leidt tot de Service Level Requirements voor beveiliging (zie ook figuur 4).

De vertegenwoordiger van de servicenemer (de klant) en de accountmanager van de serviceaanbieder (provider) treden hierover in onderhandeling. De accountmanager zal naast de gestelde Service Level Requirements zijn standaardaanbod leggen. Dat is de *Service Catalogus* van de service provider. In de Service Catalogus zijn ook de altijd geboden beveiligingsmaatregelen weergegeven: het basisniveau voor beveiliging, ofwel de *Security Baseline*. Boven dit basisniveau kan de klant aanvullende eisen stellen.

De klant en de accountmanager stellen samen vast hoe de Service Level Requirements en de Service Catalogus op elkaar passen.

Een eerste aspect is daarbij dat sommige diensten afhankelijk zijn van derden. De service provider kan hier veelal niet de volledige verantwoordelijkheid voor nemen. Voorbeeld is de beschikbaarheid van telecommunicatieverbindingen, waarop leveranciers doorgaans geen garantie geven. De service provider komt daarom met zijn klant overeen welke afspraken de provider maakt met *zijn* providers. Voorbeeld hiervan kunnen zijn: de contracten over de levering van huurlijnen, de contracten met hardwareleveranciers met betrekking tot onderhoud en responstijden. Deze overeenkomsten worden de *underpinning contracts* genoemd. Dat zijn alle afspraken waarvoor de service provider geen volledige verantwoordelijkheid kan dragen, doorgaans omdat hij geen invloed uit kan oefenen op de realisatie van die afspraken.

Het tweede aspect wordt gevormd door de *operational level agreements*. Dat zijn de diensten die door de service provider zelf worden geleverd. Voor hem is het van belang dat hij intern verantwoordelijkheden verbindt aan deze agreements. De Service Catalogus is een algemene beschrijving van de diensten. De operational level agreements daarentegen zijn de vertaling van deze algemene beschrijvingen naar alle services (*Service Delivery*) en de individuele componenten (zie de *Configuration Items* bij *Configuration Management*) alsmede de wijze waarop de afspraken over service levels intern zijn geborgd.

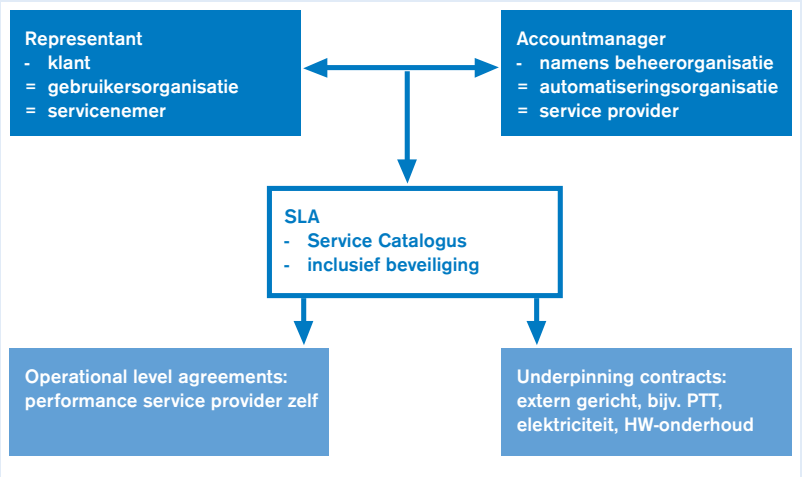


Figuur 4. Samenhangende processen.

Voorbeeld: de Service Catalogus spreekt bijvoorbeeld over 'beheer van toegangsrechten per gebruiker per persoon'. In de operational level agreements wordt dat vervolgens nader ingevuld voor alle relevante services die door de beheerorganisatie worden aangeboden. Zo wordt de wijze van implementatie van deze maatregel vastgelegd voor de afdeling die de Unix-services levert, voor VMS, voor NT, voor Oracle, enz.

Merk op dat de Service Level Requirements van de klant zo mogelijk worden vertaald naar de Service Catalogus van de provider. Eventueel worden aanvullende afspra-

Figuur 5. Opstellen van de beveiligingsparagraaf in de SLA.



ken gemaakt. Deze leiden dan tot een hoger serviceniveau dan standaard wordt geleverd.

Bij het opstellen van de SLA is het (ook) voor beveiliging van belang dat meetbare *Key Performance Indicatoren* (ofwel *KPI*) en *criteria* worden afgesproken. KPI zijn de meetbare grootheden; de performancecriteria zijn de haalbare levels van die meetbare grootheden. Soms is het moeilijk meetbare indicatoren af te spreken voor beveiliging. Voor beschikbaarheid valt dat nog mee. Beschikbaarheid is meestal wel uit te drukken in een getal. Voor integriteit en vertrouwelijkheid is dat al veel moeilijker. Daarom worden veelal abstracte maatregelen in de beveiligingsparagraaf van de SLA genoemd die op deze gebieden worden vereist. Als basisset voor de beveiligingsmaatregelen worden die van de Code voor Informatiebeveiliging gebruikt. In de SLA wordt tevens afgesproken op welke wijze de *performance* wordt gemeten. In ieder geval is noodzakelijk dat periodieke verantwoordingsinformatie van en over de beheerorganisatie (de provider) aan de gebruikersorganisatie (de klant) ter beschikking wordt gesteld.

Service Support Set

De processen uit de Service Support Set richten zich geheel op het beheer van de IT-middelen zelf. In deze paragraaf worden de processen uit deze set kort beschreven met de wijze waarop activiteiten binnen deze processen het proces Security Management dienen te ondersteunen. Zoals eerder reeds opgemerkt vindt overleg over deze voor beveiliging relevante activiteiten plaats tussen de betreffende manager en de Security Manager.

Configuration Management

Een eerste vereiste voor goed IT-beheer is dat men het proces voor Configuration Management goed heeft opgezet. Configuration Management vormt de basis voor het beheer. Configuration Management is het proces dat zorgt dat je weet wat er aan IT-infrastructuur in huis is, wat de status hiervan is, en welke relaties er zijn tussen de verschillende onderdelen van de infrastructuur (dus de relaties tussen de CI's, zie later). Ofwel, dat bekend is hoe de IT-infrastructuur is samengesteld. Door middel van het Configuration Management wordt tevens verzekerd dat wijzigingen in de IT-infrastructuur alleen op een beheerste wijze totstandkomen. Iedere wijziging komt namelijk via dit proces tot stand en iedere wijziging zal dus in het Configuration Management moeten worden vastgelegd.

Dit proces heeft als doelstelling alle componenten van de IT-infrastructuur en de daaraan gerelateerde procedures en documentatie onder controle te brengen ter ondersteuning van de overige processen.

Wanneer Configuration Management goed is ingericht is het duidelijk uit welke configuratie-items de IT-infrastructuur bestaat, wie verantwoordelijk is voor welk item, waar de items zich bevinden en in welke toestand met welke relatie(s). Configuration Management verstrekt informatie over de samenstelling van de IT-infrastructuur en is verantwoordelijk voor de correcte registratie van geautoriseerde onderdelen van de IT-infrastructuur. Bovendien verifieert Configuration Management geregeld of de registratie nog een correcte afspiegeling vormt van de werkelijkheid. Op deze wijze wordt voorkomen dat wordt gewerkt met ongeautoriseerde onderdelen die niet aan de beveiligingseisen voldoen.

Twee begrippen staan centraal: een *configuration item (CI)* is de kleinste eenheid die individueel wordt gemanaged. Het overzicht van alle CI's vormt tevens het overzicht van de totale IT-infrastructuur. Dit overzicht heet de *Configuration Management Database (CMDB)*. ITIL ziet als mogelijke configuration items: software (applicaties), hardware, documentatie en procedures.

Configuration Management en informatiebeveiliging
Ieder configuration item heeft een uniek nummer voor identificatie. Daarnaast worden per CI attributen bijgehouden, de status en de mogelijke relaties met andere CI's. Voor informatiebeveiliging is Configuration Management vooral van belang in verband met de mogelijkheid een rubricering (classificatie) aan een CI te geven. Deze rubricering koppelt de CI aan een bepaalde set beveiligingsmaatregelen ofwel een procedure.

Een classificatie of rubricering van een CI is een aanduiding van de gewenste vertrouwelijkheid, integriteit en/of beschikbaarheid van de CI. Deze classificatie wordt ontleend aan de beveiligingseisen uit de SLA. De 'klant' van de beheerorganisatie bepaalt de classificatie omdat hij als enige kan bepalen hoe belangrijk informatie of -systemen voor zijn bedrijfsprocessen zijn. De klant bepaalt de classificatie op basis van een analyse van de afhankelijkheid van zijn bedrijfsprocessen van de informatiesystemen en van de informatie zelf. Het is dan aan de beheerorganisatie deze classificatie blijvend te koppelen aan de juiste CI's. De beheerorganisatie moet tevens per classificatieniveau een pakket beveiligingsmaatregelen implementeren dat voor dat niveau geldt. Dit pakketje maatregelen kan worden samengevat in een procedure. Zo'n procedure zou bijvoorbeeld kunnen luiden: 'procedure voor omgang met gegevensdragers met privacygeclassificeerde gegevens'. In de SLA kan worden vastgelegd welk pakket beveiligingsmaatregelen voor welk classificatieniveau moet worden geïmplementeerd.

Een classificatiesysteem dient altijd op maat van de organisatie van de klanten te zijn. Voor de eenvoud van het beheer is het echter aan te raden één classificatiesysteem na te streven, ook indien een beheerorganisatie meerdere klanten heeft.

Samenvattend: classificatie is een sleutelbegrip. In de CMDB is bij iedere CI zijn classificatie opgenomen. Deze classificatie koppelt de CI aan een set beveiligingsmaatregelen die hoort bij deze classificatie, ofwel een procedure. Classificatie koppelt een CI aan specifieke activiteiten, vastgelegd als een procedure (behandelingsvoorschriften) in de documentatie (handboeken, *implementation guidelines*). Veelal zal in de procedure zijn opgenomen dat bij uitvoering een vorm van vastlegging, ofwel rapportage, vereist is.

Incident Management / Helpdesk

De nieuwe titel voor het proces Helpdesk is Incident Management. Hierna wordt verder de nieuwe naam gebruikt. De voornaamste *doelstelling* van Incident Management is de continuïteit van de dienstverlening voor de klanten.

Activiteiten van het proces Incident Management zijn het administreren, volgen en beheersen van incidenten (*incident control*). Dit proces wordt uitgevoerd door de helpdesk. Dit proces is het centrale proces waar de registratie en bewaking van *alle* incidenten plaatsvindt. De helpdesk fungeert als één loket voor alle incidentmeldingen en eerstelijnshulp. Incident Management is de 'eigenaar' van alle incidenten.

Incident Management registreert incidenten en ziet erop toe dat deze zo snel mogelijk worden opgelost. Incident Management heeft hierbij de mogelijkheid te escaleren wanneer dreigt dat een incident niet tijdig wordt opgelost. Dit geldt uiteraard ook voor incidenten die betrekking hebben op beveiliging.

De input voor Incident Management bestaat grotendeels uit meldingen van gebruikers. Voor iedere melding wordt een incident gedefinieerd. Incidenten worden gecategoriseerd en per categorie is een procedure gedefinieerd die voorschrijft welke activiteiten moeten worden ondernomen door Incident Management. Een juiste categorisering is van groot belang voor beveiliging (zie later). Veelal wordt gewerkt met een aanduiding van het effect (*impact*) van een incident. Indien het effect is dat het halen van de SLA direct in gevaar komt, dan heeft dat incident een hogere prioriteit dan wanneer dat niet het geval is. Bij het registreren van een incident wordt zo mogelijk een koppeling gemaakt met de CI waar het incident betrekking op heeft.

De output bestaat, zoals gezegd, uit directe oplossingen of alternatieve werkwijzen. In alle gevallen vindt registratie van incidenten plaats; deze vormen de input voor het proces Problem Management.

Incident Management en informatiebeveiliging

Incident Management is het centrale proces voor het melden voor beveiligingsincidenten. Voor beveiligingsincidenten kan, afhankelijk van de ernst van het incident, een andere procedure gelden dan voor gewone incidenten. Het is dus van groot belang dat Incident Management een beveiligingsincident als zodanig herkent. Beveiligingsincidenten zijn sowieso al die incidenten die het halen van de beveiligingseisen uit de SLA kunnen verhinderen. Het is nuttig in de SLA een overzicht op te nemen van het *soort* incidenten dat als beveiligingsincident moet worden beschouwd. Die incidenten die het halen van het eigen beveiligingsbasisniveau (*baseline*) verhinderen, worden altijd aangemerkt als beveiligingsincidenten.

Merk op dat deze incidentmeldingen niet altijd van de gebruikers zullen komen, maar ook van het beheer zelf, bijvoorbeeld op basis van alarmmeldingen of auditgegevens uit de systemen.

Zoals gezegd is het van groot belang dat Incident Management een beveiligingsincident herkent. Alleen in dat geval zal de juiste procedure in gang worden gezet die hoort bij de afhandeling van beveiligingsincidenten. Indien het beveiligingsincident betrekking heeft op een hoger gerubriceerde CI, kan bijvoorbeeld een speciale procedure worden gevolgd. Mogelijk ook worden in de procedure andere vervolgactiviteiten gedefinieerd, waaronder rapportage naar de klant. Het probleem is dus: hoe herkent Incident Management een beveiligingsincident.

Het is aan te raden de procedure rond verschillende soorten beveiligingsincidenten in de SLA vast te leggen en deze procedure ook te oefenen. Het is ook aan te raden een procedure af te spreken omtrent de communicatie rond beveiligingsincidenten. Het is niet de eerste keer dat een organisatie in paniek raakt vanwege een opgeblazen gerucht. Het is ook niet de eerste keer dat onnodige schade ontstaat doordat *niet* tijdig wordt gecommuniceerd over een beveiligingsincident. Het is verstandig alle communicatie met betrekking tot beveiligingsincidenten via de Security Manager te laten verlopen.

> Toets of door een oplossing geen nieuw beveiligingsprobleem ontstaat.

Problem Management

Het proces Problem Management heeft als doel de incidenten van het proces Incident Management te beheren, verbanden te leggen en de incidenten stelselmatig op te lossen. Indien de oorzaak van een probleem is vastgesteld, dan wordt een onderkende fout (*known error*) gedefinieerd. De input voor dit proces bestaat voornamelijk uit incidenten. De output van het proces Problem Management bestaat uit oplossingen, onderkende fouten (*known errors*) en Requests For Change (RFC's). Een RFC is een voorstel voor een wijziging (*Change*) in de IT-infrastructuur.

De oplossingen worden keurig gedocumenteerd en onder trefwoorden toegankelijk gemaakt voor de helpdesk. Ofwel, van incident tot leermoment. De *known errors* en de RFC's vormen de input voor het proces *Change Management*.

Problem Management en informatiebeveiliging

Als een 'probleem' uit een beveiligingsincident voortkomt, kan het zijn dat daar een aparte procedure voor wordt gevolgd. Een aantal zaken is in het bijzonder van belang. Denk allereerst na over de mensen die betrokken mogen zijn of kennis mogen hebben van het incident. Dit omdat het wenselijk is de groep mensen met kennis van het incident zo beperkt mogelijk te houden (gezichtsverlies, goede reputatie). Maar ook omdat de kennis over een mogelijk lek in de beveiliging tot een zo klein mogelijke groep beperkt moet blijven vanuit het oogpunt van misbruik en exploitatie van dat lek. Ten tweede, denk na

over de mensen die juist betrokken *moeten* zijn bij het oplossen van zo'n incident (de *Security Manager* van de beheerorganisatie, wellicht zelfs de *security officer* van de klant). En ten derde, toets bij het voorbereiden van een oplossing altijd of *door* deze oplossing geen nieuwe beveiligingsproblemen ontstaan (toets aan het halen van de SLA en de eigen baseline).

Change Management

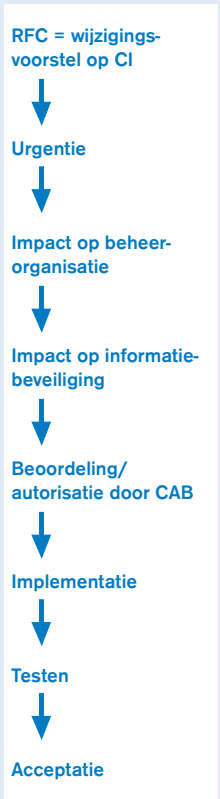
Het proces Change Management heeft als doel alle wijzigingen op of van CI's te beheersen en te beheren. Wijzigingen in de IT-infrastructuur komen altijd tot stand via dit proces. Een Change is een gecontroleerde wijziging in de IT-infrastructuur.

Input voor Change Management vormen de *known errors* en *Requests For Change* (RFC's).

De Change Manager is de eindverantwoordelijke manager voor dit proces. Onderdeel van de activiteiten is het opstellen, behandelen, verwerken en, na accordering, (doen) implementeren van een Change. De output van dit proces is een geëvalueerde en geautoriseerde Change. Onderdeel van het uitvoeren van de Change zelf is het bijwerken van de gegevens over de betrokken CI('s) in de CMDB door het proces Configuration Management.

Change Management en informatiebeveiliging

De activiteiten binnen het proces Change Management zijn veelal sterk gerelateerd aan beveiliging. Beveiliging en Change Management gaan namelijk hand in hand. Indien een situatie is bereikt met een acceptabel beveiligingsniveau, en het wijzigingsproces beheerst deze situatie, dan kan men zelf in de hand houden dat de nieuwe situatie ook een acceptabel beveiligingsniveau heeft. Daarom wordt een aantal vaste stappen onderscheiden om dit beveiligingsniveau zo goed mogelijk te waarborgen. Figuur 6 toont de stappen die moeten worden doorlopen. Input is een RFC waarin het voorstel tot wijziging van de IT-infrastructuur met onderbouwing en referentie van de betrokken CI's is opgenomen. Aan een RFC worden parameters gekoppeld die de procedure voor acceptatie beïnvloeden. De parameters in de figuur zijn als voorbeeld bedoeld, andere keuzen zijn mogelijk. Hier is gekozen voor parameters voor urgentie en impact. Dan is toegevoegd de parameter 'impact op informatiebeveiliging'. Indien het voorstel een grote invloed op de informatiebeveiliging kan hebben, zijn bijvoorbeeld zwaardere acceptatietests en -procedures noodzakelijk.



Figuur 6. Een Change.

Onderdeel van de RFC vormt ook het voorstel omtrent de invulling van de beveiliging. Hierbij geldt als uitgangspunt wederom dat wat is afgesproken in de SLA alsmede dat wat de beheerorganisatie zelf als basisniveau heeft gekozen. Dit voorstel voor de invulling van de beveiliging bestaat dus uit een verzameling beveiligingsmaatregelen. Deze maatregelen worden ontleend aan de Code voor Informatiebeveiliging.

Vervolgens wordt de RFC beoordeeld en geautoriseerd. Voor RFC's met een beperkte invloed kan dat bijvoorbeeld door de Change Manager zelf geschieden. Voor een zware RFC vindt de beslissing plaats door de Change Advisory Board (CAB). In de CAB neemt in ieder geval de Security Manager plaats, en mogelijk zelfs de security officer (beveiligingsfunctionaris) van de klant(en) indien de RFC een mogelijk grote invloed op de beveiliging heeft.

Het is overigens niet de bedoeling de Security Manager voor iedere Change in te schakelen. Beveiliging dient zoveel mogelijk een geïntegreerd onderdeel te zijn van de normale taken. De Change Manager moet in staat zijn te beoordelen of hij, dan wel de CAB, de input van de Security Manager nodig heeft. Ook voor de selectie van maatregelen voor de CI's die in de RFC betrokken zijn, is de Security Manager niet per se noodzakelijk. Immers, als het goed is staat het raamwerk voor de te treffen maatregelen al klaar en is het wellicht alleen nog de vraag op welke wijze deze moeten worden geïmplementeerd.

Bij de implementatie van de Change is het noodzakelijk direct de beveiligingsmaatregelen te implementeren en vervolgens ook mee te testen. Het testen van beveiliging verschilt van het normale functionele testen. Bij het normale testen wordt namelijk onderzocht of bepaalde functionaliteit *aan*wezig is. Het testen van beveiliging richt zich niet alleen op de aanwezigheid van (beveiligings)functionaliteit, maar ook op de *af*wezigheid van andere, niet gewenste, 'functionaliteit'. Deze laatste categorie vormt namelijk doorgaans de gaten in het systeem.

De Change Advisory Board beslist over het al dan niet accepteren van een RFC. Indien de CAB positief adviseert, wordt het wijzigingsvoorstel geautoriseerd.

Het proces Change Management is vanuit de optiek van beveiliging één van de belangrijkste. Immers, hiermee worden nieuwe beveiligingsmaatregelen in de IT-infrastructuur geïntroduceerd, samen met de wijzigingen op die IT-infrastructuur.

Software Control en Distributie

Het laatste proces uit de Service Support Set dat hier wordt besproken, is het proces Software Control en Distributie. Het doel van dit proces is het versiebeheer van de software te implementeren en de uitrol van de software te verzorgen. Input voor dit proces is een geautoriseerde RFC van het proces Change Management. Dit proces beschikt hiertoe over wat genoemd wordt de *definitive software library*. Dat is het overzicht van alle juiste, erkende en geautoriseerde software, met eventueel een verwijzing naar de broncode, het depot dan wel de installatiebestanden. Deze library hoeft overigens geen separate database te zijn; het kan gewoon een onderdeel van de CMDB vormen.

Software control en Distributie en informatiebeveiliging

Van belang is dat alle software via dit proces op beheerste wijze de organisatie binnenkomt en wordt uitgerold. Dit proces zorgt ervoor:

* dat de juiste software wordt gebruikt;
* dat deze vooraf getest is;
* dat de introductie op de juiste wijze (door middel van een Change) geautoriseerd is;

* dat de software legaal is;
* dat de software virusvrij is en ook virusvrij wordt verspreid;
* dat de versienummers bekend zijn (en geregistreerd door Configuration Management in de CMDB);
* en dat beheerste invoering plaatsvindt.

Ook dit proces werkt volgens een vaste acceptatieprocedure. In deze acceptatieprocedure dient informatiebeveiliging de nodige aandacht te krijgen. Met name is van belang dat tijdens het testen en de acceptatie de implicaties voor de beveiliging worden meegenomen. Dit betekent dat aan de in de SLA afgesproken beveiligingseisen en -maatregelen blijvend moet worden voldaan.

De Service Delivery Set en informatiebeveiliging

Ook de processen uit de Service Delivery Set hebben relaties met beveiliging. Deze processen worden hier alleen kort samengevat voorzover van belang voor informatiebeveiliging. Ze zijn in hun eigen ITIL-boekjes beschreven. Hieronder volgt een korte samenvatting.

Service Level Management

Service Level Management zorgt ervoor dat afspraken worden vastgelegd en nagekomen over de diensten die aan klanten worden geleverd. In deze service level agreements dienen tevens afspraken te worden gemaakt over de te nemen beveiligingsmaatregelen. Het doel is te komen tot een optimaal niveau van IT-dienstverlening.

Service Level Management onderscheidt een aantal samenhangende beveiligingsactiviteiten waarin Security Management een belangrijke rol speelt:
1 identificatie van de beveiligingsbehoefte van de klant (het vaststellen van de beveiligingsbehoefte blijft uiteraard de verantwoordelijkheid van de klant zelf omdat deze behoefte voortkomt uit zijn bedrijfsbelangen);
2 verifiëren van de haalbaarheid van deze beveiligingsbehoefte van de klant;
3 voorstellen doen voor, onderhandelen over en vastleggen van het gewenste beveiligingsniveau van de IT-diensten in de SLA;
4 doen bepalen, opstellen en vastleggen van interne beveiligingsnormen voor de IT-dienstverlening (de operational level agreements);
5 doen bewaken van die beveiligingsnormen (OLA's);
6 rapporteren over geleverde IT-diensten.

Voor de eerste drie activiteiten levert Security Management input en ondersteuning aan Service Level Management. De activiteiten 4 en 5 worden uitgevoerd door Security Management. Voor activiteit 6 levert onder andere Security Management input. De daadwerkelijke uitvoering van de activiteiten (wie doet wat) is een kwestie van overleg tussen de Service Level Manager en de Security Manager.

Bij het vaststellen van de SLA is veelal uitgangspunt dat er een algemeen niveau van beveiliging bestaat (het basisbeveiligingsniveau of *baseline*). Wanneer een klant een betere beveiliging wenst, dan dient dat expliciet in de SLA te worden vastgelegd.

Availability Management

Availability Management houdt zich bezig met de technische beschikbaarheid van IT-componenten. Het kwaliteitsaspect beschikbaarheid wordt geborgd door - continuïteit, onderhoudbaarheid en veerkracht. De continuïteit van een IT-dienst geeft aan in welke mate de dienst de afgesproken functionaliteit biedt gedurende een aangegeven tijdsduur. Onderhoudbaarheid is een indicatie voor het gemak waarmee onderhoud aan een dienst gedaan kan worden. Veerkracht is het vermogen van een IT-dienst om op de juiste wijze te blijven functioneren ondanks het niet goed functioneren van één of meer subsystemen.

Availability Management heeft een dominante rol in de realisatie van het aspect beschikbaarheid. In de ITIL-definitie van beveiliging valt beschikbaarheid dan ook niet onder het proces Security Management. Dit lijkt echter meer een historisch feit dan een bewuste keuze te zijn.

Aangezien vele beveiligingsmaatregelen zowel ten goede van beschikbaarheid als van de andere beveiligingsaspecten vertrouwelijkheid en integriteit kunnen komen, is afstemming over de te treffen maatregelen tussen Availability Management en Security Management noodzakelijk.

Capacity Management

Capacity Management is verantwoordelijk voor de optimale inzet van IT-middelen zoals dat met de opdrachtgever is overeengekomen. De prestatie-eisen worden afgeleid uit de kwalitatieve en kwantitatieve normen die binnen het proces Service Level Management opgesteld worden.
Bijna alle activiteiten binnen het proces Capacity Management hebben een relatie met het aspect beschikbaarheid:
* *prestatiebeheer:* het monitoren en verbeteren van prestaties ten aanzien van doorvoercapaciteit en responstijden;
* *middelenbeheer:* het bieden van inzicht in de IT-infrastructuur en het gebruik hiervan;
* *vraagbeheer:* een sturende activiteit om het gebruik van IT-diensten te beïnvloeden;
* *werklastbeheer:* bepaalt en bewaakt dat wat een systeem te verwerken krijgt als gevolg van het verwerken van applicaties;
* *applicatiedimensionering:* begroot de voor een applicatie benodigde middelen;
* *modellering:* met behulp van modellen is het mogelijk een aantal beveiligingsscenario's op te stellen en 'what if'-analyses uit te voeren.

Capacity Management heeft in eerste instantie een relatie met Availability Management, en daardoor ook met Security Management.

Contingency planning

Contingency planning zorgt ervoor dat, wanneer zich (toch) een calamiteit heeft voorgedaan, de gevolgen hiervan voor de IT-dienstverlening beperkt blijven tot een met de klant overeengekomen niveau. Het motto is: 'Een calamiteit hoeft nog geen ramp te worden'. Eén van de belangrijkste activiteiten is het opstellen, onderhouden, implementeren en testen van het uitwijkplan. Vanwege de beveiligingsaspecten van dit onderwerp zijn er banden met Security Management.

Het proces Security Management

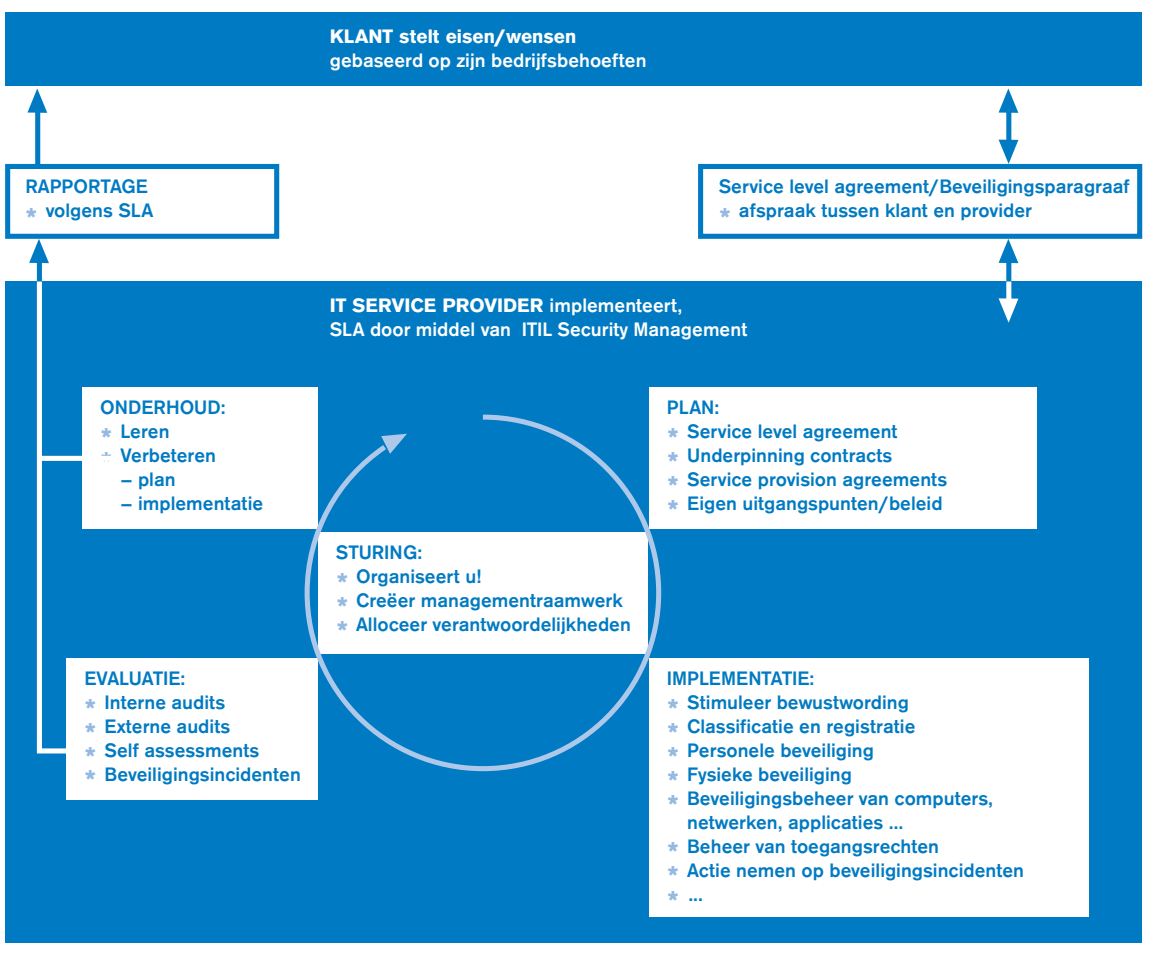
In de vorige paragraaf zijn de relaties van Security Management met de andere processen aangegeven. In deze paragraaf komen de activiteiten naar voren die ofwel door Security Management zelf worden uitgevoerd, ofwel waarvoor Security Management de aansturing verzorgt ten behoeve van de implementatie binnen een ander proces.

Figuur 7 geeft de managementcyclus voor Security Management. Rechtsboven vormen de eisen van de klant de invoer voor het proces. Deze eisen worden vertaald in de te leveren beveiligingsdiensten en -kwaliteit in de beveiligingsparagraaf van de service level agreement (SLA). De service provider detailleert deze afspraken naar zijn organisatie in de vorm van een beveiligingsplan (waarin de beveiligingsnormen of operational level agreements zijn vastgelegd). Dat plan wordt geïmplementeerd en deze implementatie wordt geëvalueerd. Vervolgens vindt onderhoud plaats op zowel het plan als de implementatie daarvan. Over de activiteiten wordt gerapporteerd aan de klant. De cyclus sluit hier zowel bij de klant als bij de provider. Ten eerste kan de klant op basis van deze rapportages zijn eisen en wensen aanpassen. Ten tweede kan de service provider op basis van zijn bevindingen zijn plan of de implementatie bijstellen, dan wel aansturen op aanpassing van de afspraken in de SLA. In het midden is de 'sturing' zelf aangegeven.

Vanuit dit overzicht worden de activiteiten binnen het proces Security Management nader besproken.

Sturing – beleid en organisatie van de informatiebeveiliging

De activiteit 'Sturing', in het midden van de figuur, is het eerste subproces binnen het proces Security Management. 'Sturing' organiseert en beheerst het proces Security Management zelf. Dit omvat de organisatie van het beheerraamwerk voor informatiebeveiliging. Dit raamwerk definieert de subprocessen: hoe beveiligingsplannen totstandkomen, hoe deze worden geïmplementeerd, hoe



Figuur 7. Het proces Security Management.

de implementatie wordt geëvalueerd en hoe de resultaten van deze evaluaties vervolgens weer worden vertaald in de beveiligingsjaarplannen (de actieplannen). Tevens wordt gedefinieerd hoe de rapportage aan de klant plaatsvindt (via SLM).

'Sturing' definieert de subprocessen, de beveiligingsfuncties, de rollen en de verantwoordelijkheden. Tevens wordt de organisatiestructuur beschreven alsmede de rapportagelijnen en de 'bevels'-lijnen (wie geeft opdrachten aan wie; wie voert uit; hoe wordt gerapporteerd over de uitvoering).
Ook in de andere ITIL-processen is een subproces 'Sturing' aanwezig. Deze sturingsactiviteiten hangen met elkaar samen. Daartoe zijn de verschillende managers van de processen onderling georganiseerd.

Onderstaande maatregelen uit de Code voor Informatiebeveiliging worden geïmplementeerd binnen het subproces 'Sturing'.
* Beleid:
– ontwikkelen en doen implementeren van beleid (relaties met andere vormen van beleid);
– doelstellingen, algemene principes en belang;
– beschrijven deelprocessen;
– functies en verantwoordelijken voor deelprocessen;
– samenhang met andere ITIL-processen, organisatie hiervan;
– algemene verantwoordelijkheden van medewerkers;
– hoe om te gaan met beveiligingsincidenten.
* Organisatie van de informatiebeveiliging:
– opzet managementkader;
– organisatiestructuur;
– nadere toekenning van verantwoordelijkheden;
– inrichting 'Stuurgroep informatiebeveiliging';
– coördinatie van informatiebeveiliging;
– afspraken over het instrumentarium (bijvoorbeeld voor risicoanalyse en het stimuleren van *awareness*);
– beschrijving van het autorisatieproces voor IT-voorzieningen (in afstemming met de klant);
– specialistisch advies;
– samenwerking tussen organisaties, interne en externe communicatie;
– onafhankelijke beoordeling (EDP-audit);
– uitgangspunten voor beveiliging van toegang door derden;
– informatiebeveiliging in contracten met derden.

Plan

Het subproces 'Plan' omvat onder meer de activiteiten die leiden tot de beveiligingsparagraaf in de SLA (in samenwerking met Service Level Management), alsmede de activiteiten in relatie tot de underpinning contracts (voorzover specifiek voor beveiliging). De algemeen geformuleerde doelstellingen in de SLA worden verfijnd en nader gespecificeerd in de vorm van operational level agreements. Deze OLA's kunnen worden gezien als de beveiligingsplannen per organisatie-eenheid binnen de organisatie van de service provider en als de specifieke beveiligingsplannen, bijvoorbeeld per specifiek IT-platform, per specifieke applicatie en per netwerk.

Behalve met de input van de SLA werkt het subproces 'Plan' ook met beleidsuitgangspunten van de service provider zelf (uit het subproces 'Sturing'). Voorbeelden van beleidsuitgangspunten kunnen zijn: 'Iedere gebruiker moet uniek identificeerbaar zijn', of 'Een basisniveau aan beveiliging wordt altijd geboden en aan alle klanten'.

OLA's kunnen worden gezien als beveiligingsplannen per organisatie-eenheid.

De operational level agreements voor informatiebeveiliging (de specifieke beveiligingsplannen) worden opgesteld en geïmplementeerd volgens de normale route. Dat betekent dat indien activiteiten binnen andere processen zijn gewenst, afstemming met deze processen plaatsvindt. Indien wijzigingen in de IT-infrastructuur gewenst zijn, dan komen deze alleen tot stand via het Change Management-proces. Security Management levert hiervoor de input. De Change Manager is verantwoordelijk voor het Change Management-proces zelf.

Dit subproces wordt afgestemd met het proces Service Level Management. Dit in verband met het opstellen van, het onderhouden van en het voldoen aan de beveiligingsparagraaf van de SLA. De Service Level Manager is voor deze afstemming verantwoordelijk.

In de SLA dienen de beveiligingseisen te worden gespecificeerd, voorzover mogelijk in meetbare termen. Een SLA is een formeel contract tussen de klant (een bedrijf) en de IT-service provider. In de beveiligingsparagraaf dient te worden zeker gesteld dat aan alle beveiligingseisen en -normen van de klant op een *controleerbare* wijze kan worden voldaan. Overigens wordt in het boek uitgebreid ingegaan op aandachtspunten voor de beveiligingsparagraaf in de SLA en de wijze waarop SLA's en OLA's totstandkomen.

Implementatie

Het subproces 'Implementatie' zorgt ervoor dat alle maatregelen zoals gespecificeerd in de plannen worden geïmplementeerd. Merk op dat binnen dit proces geen maatregelen worden gedefinieerd of gewijzigd. Dat vindt plaats via het proces Change Management, in afstemming met het subproces 'Plan'. Hieronder is een checklist opgenomen.
* Classificatie en beheersing van IT-hulpmiddelen:
– leveren van input voor het onderhoud van CI's in de CMDB;
– classificatie volgens afgesproken richtlijnen.
* Personele beveiliging:
– taken en verantwoordelijkheden in functiebeschrijvingen;
– screening;
– geheimhoudingsverklaringen personeel;
– opleiding en training;
– richtlijnen voor personeel voor de omgang met beveiligingsincidenten en geconstateerde zwakheden in de beveiliging;
– disciplinaire maatregelen;
– stimuleren van beveiligingsbewustzijn.

* Veilig beheer:
– implementatie van verantwoordelijkheden, implementatie van functiescheiding;
– schriftelijke bedieningsprocedures;
– huisregels (*house keeping)*;
– beveiliging volgt de gehele levenscyclus: richtlijnen voor beveiliging tijdens systeemontwikkeling, testen, acceptatie, de operationele fase, onderhoud tot en met uitfasering;
– scheiding van de ontwikkel- en testomgeving van de productieomgeving;
– procedures rond incidentafhandeling (uit te voeren binnen het proces Incident Management);
– implementatie van uitwijkvoorzieningen;
– input leveren voor Change Management;
– implementatie van viruscontrole;
– implementatie van specifieke maatregelen voor beheer van computers, applicaties, netwerken en netwerkdiensten;
– behandeling en beveiliging van informatiedragers.
* Toegangsbeveiliging:
– implementatie van het beleid voor toegang en toegangsbeheersing;
– onderhoud van toegangsrechten van gebruikers (en applicaties) tot netwerken, netwerkdiensten, computers en applicaties;
– onderhoud van beveiligingsscheidingen in de netwerken (firewalls, inbelfaciliteiten, bridges en routers);
– implementatie van maatregelen rond identificatie en authenticatie van computersystemen, werkstations en PC's in het netwerk.

Audit en evaluatie

Onafhankelijke evaluatie van de implementatie van de geplande maatregelen is essentieel. Deze evaluatie is noodzakelijk om het eigen functioneren te kunnen waarderen. Deze evaluatie is ook noodzakelijk voor de klanten en eventuele derde partijen. De resultaten van het subproces 'Evaluatie' worden gebruikt voor het onderhouden van de afgesproken maatregelen (in afstemming met de klant) en de implementatie zelf. Evaluatieresultaten kunnen aanleiding geven tot de wens wijzigingen te realiseren. Dan wordt een Request For Change (RFC) gedefinieerd en aangeboden aan het Change Management-proces.

Drie soorten evaluaties worden onderscheiden:
* *self assessments*; grotendeels uitgevoerd binnen de lijnorganisatie van de processen zelf;
* *interne audits*; uitgevoerd door interne EDP-auditors;
* *externe audits*; uitgevoerd door externe, nog meer onafhankelijke EDP-auditors.

Merk op dat audits (dus afgezien van self assessments) niet worden uitgevoerd door dezelfde medewerkers als in de andere subprocessen. Dit in verband met de noodzakelijke functiescheiding. Mogelijk worden voor audits medewerkers van de afdeling Interne Controle ingezet.

Verder vindt uiteraard evaluatie plaats op basis van de gemelde beveiligingsincidenten.

De belangrijkste activiteiten zijn:
* verifiëren van de naleving van beveiligingsbeleid en implementatie van beveiligingsplannen;
* beveiligingscontrole op IT-systemen;
* opsporen en reageren op ongewenst gebruik van IT-voorzieningen;
* uitvoeren van de overige EDP-audits.

Onderhoud

Onderhoud aan beveiliging is noodzakelijk. Immers, de risico's zijn aan verandering onderhevig wegens veranderingen in de IT-infrastructuur, de organisatie en de bedrijfsprocessen. Het onderhoud aan de beveiliging betreft zowel het onderhoud aan de beveiligingsparagraaf van de SLA als aan de gedetailleerde beveiligingsplannen (operational level agreements).

Het onderhoud is gebaseerd op de resultaten van het evaluatie-subproces en inzicht in zich wijzigende risico's. Deze activiteit levert alleen voorstellen op. Deze voorstellen worden ofwel ingevoerd in het subproces 'Plan', ofwel worden meegenomen in het onderhoud van de SLA als geheel. In beide gevallen kunnen de voorstellen leiden tot opname van activiteiten in het beveiligingsjaarplan (actieplan).

Merk op dat de wijzigingen zelf het normale Change Management-proces volgen.

Rapportage

Rapportage is geen subproces maar een resultaat van andere subprocessen. Rapportage vindt plaats om verantwoording af te leggen over de geleverde beveiligingsdiensten, om relevante informatie te verstrekken over beveiliging aan de klanten, maar ook omdat rapportage veelal expliciet wordt afgesproken.

Rapportage is van groot belang, ook voor de service provider. De klant moet een correct beeld krijgen van de efficiëntie van de inspanningen (bijvoorbeeld met betrekking tot realisatie van de beveiligingsmaatregelen) en van de beveiligingsmaatregelen zelf. Ook krijgt de klant een rapportage over de beveiligingsincidenten.

Een niet-uitputtende lijst met rapportagemogelijkheden is hieronder opgenomen.

Mogelijke periodieke rapportages en te rapporteren gebeurtenissen:
* Rapportage over het subproces 'Plan':
– rapportage over mate van conformering aan SLA inclusief de afgesproken KPI's voor beveiliging;
– rapportage over underpinning contracts en eventuele problemen daarmee;
– rapportage over de operational level agreements (interne beveiligingsplannen) en eigen beleidsuitgangspunten (bijvoorbeeld baseline);
– rapportage over beveiligingsjaarplannen, actieplannen.
* Rapportage over het subproces 'Implementatie':
– statusoverzicht met betrekking tot de implementatie van informatiebeveiliging; hieronder de voortgang van de realisatie van het beveiligingsjaarplan, mogelijk het overzicht van geïmplementeerde en nog te implementeren maatregelen, opleiding, resultaten van aanvullende risicoanalyses, enz.;
– overzicht van beveiligingsincidenten en de reacties op deze incidenten – mogelijk in vergelijking met de vori-

ge rapportageperiode; identificatie van trends in incidenten;
- status van het bewustwordingsprogramma.

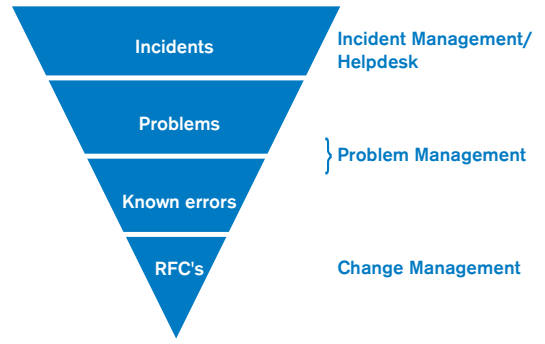
* Rapportage van het subproces 'Evaluatie':
- rapportage over het subproces zelf;
- resultaten van audits, reviews en interne assessments;
- waarschuwingen, identificatie van nieuwe dreigingen.

* Specifieke rapportages:
- Voor in de SLA vast te leggen beveiligingsincidenten dient de service provider, via de Service Level Manager, de Incident Manager en/of de Security Manager een direct kanaal te hebben naar een vertegenwoordiger van de klant, mogelijk de Corporate Information Security Officer. Voor deze communicatie in bijzondere gevallen dient een procedure te worden opgesteld.

Afgezien van de in het laatste geval genoemde uitzonderingssituaties, vinden rapportages plaats via het Service Level Management.

Tot slot: ITIL en beveiliging, samen een beheerst proces

Beveiliging en beheer zijn twee begrippen die zeer dicht bij elkaar staan. Het een kan niet zonder het ander. Beveiliging is afhankelijk van beheer, en beheer kan niet zonder goede beveiliging.



Figuur 8. ITIL – een goed beheerst proces biedt betere beveiliging.

Figuur 8 toont in de top een relatief groot aantal incidenten, waarbij de beveiligingsincidenten moeten worden herkend door Incident Management. Op ernstige incidenten is een passende reactie nodig. Daarnaast ontstaat inzicht in de effectiviteit van de beveiligingsmaatregelen op basis van een totaaloverzicht van alle beveiligingsincidenten. Problem Management neemt die zaken over die niet direct op te lossen zijn en lost ofwel het probleem op, rekening houdend met de randvoorwaarden aan beveiliging die de SLA en het basisbeveiligingsniveau stellen, ofwel identificeert een known error. Vervolgens volgt het proces Change Management, dat op basis van wijzigingsvoorstellen (RFC's) op beheerste wijze aanpassingen verzorgt in de IT-infrastructuur. Onderdeel van deze beheersing is dat tevens de noodzakelijke beveiligingsmaatregelen worden getroffen. De organisatie van de beveiligingsactiviteiten is de verantwoordelijkheid van Security Management.

Omdat met het gebruik van ITIL een beheerst proces ontstaat, zullen ook minder fouten in beheer en beveiliging ontstaan. En dat is een groot winstpunt voor beveiliging.

Literatuur

ITIL Security Management is gebaseerd op de Code voor Informatiebeveiliging:
Code of Practice for Information Security Management, draft version 2 BS7799:1999 (final).

Het ITIL-boek *Security Management* verschijnt midden 1999. Dit artikel gaat uit van de laatste conceptversie:
Security Management, final draft version 1.4a, January 1999, CCTA / BSI / DISC.