GvIB Expertbrief – September 2005
ISSN 1872-4876, Jaargang 1 – Nr. 2

Security Management KPI's
Van Kale Proces Informatie naar relevante stuurinformatie

Henk Bel

Bart Bokhorst

Lex Dunn

Ben Elsinga

Ronald van Erven

Hotze de Jong

Karin van de Kerkhof

Tonne Mulder

Fred van Noord

Ernst Oud

Frank van Vonderen

De aanleiding van deze expertbrief is de groeiende behoefte aan meetbaarheid van Security Management. Veel gepubliceerde meetbenaderingen zijn gebaseerd op checklisten afgeleid van beveiligingsstandaarden. Ze zijn vaak erg abstract en blijken in de praktijk moeilijk implementeerbaar. Het verzamelen van de juiste informatie vraagt om een behoorlijke inspanning waarbij vaak experts nodig zijn om vertaalslagen te maken. De expertgroep vraagt zich af of het mogelijk is zonder veel extra inspanning objectieve Key Performance Indicatoren (KPI's) af te leiden uit een procesmatige benadering van beveiliging. En zijn beide benaderingen ten opzichte van elkaar te positioneren?

http://www.gvib.nl/
✉ expertbrief@gvib.nl

2

INTRODUCTIE SECURITY MANAGEMENT KPI'S

De aanleiding van deze expertbrief is de groeiende behoefte aan meetbaarheid van Security Management. Veel gepubliceerde meetbenaderingen zijn gebaseerd op checklisten afgeleid van beveiligingsstandaarden als Cobit of ISO17799. Ze zijn vaak erg abstract en blijken in de praktijk moeilijk implementeerbaar of de meetgegevens leveren geen relevante stuurinformatie. Het verzamelen van de juiste informatie vraagt om een behoorlijke inspanning waarbij vaak experts nodig zijn om vertaalslagen te maken. De expertgroep vraagt zich af of het mogelijk is zonder veel extra inspanning objectieve en direct bruikbare Key Performance Indicatoren af te leiden uit een procesmatige benadering van beveiliging. En zijn beide benaderingen ten opzichte van elkaar te positioneren? Deze expertbrief is een eerste stap om een denkproces hierover op gang te brengen.

De behoefte aan KPI's is helder. In toenemende mate vereisen nieuwe wet- en regelgeving zoals de Sarbanes Oxley Act (SOX) adequate 'corporate governance'. Om aan te kunnen tonen dat een organisatie zijn processen beheerst en 'in control' is moet hierover regelmatig worden gemeten en gerapporteerd. Resultaten kunnen worden gebruikt voor externe rapportage, maar zijn primair bedoeld voor bijsturing van interne processen. Duidelijk gedefinieerde KPI's kunnen bijdragen aan een verbeterde begripsvorming en communicatie tussen ICT afdelingen en het bedrijfsmanagement.
In het kader van corporate governance wordt Security Management steeds belangrijker en ook daarvoor is behoefte aan KPI's. De in het najaar van 2005 vrij te geven nieuwe ISO standaard afgeleid van de BS7799 deel 2, stuurt eveneens aan op het definiëren van security management KPI's.

De praktijk leert dat het definiëren van bruikbare security management KPI's niet zo eenvoudig is en dat veel organisaties hiermee worstelen. Daarom is het interessant om de praktijk ervaringen nader onder de loep te nemen en hierbij een aantal kritische vragen te stellen. Is het mogelijk enige lijn te ontdekken in de warboel van security gerelateerde KPI's? Voldoen de huidige KPI's wel aan de informatiebehoefte van de verschillende doelgroepen? Zo niet, wat is de reden? Wat zijn eigenlijk de stuurvariabelen in de verschillende volwassenheidsfases van Security Management? Welke KPI's blijken effectief in de praktijk? Het verzamelen van meetgegevens over Security Management blijkt lastiger dan bij andere ITIL processen omdat het security management proces op een hoger abstractieniveau is gedefinieerd. Ook is de betrouwbaarheid van meetgegevens sterk afhankelijk van de kwaliteit van de basis processen waarvan de securityniveau moet worden beheerst.

Het verzamelen en interpreteren van gegevens kost bij elke rapportageslag weer een flinke inspanning en is daarmee een bron van kosten. Een van de uitdagingen is dan ook te onderzoeken of het mogelijk is met weinig inspanning en kosten KPI's af te leiden uit dagelijkse security management processen, zoals incidentafhandeling en applicatie change management.

Een brede ervaringsgroep van security experts van het Genootschap voor Informatiebeveiligers en het Platform Informatiebeveiliging heeft aan de hand van bovenstaande vragen en op basis van eigen ervaringen de huidige praktijk in kaart gebracht. Gezocht is naar randvoorwaarden en basisfactoren die de effectiviteit van KPI's bepalen en naar de grote lijnen hoe deze KPI's tot stand komen of zouden kunnen komen.
Deze publicatie is een weergave van de resultaten en is tot stand gekomen met medewerking van de op de voorpagina genoemde personen met Bart Bokhorst als probleemeigenaar, Ben Elsinga als facilitator, Tonne Mulder als co-facilitator en Henk Bel als ghostwriter.

DE ONDERZOEKSVRAGEN

De vragen die het expert team uiteindelijk wil beantwoorden, zijn:

- Is het mogelijk om een set objectieve meeteenheden voor security management te definiëren, die voortvloeien uit een procesmatige benadering van beveiliging? En wat is hun reikwijdte?
- Is het mogelijk de 'checklist' benadering en de 'proces' benadering ten opzichte van elkaar te positioneren?
- Is het mogelijk een raamwerk te maken met richtlijnen?

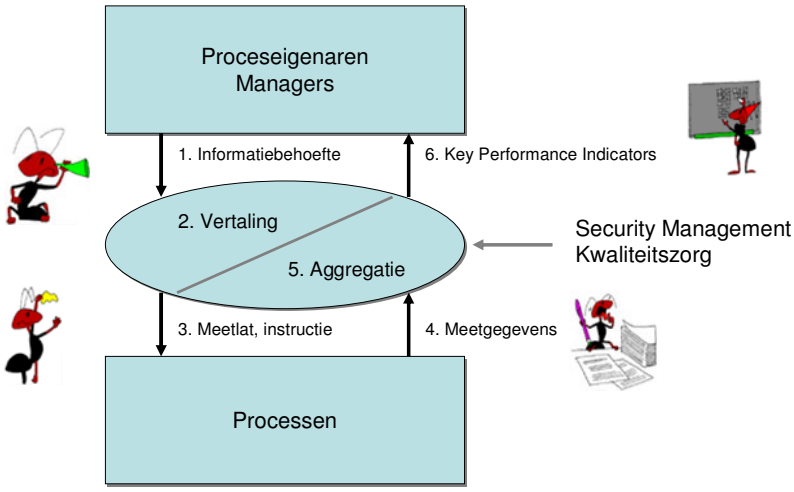
De expertgroep heeft zich nadrukkelijk niet ten doel gesteld een nieuw procesmodel te definiëren om KPI's daaraan te relateren. Over het meten aan security management processen zijn al veel publicaties verschenen o.a. door het NIST.
Het Plan Do Check Act model (Demming circle) zoals beschreven in BS7799 deel 2 biedt voldoende aanknopingspunten om KPI's te relateren aan een Information Security Management Systeem.
Ook wil de expertgroep geen antwoord geven op de vraag welke normen precies goed zijn en welke presentatievormen het beste zijn. De aanname is dat er normen zijn en dat de presentatievorm vrij te kiezen is.

RANDVOORWAARDEN VOOR DE DEFINITIE VAN KPI'S

Wie zijn de stakeholders en wat willen ze ermee sturen?

Met enige moeite kan een organisatie een enorme stroom van kale meetgegevens produceren. Het verwerken van alle gegevens kost echter veel tijd en daarom is het van belang selectief en gericht informatie te verzamelen, aansluitend bij een helder aangegeven informatiebehoefte.

Bijgaande figuur geeft een generiek beeld van het proces van informatieverzameling.



Om kosteneffectief meetgegevens te verzamelen en nuttige KPI's te definiëren moeten twee vragen helder beantwoord worden:

- Voor wie is de KPI bedoeld? Welke informatiebehoefte heeft deze persoon of rol?
- Welk proces of aspect moet gestuurd worden op basis van de KPI?

Het is weinig effectief een KPI te definiëren zonder daarbij voor ogen te hebben welk proces moet worden bijgestuurd op basis van de KPI en hoe deze bijsturing moet plaatsvinden.

Uiteindelijk moeten de kosten voor het rapporteren over de KPI wel gerechtvaardigd kunnen worden op basis van de beoogde voordelen van de processturing.
De KPI moet zodanig gedefinieerd zijn dat de persoon die verantwoordelijk is voor het bijsturen van een proces hiermee uit de voeten kan en het belang ervan ziet. Als de KPI niet op het juiste niveau is gedefinieerd aansluitend bij het te sturen proces, zal de KPI niet effectief gebruikt worden.

De informatiebehoefte van verschillende rollen in een organisatie verschilt sterk afhankelijk van het proces waar de betreffende rol verantwoordelijk voor is. KPI's voor functionarissen op strategisch of tactisch niveau zullen een ander karakter hebben dan die voor medewerkers op operationeel niveau. Het onderkennen van verschillende doelgroepen is belangrijk.

Informatiebeveiliging is voor veel proceseigenaren een lastig thema en zeker voor veel business managers. De praktijk leert dat proceseigenaren vaak moeite hebben de juiste informatiebehoefte te definiëren. Goede communicatie over de betekenis van een KPI is dan ook essentieel. Daarbij kan het proces om tot een definitie van een KPI te komen zelfs waardevoller zijn dan de exacte definitie van de KPI zelf.

De context is belangrijk

'**Meten is nog geen weten**' wanneer het gaat over KPI's. Zonder de context te kennen, zegt een kaal meetgegeven (Kale Proces Informatie) nog heel weinig over de gewenste sturing.

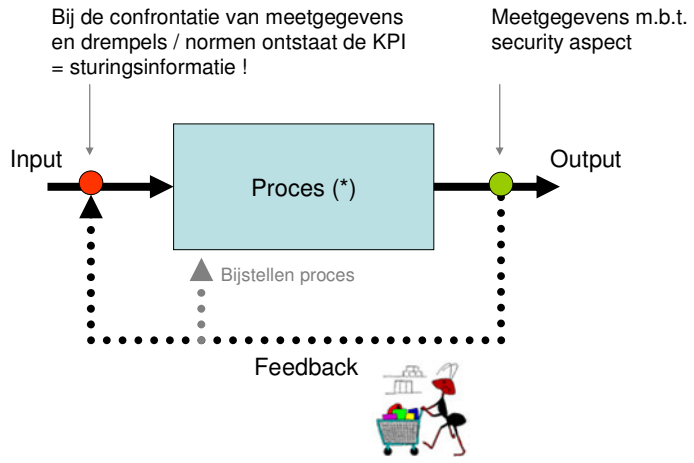
Een KPI zegt niets zonder de context te kennen!

Een mooi voorbeeld om deze problematiek toe te lichten betreft de registratie van het aantal incidenten. Een toename van het aantal geregistreerde incidenten kan verschillende reacties opleveren, zoals:

- Beveiligingsmaatregelen moeten worden aangescherpt want het aantal incidenten neemt toe.
- Doordat signalering en registratie verbeterd zijn, is een beter beeld te geven van het aantal incidenten dat plaatsvindt.

Om een KPI effectief te laten zijn moet de KPI vergezeld gaan met een *toelichting van de context en een uitleg van de trend.* De KPI moet *gerelateerd worden aan een norm om te kunnen sturen*. Ten slotte zullen veel proceseigenaren enorm geholpen worden in hun sturing als een advies wordt bijgevoegd welke maatregelen genomen zouden moeten.

Onderstaande figuur geeft nog eens weer hoe een KPI als proces stuurelement in de feedbackloop van een proces wordt gebruikt.



(*) met een te benoemen te meten security aspect

WELKE FACTOREN BEINVLOEDEN DE KEUZE VAN KPI'S?

De expertgroep heeft zich afgevraagd welke factoren van invloed zijn op de keuze van de soort KPI's en de effectiviteit ervan.

KPI's moeten aansluiten bij een business doel:

- KPI's moeten passen bij risico's of doelstellingen, die door de verschillende stakeholders worden onderkend. Als het (business) risico of de doelstelling niet helder is zal een KPI niet echt gaan leven.
  KPI's worden gemeten op maatregelen. Het is gewenst de KPI niet te specifiek te definiëren om te voorkomen dat de KPI de selectie van nog te implementeren maatregelen gaat beïnvloeden.
- Zijn de KPI's bedoeld voor intern gebruik of voor externe communicatie naar klanten, partners, aandeelhouder, belangenorganisaties, certificeringinstanties etc.? Moet worden aangesloten bij standaarden in de markt waardoor KPI's enigszins vergelijkbaar zijn tussen organisaties of is een organisatie geheel vrij om zijn eigen definitie te kiezen?
  N.B.: Zelfs wanneer uitgegaan wordt van hetzelfde kader (bijvoorbeeld Cobit) zal de vergelijkbaarheid van KPI's nooit optimaal zijn. Organisaties maken in de praktijk altijd een vertaalslag naar de eigen situatie.
  Een voorbeeld van gebruik van KPI's voor externe communicatie betreft de definitie van service levels bij outsourcing. Goed gedefinieerde KPI's helpen om meer grip te

krijgen op het niveau van de dienstverlening van de (outsourcing) partner. Rapportages over het aantal gescreende systeembeheerders, het aantal incidenten dat voorkomen is door preventieve maatregelen etc. geven meer zicht op de inspanningen van de dienstverlener dan een statement dat dienstverlening volgens best-effort zal plaatsvinden. De afnemende partij moet bij de definitie van KPI's zorgen zelf in de lead te blijven om te voorkomen dat zij door de andere partij KPI's opgedrongen krijgt die betekenisloos zijn en waar ze onvoldoende mee kan sturen.
Aangezien het definiëren van eenduidige security KPI's toch al lastig blijkt, geldt dit laatste hier in bijzondere mate.

- Hoe generiek of hoe specifiek moeten KPI's worden gedefinieerd? Zijn ze bruikbaar voor het gehele bedrijf of alleen voor een bedrijfsonderdeel?
  In een centraal geleide organisatie kunnen KPI veel generieker over verschillende processen heen worden gedefinieerd dan in een decentraal gestuurde organisatie. Immers in een decentraal georganiseerde organisatie zullen gelijksoortige processen meer verschillen en dus ook de meetbaarheid en stuurmogelijkheden. En KPI's moeten optimaal bij het proces aansluiten om effectief te zijn.
- Zijn KPI's stabiel tijdens de life-cycle van het te meten onderwerp of niet?
  Tijdens de life-cycle van een applicatie bijvoorbeeld verschuift de behoefte aan meetgegevens. KPI's die een rol spelen in de ontwikkelingsfase van applicaties zijn andere dan die in de operationele fase. Ook de doelgroep waaraan gerapporteerd wordt kan verschuiven tijdens de life-cycle.

Meetwaarden moeten betrouwbaar en zinvol zijn

- Welk maturity level heeft een organisatie of een proces en welke KPI's zijn nuttig voor dit maturity level? Het controleerbaar meten van bepaalde KPI's vereist reproduceerbaarheid en een vast stramien bij het uitvoeren van beheerprocessen. KPI's bedoeld voor het bijsturen van een beheerproces dat er (nog) niet is hebben weinig toegevoegde waarde. Het verzamelen van gedetailleerde meetgegevens en trend informatie over intrusions bijvoorbeeld heeft niet veel zin als een organisatie zijn basis incident management proces niet op orde heeft.
- De meetbaarheid van de gewenste informatie is belangrijk.
  Het ingevuld zijn van de beveiligingsparagraaf in een project fase document is eenvoudig te meten. Of de paragraaf kwalitatief voldoende is ingevuld is al veel lastiger te bepalen en levert zonder betrokkenheid van security experts waarschijnlijk geen juiste en objectieve informatie.
- In alle gevallen is de integriteit van metingen van groot belang. En de kosten van de meting moeten in balans zijn met het te bereiken doel. Vaak is tooling nodig om metingen over langere tijd kosteneffectief te houden, de integriteit te kunnen garanderen en rapportages consistent te houden. Bij handmatige aggregatie van gegevens is manipulatie mogelijk en kan de betrouwbaarheid niet altijd gegarandeerd worden.

Andere aspecten

- KPI's op verschillende niveaus moeten gecorreleerd zijn en een consistent beeld geven. Meerdere KPI's op een lager niveau kunnen samen vertaald worden naar één KPI op een hoger niveau. Omdat deze KPI's meestal bedoeld zijn voor een andere doelgroep en een hoger aggregatieniveau hebben, moet daarbij vaak ook het woordgebruik van de toelichting worden aangepast. Het woordgebruik moet aansluiten bij de belevingswereld en belangen van de doelgroep. Hoger management

zal bijvoorbeeld meer afgerekend worden op het percentage van applicatie ontwikkelingsprojecten waarbij tijdig een risico analyse is uitgevoerd dan op de compleetheid en diepgang van de uitgevoerde analyse voor een specifiek ontwikkelproject.

- Naast standaard rapportage moet er een mechanisme zijn voor exceptie rapportage. Excepties zijn belangrijk om mensen wakker te houden. Bij exceptierapportages is het vaak erg effectief om '**de blote waarheid**' te vermelden. Laat de werkvloer spreken en probeer de werkelijkheid niet mooier voor te stellen dan hij is. Als bijvoorbeeld het management van een afdeling incidenten die structureel optreden niet aanpakt en hierover in rapportages vaag blijft, kan het handig zijn een incident met meer dan gemiddelde impact nadrukkelijk 'uit te vergroten'. Zorgvuldigheid ten aanzien van bekend worden van gevoelige informatie blijft daarbij belangrijk.
- De kans dat security management KPI's effectief gebruikt worden is het grootst indien wordt aangesloten bij processen waarbij men al gewend is te rapporteren over andere kwaliteitsaspecten door middel van KPI's.
  Dit pleit er voor Security Management KPI's zoveel mogelijk vanuit de proces benadering te definiëren en te zorgen dat deze KPI's zoveel mogelijk worden ingebouwd in processen waar beveiliging aan de orde is, zoals incident management en change management.

DEFINITIE VAN KPI'S: HOE BEGINNEN?

Als een organisatie wil beginnen met het definiëren van KPI's kan zij op hoofdlijnen twee benaderingen kiezen, de top-down benadering waarbij eerst management commitment moet worden verkregen en de bottom-up benadering waarbij initiële rapportages op basis van aanwezige meetgegevens de prikkel zijn om meer en scherper te gaan rapporteren.

Top-down
Als voorbeeld is hier gekozen voor de Security Metrics Guide for Information Security van het NIST dat een model weergeeft met een top-down benadering. De onderstaande figuur geeft een component model weer, waarbij gesteld wordt dat alle componenten ingevuld moeten worden bij het opzetten van een effectief security metrics systeem.
De basis en startpunt in het model is het verkrijgen van een sterk top-level management commitment. Vervolgens moeten policies en meetgegevens worden gedefinieerd.

De werkgroep deelt deze visie maar ten dele en is van mening dat deze benadering lang niet altijd optimaal is.

De top-down benadering zal met name werken als er grote externe druk bestaat op het management, zoals bij het tijdig compliant zijn met de SOX wetgeving. Dit is alleen binnen korte termijn te realiseren met voldoende management commitment. Deze aanpak zal in bijna alle gevallen gebaseerd zijn op checklisten uit bestaande modellen als Cobit.

Maar zoals eerder aangegeven, leert de praktijk dat proceseigenaren het lastig vinden om de juiste informatiebehoefte te definiëren voor KPI's. De kans is groot dat het hele proces van KPI definitie veel te lang gaat duren, het hele bouwwerk te complex en te theoretisch wordt, veel geld kost, tot grote frustratie leidt en uiteindelijk op niets uitloopt.

Bottom-up
Een alternatieve benadering is om 'maar gewoon ergens te beginnen' met het presenteren van eenvoudige te verkrijgen meetresultaten uit operationele processen. Op deze manier wordt het management bewust gemaakt dat er interessante informatie uit de processen gerapporteerd kan worden waar op gestuurd kan worden. Initieel zal de geboden informatie niet goed overeenkomen met de informatiebehoefte van de proceseigenaar, maar het voorstellingsvermogen van de proceseigenaar zal geprikkeld worden en hij zal beter in staat zijn een aangepaste KPI te definiëren die meer aansluit bij zijn behoefte.
Door middel van een iteratief proces kunnen KPI's telkens verbeterd worden. Belangrijk bij deze bottom-up benadering is dat verwachtingen goed gemanaged worden om te voorkomen dat de proceseigenaar voortijdig afhaakt en zijn vertrouwen verliest.

N.B. Opgemerkt dient te worden dat ook bij een top-down benadering vaak meerdere iteratieslagen nodig zijn om bruikbare KPI's te definiëren. Veel bedrijven die via de top-down benadering SOX rapportages afdwingen binnen hun organisatie ervaren dat. Ook daarbij is het risico aanwezig dat proceseigenaren hun vertrouwen verliezen als ze zien dat enorme rapportage inspanning die ze moeten doen niet snel genoeg tot bevredigende resultaten leidt.

De top-down methode heeft als risico dat het rapporteren veel tijd gaat kosten omdat het meten niet op een natuurlijke manier aansluit bij bestaande processen. De bottom-up methode heeft als risico dat KPI's vooral op operationeel niveau stuurinformatie opleveren, maar onvoldoende op tactisch en strategisch niveau voor het hogere management.

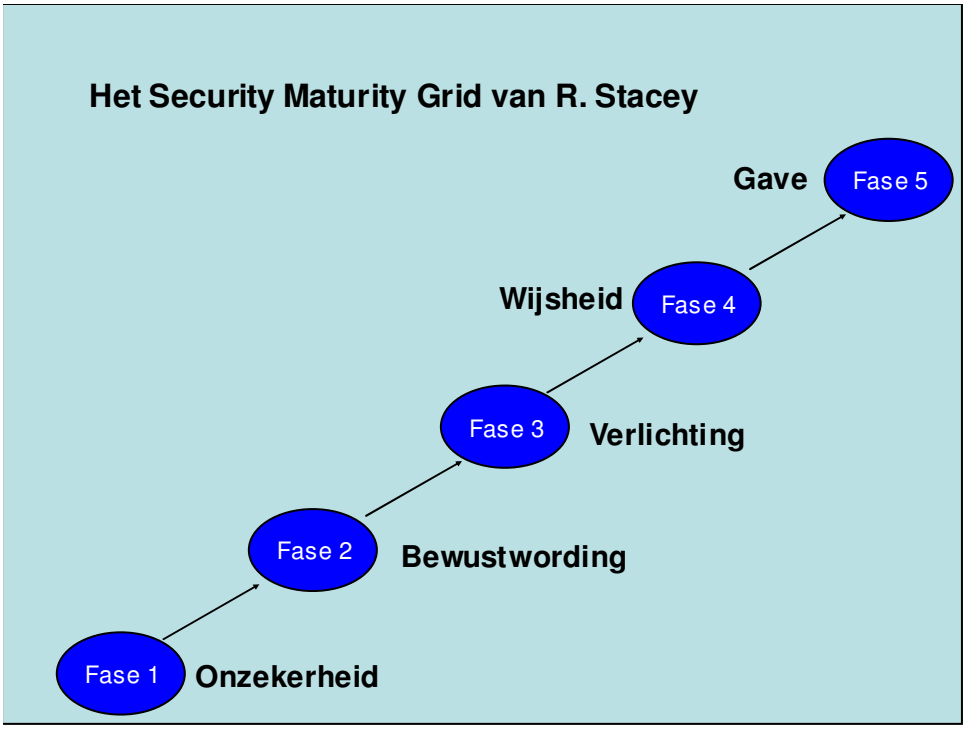
Simpel stappenplan voor bottom-up benadering

Voor organisaties die niet met Security KPI's werken en waar het management niet vraagt om security KPI's, stelt de expertgroep voor de bottom-up methode te kiezen. Daarbij kan het volgende stappenplan een handige leidraad zijn:

1	[Optioneel] Bepaal security maturity bijvoorbeeld aan de hand van security model van Stacey (zie onder)
2	Houdt registraties bij: • Incidenten (reactief) • Geïdentificeerde risico's (proactief) Classificeer deze, b.v. naar soort, object, afdeling etc. Denk daarbij ook buiten de IT afdeling
3	Personaliseer rapportage naar doelgroep Bijvoorbeeld: Juridische zaken, HRM, financiële zaken. Doel is bewustwording te vergoten
4	Toelichten rapportages per deelgebied - Consequenties aangeven per verantwoordelijkheidsgebied Refereer aan schade tabel, waarin schadecategorieën gedefinieerd staan
5	Bouw dit uit: • Formaliseer KPI's: Waar ligt de lat? • Stel trends vast • Geef sturing door trend te koppelen aan geadviseerde maatregelen.

Security Maturity modellen

Maturity modellen helpen een organisatie zichzelf een spiegel voor te houden om te bepalen hoe volwassen haar processen zijn. Per niveau worden typische kenmerken gegeven van de mate waarin een organisatie zijn processen beheerst. Het Security Maturity model van Stacey is een simpel model dat gebruikt kan worden op het vlak van security.



Onzekerheid	De onderneming begrijpt niet waarom het steeds problemen heeft met zijn informatie assets. Het heeft een hoge fout rate, haar informatie assets lijken kwetsbaar, onstabiel en niet nauwkeurig. Bedrijfsgeheimen lijken publiekelijk bekend.
Bewustwording	De onderneming in fase 2 begrijpt niet waarom het steeds problemen heeft met de security van zijn informatie assets. Het heeft een hoge incident rate, de informatie assets lijken kwetsbaar en haar geheimen lijken onbeschermd.
Verlichting	Door management commitment en gerichte ontwikkeling van beveiliging, identificeert, prioriteert en beveiligt de organisatie zijn informatie assets. De organisatie zoekt naar preventie in plaats van uitsluitend te reageren op incidenten als ze voorkomen.
Wijsheid	De informatiebeveiligingsactiviteiten van de onderneming zijn gepland, gebudgeteerd en routine. Door het gebruik van een ondernemingsspecifiek dreigingsmodel en gerichte risicoanalyses begrijpt de onderneming zijn kwetsbaarheden en beschermt ze haar informatie assets.
Gave	De onderneming in fase 5 weet dat haar informatie assets beschermd zijn en dat ze dat ook in de toekomst blijven. Deze assets blijven beschermd doordat de onderneming haar informatiebeveiligingsactiviteiten actief blijft bijsturen en ze haar strategieën optimaliseert.

Uiteraard kunnen ook andere modellen gebruik worden zoals het security maturity model van Gartner.

CONCLUSIES EN VERVOLG

Ten aanzien van de onderzoeksvragen heeft de expertgroep nog weinig echte conclusies kunnen trekken.
Het is zeker mogelijk KPI's te definiëren die voorvloeien uit metingen aan bestaande security management processen. Hierbij is het echter nog onvoldoende duidelijk of en in hoeverre deze KPI's objectief meetbaar zijn en generiek betekenisvol zijn voor verschillende omgevingen.
In deze expertbrief is enigszins een onderlinge positionering aangegeven van de top-down 'checklist' benadering en de bottom-up 'proces' benadering met hun voor- en nadelen. Er is echter behoefte aan een verdere uitdieping van beide benaderingen.
Voor het definiëren van een raamwerk met richtlijnen voor KPI's in verschillende situaties is het nog te vroeg. Hiervoor zijn meer ervaringsgegevens nodig en is verdere verdieping gewenst.

Wel zijn in de discussie nuttige constateringen gedaan en pleit de expertgroep ervoor de proces gerichte bottom-up benadering verder uit te werken, omdat deze het meest natuurlijk aansluit op de processen in een organisatie. Omdat security op de langere termijn steeds meer een 'gewoon' kwaliteitsaspect zal worden is het wenselijk zoveel mogelijk aan te sluiten op kwaliteitsrapportages waar organisaties al mee bekend zijn.

De werkgroep realiseert zich dat het definiëren van Security KPI's nog in de kinderschoenen staat en dat deze expertbrief niet meer is dan een aanzet tot verdere discussie.

Belangrijke constateringen:

- Voorwaarde voor het definiëren van security KPI's is dat helder moet zijn wat de stuurvariabelen zijn in een organisatie en welke rol verantwoordelijk is voor deze sturing. KPI's moeten daarop aansluiten.
  De KPI moet zodanig gedefinieerd zijn dat de functionaris die verantwoordelijk is voor het bijsturen van een proces hiermee effectief kan sturen en het belang ervan ziet.
- Het is belangrijk te onderkennen dat verschillende doelgroepen verschillende informatiebehoefte hebben en dat er dus KPI's per doelgroep moeten zijn.
- Bij de keuze van KPI's moet het doel helder zijn, moet de organisatie een beeld hebben van zijn eigen security maturity level en moet vastgesteld worden of de KPI kosteneffectief, betrouwbaar en controleerbaar is.
- "Meten is nog geen weten". Een KPI zegt niets zonder de context te kennen.
- De twee hoofd benaderingen voor het definiëren van KPI's zoals toegelicht in dit artikel hebben beiden hun specifieke voordelen en nadelen. De keuze is mede afhankelijk van het doel (externe vergelijkbaarheid of uitsluitend interne processturing)
- Voor organisaties die nog geen security KPI's gedefinieerd hebben en waar weinig externe druk bestaat om ze te definiëren, lijkt de bottom-up methode handig om te starten en om zo mogelijk een aantal quick wins te realiseren.

12

Hoe verder?

Door de complexiteit van de materie en de beperkte tijd waarin dit onderwerp besproken is, zijn er nog vele vragen onbeantwoord gebleven:

- Zijn we in staat een raamwerk te maken met praktische richtlijnen?
- Een aantal valkuilen zijn genoemd. Welke valkuilen zijn er nog meer te onderkennen?
- Zijn er generieke KPIs te onderkennen die voor elke organisatie gelden?
- Kunnen we een top 10 vaststellen met KPIs die in de praktijk goed werken?
- Wat zijn de stuurvariabelen in de verschillende volwassenheidsfases van Security Management?
- Kunnen we KPI's koppelen aan de doelgroepen van het INK model?
- Kunnen audit processen sneller en goedkoper worden als er goede KPI's zijn gedefinieerd omdat de focus van het audit proces dan kan verschuiven naar het KPI meetproces? Kan het karakter van audits daarmee verschuiven van momentopname naar trajectcontrole?
  Of te wel: Van digitale flitskast naar trajectcontrole
  …. en we weten allemaal hoe effectief trajectcontrole is ☺

Dit artikel is niet meer dan een eerste aanzet om een brede discussie op gang te brengen, waarbij de input van zoveel mogelijk betrokken gewenst is. De expertgroep nodigt u dan ook uit om te reageren.

U kunt uw reactie op dit artikel sturen naar expertbrief@gvib.nl

Ook indien u deze expertbrief heeft kunnen waarderen stellen wij een e-mailtje op prijs!

LITERATUURLIJST

Voor het tot stand brengen van de expertbrief 'Security KPI's – Van Kale Proces Informatie naar relevante stuurinformatie' heeft de werkgroep de volgende literatuur geraadpleegd:

NIST, Secuirty Metrics Guide for Information Technology Systems

IT Governance Institute, *Cobit*

A Koot, *Enhanced Security Management*

A Koot, *Beveiliging: Balanceren tussen vraag en aanbod,* Informatiebeveiliging mei 2004

Ernst Oud, *Kosten en baten Informatiebeveiliging*, artikel Jaarboek 2002

A van Gils, Philips, *Meten op basis van Cobit*, presentatie GvIB 19 maart 2002

ISO, *ISO/IEC 1st WD24742 Information security management metrics and measurements,* 2004

Robert Veenstra, NFI, *Meten is weten, Evaluatie van Informatiebeveiliging, Balanced Scorecard*

GIGA Group, *A Balanced Scorecard for Security*

SABSA limited, *White paper Systems and Business Security Architcture*

Peter van der Wulp, Erasmus Universiteit, *referaat Het meten aan security*, KoSMoS

Ben Elsinga, Presentatie *Overwegingen en voorbeeld modellen/ kapstokken. KPI's ten bate van informatiebeveiliging*.

The Information Security Program Grid", Timothy R. Stacey, Data Security Management, Auerbach Publications 1996

14

APPENDIX GEBRUIKTE LICENTIEVORM

De expertbrief wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by-sa/2.5/

Deze pagina ziet er op het moment van schrijven als volgt uit:

creative commons

COMMONS DEED

Naamsvermelding-GelijkDelen 2.5

De gebruiker mag:

- het werk kopiëren, verspreiden, tonen en op- en uitvoeren
- afgeleide werken maken
- gebruik maken van het werk voor commerciële doeleinden

Onder de volgende voorwaarden:

BY: **Naamsvermelding**. De gebruiker dient de naam of andere aanduiding van de maker te vermelden.

Gelijk delen. Indien de gebruiker het werk bewerkt kan het daaruit ontstane werk uitsluitend krachtens dezelfde licentie als de onderhavige licentie worden verspreid.

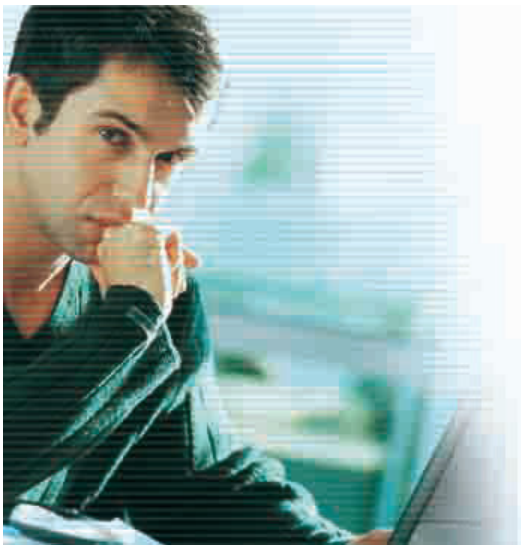
- Bij hergebruik of verspreiding dient de gebruiker de licentievoorwaarden van dit werk kenbaar te maken aan derden.
- De gebruiker mag uitsluitend afstand doen van een of meerdere van deze voorwaarden met voorafgaande toestemming van de rechthebbende.

Het voorgaande laat de wettelijke beperkingen op de intellectuele eigendomsrechten onverlet.

Dit is de vereenvoudigde (human-readable) versie van de volledige licentie.

Vrijwaring

WORDT LID VAN HET GVIB, SPEEL OP ZEKER EN BEVEILIG SAMEN...



Informatiebeveiliging is reeds jaren lang een noodzakelijk, spannend en dynamisch vakgebied. Vrijwel alle beroepen hebben meer dan ooit te maken met vertrouwelijkheid, beschikbaarheid en integriteit van informatie. of u nu als directeur, manager, adviseur of programmeur werkzaam bent. Het Genootschap van Informatie Beveiligers (GvIB) kan u behulpzaam zijn bij al uw vraagstukken op het gebied van informatiebeveiliging.

Wat is het Genootschap van Informatie Beveiligers?
Het GvIB is een open, breed samengesteld genootschap waarin professionals elkaar vinden om professioneel inhoud te geven aan informatiebeveiliging, door het uitwisselen van ideeën, informatie, kennis, inzichten en vooral veel praktijkervaring.

Wat willen wij bereiken?
Wij willen de fysieke, (systeem)technische & organisatorische beveiliging van gegevens en van de gegevensverwerkende middelen tegen inbreuken van binnenuit of buitenaf bevorderen. Ook willen wij de uitwisseling van kennis en ervaring en het netwerken van de in het vakgebied werkzame personen bevorderen. Bijvoorbeeld door middel van deze expertbrief.

De doelgroep
De doelgroep van het GvIB omvat iedereen, die door studie of beroepshalve te maken heeft met informatiebeveiliging, of hiervoor een bijzondere belangstelling heeft. Het snel groeiende ledenbestand kent vele disciplines zoals studenten, informatiearchitecten, technici, managers, organisatieadviseurs, juristen, beveiligingsfunctionarissen en ICT auditors. Onze leden komen voort uit alle mogelijke opleidingen, bedrijven, overheden, organisaties en leveranciers.

Voor de diverse soorten van lidmaatschap verwijzen wij u gaarne naar:

http://www.gvib.nl/afy_info_ID_1022.htm