PvIB Expertbrief – Mei 2010
ISSN 1872-4876, jaargang 6 – Nr. 2

Integrale beveiliging

Douwe de Jong

Mark Hoevers

Lambert Hofstra

Alf Moens

Fred van Noord

Ernst Oud

Joost Pol

Linda van Rens

Kelvin Rorive

Marcel Schrager

Integrale beveiliging is al jarenlang een veel gehoord begrip. Maar wat wordt er mee bedoeld en wat is het effect? Is er sprake van een hype, een modekreet, een verkoopargument of bittere noodzaak? Beveiligingsexperts hebben hun krachten gebundeld om hierover duidelijkheid te verschaffen en een bijdrage te leveren om de noodzaak van een integrale aanpak van beveiliging vast te stellen en om aan te geven wat nodig is om deze tot een succes te maken.

De focus van deze Expertbrief lijkt te liggen op integratie vanuit de informatiebeveiligingsdiscipline, alleen al omdat wordt gesproken over beveiliging en niet over veiligheid. Maar omdat het in deze expertbrief vooral om het integratieaspect gaat, het samenwerken met aanpalende disciplines, is dit document van toepassing op alle integratie-initiatieven en daarmee ook op integrale veiligheid.

Pagina

2 **INLEIDING**
- Aanleiding
- Probleemstelling
- Totstandkoming expertbrief
- Uitingen van een integrale benadering

5 **ONDERZOEKSVRAGEN**
- Belemmeringen integratie
- Benefits integrale beveiliging
- Succes integrale beveiliging

8 **WERKVELD INTEGRALE BEVEILIGING**
- Risicoprofiel
- Enterprise Risk Officer

10 **CONCLUSIE**
- Vervolgonderzoek

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

2 INLEIDING

Aanleiding

Aanleiding voor de Expertbrief Integrale Beveiliging is de hernieuwde belangstelling vanuit de markt en de universitaire wereld naar eerdere (2003!) publicaties over de integratie van logische en fysieke beveiliging. Daarnaast zijn er tijdens de Infosecurity.nl beurs najaar 2009 enkele voordrachten gehouden over 'Security Convergence' waaruit het belang blijkt voor een integrale aanpak maar waar ook duidelijk wordt dat die aanpak gepaard gaat met grote uitdagingen en moeizame afwegingen.

Er is gekozen voor een Expertbrief omdat "Expertbrieven bedoeld zijn om snel een mening neer te zetten namens de 'experts' van de IB verenigingen over onderwerpen die leven onder de leden, de markt of de maatschappij" (bron PvIB website). Op deze website is tevens meer informatie te vinden over het proces om te komen tot een expertbrief en de verschillende expertbrieven die reeds zijn gepubliceerd.

Ter oriëntatie is onderstaande probleemstelling opgesteld.

Probleemstelling

Al eind negentiger jaren werd gesproken over integrale beveiliging en zijn initiatieven ontwikkeld om logische en fysieke beveiliging met elkaar te verbinden.

Toch is er in de huidige beveiligingspraktijk nog weinig van te merken. Individuele initiatieven zijn er nog steeds; op een enkel gebied, zoals bij toegangsbeheer, iets structureler maar bij nader inzoomen blijkt ook daar samenwerking niet vanzelfsprekend. Fysieke beveiligers zijn huiverig om de technische infrastructuur aan te laten sluiten op de ict-infrastructuren en ict-ers lijken deze scheiding wel prima te vinden.

Er zijn ook hoopgevende initiatieven. In opleidingen worden fysieke en logische beveiligingsmodules steeds meer gekoppeld; je ziet vakdocenten van verschillende beveiligingsdisciplines binnen eenzelfde module lesgeven. In het lezingencircuit zie je regelmatig integratieaspecten op de agenda staan. De Securitybeurs 2009 had twee lezingen met als titel Security Convergence; maar ook dan blijkt het integreren van beveiligingsdisciplines een weg geplaveid met mentale vooroordelen en technische hindernissen. Bij beveiligingsadviezen wordt steeds vaker gesproken over een integrale aanpak maar het gras is minder groen dan het lijkt; te vaak wordt integraal gebruikt als modekreet om aan te geven dat met de tijd wordt meegegaan maar bij nadere beschouwing dekt de vlag de lading niet.

Via de zogenaamde expertaanpak van het PvIB wordt beoogd inzicht te krijgen in nut en noodzaak om verschillende beveiligingsdisciplines samen te laten werken met zicht op de drempels die daarvoor moeten worden beslecht. Tevens zullen praktische aanbevelingen worden gedaan om de integrale benadering in beveiligingsland een impuls te geven. En volgens onderstaand citaat ligt een eerste resultaat al binnen handbereik!

> *"Op het moment dat een aantal participanten het initiatief nemen om met elkaar te gaan praten over een mogelijke integratie van beveiligingsactiviteiten is in feite het*

eerste resultaat al binnen. Het geeft immers aan dat men bereid is om in breder perspectief te kijken naar mogelijkheden om gezamenlijke problemen aan te pakken".

Dit schrijft Jan Seij september 2000 in de reader post-HBO-opleiding Integrale Veiligheid "Een integrale benadering van beveiliging; toekomst of utopie?".

Totstandkoming expertbrief
De expertgroep bestond uit 10 deelnemers, deels aangemeld na de oproep van het PvIB en deels gevraagd in verband met een evenwichtige vertegenwoordiging vanuit de fysieke, logische en organisatorische beveiligingsdisciplines. Ook de veiligheidssector is vertegenwoordigd.

De deelnemers is gevraagd documentatie op te sturen waarvan ze vinden dat het een bijdrage kan leveren aan de discussie. Het organisatiecomité van deze expertbrief heeft deze stukken beoordeeld, voorzien van leeswijzers en materiaal geselecteerd voor de expertbijeenkomst; zie bijlage A.

Woensdag 10 maart 2010 is de expertgroep bijeen geweest. De aanwezigen zijn begonnen met het uitwisselen van ervaring met de integrale benadering van het beveiligingsvraagstuk om zich daarna te richten op de onderzoeksvragen. Het bijzondere van de bijeenkomst is dat met het benoemen van belemmeringen en de te bereiken doelen min of meer 'als vanzelf' zich de oplossingsrichting aandient zoals die in deze Expertbrief wordt verwoord.

Uitingen van een integrale benadering
Ter oriëntatie wordt nader ingezoomd op de actualiteit van verschillende verschijningsvormen rond de integrale benadering van het beveiligingsvraagstuk.

Voor informatiebeveiligers is de ISO27001 de algemeen geaccepteerde beveiligingsnorm en hierin is uiteraard ook een paragraaf fysieke beveiliging opgenomen, echter primair gericht op de fysieke bescherming van ruimten waarin zich de ict-componenten bevinden. Het is afhankelijk van het blikveld van de beveiligingsspecialist wat dit in de praktijk betekent. Vooral bij overheidsinstellingen wordt in het beveiligingsbeleid vaak naast informatiebeveiliging expliciet aandacht gevraagd voor gebouwbeveiliging en soms zelfs veiligheid van het personeel. Voor de Nederlandse Politie is jaren geleden een Basisbeveiligingsniveau opgesteld met daarin een Leidraad Fysieke Beveiliging die een stuk verder gaat dan de ISO27002 en zich richt op de bescherming van de bijbehorende gebouwen en omgeving [17].

Fysieke beveiliging maakt in toenemende mate gebruik van ict-hulpmiddelen maar dat betekent niet dat als vanzelfsprekend de nodige aandacht wordt besteed aan bedreigingen die ontstaan vanuit die ict-componenten. En toch zijn er ook vanuit de discipline fysieke beveiliging initiatieven om daar waar er raakvlakken liggen, de link te leggen naar informatiebeveiliging. Daarvan twee voorbeelden: de Borg-regeling en DHM.
1) De BORG-regeling is gebaseerd op een eenvoudige en praktische risicoanalyse waarmee een beveiligingsniveau voor bouwkundige, organisatorische en electronische (OBE-) maatregelen kan worden bepaald. Vanuit een ad hoc werkgroep Integrale beveiliging is enkele jaren terug een voorstel gedaan om hierin het belang van de informatievoorziening mee te laten wegen en aan de OBE-maatregelen ook I- (informatiebeveiligings)maatregelen toe te voegen [18].

2) Net zoals voor informatiebeveiligers de Afhankelijkheids- en Kwetsbaarheidsanalyse een referentiekader is met in de praktijk een diversiteit aan toepassingen, is dat voor de fysieke beveiliging De Haagse Methodiek. Centraal in die methodiek staat weer de OBE-meetlat. Door daar de ict-component aan toe te voegen spreekt men over een integrale aanpak [2]. Maar een OBE"I"-meetlat maakt van DHM nog geen integrale beveiligingsmethodiek.

Integrale uitingen bij de veiligheidsdisciplines zijn bijvoorbeeld te vinden in het boek "Integrale Veiligheidszorgmanagement" van drs. Abraham de Zwart van 1998. De HBO-opleidingen "Integrale Veiligheid" of "Veiligheidsmanagement" besteden al jarenlang aandacht aan het complete beveiligingsspectrum. Voor zorginstellingen is sinds 2010 bij wet het Veiligheidsmanagementsysteem zorg (VMS-Z), ook wel het patiëntveiligheidssysteem genoemd, verplicht. In het normenkader voor dit VMS-Z wordt in paragraaf 1.3 'Identificatie risicovolle processen' expliciet gesproken over "het waarborgen van de privacy, het actueel houden van gegevens, de toegang tot gegevens en het gebruik maken van ICT" [7].

Een vermeldenswaardig aspect is de mate waarin de informatiebeveiliger geconfronteerd wordt met het feit dat andere beveiligheidsdisciplines een belangrijkere rol gaan opeisen en de aandacht voor informatiebeveiliging overschaduwen. Vanuit de veiligheidsdisciplines wordt onderkend dat informatiebeveilging bestaat en belangrijk is en "that's it". Doorgaans wordt het alleen genoemd als "derde" discipline maar zie je inhoudelijk niets terug in plannen of budgetten. De informatiebeveiliger moet noodgedwongen actief naar buiten om aansluiting bij de andere veiligheidsdisciplines te borgen, andersom gebeurt het niet.

Beveiliging versus veiligheid lijkt meer een traditioneel verschil dan substantieel anders. De bedoeling van integrale beveiliging is risico's te adresseren. Bij fysieke beveiliging (erg zichtbaar) en ICT beveiliging (erg nieuw, iets van de laatste 30 jaar...) is de bewustwording misschien wat groter. Veiligheid en veiligheidsbewustzijn op andere gebieden bestaat al veel langer, maar is nooit zo expliciet genoemd. Pas met bv. Basel-II worden expliciete eisen gesteld aan financiële buffers om risico's af te dekken, tot die tijd was het meer "common sense" en "best practice", daar werd niet over nagedacht.

In de inleiding is al aangegeven dat er steeds meer verzoeken uit de markt komen om beveiliging integraal te benaderen. De hier geschetste uitingsvormen van een integrale benadering overziende, is dat niet te verwonderen. Belangrijkste aanleiding voor de behoefte aan een integrale aanpak lijkt de toenemende overlap tussen de verschillende beveiligingsdisciplines en de groeiende aandacht voor risicobeheersing als gevolg van wet- en regelgeving (Memorandum DNB, Code Tabaksblat en Sarbanes Oxley).

ONDERZOEKSVRAGEN

De expertgroep heeft zich ten doel gesteld een antwoord te geven op de vraag:

“Hoe wordt integrale beveiliging een succes?”

Deze onderzoeksvraag is verder uitgewerkt aan de hand van de volgende deelvragen:
- Wat zijn de belemmeringen voor integratie?
- Wat zou integrale beveiliging moeten opleveren?

Deze vragen komen in de navolgende paragrafen aan de orde.

Wat zijn de belemmeringen voor integratie
Om het terrein te verkennen is begonnen met een inventarisatie van mogelijke belemmeringen en de te bereiken doelen. Alhoewel er veelvuldig wordt gesproken over integrale beveiliging en heel wat organisaties de intentie hebben beveiligingsaspecten integraal aan te pakken gaat dat vaak erg moeizaam. De door de expertgroep gesignaleerde belemmeringen worden beschreven vanuit de organisatie, de werkvloer en voortschrijdende technische ontwikkelingen.

Organisatorische belemmeringen
In veel organisaties wordt beveiliging nog gezien als de verantwoordelijkheid van de ICT-afdeling of van de facilitaire dienst. Dit staat een integrale aanpak in de weg. Het effect van dreigingen en de gevolgen van incidenten strekt zich meestal uit over meerdere afdelingen en heeft betrekking op meerdere processen. Welke proceseigenaar voelt zich verantwoordelijk? Of zijn proceseigenaren überhaupt niet benoemd? En als er in het gunstigste geval vanuit een integrale benadering maatregelen worden getroffen is de kans groot dat die verwateren omdat de verantwoordelijkheden niet duidelijk zijn belegd.

Integrale beveiligingsinitiatieven zijn per definitie afdelingoverschrijdend maar het middenmanagement is primair gefocused op haar eigen functionele eenheid en eigen (afgeleide) doelstellingen. Rekening houden met afdelingoverstijgende zaken biedt geen direct toegevoegde waarde aan het resultaat van de afdeling en het verdwijnt dan gemakkelijk op de achtergrond. Vele integratie-initiatieven stranden dan ook door een gebrek aan organisatiebrede visie van het topmanagement.

Dit leidt tot de situatie dat daar waar moet worden samengewerkt om tot een integrale benadering te komen, het gevaar groot is dat het resultaat eenzijdig en onevenwichtig wordt waardoor organisatiebrede risico’s niet voldoende worden weggenomen. Een veel gehoorde klacht is dat er door meerdere afdelingen tijd wordt geclaimd voor het beoordelen van vergelijkbare risico's (ineffectiviteit).

Belemmeringen op de werkvloer
Beveiligingsdisciplines die op de werkvloer met elkaar proberen samen te werken ondervinden vaak problemen als gevolg van kennis- en cultuurverschillen. Het is niet vanzelfsprekend dat bijvoorbeeld technische medewerkers, systeembeheerders of arbo-medewerkers met elkaar in gesprek gaan over een gezamenlijk beveiligingsvraagstuk. De opleidingen zijn niet met elkaar te vergelijken en er worden diverse terminologieën gebruikt. Denk aan de facilitair manager, verantwoordelijk voor fysieke beveiliging die de opleiding De Haagse Methodiek heeft gevolgd, de informatiebeveiliger die vertrouwd is met de

Afhankelijkheids- en Kwetsbaarheidsanalyse en de arbo-medewerker die vooral geschoold is in de sociale en safety aspecten van een organisatie. Ook de werkwijze kan zeer divers zijn, van praktijkgericht tot meer theoretisch. En medewerkers zijn vooral gefocused op hun eigen werkterrein.

Belemmeringen door toenemende complexiteit en specialisaties

Beveiligingsdisciplines zijn steeds meer afhankelijk van de techniek en de technologische ontwikkelingen zorgen voor een toenemende complexiteit en specialisaties. Een voorbeeld waarbij fysiek en logisch niet zonder elkaar kunnen is een CCTV systeem op basis van TCP/IP. De leverancier / specialist van het camerasysteem heeft veel verstand van onder andere de opstelling, beeldkwaliteit en robuustheid van de camera's. Steeds meer camera's kunnen worden aangesloten op het bedrijfsnetwerk. Dit is kosteneffectief en biedt mogelijkheden om de camerabeelden geautomatiseerd te analyseren, wat de meldkamerfunctie goedkoper kan maken. Maar het CCTV systeem is daarmee wel afhankelijk van de betrouwbaarheid van het bedrijfsnetwerk. Je hebt dan te maken met een aantal dilemma's zoals

- inbraakbeveiliging moet buiten kantoortijd optimaal werken terwijl ict-ers gewend zijn om onderhoudswerkzaamheden aan het kantoornetwerk juist buiten kantooruren uit te voeren
- hoe lang bewaar je camerabeelden? Verstoort de benodigde bandbreedte wellicht de beschikbaarheid van de transactiesystemen?
- fysieke beveiligers hebben toegang tot alle kantoren en beveiligde ruimtes, worden vaak ingehuurd, zijn ze gescreend?

Een ander voorbeeld waarbij innovatieve integrale beveiliging leidt tot extra complexiteit is het koppelen van logische toegang aan de fysieke locatie. Een medewerker kan niet op een computer inloggen als hij niet in ieder geval die dag bij de hoofdingang een toegangspas heeft aangeboden om het pand te betreden. Dit ondersteunt technisch het oneigenlijk gebruik van toegangspassen, maar vereist ook technische koppelingen tussen systemen en dus afstemming tussen diverse betrokken partijen.

Het zijn voorbeelden van technische mogelijkheden die pas zichtbaar worden als je over de grenzen van je eigen discipline heen kijkt. Ook al lijken technologische ontwikkelingen integratie te bevorderen en soms zelfs te versterken, dan moeten aanpalende disciplines daar wel op inspelen en is de échte uitdaging dit ook organisatorisch en cultureel in te bedden. Het dwingt afdelingen samen te werken die vanuit andere achtergronden zijn ontstaan en veelal verschillende denkwijzen (cultuur) hebben in relatie tot beveiliging of veiligheid, zie ook paragraaf organisatorische belemmeringen, Je ziet nu te vaak dat dit de belemmerende factoren zijn.

Samenvattend kan gesteld worden dat beperkte of gebrekkige communicatie de belangrijkste belemmerende factor is in het integratievraagstuk.

Wat zou integrale beveiliging moeten opleveren?

De vraag die hieraan voorafgaat is: "Waarom is beveiligen belangrijk en waarom zou je beveiliging integraal willen benaderen?" Je kunt stellen dat er wordt beveiligd om de continuïteit van een organisatie te garanderen. Onderdeel daarvan zijn onder andere:

- fysieke beveiliging (afschermen van objecten en onbevoegde indringing tegengaan);

- informatiebeveiliging (met aandacht voor betrouwbaarheidsaspecten voor de informatievoorziening);
- personele veiligheid (beschikbaarheid en welbevinden van medewerkers);
- financieel beheer (zorgdragen voor voldoende financiële middelen),

Integrale beveiliging zou moeten bewerkstelligen dat de verschillende beveiligingsmaatregelen vanuit de verschillende beveiligingsdisciplines de continuïteit van de bedrijfsvoering versterken. Maatregelen mogen elkaar niet overlappen, elkaar vooral niet tegenwerken en onderlinge prioriteiten moeten worden afgestemd. Sprinklers in de serverruimte zijn bijvoorbeeld vanuit fysieke beveiliging gezien zeer gewenst maar voor het beveiligen van ict-componenten een ramp. Beveiligingsmaatregelen als gevolg van de integrale benadering moeten op de werkvloer als logisch en vanzelfsprekend worden ervaren. Dit verbreedt het draagvlak, versterkt het beveiligingsbewustzijn en bevordert zelfregulering. Kortom, er is samenhang in beleid *en* uitvoering nodig zodat bedrijfsrisico's herkenbaar en beheersbaar worden.

Hoe wordt integrale beveiliging een succes?
Uit de hiervoor beschreven belemmeringen voor een integrale aanpak blijkt dat die vooral op het communicatieve vlak liggen. Eén van de mogelijkheden om de communicatie te bevorderen is het zoeken naar raakvlakken om die vervolgens uit te buiten. Uit het eerder genoemde CCTV-voorbeeld blijkt dat er op een coördinerend niveau kennis van elkaars diensten aanwezig moet zijn. Ook een organisatiebrede incidentregistratie is een prima platform om vanuit verschillende disciplines gezamenlijk te evalueren en te zoeken naar verbeterpunten. Er wordt al snel voordeel behaald als men meedenkt met andermans problemen, verder te kijken dan je eigen verantwoordelijkheid, op alle organisatieniveaus. Neem daarvoor de tijd en erken dat er een gewenningsfase nodig is.

De eerste stap is samenwerken. Weten dat de andere discipline bestaat. Er hoeft niet noodzakelijk een gemeenschappelijk document of aanpak te zijn, als je de raakvlakken of overlap maar identificeert en adresseert. Dus…

Integraal beveiligen begint met samenwerken!

Samenwerken lukt alleen als voor de verschillende afdelingen elkaars verantwoordelijkheid duidelijk is. Zowel voor fysieke als logische toegang mogen de afspraken met derden niet tegenstrijdig zijn. Beleg bijvoorbeeld contractbeheer op centraal niveau, inclusief controle/monitoring. Een gezamenlijke aanpak maar wel binnen strategisch afgestemde kaders. Hoe hoger in de hiërarchie hoe breder de verantwoordelijkheid en hoe beter de afstemming bestuurd kan worden. Een integrale benadering vergt een brede afstemming. Besluiten moeten op een voldoende hoog niveau worden gemaakt, wat meestal in de praktijk neerkomt op een strategisch niveau. Een integrale benadering kan niet zonder deze top-down aansturing.

Integraal beveiligen niet mogelijk zonder strategisch denken!

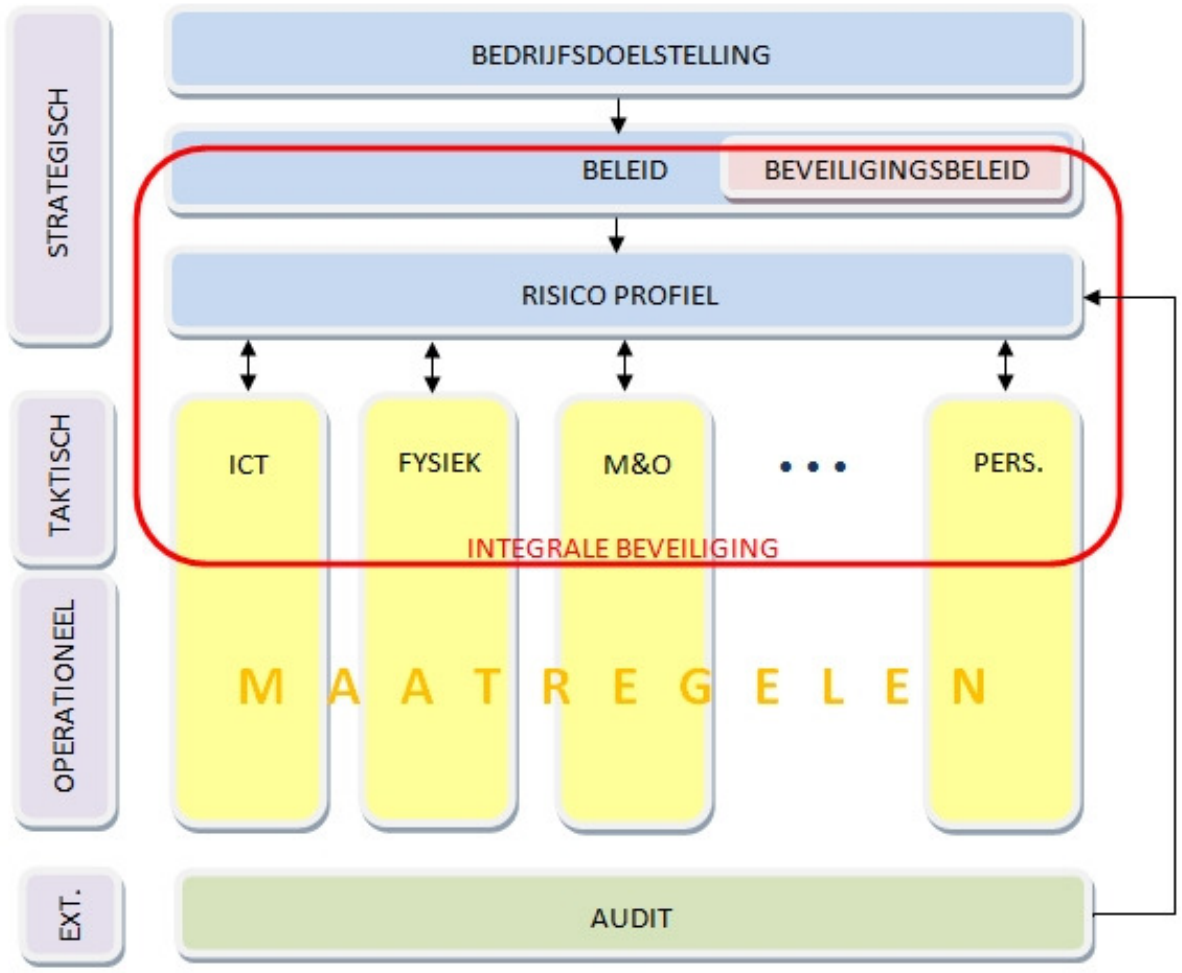
Een beveiligingsketen is zo sterk als de zwakste schakel. Dit geldt zowel in de diepte als in de breedte. Het beheersen van bedrijfsrisico's vereist een evenwichtige benadering van de verschillende oplossingen. Kiezen we voor een extra slot op de deur of gebruiken we

encryptie van data achter de deur…. Als er geen balans is in de afweging van mogelijke risico's, genereert dat wellicht een nieuw risico. Een integrale benadering van risicoanalyses met betrekking tot mensen, middelen en diensten verbindt de verschillende disciplines. De gezamenlijke benadering van beveiligingsvraagstukken vanuit strategisch denken betekent dat integrale beveiliging deel uitmaakt van Enterprise Risk Management.

ERM belangrijkste succesfactor Integrale beveiliging!

WERKVELD INTEGRALE BEVEILIGING

Vastgesteld is dat Enterprise Risk Management een belangrijke succesfactor is voor integrale beveiliging. Met dit uitgangspunt is onderstaande figuur samengesteld door de expertgroep.



Integrale beveiliging is gepositioneerd binnen de bestaande organisatie door middel van horizontaal overleg met vertegenwoordigers vanuit strategisch en tactisch niveau met de business als risico-eigenaar.

Het werkveld integrale beveiliging:
Organisatiebrede en gecontroleerde samenwerking.

Het initiatief voor integrale beveiliging ligt op strategisch niveau. Topmanagers moeten zich afvragen wat, waartegen en waarom ze willen beschermen. En minstens zo belangrijk, zijn de consequenties aanvaardbaar als er een aspect niet wordt beschermd? Deze vraagstukken worden geadresseerd met een bedrijfsrisicoprofiel (zie paragraaf Risicoprofiel). Op basis van dit risicoprofiel wordt per discipline of specialisme vastgesteld welke beveiligingsoplossingen noodzakelijk zijn. De oplossingen gezamenlijk vormen zo een evenwichtige set van beveiligingsmaatregelen ter beheersing van de bedrijfsrisico´s vanuit het risicoprofiel. De gehele coördinatie van deze samenhang en afwegingen wordt uitgevoerd door een Enterprise Risk Officer (zie paragraaf Enterprise Risk Officer).

Risicoprofiel
Het centrale punt van het werkveld integrale beveiliging is het risicoprofiel, gebaseerd op de verschillende beveiligingsaspecten voor personeel, materieel, financiën en informatie. Een normenkader, opgesteld vanuit wet & regelgeving en de te beschermen bedrijfsdoelen, kan een goede invulling geven aan een risicoprofiel. Best practices voor beveiligingsnormen zoals de ISO27002 en opgelegde in-control-statements vanuit de financiële en administratieve markt kunnen als start erg handig zijn maar ook niet meer dan dat. Het is aan te bevelen een bedrijfseigen risicoprofiel te ontwikkelen waarin risico's voor de verschillende bedrijfsaspecten in onderlinge samenhang worden beschouwd. Zorg dat managers oog hebben voor relevante dreigingen en de daaruit voortvloeiende risico's. Beoordeel risico's voor de verschillende bedrijfsaspecten in onderlinge samenhang en stel prioriteiten vast. Dit lukt niet op operationeel niveau omdat daar het totaalbeeld ontbreekt.

Enterprise Risk Officer
De belangrijkste rol in dit werkveld integrale beveiliging is weggelegd voor de Enterprise Risk Officer (ERO). De ERO kan een staffunctionaris of beveiligingsspecialist zijn met als belangrijkste taak de verbinding te vormen tussen de verschillende middenlijnmanagers en beveiligingsspecialisten. De ERO dient daarmee minimaal bedrijfskundige- en beveiligingskennis als competenties te hebben en zeker ook over goede communicatieve vaardigheden te beschikken.

De ERO is verantwoordelijk voor de verbanden tussen de verschillende disciplines. Op lager niveau vindt interdisciplinair overleg plaats met de ERO als voorzitter en op hoger niveau coördineert de ERO audits en rapportages. De ERO regelt ook de afstemming met tactisch en operationeel niveau, zorgt dat problemen worden gesignaleerd en dat er aanspreekpunten zijn voor terugkoppeling naar boven. De ERO zorgt ervoor dat elke lijnmanager is geïnformeerd over informatiebeveiliging en het belang inziet van een integrale benadering. Eventueel laat een lijnmanager zich vertegenwoordigen door een specialist.

Een ERO is vergelijkbaar met de positie van een Chief Information Security Officer (CISO). Ook de CISO zoekt naar oplossingen op basis van risicoafwegingen. In de werkgroep is geen verder onderzoek gedaan naar het verschil tussen de ERO en CISO. Mogelijk dat het twee namen zijn voor eenzelfde functie, of dat de ERO een breder werkveld heeft dan de CISO die zich beperkt tot beheersing van risico's rond bedrijfsinformatie. Een aanvullende expertsessie dient uitgevoerd te worden om het onderscheid tussen ERO en CISO helder te krijgen.

10

CONCLUSIE

Aan het eind van de expertsessie is de conclusie dat integrale beveiliging geen hype is maar een logisch gevolg van voortschrijdende techniek en maatschappelijke ontwikkelingen. De integrale benadering kan een succes worden als aandacht wordt besteed aan samenwerken, aan sturing op strategisch niveau en aan een bedrijfsbrede aanpak. Integrale beveiliging kan worden omschreven als *'beveiligen door een gecontroleerde samenwerking'* waarbij gecontroleerd een aspect is van Enterprise Risk Management uitgevoerd door een 'integraal opererende' beveiliger, de Enterprise Risk Officer. Met het benoemen van een dergelijke functionaris aangevuld met de noodzakelijk organisatorische overlegorganen is aan alle randvoorwaarden voldaan en staat niets een succesvolle integrale beveiligingsaanpak meer in de weg.

Vervolgonderzoek?!

Zoals in de introductie al is aangegeven is het integratieaspect primair benaderd vanuit de invalshoek beveiliging en niet uit die van de veiligheid. Het zou een waardevolle aanvulling op deze expertbrief kunnen zijn om te onderzoeken in hoeverre het geschetste werkveld ook van toepassing is of aanvulling behoeft voor het integraal veiligheidsdenken. Er zijn post-HBO-opleidingen integrale veiligheid; wellicht is deze expertbrief een aanleiding voor een onderzoeksopdracht? Of voor een volgende expertsessie?

BIJLAGE 1. BRONDOCUMENTEN

Onderstaande tabel geeft een opsomming van de documenten die zijn verzameld. De documenten zijn beoordeeld door het organisatiecomité. In kolom 3 is aangegeven welke informatie is geselecteerd om te gebruiken tijdens de sessie. In de overige kolommen is weergegeven welke relatie er is tussen het artikel en de hoofdvraag en subvragen van de probleemstelling.

Nr	Brondocumenten	Specifiek doorgenomen ter voorbereiding
1	*Beleidsplan Integrale Veiligheid HCAM* TU Delft, augustus 2009	Blz 12
2	*Integrale veiligheid als trend* presentatie lezing Bert Duijndam, PvIB 2008	Blz 9 en 10
3	*Logical & Physical Convergence* Aberdeen Group, december 2007	Blz 18 en 19
4	*Convergence of enterprise security organizations* Booz Allen Hamilton, november 2005	Blz 4,18, 21 en 27
5	*Let's get logical* Burton Group, februari 2008	Blz 1 t/m 13 en 25
6	*Open staan* van Jo Koppes, Trends in IT-beveiliging 2008	Blz 93 t/m 95
7	*Integraal RM maakt ziekenhuis veiliger* Gerard Gerritsen cs, Medisch contact 2009	Geheel
8	*The Convergence of Physical and Information Security in the context of ERM*; Deloitte	Blz 6, 39 t/m 43 en 52
9	*Integrale beveiliging: een koppeling van begrippen* Thimo Keizer, Informatie 2008	Geheel
10	*Integratie van fysieke en logische beveiliging* Mohammed Al Ayachi, Security Management 2008/12	Geheel
11	*Handreiking Security Management* VROM Ruimte & Milieu, juli 2008	Blz 3, 16 en 22
12	*Combineer fysieke en logische toegangsbeveiliging* Informatie mei 2004	Geheel
13	*Is iedereen Integraalbeveiliger?* Ronald Eygendaal; periodiek VBN 2008	Geheel
14	*Convenience meets security at the desktop* presentatie Debra Spitler / RSA april 2009. http://www.trustedcomputinggroup.org/files/static_page_files/F7D87AE2-1D09-3519-AD5ACF0E7480AE8A/RSA%202009%20-%20Draft%205%20-%20041309.pdf	Blz 3 en 8
15	*Encrypting PIN Pad*; Security Requirements v2.1 PCI Security Standards Council januari 2009. https://www.pcisecuritystandards.org/security_standards/ped/download.html?id=22	Inhoudsopgave en blz 1
16	*Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)* NIST November 2008. http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf	Pagina 1, overview

12

Nr	Brondocumenten	Specifiek doorgenomen ter voorbereiding
17	*Informatiebeveiliging én fysieke beveiliging* Douwe de Jong; Informatiebeveiliging 2002 de nummers 4,5,6. Voor een samenvatting zie http://www.dejong-itadvies.nl/media/Ib&Fb%20mngt%20samenvatting.doc	Verwijzing vanuit § 1.4 van de Expertbrief
18	PP-presentatie *BORG & ICT voor het MKB* tijdens congres Integrale Veiligheid 2003; Platform Integrale beveiliging. http://www.dejong-itadvies.nl/media/Borg%20en%20ICT%20voor%20het%20MKB%20v1_1.ppt	Verwijzing vanuit § 1.4 van de Expertbrief

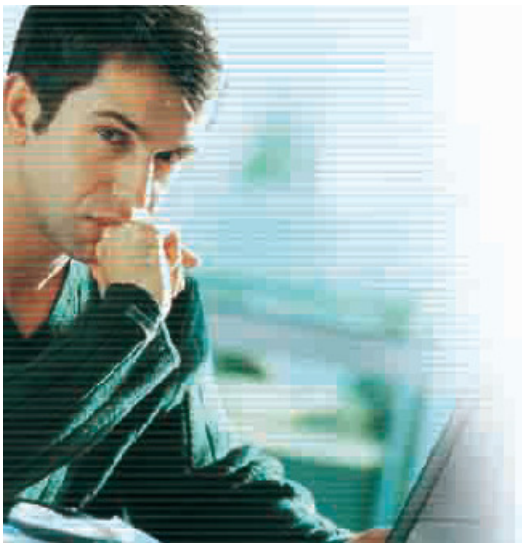
APPENDIX GEBRUIKTE LICENTIEVORM

De expertbrief wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by/3.0/nl/

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

14

WORDT LID VAN HET PVIB, 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 Platform voor Informatiebeveiliging kan u behulpzaam zijn bij al uw vraagstukken op het gebied van informatiebeveiliging.

Wat is het Platform voor Informatiebeveiliging?
Het PvIB is een open, breed samengesteld platform 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 PvIB 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 IT 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:

https://www.pvib.nl/abonnementsinformatie