december 2010 nummer 8

INFORMATIEBEVEILIGING

Neelie Kroes en haar Digitale Agenda

Verslag: Het Govcert-symposium 2010

Verizon zet onderzoekskaders in tegen cybercriminaliteit

Achter het nieuws: Nationaal Trendrapport Cybercrime

PvIB
Platform voor InformatieBeveiliging

ib

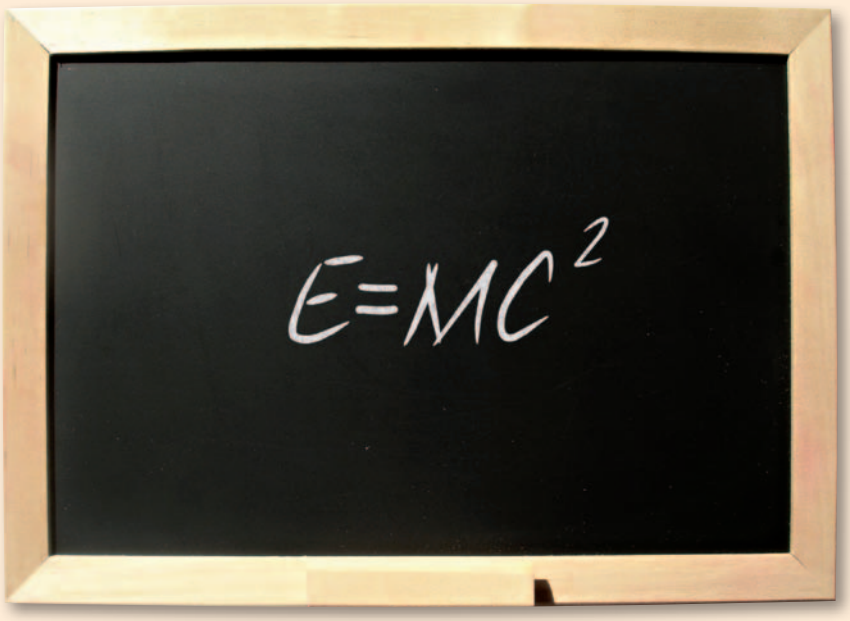
Er is niets zo praktisch als een goede theorie

Auteur: Yuri Bobbert MSc > Yuri Bobbert MSc is Managing Director van B-Able en onderzoeker aan het ITAG Research Institute van de Universiteit Antwerpen. Yuri is bereikbaar via yuri.bobbert@b-able.nl

Dit artikel is samengesteld naar aanleiding van uitgebreid onderzoek onder mid market managers in verschillende sectoren als gezondheidszorg, overheden, educatieve instellingen, financiële instellingen en mediabedrijven. Naast de meest praktisch toepasbare maatregelen is beoordeeld welke beveiligingverhogende maatregelen dit mid-market segment zelf als beste beoordeelt. Tevens welke barrières deze organisaties ervaren bij het doorvoeren van de juiste maatregelen. De onderzoeksbevindingen en aanbevelingen zijn samengevat in het boek 'Maturing business information security'. Dit boek is de basis voor uitgebreid vervolgonderzoek aan de Universiteit van Antwerpen naar de mate van toepasbaarheid in verschillende sectoren en meetbare mate van effectiviteit over een bepaalde periode.

Het is 14 oktober 2010. Enigszins verdoofd neem ik een kop koffie en evalueer voor mezelf de dag ervoor. Een dag- en avondvullend seminar over informatiebeveiliging heb ik tot me genomen. Verschillende onderwerpen passeerden de revue en boeiden mij zowel als wetenschapper als practicus. Onderwerpen als ITIL v3, GRC, ERMPlus etc. Interessante onderwerpen met een sterk theoretisch karakter en voor de succesvolle effectuering ervan afhankelijk van organisatie en proces. Vanuit theoretisch en wetenschappelijk kader interessant maar vanuit praktisch perspectief minder relevant en misschien wel discutabel. Een mogelijke 'ver van mijn bed show'. Om wat specifieker te zijn een 'ver van de kleinere organisatie show'.

Zogenaamde mid-size market[1]-organisaties worstelen met complexe enterprise gerichte raamwerken en theorieën als ISO, ITIL en dergelijke om informatiebeveiliging te operationaliseren. Überhaupt zijn de toepasselijkheid van theoretische raamwerken en standaarden, en de effecten ervan, discutabel (Siponen, 2009). Dit blijkt ook uit in 2008 uitgevoerd onderzoek door Kluge en Sambasivam in Europa's grootste economie, Duitsland. Daaruit blijkt dat 'medium enterprise'-organisaties moeite hebben standaarden als ISO27000 te operationaliseren (Kluge & Sambasivam, 2008).

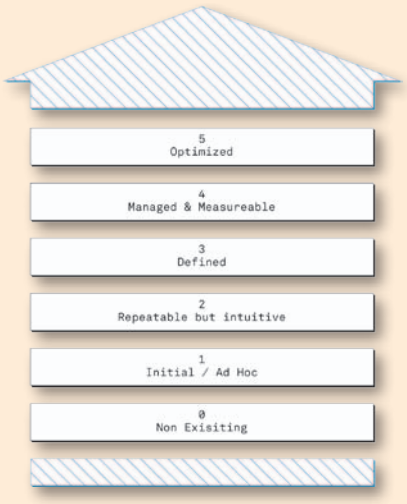


Dat terwijl aan de andere kant de noodzaak voor goede beveiliging en betrouwbare auditing toeneemt (ISACA, 2009). Enerzijds door de toename aan incidenten en de toename van de kosten van zo'n incident (Richardson, 2008)[2]. Anderzijds door de toename van het aantal mid-size-organisaties in de Europese unie en de noodzaak voor deze bedrijven om te voldoen aan accountancy wet- en regelgeving. Dit stelde mezelf, maar daarmee wellicht ook andere beoefenaars van het beveiligingsvak, voor een aantal relevante vragen, namelijk:

1. Is dit marktgebied wel van enige economische en sociale relevantie voor ons vakgebied?
2. Erkent dit mid-size marketsegment zelf wel de behoefte dan wel de noodzaak voor beveiliging?
3. Kunnen we de bekende theoretische methodes en raamwerken die werken voor grote organisaties niet gewoon 'loslaten' op deze organisaties?
4. Waarom is dit type organisatie onderbelicht op onze symposia en seminaries?

Aan de hand van verschillende onderzoeken alsook persoonlijke praktijkervaringen binnen honderden mid-marketorganisaties zet ik de antwoorden op deze vragen stap voor stap uiteen.

1 De Europese commissie doet constant onderzoek naar marktomvang alsook de samenstelling ervan (per industrie). Marktmetingen worden gedaan op basis van totale omzet per industrie alsook het aantal werkzame personen in deze industrie. De indruk kan worden gewekt, dat de Europese Unie wordt gedomineerd door grote organisaties die veel werkgelegenheid bieden en hoge omzetten. Echter niets is minder waar. Maar liefst 99% van alle Europese organisaties bestaat uit kleine en mid-size marketbedrijven. Ze voorzien in maar liefst tweederde van de werkgelegenheid en de helft van de omzet van alle organisaties in de EU.



Daarmee is dit marktsegment de economische en sociale ruggengraat van de Europese Unie. Bron: Annual Report of the EU (EU, 2009).

Met de steeds strikter wordende wet- en regelgeving op het gebied van financiële verslaglegging voor veel van deze bedrijven moeten we de relevantie voor ons vakgebied meer en meer erkennen. Belangrijke kanttekening die we moeten maken is dat negen van de tien bedrijven microbedrijven zijn met minder dan tien medewerkers. Deze bedrijfsgrootte speelt een belangrijke rol in de economie, echter is vanuit ons vakgebied niet relevant voor de toepassing van theoretische raamwerken. Vooral omdat het raamwerk bij kleinere organisaties niet volledig tot zijn rechtkomt bij gebrek aan processen en resources. Daar zijn ze simpelweg te klein voor.

Dit artikel richt zich met name op organisaties met tussen de 100 en 2500 geautomatiseerde systemen die zo groot zijn dat ze dienen te voldoen aan wet- en regelgeving (WbP, wet op jaarrekening, EDP audit) maar te klein zijn voor eigen security-afdelingen, -functionarissen en -processen die vanuit raamwerken veelal vereist zijn.

2 Als onderzoeker, wetenschapper of beoefenaar van het vak van informatiebeveiliging kunnen we wel vinden dat de beveiliging voor deze bedrijven relevant is maar wijst de praktijk het ook uit? Niets is zo moeizaam dan iets op te dringen waar geen behoefte aan is. Niets is zo praktisch onuitvoerbaar als een slechte theorie. Belangrijke vraag die ik mezelf als onderzoeker in dit vakgebied stel is of dat wat ik wil onderzoeken ook wel een praktische toepassing kan krijgen? In recent door mezelf uitgevoerd onderzoek onder 40 Nederlandse mid marketorganisaties wordt aangetoond dat 100% van de organisaties informatiebeveiliging als aandachtspunt ziet. Niet alleen door de toename van IT-afhankelijkheid maar ook door de sociale impact ervan als er iets verkeerd gaat. De publieke schande is door de snelheid van sociale media enorm, met als voorbeeld DSB. Dit maakt dat de mid-marketorganisaties uit het onderzoek allemaal erg bewust zijn over de noodzaak van beveiligen en hun organisatiebeveiligingsniveau allemaal willen verhogen, als we het afzetten tegen een volwassenheidsmodel met vijf schalen (zie de figuur). Uit dit onderzoek blijkt dat maar liefst 47% van de organisaties de beveiliging meetbaar onder controle wil hebben binnen twee jaar.

Met de huidige manier van werken en ruime ervaring met bestaande theorieën lijkt het meetbaar onder controle hebben (niveau 4) van beveiliging onbegonnen werk. Vooral als we terugkijken en zien dat 21% ad hoc en 39% intuïtief haar beveiliging praktiseert. Is dit dan met al tientallen jaren ervaring op het gebied van IT en security de status quo? Hebben theoretische raamwerken dan echt zo weinig bijdrage geleverd voor de mid-marketpraktijk? De op grote organisaties gerichte raamwerken en theorieën als ISO, ITIL, COBIT schijnen hun doel te missen als het gaat om de operationalisering ervan binnen mid-marketbedrijven. Dit tonen Kluge en Sambasivam aan voor organisaties in Duitsland en ik zelf voor Nederland. De geïnterviewden gaven aan door de bomen van maatregelen en controls het bos niet meer te zien. De hoeveelheid van bestaande en nieuwe methodes blijken voor dit segment hun doel te missen. Om dit niet alleen te stellen maar ook feitelijk te onderbouwen geef ik enkele voorbeelden:

- Tachtig procent van de organisaties weet niet welke wet- en regelgeving er van toepassing is op haar eigen organisatie, ondanks dat theorieën de noodzaak hiervan voorschrijven;
- In 41% van de gevallen wordt het management niet betrokken bij het opstellen van een strategie voor het beveiligen van bedrijfskritische informatie, ondanks dat de theorie dat voorschrijft;
- De helft van de organisaties monitort of logt geen security events/incidenten, ondanks dat wet- en accountancyregelgeving dit eist in veel gevallen;
- Meer dan de helft van de organisaties voert geen wijzigingsbeheer uit op kritieke beveiligingsapparatuur, vergelijkbaar met een sleutel in je voordeur die je er maanden in laat zitten;
- Meer dan tachtig procent doet niets aan bewustwording, dat terwijl theorieën dat voorschrijven en de onbewuste medewerker de grootste oorzaak van incidenten is.

Onderzoek (Kluge & Sambasivam, 2008) (Siponen, 2009), ik zelf (Bobbert, 2010) en de geschiedenis leert ons hiermee dat de bestaande theorieën en raamwerken niet gewoon losgelaten kunnen worden op mid-marketorganisaties. Sterker nog, het stelt ze ter discussie op effectiviteit en eenvoud van implementatie. Het creëert noodzaak voor verder toegepast onderzoek naar andere meer praktische methoden zoals SABSA[3], Total Secure (Bobbert, 2010), COBIT 5 (ISACA, COBIT 5 Design Paper (Exposure Draft), 2010) die vanuit bedrijfsdoelstellingen de beveiliging pogen te operationaliseren.

LEVEL INDICATIONS	INDICATE, BASED UPON THE MATURITY MODEL LEVELS, YOUR CURRENT SECURITY MATURITY LEVEL	INDICATE, BASED UPON THE MATURITY MODEL LEVELS, YOUR DESIRED ORGANIZATION SECURITY MATURITY LEVEL AT 2012
1 Initial Ad Hoc	21%	3%
2 Repeatable but intuitive	39%	6%
3 Defined	21%	36%
4 Managed & Measureable	16%	47%
5 Optimized	3%	8%

Onderschrift: COBIT Security maturity levels.

Er is niets zo praktisch als een goede theorie

3 Tot slot van dit artikel stel ik mezelf de vraag: Hebben de bestaande raamwerken een aanvullende functie voor dit mid-marketsegment? Jazeker, met name richtinggevend maar zeker ook praktisch toepasbaar mits ze geaccepteerd zijn. Zo heeft de selectie van effectieve en gemakkelijk te implementeren maatregelen op basis van de 'Universiteit van Antwerpen methode' toegevoegde waarde (Grembergen & De Haes, 2004) gehad in het business & IT alignment-vakgebied. Deze succesvolle kwalitatieve methode van selecteren van maatregelen is tevens bruikbaar voor het selecteren van effectieve en gemakkelijk te implementeren beveiligingsmaatregelen in elk willekeurig mid-marketsegment. Door gebruik te maken van deze methode ontstaat een kernselectie van maatregelen, specifiek per branche. Door deze vervolgens te valideren in dezelfde branche, vergroot men de begrijpbaarheid en acceptatie van dit theoretische raamwerk. Op moment van schrijven is deze manier van security operationaliseren onderwerp van vervolgonderzoek aan de Universiteit Antwerpen (ITAG Research Institute[4]) onder leiding van mezelf, Prof. Dr. Steven de Haes en Prof dr. Wim van Grembergen. Met deze methode wordt geredeneerd vanuit de toepasselijkheid op de market (per branche) naar het samenstellen van een theoretisch model in plaats van andersom.

4 Het antwoord op de laatste vraag is wellicht een inleidende voor verdere discussie. Wetenschappers genereren graag modellen en nieuwe methodes. Veelal afgeleid van een bestaande theorie of model. Zo kennen we een aantal op bestaande modellen voortbordurende versie drie van ITIL, versie 5 van Cobit enz. Beter kunnen we onze seminars en symposia laten voeden met meer praktijkgevallen die de bestaande modellen vanuit de praktijk verrijken en aanscherpen. Op die manier maken we theorieën niet alleen toepasbaar voor de ideale organisatie waarin de theorie perfect kan landen maar ook toepasbaar voor de ad-hoc organisatie die bezig is zijn hoofd boven water te houden in een dynamische wereld. Laten we het proberen vooral simpel te houden en niet te complex te maken. Eenvoud in complexiteit (Mulder, 2006).

Bibliografie

Bobbert, Y. (2010). *Maturing Business Information Security, A framework to establish the desired state of securtiy maturity.* Utrecht: Institute for Business and Information Security Alignment (IBISA.EU).

EU, A. R. (2009). *Annual Report on EU small and medium size Enterprises 2009.* Brussels: EIM Business & Policy Research.

Grembergen, W., & De Haes, S. (2004). *IT governance and its Mechanisms.* Antwerp: ISACA.

ISACA. (2009). *An Introduction to the Business Model for Information Security.* United States: ISACA.

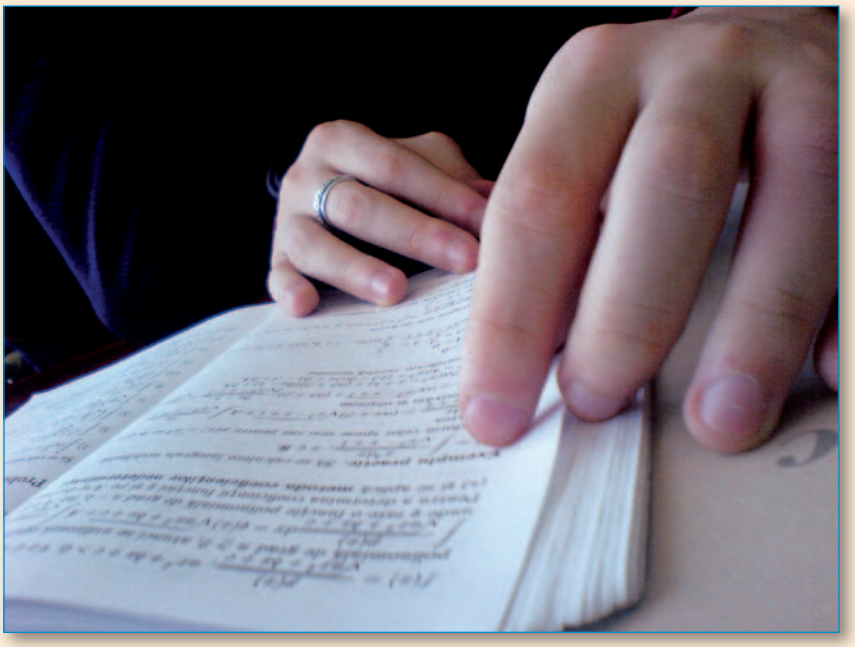
ISACA. (2010). *COBIT 5 Design Paper (Exposure Draft)* . United States: ISACA.

Kluge, D., & Sambasivam, S. (2008). *Formal Information Security Standards in German Medium Enterprises.* Phoenix: Edsig.

Mulder, J. (2006). *Eenvoud in Complexiteit.* Rijswijk.

Richardson, R. (2008). *CSI Somputer Crime & Security Survey.* United States: CSI, edition 13.

Siponen, M. W. (2009). *Information Security management standards: problems and solutions.* Finland: Information & Management 46.



1 Midmarktorganisaties worden gedefinieerd op basis van aantal geautomatiseerde systemen, in dit geval tussen de 100 en 2500.
2 Door CSI en Applied Research worden de kosten van een incident geschat op tussen de 150.000 en 232.000 euro.
3 SABSA, Sherwood Applied Business Security Architecture
4 ITAG, Information Technology Alignment and Governance Research Institute, http://www.antwerpmanagementschool.be/ITAG