

CHAPNEWS



Netherlands Chapter

Colofon

Deze nieuwsbrief is een uitgave van ISACA NL Chapter.

Redactie: T. Bakker,
B. van Staveren
A. Shahim en

Het redactieadres:
ISACA NL Chapter
t.a.v. Redactie
Nieuwsbrief
secretary@isaca.nl

VOORZITTER

Hieronder is een introductie gegeven van de verschillende bestuurleden van ISACA die antwoord moesten geven op een aantal specifieke vragen zoals wie ze zijn, wat ze willen maar ook wat hun opmerkelijkste ICT gebeurtenissen zijn.

We beginnen met de vijf van de nieuwe president van ISACA.

1 Wie ben jij?

Dat is een moeilijke vraag, zeggen ze altijd. Gewoon dan maar wat feiten. Ik heet Klaas Piet Meindersma (50 jr) en ben sinds mei 2007 president van ISACA Nederland. Na mijn middelbare school heb ik bedrijfskunde op de HTS in Leeuwarden gedaan en daarna, naast mijn werk bij onder andere de Politie, Bedrijfseconomie, Bestuurlijke informatiekunde op de Universiteit van Amsterdam en Groningen gedaan. Vervolgens heb ik, omdat mijn toenmalige werkgever daar prijs op stelde, nog Accountancy en IT-Audit gedaan. Recentelijk heb ik nog CISA gevolgd en ben gelukkig geslaagd. Ik moest er niet aan denken dat ik zou zakken, als (toen) vice-president ten opzichte van collega's en medewerkers. Na veel jobhoppen, vanaf 1980 bij TNO, heb ik in 1997 CSI mede opgericht en ben daar nu partner mede-eigenaar van. Tja, CSI is momenteel een groep van zo'n 70 professionals werkend in de IT audit en security, wereldwijd opererend. Thuis is Hilversum, met mijn vrouw en veel te weinig tijd voor mijn drie kinderen Cisca (cisa), Pieter en Niek.

2 Hoe en waarom bij ISACA?

In 2003 werd ik door Bart Sibon gevraagd of ik hem, wegens tijdgebrek, wilde vervangen in het bestuur en helpen bij de organisatie van de RT. Het leek mij leuk de RT's mede te organiseren omdat je dan ook direct invloed kan uitoefenen op de onderwerpen die aan de orde komen. Ook sprak mij aan dat iemand van CSI zo wat meer bij de organisatie en het bestuur van ISACA betrokken raakte. Ik verwachtte een leuke, gezellige groep medebestuurders die samen met elkaar de strategische doelen van ISACA willen proberen te verwezenlijken. En dat is ook zo uitgekapt.

3 Welke ambities heb je binnen ISACA?

Zoals ik in het begin al heb aangegeven ben ik binnengekomen om de RT's te organiseren. Na 1 jaar ben ik na de reorganisatie vice-president geworden met dezelfde taken en het vervangen van de president. Begin 2007 ben ik de vorige president opgevolgd en daarmee is mijn functieambitie wel zo'n beetje ingevuld. Over 2,5 jaar, als er een nieuwe president moet komen, hoop ik in internationaal ISACA-verband wat te kunnen gaan doen; dan door een functie in the board. Ik vind het leuk om te zien hoe ISACA zich internationaal ontwikkeld maar ook om de ontwikkelingen in het vakgebied bij te houden.

4 Jouw opmerkelijkste IT gebeurtenissen?

Wat een vraag. Goed. Wat ik opmerkelijk vind in de techniek - maar dat heeft niet direct met het vakgebied audit te maken - is dat de prijsontwikkeling van de geheugens de mogelijkheden van de IT in het dagelijkse leven bepalen. We begonnen met nullen en enen en zijn via tweedimensionale tekeningen en interfaces doorgroeid naar multimedia, zoals films, etc. Met het nog goedkoper worden van opslagcapaciteit zal er nog veel meer mogelijk worden.

In organisatieverband vond ik het meest opmerkelijk dat een projectleider van een groot ICT-traject (we praten over een kleine 80 miljoen euro) aangaf als projectleider te stoppen omdat hij vond dat hij na anderhalf jaar een nieuwe uitdaging zocht. Opmerkelijk dat hij daar nog mee weg kwam ook. Ik kan me herinneren dat ikzelf een redelijk groot project tot een goed einde bracht en daar erg mee in mijn schik was. Ik weet nog dat ik het zo leuk vond, dat ik erg moeilijk afscheid kon nemen van het project. Het was zelfs zo erg dat ik daar op het laatst wel gratis wilde werken. Vervolgens maar - dat is misschien wel in het verlengde hiervan - begrijp ik niet dat men nog steeds zoveel IT-projecten in het honderd laat lopen. Ik zeg bewust laat lopen want een projectleider met een beetje ervaring ziet toch al snel wanneer een project niet goed in de steigers staat en gedoemd is te mislukken.

5 Wat doe je in je spaarzame vrije tijd?

Dat valt nogal mee hoor, met dat spaarzame. Als het weer een beetje meezit schaats of zeil ik. Als dat laatste in Nederland niet lukt, zeil ik op de Middellandse Zee. Met schaatsen is het wachten op mijn vierde elfstedentocht. Gezien de mogelijke klimaatveranderingen zou ik in '97 wel eens mijn laatste elfstedentocht kunnen hebben geschaatst. Verder ga ik zo nu en dan winkelen met mijn dochttertje van 10 en speel ik een computergame met een van de jongens. Verlies ik nu al van. Ook kook ik graag. En ik kijk graag films, (minimaal) twee speelfilms per week die ik selecteer uit mijn filmhandboek "1001 meest spraakmakende films". Ik kan dus nog heel wat jaren vooruit. Tip: kijk eens naar Lulu Rennt, een prachtige onthaast film.

CISA TRAINING

Elk jaar wordt op diverse plaatsen op de wereld en dus ook in Nederland CISA examens georganiseerd. Eén examen in het voorjaar (**14 juni 2008**) en één examen in het najaar

(**13 december 2008**). Bij voldoende belangstelling organiseert het ISACA NL Chapter trainingen ten behoeve van deze examens.

Er is één trainingsvariant ontwikkeld die zowel basiskennis als examen training omvat. Alle relevante onderwerpen worden systematisch behandeld en er wordt geoefend op de specifieke examenteknik die gehanteerd wordt tijdens het examen. Het betreft een multiple choice examen waarbij in relatief korte tijd 200 vragen moeten worden beantwoord. Veel tijd om na te denken is er vaak niet.

De **CISA training** duurt 8 avonden en wordt gegeven in april-mei en oktober-november 2008.

**IT Governance
Global Status Report – 2008**

From July until October 2007 a survey reaching members of the C-suite was conducted to determine their sense of priority and actions, as well as tools and services needed, relative to IT governance. Focus points include the:

Degree to which the concept of IT governance is recognised, established and accepted within boardrooms and especially by CIOs

Level of existing IT governance expertise and which frameworks are known and are (or will be) adopted

Extent to which ITGI's own framework, COBIT, is selected and how it is perceived.

Because this report is the third consecutive undertaking of this IT governance research project, the project team was able to use historical data from the previous reports to discover trends in a number of areas.

Wegens succes herhaald.

Wegens het succes van de in 2007 georganiseerde training "IT governance en –assurance met COBIT 4.1" wordt deze training in 2008 herhaald.

Doelstelling

Deze tweedaagse training heeft tot doel de deelnemers een diepgaand inzicht te geven in COBIT4.1 als pragmatisch instrumentarium voor de implementatie van IT governance en voor het uitvoeren van IT assurance opdrachten.

Doelgroep

Deze training is bestemd voor CIOs, IT managers, (IT-) auditors, (IT-)controllers, security officers, risk managers, businessmanagers en IT governance professionals.

Waarom deze training?

Deze tweedaagse training hanteert een modernere en enigszins andere aanpak voor een dergelijke cursus dan u normaliter gewend bent. Deze nieuwe benadering gaat uit van de basisprincipes van IT governance en -assurance, en gaat in op de implementatie ervan met behulp van een internationaal aanvaardbaar raamwerk, te weten: COBIT 4.1.

Data en locatie

Deze training vond op 21 en 22 april in Hotel Breukelen plaats en zal in het najaar opnieuw worden georganiseerd.

Trainer

Uw hoofdtrainer is de heer Wim van Grembergen. Hij is professor aan en voorzitter van de Information Systems Management Department van de Economie en Management faculteit van de Universiteit Antwerpen. Daarnaast is hij executive professor op de Universiteit Antwerpen Management School. Wim van Grembergen is continu betrokken bij de ontwikkeling van COBIT als een raamwerk voor IT governance en heeft veel onderzoek gedaan. Met zijn uitgebreide ervaring op dit interessante en uitdagende gebied heeft hij dan ook veel publicaties op zijn naam staan. Tijdens de training wordt de heer Van Grembergen geassisteerd door de heer Steven de Haes die eveneens ruime COBIT ervaring bezit.

Aanmelding

Voor aanmelding en nadere informatie omtrent deze training wordt verwezen naar www.isaca.nl.

ENKELE AANDACHTSGEBIEDEN IN INFORMATIE- BEVEILIGING

In het vorige decennium is de bekende en terechte hype rond informatiebeveiliging ontstaan waarvoor toentertijd vooral een technische insteek werd gehanteerd. Digitale communicatie was steeds vaker gewenst en IT-oplossingen werden steeds vaker aan elkaar gekoppeld om de businessprocessen adequaat te ondersteunen. De focus werd daarbij hoofdzakelijk gelegd op de beveiliging van netwerken en platformen en op het gebruik van tools die dergelijke activiteiten mogelijk maakten. Informatiebeveiliging heeft zich inmiddels ontwikkeld tot één van de meest besproken strategische onderwerpen met een breed werkterrein. Als gevolg van deze evolutie is dit indrukwekkende vakgebied hoger op de agenda van Chief Information Officers (CIOs) en andere mensen op C-niveau komen te liggen. Door deze positionering hebben organisaties op hun eigen specifieke manier aandacht en invulling gegeven aan informatiebeveiliging. Ondanks dat dit boeiende vakgebied tegenwoordig vele ladingen dekt, zijn enkele interessante aandachtsgebieden te herkennen waaronder de mentale omslag van organisaties.

In dit nummer van ChapNews staan wij stil bij twee van de door ons op de markt geconstateerde aandachtsgebieden, te weten: business continuity en financiële onderbouwing van beveiligingsinvesteringen. In de praktijk merken wij dat een toenemende belangstelling is voor het beschikbaar houden van de bedrijfsprocessen zelfs in tijden van de meest verschillende calamiteiten. Eén veel besproken thema daarbij is pandemie die een epidemie is op wereldwijde schaal en kan ontstaan als sprake is van een nieuwe ziekte. Een ander onderwerp dat ook veel aandacht trekt in de informatiebeveiliging is een kwantitatieve aanpak. Binnen de risicomangementpraktijk richten dergelijke benaderingen zich met name op kosten-batenanalyses om zodoende beveiligingsgerelateerde investeringen te kunnen onderbouwen met een financiële argumentatie.

Als redactie van ChapNews hopen wij dat wij met in dit nummer gepresenteerde artikelen en de daarin behandelde onderwerpen de lezer een dienst hebben bewezen. Wij wensen u veel leesplezier.

Dr. A. Shahim RE

CISM TRAINING

Elk jaar wordt op diverse plaatsen op de wereld en dus ook in Nederland CISM examens georganiseerd. Eén examen in het voorjaar (**14 juni 2008**) en één examen in het najaar (**13 december 2008**). Bij voldoende belangstelling organiseert het ISACA NL Chapter trainingen ten behoeve van deze examens.

Er is één trainingsvariant ontwikkeld die zowel basiskennis als examentraining omvat. Alle relevante onderwerpen worden systematisch behandeld en er wordt geoefend op de specifieke examenteknik die gehanteerd wordt tijdens het examen. Het betreft een multiple choice examen waarbij in relatief korte tijd 200 vragen moeten worden beantwoord. Veel tijd om na te denken is er vaak niet.

VOORBEREIDING OP EEN PANDEMIE

Inleiding

Er zijn al veel artikelen gepubliceerd waarin geconcludeerd wordt dat het optreden van een pandemie slechts een kwestie van tijd is. Hierbij worden ter onderbouwing steevast de grieppandemieën uit de vorige eeuw(en) aangehaald. In dit artikel staan we stil bij de impact die een pandemie kan hebben en gaan we in op de typen maatregelen die organisaties kunnen treffen tijdens en in voorbereiding op het uitbreken van een pandemie. Deze maatregelen richten zich op het aspect beschikbaarheid van bedrijfsprocessen.

Impact van een pandemie

Een pandemie zal op verschillende niveaus impact hebben. Op persoonlijk niveau bestaat de kans op infectie, gezondheidsklachten en mogelijk zelfs overlijden. De kans bestaat ook dat de ziekte zich openbaart bij familieleden en kennissen.

Voor bedrijven wordt voorspeld dat het ziekteverzuim hierdoor kan oplopen tot meer dan 30 procent. Nauwkeurige schattingen hierover kunnen nauwelijks worden gemaakt, omdat onzeker is hoe de factor angst voor besmetting het verzuim zal beïnvloeden. Het verzuim kan grote gevolgen hebben voor de bedrijfsvoering. Daarnaast geldt dat overheden in een pandemiescenario handels- en transportbeperkingen kunnen opleggen. Bedrijven kunnen verder te maken krijgen met markteffecten. Hoe klanten zullen reageren en welke impact dit heeft, verschilt per sector en per dienst. Markteffecten en de mate waarin ondernemingen in staat zijn de pandemie het hoofd te bieden zullen waarschijnlijk hun weerslag hebben op de aandelenkoersen. De vraag naar gezondheidszorg zal waarschijnlijk toenemen, evenals de vraag naar telecommunicatie (internet, telefonie) en diensten van internetwinkels. Mogelijk zullen mensen massaal voedsel inkopen om thuis een voorraad aan te leggen. De horeca en de entertainmentsector, evenals andere bedrijven die mensen fysiek bij elkaar brengen krijgen waarschijnlijk te maken met een dalende vraag. Voor bijvoorbeeld verzekeringsmaatschappijen is de verwachte situatie complexer: zorgverzekeringen en overlijdensrisicoverzekeringen zullen naar verwachting te maken krijgen met meer en hogere claims, maar wat pensioenen betreft kan een pandemie leiden tot financiële meevallers. Afgezien van de financiële impact zal een pandemie in ieder geval leiden tot een groot aantal mutaties, en dus behoefte aan capaciteit in de callcenters.

Indien bedrijven en openbare instanties door een pandemie moeite hebben hun dienstverlening op peil te houden kan dit verder consequenties hebben voor het functioneren van de economie ketens en de maatschappij als geheel. Een combinatie van een run op voedsel, beperkte productie- en distributiecapaciteit, faillissementen en beperkte hoeveelheid "blauw op straat" zou bijvoorbeeld kunnen leiden tot sociale spanningen en veiligheidsrisico's. Voor wat betreft de impact op de wereldeconomie geeft DNB aan dat deze groter is dan bij normale economische schokken, doordat verschillende sectoren en regio's in de wereld gelijktijdig of kort op elkaar volgend worden getroffen.

Maatregelen ter voorbereiding op een pandemie

De impact van een pandemie kan worden beperkt door voorzorgsmaatregelen te treffen³. In dit artikel beperken we ons tot maatregelen die organisaties zelf kunnen treffen om hun continuïteit zo goed mogelijk te waarborgen. Waar moet een bedrijf beginnen bij het kiezen en uitwerken van maatregelen en hoe verhoudt dit zich tot andere risicomanagementprocessen? Een pandemie kan worden beschouwd als een van de vele dreigingen voor de continuïteit van de bedrijfsprocessen en kan daarom als onderdeel van het reguliere continuïteitsmanagement worden benaderd. Hierbij kan wel worden opgemerkt dat een pandemie een aantal specifieke kenmerken heeft die deze dreiging onderscheiden van

veel 'traditionele' dreigingen waarop organisaties zich voorbereiden. Veel traditionele continuïteitsplannen gaan uit van scenario's waarin fysieke middelen, waaronder IT-hardware en gebouwen, permanent verloren gaan. Bij een pandemie staan de – tijdelijke maar langdurige - uitval van medewerkers en veranderende vraag- en aanbodpatronen centraal. Een ander verschil is geografisch van aard. Een centrale oplossing voor veel traditionele continuïteitsdreigingen is uitwijk van IT en bedrijfsprocessen naar een (centrale) locatie op afstand. Voor een pandemie is deze maatregel niet echt een oplossing, omdat deze zich wereldwijd manifesteert. De aanpak voor pandemieplanning kan er - in lijn met gangbare cycli voor continuïteitsmanagement - op hoofdlijnen als volgt uitzien:

Risicoanalyse, business impact analyse en strategie: in deze fase wordt geanalyseerd welke processen kritiek zijn voor de continuïteit van de bedrijfsvoering, en welke consequenties een pandemie naar verwachting zou hebben op de verschillende processen. Hierbij worden specifieke kwetsbaarheden in de processen geïnventariseerd. Ook worden in deze fase uitgangspunten, randvoorwaarden en doelstellingen ten aanzien van pandemieplanning geformuleerd, bijvoorbeeld ten aanzien van veiligheid van medewerkers en hun families. Op basis hiervan worden bedrijfsprocessen en maatregelen in de volgende fasen geprioriteerd.

Ontwerp van maatregelen en opstellen van een draaiboek: uitgaande van de geïdentificeerde kwetsbaarheden en kritieke processen worden maatregelen geselecteerd en uitgewerkt. Bij het opstellen van het pandemiedraaiboek is van groot belang dat de taken en verantwoordelijkheden duidelijk zijn belegd, en dat een robuuste crisisorganisatie is geformeerd. Verder kan in het draaiboek aan de hand van de fasering van de Wereldgezondheidsorganisatie (WHO) een escalatieschema worden gemaakt, waarbij per fase is beschreven welke maatregelen van kracht worden. Mogelijke maatregelen zijn:

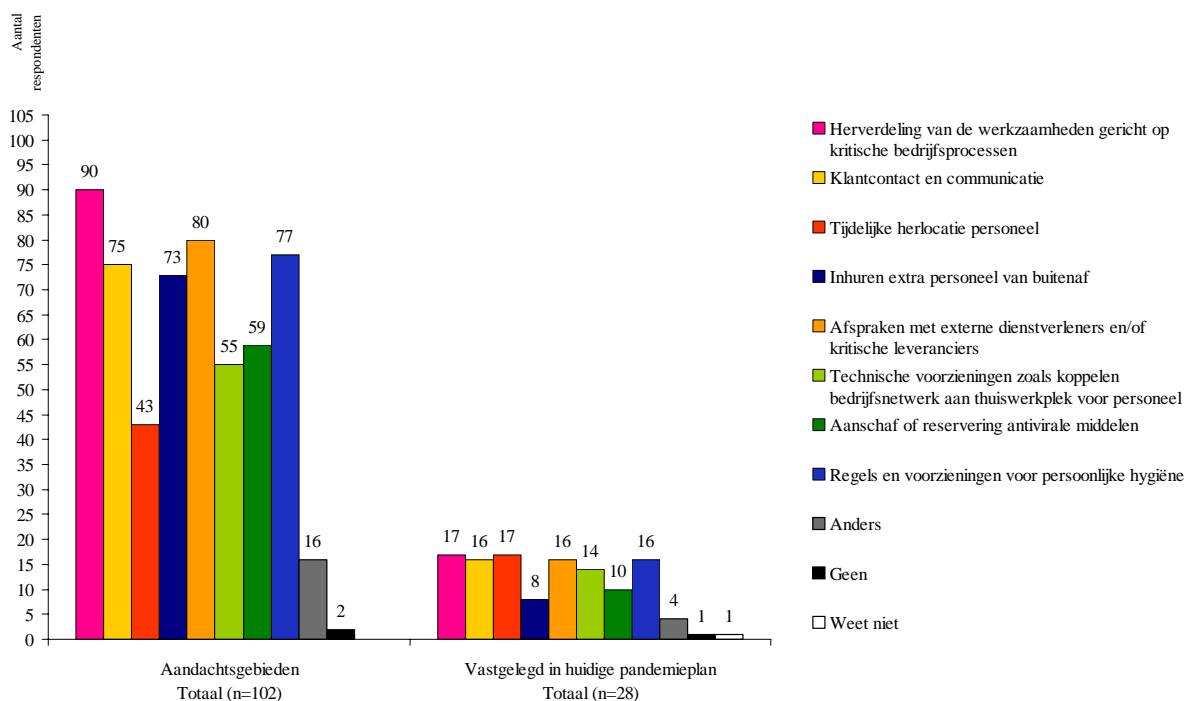
- Taakrotatie (incl. cross training) en uniformeren van werkprocessen met het oog op flexibele inzet medewerkers ten tijde van een pandemie;
- Inrichten van faciliteiten voor telewerken en virtuele vergaderzalen (teleconferencing), zodat medewerkers niet onnodig hoeven te reizen en samen te komen;
- Afspraken maken met leveranciers over levergaranties en procedures ten tijde van een pandemie;
- Op voorraad houden en/of (preventief) toedienen van virusremmers en vaccins claimen zodra deze beschikbaar zijn.
- Invoeren van gedragsregels ten aanzien van persoonlijke hygiëne met daarbij de aanschaf van eventueel middelen zoals handschoenen, mondmaskers;
- Invoeren van reisbeperkingen (zakelijk en privé) voor medewerkers;
- Aanpassen bezoekersregeling;
- Verzuimreglement uitbreiden en communiceren;

Uit een recent telefonisch onderzoek van KPMG naar de voorbereiding van organisaties op een pandemie is gebleken dat organisaties bij pandemieplanning denken aan een combinatie van een aantal maatregelen. Hierbij is het herverdelen van werk gericht op continuïteit van de kritieke processen het belangrijkste aandachtsgebied; zie ook figuur 1.

Implementatie van maatregelen: een aantal van de geselecteerde maatregelen zal al in de huidige WHO-fase (fase 3, met als kenmerken besmetting van mensen met een nieuw subtype griepvirus, maar nog nauwelijks mens-tot-mens besmetting) van kracht zijn en kan dus direct worden geïmplementeerd. Voorbeelden zijn de invoering van taakrotatie, afspraken maken met leveranciers en de invoering van (extra) faciliteiten voor thuiswerken en teleconferencing.

Evaluatie en onderhoud van maatregelen: in deze fase worden het draaiboek en de getroffen voorzieningen getest en onderhouden. Het pandemiedraaiboek kan op verschillende manieren worden getest. Een oefening van bescheiden omvang is bijvoorbeeld het houden van een walk-through sessie met de leden van het crisisteam, waarin de leden aan de hand van een praktijkcasus worden getraind, en de inhoud van het draaiboek kritisch tegen het licht wordt gehouden. Een uitgebreide vorm van testen is het uitvoeren van een simulatie samen met ketenpartners en/of andere organisaties uit dezelfde sector. Een voorbeeld hiervan is de oefening die in de UK is gehouden door de FSA (de Britse financiële toezichthouder) eind 2006. 70 organisaties namen hieraan deel (totaal 3500 mensen waren hierbij betrokken). In deze oefening ging men zelfs zover dat de uitval van personeel opliep tot 49%! Naast het afwezigheids aspect werden ook financiële gevolgen in de simulatie meegenomen zoals b.v. dalende koersen, stijgende olieprijs. U kunt hier meer over lezen in: <http://www.fsa.gov.uk/pubs/other/mwe2006.pdf>

Figuur 1: Aandachtsgebieden bij uitbraak pandemie (KPMG, 2007)



Dilemma's

- Bovenstaande maatregelen lijken simpel maar voordat die ingevoerd kunnen worden krijgt men te maken dilemma's die nog opgelost moeten worden, zoals:
- Reisrestricties: kun je personeel verbieden privé naar risico gebieden te reizen?
- Indien gekozen is voor anti-virale middelen. Voor het hele personeel of alleen sleutelpersoneel? En dan ook voor gezinsleden (als die ziek zijn komt de medewerker toch niet opdagen)?
- Moet woon-werk verkeer geregeld worden? Openbaar vervoer kan uitvallen.
- Werkverplichting of vrijwillig werken? Extra belonen?

- Catering of niet (besmetting)?
- Sluiten van locaties of panden (denk daarbij ook aan cross training)?
- Telewerken: zijn de kritieke bedrijfsprocessen daar voor geschikt (b.v. papieren dossiers) en is het technisch mogelijk (voldoende lijnen/capaciteit)? Stel dat er geen internet is?

Tot slot

Dat een pandemie zich weer zal voordoen is zo goed als zeker. Wanneer de volgende pandemie zal toeslaan is onbekend, evenals de exacte gedaante ervan en de consequenties die deze zal hebben voor mensen, organisaties en de maatschappij als geheel. Deze onzekerheden zouden echter geen excuus mogen zijn voor organisaties om geen voorzorgsmaatregelen te treffen. Uit (historisch) wetenschappelijk onderzoek zijn voldoende lessen te trekken om nu zinvolle maatregelen te kunnen nemen, waarvan overigens ook onder normale omstandigheden of in andere noodscenario's dankbaar gebruik kan worden gemaakt.

Websites voor meer informatie over pandemie in relatie tot business continuity:

<http://www.minvws.nl/images/fo-grieppandemie-bedrijfsleven-tcm19-155722.pdf>

<http://www.bedrijfenpandemie.nl>

Tom Bakker RE RI CISA CISM is als group security officer werkzaam bij Delta Lloyd, e-mail: tom_bakker@deltalloyd.nl

Ir. Antoine Wijsman RE MBCI is national service manager BCM bij KPMG IT Advisory, e-mail: wijzman.antoine@kpmg.nl

COBIT Mapping: Mapping of NIST SP800-53 Rev. 1 With COBIT® 4.1

This document contains a detailed mapping of NIST SP800-53 Rev 1 with COBIT 4.1 and also contains the classification of the standards discussed in this paper as presented in the overview document COBIT® Mapping: Overview of International IT Guidance, 2nd Edition.

NIST SP800-53 is a security-related technical standard issued by NIST. It is one of NIST's SP800-series of reports 'providing research, guidelines, and outreach efforts in information systems security, and its collaborative activities with industry, government, and academic organizations'. Although this is a US federal government standard, it is applicable for all organisations interacting with the US federal government. More important, the standards included in NIST are good security practices for all organisations and therefore need to be looked at and used from that perspective.

EEN KWANTITATIEVE AANPAK IN DE INFORMATIEBEVEILIGING

Recent onderzoek wijst uit dat organisaties steeds afhankelijker worden van goed functionerende informatie- en communicatiemiddelen. Terwijl de omgeving van een organisatie alsmaar complexer en meer onderhevig aan veranderingen wordt, stijgen de gemaakte verliezen door slecht beheer van (informatie) beveiliging en een slechte staat van risicobeheersing.

Management van informatie gerelateerde risico's is niet alleen maar een kwestie van het implementeren van bewezen bestaande oplossingen, al kan dit er wel een wezenlijk onderdeel van zijn. Soms worden bepaalde risico's niet door de standaardoplossingen afgedekt en zijn er additionele maatregelen nodig om het risico naar een acceptabel niveau te doen dalen. Hieruit ontstaat de vraag naar een aanpak die inzicht geeft in, en controle geeft over het restrisico van een organisatie met betrekking tot de informatievoorziening.

Aanpak

Vandaag de dag wordt er vaak gekozen voor een kwalitatieve aanpak voor het beheeren van (informatie) restrisico's. Bij deze aanpak wordt een oordeel en prioriteitstelling gegeven van risicoblootstelling en maatregelen om zodoende het risiconiveau te kunnen beïnvloeden. Deze prioriteitstelling is van belang gebleken voor een snelle selectie van maatregelen. De globale inslag van deze aanpak zorgt ervoor dat er concessies gedaan moeten worden met betrekking tot de informatie waarop de beslissingen gebaseerd zijn. Er wordt geen of minimaal gebruik gemaakt van specifieke gegevens over impact, bedreigingen en kwetsbaarheden.

De kwantitatieve aanpak maakt wel gebruik van specifieke gegevens en voorspellingen waar de beslissingen op gebaseerd kunnen worden. Waar de kwalitatieve aanpak vaak als 'te ruim' wordt gezien met een zwak fundament, biedt een kwantitatieve aanpak de bouwstenen om te voorzien in een rigide basis voor de beslissingen. De keerzijde van de medaille is dat deze aanpak nogal wat voeten in de aarde kan hebben. Ook de beschikbaarheid en de kwaliteit van de gegevens spelen een belangrijke rol in een correcte risicoanalyse. Zelfs als de invoer van hoge kwaliteit is en het onderliggende model geverifieerd correct, blijven de uitkomsten onderhevig aan interpretatie van de eindgebruiker. Een verkeerde interpretatie van correcte gegevens kunnen, evenals een juiste interpretatie van verkeerde gegevens, leiden tot verkeerde beslissingen.

Kwantitatief

De term 'een kwantitatieve aanpak' is een weinig specifiek met betrekking tot de te kwantificeren eenheden. De kwantitatieve stromingen binnen de risicomangement praktijk richten zich vooral op kosten-baten analyses om zodoende beveiligingsgerelateerde investeringen te kunnen onderbouwen met een financiële argumentatie. Termen die dan al snel boven water komen zijn 'variability of losses' en 'value at risk'. Hoewel deze aanpakken nuttig zijn gebleken voor enkele kapitaalmanagement toepassingen, zijn ze niet altijd toepasbaar in elke situatie.

Een gebrek aan een grote hoeveelheid specifieke en accurate informatie weerhoudt ons er op dit moment van gebruik te maken van aanpakken gebaseerd op distributiefuncties. Dit gebrek is lastiger op te lossen dan men aanvankelijk wellicht denkt. In de informatiebeveiliging zijn er veel scenario's met een grote impact maar met een lage waarschijnlijkheid te bedenken. Juist over deze scenario's zal weinig informatie beschikbaar zijn.

Zelfs al zouden we de 'variability of losses' en 'value at risk' vast kunnen stellen per scenario, dan nog zouden we weinig conclusies kunnen trekken aangaande de totale risicoblootstelling. Onze kennis van afhankelijkheden en correlaties tussen de scenario's is immers beperkt en dit weerhoudt ons ervan om de risico gerelateerde kwantiteiten te aggregeren.

Annual Loss Expectancy

Een mogelijke aanpak zou 'annual loss expectancies' (ALE) kunnen zijn. Het voordeel van deze aanpak is dat er geen kennis van onderliggende distributies of interacties tussen scenario's nodig is om tot een model te komen dat een nauwkeurige representatie kan geven van de risicoblootstelling van een organisatie. Aggregatie van risico's kan een kwestie zijn van simpele sommatie. De simpliciteit van de aanpak zorgt ervoor dat hij flexibel is en aangepast kan worden aan onze wensen. Niet elke aanpassing zal uiteindelijk echter even eenvoudig blijken (bijvoorbeeld: tijdsafhankelijkheden, overlappende effecten van countermeasures en controls).

Als we een informatiebeveiligingsrisico definiëren als een combinatie van een impact van een event en een waarschijnlijkheid van dit event zullen we zowel impact als waarschijnlijkheid moeten modelleren.

Impact

Aangezien we in dit voorbeeld gebruikmaken van 'loss expectancies' ligt het voor de hand het risico uit te drukken met behulp van een verliesfunctie. Het is aan de eindgebruiker om hier een functie voor te definiëren welke een zo een realistisch mogelijk beeld geeft van de werkelijk te verwachten risico's.

Voorbeeld impactfunctie:

Als we er vanuit gaan dat verliezen zich manifesteren op procesniveau en worden gerealiseerd door een breuk van bepaalde informatie criteria, dan kan een verliesfunctie er als volgt uitzien:

$$L^{\max}(p) = \sum_{k \in K} (L_k^{\max}(p))$$

Het maximale verlies (L^{\max}) te realiseren in een bedrijfsproces p , is de sommatie van de separaat aan te duiden verliezen door breuk van informatie criterium k .

Noot: Het moge duidelijk zijn dat hier een additiviteitsaannname geldt met betrekking tot de separate verliesposten.

In het voorbeeld wordt gebruik gemaakt van een 'worst-case scenario' met een maximaal mogelijk verlies per bedrijfsproces. Dit is een veilige manier omdat men zo zoveel mogelijk verlies en dus risico zal willen afdekken. Niet iedereen zal echter dezelfde strategie met betrekking tot het nemen van risico's volgen. De verliesfunctie dient aangepast te worden aan de risicostrategie van de organisatie.

Waarschijnlijkheid

De waarschijnlijkheid dat een breuk van een informatiecriterium leidt tot verlies wordt bepaald door bedreigingen die kwetsbaarheden exploiteren. Deze kwetsbaarheden vinden bijvoorbeeld hun oorsprong in de applicaties die gebruikt worden in de bedrijfsprocessen. De vraag is echter, hoe komen we aan de waarschijnlijkheidsinformatie van alle scenario's?

In sommige situaties zal het voorkomen dat waarschijnlijkheidsinformatie aanwezig is door eerder uitgevoerd onderzoek. Ook kan het mogelijk zijn informatie over soortgelijke scenario's uit andere bedrijfstakken te extraheren. Dit zal echter in veel situaties niet mogelijk zijn.

Een alternatief is te vinden in het inschatten van waarschijnlijkheid naar aanleiding van een aantal karakteristieke kenmerken van de bedreiging of kwetsbaarheid. In dit geval ligt de uitdaging in het selecteren van de juiste karakteristieken om zo de voorspellende waarde van de kenmerken te maximaliseren. Gelukkig zijn er methoden en technieken te vinden die helpen in de automatische selectie van karakteristieken met de hoogste voorspellende waarde gegeven een bestaande dataset. Zo kan het model automatisch lering trekking uit bestaande situaties en zichzelf aanpassen bij introductie van nieuwe gegevens.

Scenario

Het beschouwen van losstaande bedreigingen en kwetsbaarheden geeft weinig inzicht in het risiconiveau van een organisatie. Bedreigingen en kwetsbaarheden vorm gegeven in een abstracte vorm van een scenario kunnen echter wel helpen bij het bepalen van het te lopen risico. Door gebruik te maken van een scenario, of combinatie van een kwetsbaarheid met één of meerdere bedreigingen, kan de waarschijnlijkheid van een incident berekend worden door gebruik te maken van de afzonderlijke waarschijnlijkheden van zowel kwetsbaarheid als bedreiging. De waarschijnlijkheid van het incident kan dan met relatief simpele berekeningen (met voorwaardelijke kansen) worden bepaald.

Bayesian Network

Een voorbeeld van het bovenstaande scenario-mechanisme kan gegeven worden door gebruik te maken van een zogenaamd 'Bayesian network'. Bayesian networks zijn zogenaamde 'directed acyclic graphs' (DAGs) waar de separate elementen in het netwerk de variabelen weergeven en waar de links tussen de elementen een causaal verband weergeven tussen deze variabelen. Hoe sterk dit verband is hangt af van de voorwaardelijke kans tussen de variabelen.

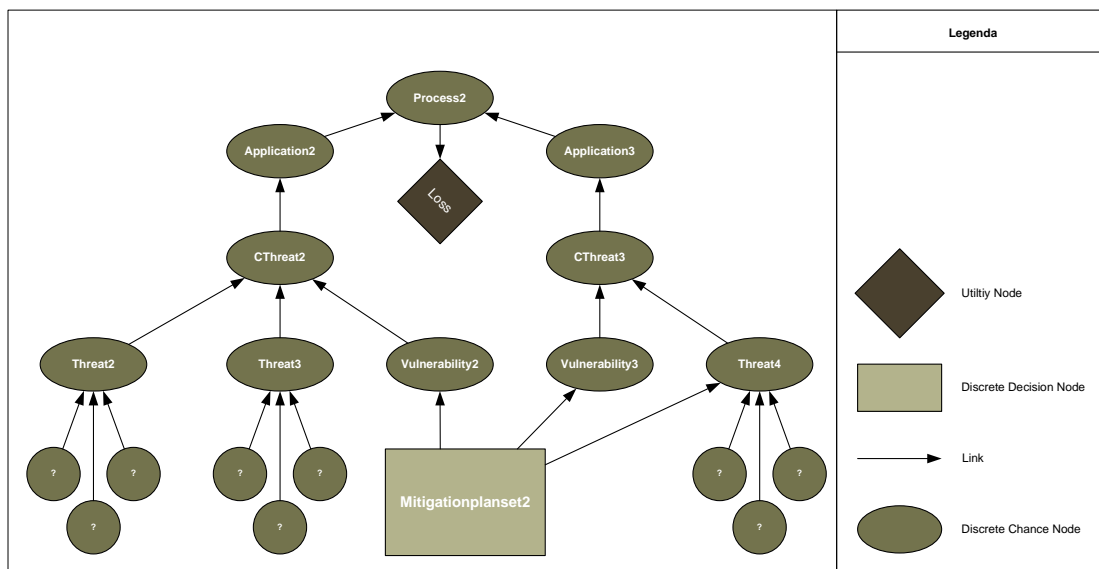


Figure 1 - Bayesian network example

Het voorbeeld uit Figure 1 laat een voorbeeld zien van hoe een Bayesian network gebruikt kan worden voor het modelleren van waarschijnlijkheden tot op een procesniveau. Naast de elementen zoals bedreiging (threat) en kwetsbaarheid (vulnerability) laat het figuur zien dat deze elementen worden samengevoegd als een 'cumulative threat' waarvan de waarschijnlijkheid berekend kan worden. De additionele elementen zoals de 'discrete decision

node' (om mitigationplans te modelleren) en de 'utility node' (om mogelijke verliezen te modelleren) zijn onderdeel van een uitgebreidere implementatie welke hier niet verder zal worden besproken.

Huidig Risico

Als we de twee bovenstaande componenten van impact en waarschijnlijkheid in ons achterhoofd houden kunnen we een functie definiëren die de huidige situatie weer kan geven met betrekking tot het risico.

Voorbeeld risicofunctie:

We definiëren de huidige risicofunctie R_{cur} van 'cumulative threat' c op proces p als zijnde een combinatie van impact en waarschijnlijkheid.

$$R_{cur}(p, c) = \left(\sum_{k \in K} (T_k L_k^{\max}(p)) \right) \cdot P(c)$$

De functie laat duidelijk de scheiding zien tussen impact en waarschijnlijkheid. De toegevoegde T_k is een zogenaamde 'cumulative threat type toggle' welke 0 of 1 is naar gelang de positie van de cumulative threat in een binaire ruimte met k dimensies (toggle is 1 als de cumulative threat een informatie criterium k kan breken wat kan resulteren in verlies).

Zodra we het informatierisico kunnen berekenen per cumulative threat in een proces kunnen we de risicowaarden simpel aggregeren door te sommeren over alle cumulative threats in een applicatie, alle applicaties in een bedrijfsproces en alle bedrijfsprocessen in een organisatie. Hierbij dient wel de onafhankelijkheid van componenten en dus additiviteit van risicowaarden in het achterhoofd gehouden te worden.

Restrisico

Analoog aan bovenstaande functie kunnen we een functie maken welk het restrisico van een organisatie weergeeft. Dit is, zoals eerder beschreven, het risico dat men loopt na implementatie van controls en countermeasures. Als we er vanuit gaan dat we met deze controls en countermeasures invloed uitoefenen op de cumulative threat, kunnen we c_m definiëren wat staat voor de cumulative threat na invoering van mitigation plan m .

Controls en Countermeasures

Bij de voorgaande definitie van het restrisico gaan we er vanuit dat het beste plan voor controls en countermeasures bekend is. Ook dit is echter een probleem wat relatief gemakkelijk om te zetten is naar een abstracte wiskundige representatie.

De selectie van de juiste countermeasures is feitelijk niets anders dan een optimalisatieprobleem waar men de baten (p) van een collectie countermeasures wil maximaliseren en de kosten (w) van deze collectie onder een bepaald budget wil houden (d). Dit probleem is weer te geven als een 'multiple-choice binary knapsack problem' zoals hieronder weer geven.

$$\begin{aligned} & \text{maximize} && \sum_{i=1}^n p_i x_i \\ & \text{subject to} && \sum_{i=1}^n w_i x_i \leq d \\ & && x_i \in \{0,1\}, \quad i \in \{1, \dots, n\} \end{aligned}$$

Dit optimalisatieprobleem is bewezen NP-hard en kan worden opgelost in pseudo-polynomial time door gebruik te maken van een 'branch-and-bound' algoritme, dynamisch programmeren, of een combinatie van beide. De resultaten zijn representatief voor de optimale combinatie van controls en countermeasures onder een budgettair limiet.

Relatieve Verbetering

De bovenstaande componenten geven nu genoeg houvast om zowel de huidige situatie als de situatie waarin controls en countermeasures zijn geselecteerd te vergelijken. Aangezien er in het model ruimte is voor aannames en schattingen, en redeneert onder een zekere mate van onzekerheid heeft het op dit punt weinig zin om absolute resultaten te presenteren. Wel mogelijk is het aangeven van een verbetering van de nieuwe situatie in vergelijking met de voorgaande situatie. Denk hierbij aan de volgende constructie:

$$\frac{100 \cdot (R_{cur} - R_{res}(M))}{R_{cur}}$$

Deze functie geeft de relatieve verbetering weer waar een uitkomst van 0 duidt op geen verbetering en een uitkomst van 100 duidt op een situatie waar geen (gedefinieerd) restrisico meer aanwezig is.

Conclusie

Het gebruik van kwantitatieve methodieken in risicoanalyses is niets nieuws. De grondslagen voor een kwantitatieve aanpak met betrekking tot informatie (technologie) risico analyses werden gelegd in de vroege jaren '80. Hoewel deze aanpak sindsdien uit de gratie lijkt te zijn geraakt door enkele tekortkomingen, is het toch zaak de aanpak niet geheel uit te sluiten als zijnde een waardevolle toevoeging aan de risk assessment toolbox.

Doordat de tekortkomingen van de vroege generatie (ALE) modellen tenietgedaan kunnen worden door zowel technologische als theoretische ontwikkelingen kan deze kwantitatieve aanpak inzicht geven in, en controle geven over het informatie restrisico van een organisatie. Als de beperkingen en het toepassingsgebied in het achterhoofd worden gehouden kan het een welkome aanvulling zijn op de hedendaags veel gebruikte kwalitatieve aanpak.

Jarno Roos MSc is werkzaam bij KPMG IT Advisory, email: Jarno.roos@kpmg.nl

