02/2013

INFORMATIE BEVEILIGING

PvIB
Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 2 - 2013

VAN RISICOMANAGEMENT NAAR SUCCES GOVERNANCE

EXPERTGESPREK - I&AM VOLWASSENHEID

STARREVELD KOMT WEER UIT DE KAST

ENCRYPTION WITH A TWIST - INTERVIEW MET JUUSO PESOLA

Overheid &ict

www.overheid-en-ict.nl

23 t/m 25 april 2013
Jaarbeurs Utrecht

Overheid & ICT is hét platform voor ICT-toepassingen en -diensten voor de overheid

Vraag nu gratis uw toegangsbadge aan via overheid-en-ict.nl

MEDE MOGELIJK GEMAAKT DOOR

ETTU the art of sharing
Decos Information Solutions
BlackBerry

KENNISPARTNER

VNG Vereniging van Nederlandse Gemeenten

BRANCHEORGANISATIES

KING Kwaliteitsinstituut Nederlandse Gemeenten
Logius
GBO provincies
HetWaterschapshuis
GIN

HOOFDMEDIAPARTNERS

BB
Kluwer a Wolters Kluwer business

MEDIAPARTNERS

GIS Magazine
infosecurity.nl Magazine
Cloud Works
ambtenarennieuws
Gemeente.nu

vnu exhibitions europe

VOORWOORD

De Fyra. Het is een synoniem geworden voor een mislukt project op het spoor. Maar is het wel zo mislukt? Eigenlijk hebben we precies gekregen wat we hebben gevraagd: Een goedkope trein die er snel uitziet en ook wat sneller dan normaal over het spoor kan rijden, voor een hoge snelheidsdienst over korte afstanden. De Benelux is nu eenmaal veel kleiner dan Frankrijk of Duitsland. Goedkoop was het belangrijkste criterium, om een aantal redenen:

- de NS had zich al te duur ingekocht op de lijn;
- er woedt nou eenmaal een economische crisis;
- op die korte trajecten kom je niet aan topsnelheden;
- treinkaartjes zijn al te duur, vindt het grote publiek.

Een treinbouwer in Italië mag de treinen leveren - zij hebben de aanbesteding op prijs gewonnen. De treinen zijn geleverd, maar voldoen niet aan de verwachting. In België hebben ze zelfs een rijverbod. Resultaat: De tussenoplossing: oude, degelijke Duitse intercity-treinen rijden nog steeds op het traject tussen Amsterdam en Breda.
Het diepgaande onderzoek naar de Fyra moet nog gedaan worden, dus het kan zijn dat ik wat details verkeerd heb. Maar in grote lijnen komt het hier op neer: We wilden kwaliteit voor weinig geld, té weinig geld en hebben dat niet gekregen. "You get what you pay for", in goed Engels gezegd.
Ik zie tegenwoordig hetzelfde gebeuren bij IT projecten, zeker wat betreft de security. Security expertise is iets wat alleen de grote organisaties binnenshuis kunnen kweken.
De meesten zullen deze bij projecten tijdelijk extern moeten inkopen. Daar is niets mis mee, hetzelfde geldt voor andere automatiseringsspecialismen.
Maar er komt een effect bij: de experts moeten steeds vaker voor behoorlijk minder aan de slag. Dat is niet omdat ze hun vakgebied niet hebben bijgehouden, maar omdat er goedkoper aanbod op de markt is verschenen en de inkopers puur op prijs beslissen.
Bij concurrentie op basis van prijs is de bijbehorende waardepropositie "operational excellence" - een goed product voor de laagste prijs. Hierbij geldt wel dat er een verband is tussen de kwaliteit en prijs.
En waardeproposities als "product leadership" of "customer intimacy" zijn niet eens meer aan de orde, want dan kun je je op prijs niet meer onderscheiden.
Je hebt als expert je grenzen om mee te kunnen bewegen op prijs. Het kost tijd en geld om je expertise te onderhouden. En wil je je onderscheiden op één van de twee andere waardeproposities, dan kom je in de huidige markt van een koude kermis thuis.
Kortom, ik zie bij veel projecten zulke lage prijzen betaald worden voor beveiligingsexpertise, dat ik bang ben dat we op dit vlak ook grootschalig Fyra's aan het aanschaffen zijn.
Dat weten we nu nog niet, maar daar komen we wel achter, wanneer het in IT-land eens goed gaat sneeuwen en vriezen... ●

Lex Borger, hoofdredacteur

INHOUDSOPGAVE

Foto Omslag: "Daly Waters pub", cc-by-nc-sa by Peter Nijenhuis.

VAN RISICOMANAGEMENT NAAR SUCCES GOVERNANCE

Rieks Joosten is Wetenschappelijk onderzoeker bij TNO

Alle IT incidenten die WebWereld in oktober 2011 [1] heeft gemeld, zijn veroorzaakt door één van de top 10 exploits, zoals die op het OWASP-afstreeplijstje van 2010 reeds zijn vermeld [2]. Het is merkwaardig dat regelmatig wordt gemeld dat servers zijn gecompromitteerd doordat, bijvoorbeeld, security updates niet tijdig zijn geïnstalleerd, terwijl zelfs consumenten weten dat ze dit – liefst automatisch – moeten doen.

Op basis van verschillende gesprekken met IT professionals geloven we dat zij voor het overgrote deel welwillend en competent zijn, ondanks dat ze soms dingen doen die tegen het beveiligings- (of ander) beleid ingaan. Waar we dat hebben nagevraagd, bleek men verrassend vaak hele goede redenen te hebben om te doen wat men doet. Ook gaan we ervan uit dat grote partijen, die het belang van informatiebeveiliging publiekelijk onderstrepen (bijvoorbeeld door deel te nemen aan organisaties als de Nationale Cyber Security Raad), security ook echt belangrijk vinden, ondanks dat ook zij lijden aan incidenten als hiervoor genoemd.
Kennelijk werkt de huidige manier waarop we risicomanagement doen niet (meer). In dit artikel geven we hiervoor een aantal redenen en stellen we een richting voor waarvan wij denken dat deze leidt tot een efficiëntere en effectievere aanpak.

Risicomanagement anno nu

Hoewel er ongetwijfeld uitzonderingen zijn en er natuurlijk ook dingen goed gaan, zijn we door de bank genomen tamelijk sceptisch over de efficiëntie en effectiviteit van het huidige risicomanagement (RM) en de mate waarin het wordt gedragen door de business. Wij onderbouwen onze scepsis aan de hand van verschillende signalen die we in de praktijk zijn tegengekomen en geven aan wat wij denken dat de oorzaak daarvan is.
Signaal 1: het periodiek uitvoeren van risicoanalyses. Het probleem hiermee is, dat als je de periode kort maakt, dit ten koste gaat van draagvlak, kosten en effort. Toch blijft het ook met korte periodes mogelijk om een risico te missen dat ontstaat door een net nieuw bekend geworden exploit of kwetsbaarheid te missen, die dan mogelijk een tijdlang niet gemanaged wordt. Bij langere periodes wordt dit effect alleen maar groter.
Signaal 2: beginnen met het inventariseren van 'assets' en 'threats' (en 'vulnerabilities'). Omdat je dan (nog) niet weet wat voor de business belangrijk is en wat niet, kun je ook (nog) niet vaststellen of je de belangrijkste assets, threats en vulnerabilities hebt en ben je dus mogelijk inefficiënt bezig. Je stopt dan effort in zaken waarvan later kan blijken dat ze niet (zo) van belang zijn voor de business objectives.

> Kennelijk werkt de huidige manier van risicomanagement niet meer

Signaal 3: voor een risico-inventarisatie en –analyse sessie worden alle stakeholders uitgenodigd, zoals portfoliomanagement, inkoop, verkoop klantenservice, proceseigenaren, functioneel beheer, technisch beheer, netwerkbeheer, quality & control, etc. Vaak is zo'n sessie een soort Poolse landdag: mogelijk gezellig, maar matige resultaten.
Signaal 4: naast policies (security objectives) is niet veel geregeld. Het kan zijn dat er geen verantwoordelijke is – dan weet je niet wie je moet aanspreken. Het kan ook zijn dat een objective niet voorzien is van een criterium, waaraan je kunt weten wanneer er wel/niet aan is voldaan (dat tot onenigheid kan leiden). Het kan zijn dat er geen link is met de business – dan weet je niet of de policy je meer kost dan dat hij (business wise) oplevert en je weet ook niet hoe zwaar je moet inzetten om hem na te (laten) leven. Of het klakkeloos overnemen van ISO 27001 objectives wel zo'n goed idee is, is dan ook nog maar de vraag…
Signaal 5: men weet niet goed wat een dreiging is. Soms wordt 'bliksem-inslag' zonder discussie als dreiging opgevoerd. Maar hoewel dit voor het elektriciteitsbedrijf weliswaar een dreiging is die haar bedrijfsvoering grondig kan verstoren, kan dit voor de journalist een uitgelezen kans zijn op een primeur. Of blikseminslag een dreiging is, hangt er vanaf of het onvoorziene (negatieve) impact heeft op je business.
Signaal 6: men weet niet goed wat de impact is. Soms is er sprake van "DE impact van een blikseminslag in een transformatorstation". Maar er is niet zoiets als 'DE' impact – dat moet worden gerelateerd aan de context. Voor het elektriciteitsbedrijf betekent dit het moeten mobiliseren van monteurs, voor huishoudens die geen elektriciteit meer krijgen kan de voorraad in de vriezer verloren gaan. De bakker die zijn oven 'uit' ziet gaan, kan zijn bruiloftstaart niet meer leveren

en de getroffen bruid zou daar erg emotioneel onder kunnen worden…
Signaal 7: rapportages waarvan de gegevens niet leiden tot inzicht en of actie. Stel dat een rapport het aantal incidenten van afgelopen jaar vermeld en erbij zegt dat het ten opzichte van vorig jaar is verdubbeld. Wat kun je daar dan mee? Heb je nu een probleem (omdat er echt meer incidenten zijn geweest) of was de awareness training succesvol?
Signaal 8: er wordt gezwaaid met certificaten en/of afspraken (SLA's) die standaard security paragrafen bevatten. Echter, de redeneerlijn die ertoe leidt dat juist deze dingen de assurance opleveren die je graag wilt, ontbreekt doorgaans. Het komt regelmatig voor dat (ook hier) de link met business objectives zoek is. In zulke gevallen stelt de betekenis van het hebben van certificaten of het vragen aan toeleveranciers of ze gecertificeerd zijn, niet veel voor.

Oorzaken

Mensen willen graag complexe dingen realiseren, in de bouw, de IT enzovoorts (het is opmerkelijk dat het gebouw van het Europese parlement in Straatsburg erg lijkt op de toren van Babel in het bekende schilderij van Breughel).

We weten niet goed wat een dreiging is

Dat is erg moeilijk, onder meer door de fysiologische beperking dat een persoon niet meer dan 7 +/– 2 dingen tegelijkertijd kan overzien in hun onderlinge samenhang [3]. Daarom hebben we bedacht dat mensen zich kunnen specialiseren – het 'Division of Labor' paradigma. Als iedereen zich specialiseert (de een verzorgt de inkoop, de ander verkoop, enz.) kun je met een groep mensen toch een complex geheel maken. Maar wie zich specialiseert, vervreemdt ook (tot op zekere hoogte) van het geheel en kan niet (zo goed) overzien wat anderen doen. Dat verklaart bijvoorbeeld het 'Swiss Cheese' effect [4], waarbij een relatief klein incident kan uitgroeien tot een enorme catastrofe.

Specialisatie zien we steeds vaker optreden in de vorm van uitbesteden. In deze vorm van specialisatie wordt ook een deel van de verantwoordelijkheden – namelijk die voor de operationele uitvoering – overgedragen aan anderen, waardoor risico's steeds meer onder het maaiveld dreigen te verdwijnen. Dat dit aanleiding is voor een andere kijk op risicomanagement is al eerder aangegeven [5].

Gebouw van het Europese Parlement in Brussel

Bij veel risico-inventarisaties en -analyses wordt de scope vastgesteld (dat gebeurt als het goed is in de eerste stap), maar vaak zo groot dat die niet meer te behappen is. Daarom worden er – en dat is onontkoombaar – fouten gemaakt. Scopes moeten zo klein zijn, dat ze 'behapbaar' zijn (d.w.z. "kleiner dan of gelijk aan 7 +/– 2"). Het is dus, ofwel fouten maken, ofwel een manier zien te vinden om die scopes klein genoeg te krijgen.
Een tweede oorzaak is dat de business liever focust op succes dan op risico. De eerste associatie bij risico is immers: 'falen'. Het is overigens ook al een oude hartenkreet van de business (en risicomanagers), dat RM (beter) moet aansluiten bij de business.

Van risicomanagement naar Succes Governance

El Metodo is een methode voor Succes Governance die is voortgekomen uit de ideeën van 'gescoopt risicomanagement' [6] en hoe die in ketens te gebruiken [7] en is in de basis erg simpel, omdat het op een natuurlijke wijze aansluit op de manier waarop mensen al sinds jaar en dag met risico's omgaan. We beschrijven de methode hier op hoofdlijnen.

Het gebouw van het EP lijkt op de toren van Babel

El Metodo heeft een paar uitgangspunten:

- jij bent succesvol in de mate waarin jij jouw verplichtingen aan anderen (of jezelf) nakomt – daar worden jij en die anderen immers blij en tevreden van.
- bestuur alleen je eigen succes, de anderen doen dat ook voor zichzelf.
- door jouw succes te koppelen aan c.q. te delen met dat van anderen, worden jullie ook als geheel succesvol.

El Metodo ondersteunt dus expliciet de (soms als 'lastig' ervaren) koninkrijkjes. Als ze echter hun succes gaan delen zijn ze niet (meer) zo lastig, omdat ze gaan bijdragen aan het succes van het geheel. Eerst moet je dus weten hoe je zelf succesvol kan zijn, d.w.z. dat je jouw verplichtingen ten aanzien van anderen moet kennen. Als je het overzicht niet meer houdt, dan is dat een teken dat je minder verplichtingen op je moet nemen – je moet je verplichtingen kunnen blijven besturen. Hou het behapbaar voor jezelf.

Activiteit "Business Impact Assessment" (BIA)

Maak een lijstje waarin al je verplichtingen zijn opgesomd, althans voor zover die van belang zijn voor jouw succes. Zet bij elke verplichting een score (bijvoorbeeld L, M of H) die dat belang aangeeft (c.q. hoeveel

Toren van Babel van Pieter Brueghel

schade jij leidt als je de verplichting niet nakomt [8]). We noemen deze score de 'impact' van de betreffende verplichting [9]. Deze activiteit is klaar, als je er van overtuigd bent dat er geen verplichting meer is die zodanig van belang is voor jou dat je hem zou willen managen.
Het inrichten van je succes bestaat hieruit dat je van elke verplichting in de gemaakte lijst gaat bepalen hoe je die gaat waarmaken. Wat doe je zelf? Wat verwacht je van anderen? Inventariseer deze verwachtingen en hou vooral ook bij voor welke van jouw (belangrijke) verplichting(en) die relevant zijn. Je kunt aan elke verwachting ook een 'belang' toekennen, dat je relateert aan de mate waarin de gerelateerde verplichtingen aan je succes bijdragen. Zo weet je op welke verwachtingen je het meest alert moet zijn.

Activiteit "Succes Inrichten" (SI)
Maak een lijst waarin al je verwachtingen zijn opgesomd voor zover die van belang zijn voor jouw succes. Geef bij elke verwachting aan voor welke verplichting(en) de verwachting relevant is. Dat kan op verschillende manieren. Kies de manier die jou het beste helpt in de stappen die nog volgen [10]. Geef op dezelfde manier, zoals je bij verplichtingen hebt gedaan, het belang aan van elke verwachting. Deze activiteit is klaar als je er voor elke verplichting van overtuigd bent dat je zonder meer aan die verplichting gaat voldoen [11], als is voldaan aan alle verwachtingen waarvan die verplichting afhankelijk is.

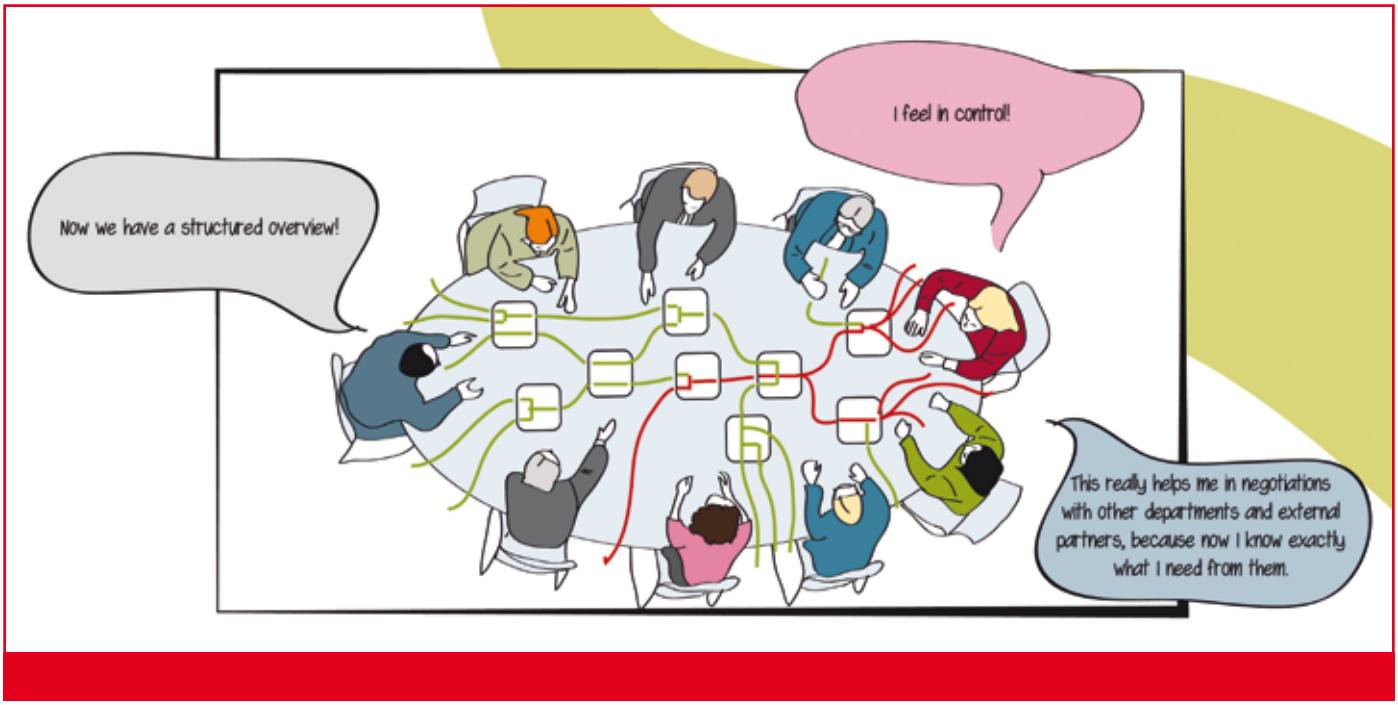
Het besturen van je succes bestaat hieruit dat je een zodanige inrichting vindt dat je alle (belangrijke) verplichtingen kunt waarmaken.
Je moet dus eerst kunnen vaststellen of je een verplichting al dan niet gaat waarmaken. Dat doe je door eerst van de verwachtingen in te schatten of ze waargemaakt zullen worden (door de anderen), te kijken hoe dat bijdraagt aan het waarmaken van jouw verplichting (afhankelijkheden heb je immers al in kaart gebracht), en in te schatten in welke mate jij dus aan die verplichting gaat voldoen (en dus succesvol zult zijn). Je kunt ook zeggen: in welke mate je niet aan die verplichting gaat voldoen en dus hoeveel risico je loopt. Dat zijn twee kanten van dezelfde medaille.

El Metodo is een methode voor Succes Governance

Activiteit "Kansen Inschatten" (KI)
Schat voor elke geïnventariseerde verwachting in hoe groot de kans is dat eraan voldaan gaat worden [12]. Schat dan voor elke verplichting in hoe groot de kans is dat jij die waar gaat maken, gegeven de ingeschatte kansen voor verwachtingen. Deze activiteit is klaar als je ervan overtuigd bent dat – gegeven alle informatie die voorhanden is – alle kansen ingeschat zijn en jij je voldoende zeker voelt dat deze inschattingen correct zijn.

Activiteit "Succes Besturen" (SB)
Ga voor alle verplichtingen na of het risico dat je er niet aan gaat kunnen voldoen acceptabel is, gegeven de ingeschatte kans (uit activiteit "KI") en impact (uit activiteit "BIA"). Deze activiteit is klaar als voor alle verplichtingen die in de BIA zijn geïnventariseerd, is vastgesteld dat het risico op het er niet aan voldoen, voor jou acceptabel is.

Waar het uiteindelijk om gaat, is dat het resultaat van "Succes Besturen" wordt gehaald. Dat kan (zie de hiervoor gegeven beschrijving) alleen als er een BIA is uitgevoerd en als de risico's van de erin genoemde verplichtingen zijn vastgesteld. Als dat op een biervilte kan is dat prima. Wie dat wat uitgebreider wil doen kan



"Kansen Inschatten" uitvoeren, ook als "Succes Inrichten" nog niet is uitgevoerd. Als de kansen onvoldoende zeker zijn, kan SI alsnog worden uitgevoerd. Daarom schrijft El Metodo geen volgorde voor waarin activiteiten moeten worden uitgevoerd, maar definieert El Metodo het te behalen resultaat als een toetsbaar criterium voor het hebben uitgevoerd van een bijbehorende activiteit (die we een naam geven) zodat iedereen kan vaststellen of dit resultaat ook is gerealiseerd. Als, om dat resultaat te halen, andere resultaten nodig (zouden kunnen) zijn, dan worden ook die gespecificeerd, middels een toetsbaar criterium en de naam waarmee we de activiteiten benoemen waarin dat resultaat wordt geproduceerd.

Afspraken over resultaten van activiteiten in plaats van over uitvoering van activiteiten

El Metodo schrijft nergens een werkwijze voor, omdat het ervan uitgaat dat uitvoerders competent zijn en dus zelf wel weten hoe de resultaten te behalen. Vaak zijn werkwijzen elders al beschreven – ISO 31010 somt meer dan 30 technieken op voor risk assessment – en die kunnen gewoon worden toegepast zolang de binnen El Metodo gespecificeerde resultaten uiteindelijk maar worden opgeleverd.

El Metodo is dus een framework waarin activiteiten worden gedefinieerd in termen van specifieke, toetsbare resultaten die het uitvoeren ervan moet opleveren, en een naam om naar zulke activiteiten te kunnen verwijzen. El Metodo kan dus ook worden uitgebreid met zulke definities. Criterium om een activiteit in het framework op te nemen is dat het een specifiek, toetsbaar resultaat oplevert dat bruikbaar is in één van de bestaande activiteiten van het framework.

Zo kan bijvoorbeeld een activiteit "SLA afsluiten" worden gedefinieerd met een zekere (andere) partij ten aanzien waarvan jij tenminste één verplichting of verwachting hebt. Het resultaat-criterium is: "elke SLA-partij (jij en die ander dus) heeft vastgesteld dat voor elke verplichting en verwachting die deze SLA-partij heeft t.a.v. een andere SLA-partij, die andere SLA-partij een verwachting c.q. verplichting heeft ten aanzien van de eerste SLA-partij en dat die verwachting c.q. verplichting met zijn eigen verplichting c.q. verwachting overeenkomt".
Een dergelijke activiteit kan bijdragen aan het verkrijgen van de "voldoende zekerheid" die nodig is in het proces "Kansen Inschatten". Merk op dat een activiteit met het aldus gespecificeerde resultaat meteen de inhoud van een SLA oplevert, waarbij alles te herleiden is naar je eigen succes (verplichtingen).
Het maken van afspraken over de resultaten van activiteiten, in plaats van over hoe een activiteit moet worden uitgevoerd, heeft als voordeel dat iedereen zijn eigen werkwijzen kan blijven hanteren, terwijl – vanwege de gemaakte afspraken – de resultaten toch door anderen gebruikt kunnen worden. Dit is bijvoorbeeld van belang als twee partijen die onderling verplichtingen en verwachtingen hebben, de kansen zouden delen dat er niet aan voldaan gaat worden, om zo de risico's over ketens te gaan delen [7].

Samenvatting

De huidige manier van risicomanagement werkt niet. We hebben een aantal voorbeelden uit de praktijk gegeven die dit aantonen. We hebben ook een acht-tal signalen geïdentificeerd die deze manier van risicomanagement identificeren en aangegeven waarom dit tot inefficiëntie of ineffectiviteit leidt. Daarna hebben we als oorzaak voor het falen van deze werkwijze genoemd dat mensen fysiologische begrenzingen hebben die niet worden gerespecteerd (wat tot fouten leidt) en dat de business meer in succes dan in falen (risico's) is geïnteresseerd. Vervolgens hebben we op hoofdlijnen een framework beschreven, El Metodo, die deze begrenzingen wel respecteert en geformuleerd is in termen van wat de business wil (resultaten, succes en kansen). Grote veranderingen beginnen met een eerste stap. Wij dagen je uit om een eerste stap te zetten, een toets te doen op je huidige aanpak en daarin, op basis van onze aanpak, die zaken te identificeren die je niet helpen bij het managen van relevante risico's. Graag vernemen wij hoe het je daarbij is vergaan. ●

Referenties

[1] *WebWereld Lektober: maand van het privacylek (http://webwereld.nl/dossiers/8/lektober-maand-van-het-privacylek.html).*

[2] *OWASP Top 10 Application Security Risks – 2010. (https://www.owasp.org/index.php/Top_10_2010-Main)*

[3] *G. Miller, "The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information", The Psychological Review, 1956, vol. 63, pp. 81-97.*

[4] *Reason, J. "Human Error". New York, NY: Cambridge University Press, 1990.*

[5] *Smulders, A. "Cybersecurity als driver voor andere aanpak risicomanagement", Informatiebeveiliging, nummer 4, 2011.*

[6] *Joosten, R. "'Gescoopt' Risico Management"; Informatiebeveiliging, oktober 2010, pp 12-17.*

[7] *Hoeve, M. v.d. et. al.: "El Metodo - Managing Risks in Value Chains"; Proceedings of the ISSE 2011 - Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe 2011 Conference, 22 -23 November 2011; Prague, Czech Republic.*

[8] *We gaan er gemakshalve van uit dat elke verplichting die erg belangrijk voor je succes is, ook veel schade oplevert als hij niet wordt nagekomen en omgekeerd.*

[9] *Je kunt ook een tekening maken in bijvoorbeeld PowerPoint of Visio, daarin je verplichtingen als tekst in rechthoeken tekenen en de impact score aangeven als kleur (rood, oranje of groen) voor de (dikke) rand.*

[10] *Als je een tekening maakt, kun je ook de verwachtingen intekenen als een rechthoek met afgeronde hoeken (om ze te onderscheiden van verplichtingen); je kunt dan een lijn trekken tussen verwachtingen en verplichtingen die van elkaar afhankelijk zijn. Kleuren van randen, achtergronden, lijndiktes e.d. kun je gebruiken om attributen als 'belang', 'impact' en later ook 'risico' mee aan te geven.*

[11] *Alternatief: je bent er van overtuigd dat het rest-risico acceptabel is.*

[12] *Dat kan bijvoorbeeld door in de tekening de verwachtingen een achtergrondkleur te geven (bijvoorbeeld rood, oranje of groen).*

EXPERTGESPREK

I&AM VOLWASSENHEID

Lex Borger is als consultant werkzaam bij I-to-I. Lex is een expert op het gebied van informatiebeveiliging en identity&access management. Hij is te bereiken via l.borger@i-to-i.nl.

Onlangs had ik een gesprek met een aantal experts over de relatie tussen volwassenheid van een organisatie en de inrichting van identity&access management (I&AM). Welke gevolgen zijn er voor I&AM als een bedrijf zijn processen meer formaliseert en een meerlaags organisatiemodel gebruikt voor informatiebeveiliging?

De gespreksdeelnemers zijn:

Ali Agzanay, security officer bij Univé, met een achtergrond in security en architectuur. Hij is te bereiken via A.Agzanay@unive.nl

Eefje van der Harst, product manager SURFconext bij SURFnet, de cloud integrator voor hoger onderwijs en onderzoek. [1] Zij is te bereiken via eefje.vanderharst@surfnet.nl

Bart Giesbers, I&AM specialist bij VKA en heeft o.a. opdrachten gedaan op dit vlak bij ICTU, VGZ en defensie. Hij is te bereiken via bart.giesbers@vka.nl

De gespreksleider Lex Borger nam ook inhoudelijk deel.

Als gangmaker voor het gesprek waren vooraf een aantal stellingen en vragen opgesteld. Dit verslag bevat een samenvatting van het gesprek en de conclusies.

Stelling: I&AM hoort door de business opgepakt te worden, maar die laten het maar al te graag aan de IT afdeling over.

I&AM gaat over toegang tot applicaties en systemen. In beginsel is dat wat de organisatie wil. Je merkt echter dat op een gegeven moment een besef van informatiebeveiliging groeit, dat acties gevolgen kunnen hebben in de buitenwereld, vermelding in de pers of financiële schade. Dan heeft de organisatie een belang om ook goed zicht te hebben op de autorisaties die hun medewerkers hebben, wat ze daarmee kunnen en of het verder wel goed zit dichtgetimmerd.

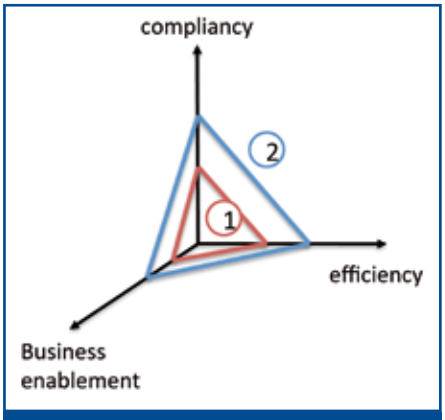
Business heeft eigenlijk geen behoefte aan I&AM, maar behoefte aan veilige toegang tot systemen. Zij willen bij een applicatie kunnen, zij willen een korte doorlooptijd bij een accountaanvraag, zo min mogelijk wachtwoorden, zo min mogelijk tokens. Maar ze hebben niet als doel op zich "Wij willen I&AM".

Er zijn over het algemeen drie soorten drivers voor I&AM die niet noodzakelijk met elkaar samenvallen. Die worden ook door Gartner genoemd en kunt ze weergeven in een spinnenwebdiagram. Op de drie assen zet je uit:

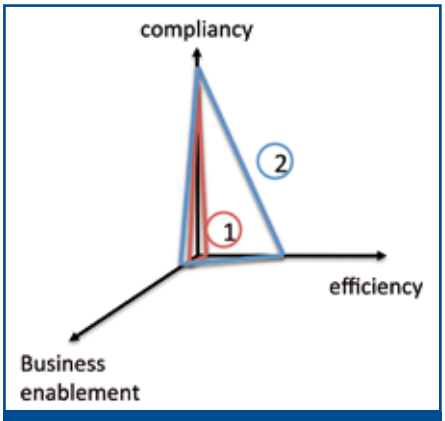
- Compliance
- Business enablement
- Efficiency

Deze drie assen kunnen binnen de organisatie allen een andere trekker hebben: compliance, business en IT. En dan is de kunst om bij een implementatie de as te pakken waarbij er duidelijk een belanghebbende vooraan staat of je moet een mix vinden die werkt.

De driver of drivers zoals die specifiek voor een organisatie gelden, bepalen of er focus op één van de assen gelegd moet worden, of dat er een combinatie gezocht kan worden. Eén van de belangrijke drivers is 'beter in control' komen.



Figuur 1 - Gelijkmatige groei langs alle assen – ©VKA, Bart Giesbers



Figuur 2 - Focus op compliance eerst, dan efficiency – ©VKA, Bart Giesbers

De sector waarin een organisatie actief is, bepaalt al veel over de drivers voor I&AM. Bij een zorginstelling en een financiële instelling is compliance heel belangrijk is (denk aan BASEL III,

SOLVENCY II, NEN 7510), bij het hoger onderwijs draait het meer om business enablement, de vraag wat I&AM allemaal mogelijk maakt, ook al staat compliance natuurlijk wel op de radar.

Als je apart naar identity management en access management kijkt, zie je verschillen. De business laat identity management heel makkelijk over aan IT. Snel toegang regelen voor mensen die in dienst komen, wordt veel meer gezien als hands-off door de business: regel dat maar. De relevantie voor de business is echter niet per definitie kristalhelder. Als je bijvoorbeeld de HR-administratie leidend laat zijn voor een identiteit, dan zit er wel een afhankelijkheid van de business bij, die de andere afdelingen niet altijd zien. Wanneer komt iemand in dienst, wanneer verandert hij van functie en wanneer verlaat hij de organisatie. Zelfs HR ziet dat niet altijd, want die richten zich op tijdige salarisbetalingen en niet op de IT-toegang op de eerste werkdag van een nieuwe medewerker. Het geldt ook voor een medewerker die van werkzaamheden veranderd. Dat registreren en gebruiken als basis voor je business rules voor toegang is ook niet altijd vanzelfsprekend. Het komt niet altijd tijdig door bij HR. Uitdiensttreding ook niet. Je moet heel erg kijken waar de drijfveer voor melding van uitdiensttreding zit.

Bij access management - de autorisaties tot gebruik van de systemen - zit vaak juist een ingewikkelde verwevenheid met de generieke en specifieke business processen. Het gaat hier vaak om een hulpvraag van de business over enablement of compliance, waarbij men veel nadrukkelijker mee wil doen in de sturing en het bedenken van oplossingen om het ook hanteerbaar te maken. De vraag hoe je compliant bent, vergt heel veel kennis van de processen en de inhoud van de business.

Als je bijvoorbeeld een kernsysteem bij een bank neemt dat automatisch aandelen verhandeld, waar niveaus van goedkeuring tussen zitten en waarbij je te maken krijgt met functiescheiding die gehandhaafd moet worden, dan kun je niet simpel een opdracht geven aan IT om dat in te regelen. In dat geval moet de business, IT voeden met de gedetailleerde operationele informatie om zowel het proces als het systeem goed te kunnen inrichten. Complicatie hierbij is dat het hanteerbaar moet zijn voor de business, dat is niet vanzelfsprekend. Je ziet dit wel eens als valkuil voorbij komen, dat de business de IT niet meer begrijpt - en andersom.

Deze scheiding tussen business en IT hoeft helemaal geen probleem te zijn, mits er gezorgd is voor een goed koppelvlak. Een informatiemanagement (IM) functie kan bij uitstek enerzijds aansluiten op IT, maar heeft anderzijds kennis van hoe de business werkt. Daardoor kunnen ze de link maken. Er moet ergens een generieke IM functie belegd zijn, want "de" business bestaat niet. De business bestaat uit verschillende samenwerkende onderdelen, maar wel elk met hun eigen takenpakket en dus ook eigen belangen en expertises. Die kunnen zelfs in conflict zijn met andere business onderdelen.

Lex: De business laat identity management makkelijk over aan IT

De tools voor centrale I&AM zijn ontstaan op basis van noodzaak bij IT en de business. Dit is echter onderhevig aan veranderingen. Het zou zomaar kunnen groeien naar een situatie waarin alle I&AM zo transparant en duidelijk standaard in systemen geregeld is, dat je geen specifiek centrale administratie meer nodig hebt om die gegevens automatisch uit andere systemen te trekken. Dat zal echter niet 1–2–3 gebeuren, dus voorlopig is het nog goed om die centrale I&AM administraties op te zetten en in stand te houden. Voor identiteitenbeheer zul je dat wellicht wel eerder zien. Je zult een administratie nodig hebben, maar wellicht dat bestaande voorzieningen voor HR, service management of Active Directory die kant op evolueren.

Stelling: IT neemt de lead bij I&AM trajecten, zowel IT als de business leveren hun eisen en wensen.

I&AM is niet een gewoon traject. I&AM gaat door de hele organisatie heen, raakt iedereen, heel veel systemen, en de processen binnen IT, functioneel beheer, informatiemanagement en de business. Dat is lastig. Het vergt brede input vanuit IT en de business.

IT kan goed omgaan met technische complexiteit, denkt in termen van techniek als oplossing en stelt daar

veel en gedetailleerde eisen aan. De business komt waarschijnlijk met een paar algemene eisen op hoog niveau. Het is moeilijk om hier een balans te bereiken. Als niemand controleert dat de optelsom van al die eisen ook invult wat de organisatie wil bereiken, heb je een probleem.

Daarom zou IT niet in de lead moeten zijn. Er is een veel bredere focus nodig om het tot een succes te maken. Informatiemanagement in de lead zou wel kunnen, maar dan in een goede mix om de sturing helder te houden. En alle stakeholders moeten er echt van het begin tot het eind bij zitten.

Neem bijvoorbeeld single sign-on: De business vraagt om laagdrempelige toegang tot applicaties, met zo min mogelijk gedoe. De oplossing kan single sign-on zijn, maar om dat te kunnen valideren zijn er een aantal vervolgvragen die ingevuld moeten worden. "Single" in welk domein? Hoe vul je de integratie in? Enzovoorts. Als het in de context van een pakketselectie speelt, dan zet een leverancier maar al te graag een check bij dit component en voor je het weet kost het een halve ton extra. Dit geldt ook voor de andere opties zijn die je bij de pakketten kunt krijgen. En soms zijn het opties waarvan je verwacht zou hebben dat het standaard meegeleverd wordt, zoals een workflow voor attestatie.

Eefje: Informatiemanagement kan aansluiten op IT en heeft kennis hoe de business werkt

Je wilt eigenlijk vóór een pakketselectie duidelijk hebben wat de business allemaal nodig heeft. Vergelijk het met de emotionele beslissing "Ik wil een iPad hebben", in plaats van te kijken welke functionaliteit nodig is. Wellicht is de uitkomst dan een laptop of een mobiele telefoon in plaats van die iPad.

Het uitgangspunt vooraf moet niet zijn dat er een tool moet komen, van díe bepaalde leverancier, met de verwachting dat het dan vanzelf wel goed komt. Vaak blijkt dan achteraf dat er functies missen of dat er maatwerk nodig is, waardoor de implementatie onverwacht duurder wordt. Als je dat aan het begin al helder hebt, scheelt dat in het project. Het is een stuk beleid en architectuur dat je als basis moet nemen, zónder dat je je daarin gaat verliezen. Want een I&AM traject vereist een lange adem én kort-cyclische zichtbare resultaten.

Stelling: IT wordt meestal de systeemeigenaar en IM de I&AM proceseigenaar. Deze eigenaren rapporteren functioneel ook weer binnen IT en IM.

In de praktijk is het best denkbaar dat het I&AM systeem uiteindelijk in de exploitatie bij IT terecht komt. Wat je wilt voorkomen is dat de business zich na implementatie terugtrekt en verwacht dat het allemaal goed draait bij IT. Een eigenaarschap buiten IT kan dit voorkomen, maar waar het dan wel kan liggen verschilt per organisatie. Binnen een financiële instelling, die werkt met het "three lines of defence" model, komen de I&AM zaken die aan compliance gerelateerd zijn, al snel in de tweede laag terug [zie kader].

- De eerste lijn is het operationeel management van de organisatie.
- De tweede lijn is de risicomanagementfunctie.
- De derde lijn is de interne auditfunctie.
- Voor meer informatie zie het paper van FERMA en ECIIA hierover. [2]

Figuur 3 – Three Lines of Defence

Alle partijen in het I&AM proces horen in ieder geval méde de rapportages te krijgen, waarop ze kunnen sturen en andere verantwoordelijken in de vraag en aanbod relaties kunnen aanspreken. Duidelijke metrics (zoals doorlooptijden van aanvragen, het aantal log-ins, het aantal met problemen, afwijkingen van gemiddelden) kun je afleiden uit de business drivers en de project requirements. Dit is cruciaal, het is een illusie om te denken dat wanneer je een oplossing neerzet, dat die dan ook meteen af is. Juist in het gebruik merk je waar er nog bijgeschaafd moet worden.

Vraag: Wat zijn de issues bij I&AM in de cloud? Wat komt er bij kijken? Waar gaat het naartoe?

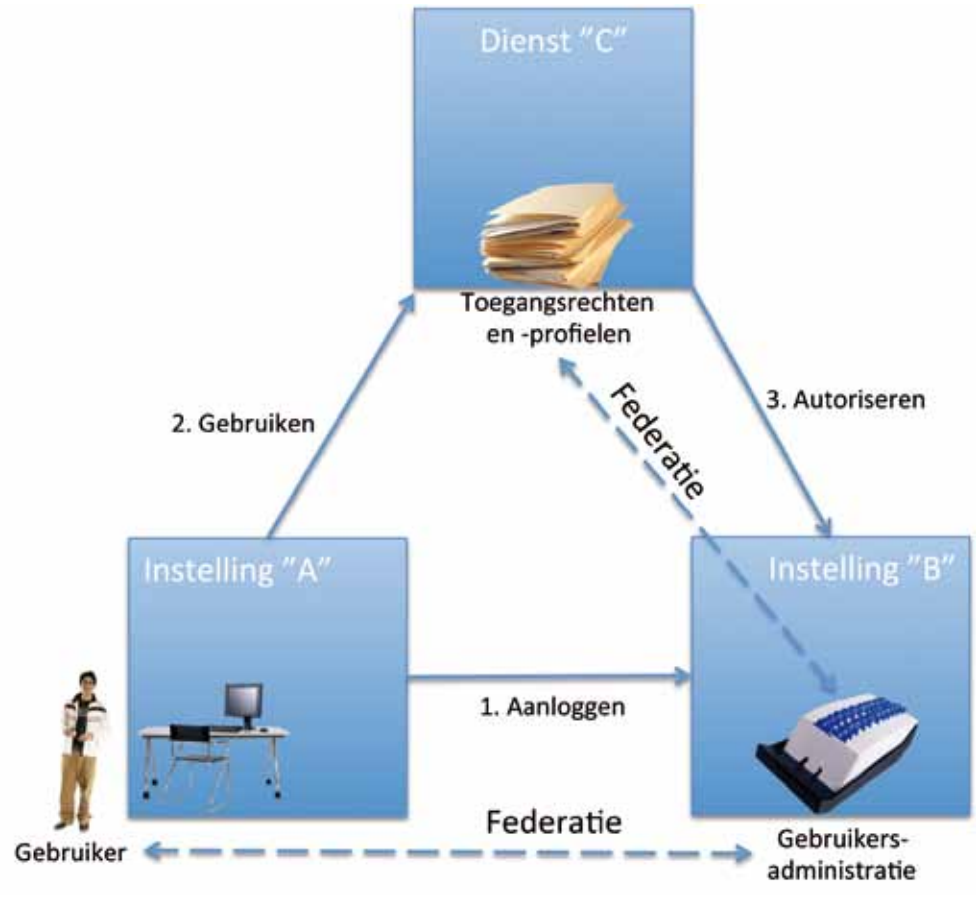
In het hoger onderwijs is heel bewust voor een federatieve oplossing gekozen, waarbij je standaardiseert en afspraken maakt met elkaar, over welke attributen je ondersteunt en welke je bereid bent uit te wisselen met cloudleveranciers. Dit wordt gedreven vanuit de business enablement: hoe kunnen onderwijsinstellingen met elkaar samenwerken? Zolang je diensten op een standaard manier koppelt op de infrastructuur, bijvoorbeeld met SAML 2.0, kun je de autorisatie-beslissingen door de cloudleverancier laten nemen, maar houd je de authenticatiebeslissingen lokaal bij de onderwijsinstellingen zelf. Bij I&AM in de cloud moet je die scheiding ook aanbrengen. Het gaat zelfs verder dan dat: de gebruiker kan werken vanaf een andere instelling dan die de authenticatie uitvoert, wat weer een andere partij is dan de dienstuitvoerder die moet autoriseren, zie figuur 4.

> Bart: Alle stakeholders moeten er echt van begin tot eind bij zitten

Een aspect hierbij is de betrouwbaarheid van de authenticatie. Je kunt meerdere betrouwbaarheidsniveaus onderscheiden, zoals bij e-Herkenning en DigiD. Hoe gevoeliger de applicatie of content die je benadert, hoe hoger het betrouwbaarheidsniveau moet zijn. Je moet dan weten welk niveau van betrouwbaarheid nodig is voor een dienst en hoe die wordt geleverd door de hele betrokken keten. Bij e-Herkenning heb je de uitgever van middelen, degene die authenticeert, degene die bevoegdheden vastlegt en degene die de routering verzorgt.

> Eefje: Hoe gevoeliger de content, hoe hoger het betrouwbaarheids-niveau van de authenticatie

Je ziet de commerciële cloud diensten (Facebook, Hyves, LinkedIn) ook gebruikt gaan worden voor



Drie partijen werken samen aan authenticatie en autorisatie met federatie

authenticatie. Neem bijvoorbeeld bibliotheek.nl, die vorige week aangaf de login van Facebook, LinkedIn, Hyves als authenticatievoorziening te willen gebruiken als toegang tot bibliotheek-voorzieningen. Dit is één niveau van betrouwbaarheid. Voor een andere dienst heb je bijvoorbeeld een hoger niveau van betrouwbaarheid nodig. Dit moet nadrukkelijk terugkomen in de standaardisatie en afspraken. Dit zie je in Nederland bij e-Herkenning en DigiD en op Europees niveau bij large scale pilots als STORK en PEPPOL.

Identity Management as-a-service komt ook op: IAM4Cloud van Traxion, PingOne van Ping, iWelcome van Everett. Het is hot, maar veel organisaties zijn angstig over wat er mag… van de Nederlandsche Bank, en wat een andere mogendheid zou kunnen … zoals de Verenigde Staten.

Afsluitende vraag: Wat zijn succesfactoren en wat zijn de addertjes onder het gras?

Ali Agzanay: De business betrekken, de beheerorganisatie betrekken bij de ontwikkeling en tijdig trainen. Ze moeten in hun rol kunnen groeien. Bij outsourcing: Weet wie het onderhoud gaat doen, zodat je vooraf weet dat je contact gaat krijgen met ondersteuning uit India. Weet hoe lang je veranderings-verzoeken kunnen duren. I&AM vergt een change proces met een hoger volwassenheidsniveau. Wijzigingen moeten goed en tijdig verwerkt worden. Neem risico's mee.

Bart Giesbers: Het eerste is: Focus. Er zijn veel definities wat I&AM is, met legio ondersteunende modellen. Stap één is je afvragen waar je op wil focussen. Wat is de driver? Welk deelgebied? Wat wil je als resultaat behalen? En houdt die focus ook vast en laat hem terugkomen in tussenresultaten.

Blijvende business betrokkenheid is twee. Alles wat opgeleverd wordt, moet getoetst worden of het ook iets is wat wordt gesnapt door de business. Zaken zoals: Hoe is een systeem in het verleden ingericht? Hoe zien de autorisaties er uit? Is dat begrijpelijk voor de business of moet het eerst nog vertaald worden?

En wat zaken over de inrichting van de tooling: Wat is in het Nederlands? Wat is Engels? Worden er business-termen gebruikt en geen IT-termen?

> Ali: Betrek de business, de beheerorganisatie bij de ontwikkeling en train tijdig

Er moet een blijvende link zijn met de business - primair en gerelateerde partijen zoals HR en IT. Als je je richt op in control komen op het gebied van autorisaties, vraag je dan af voor welke delen dat echt belangrijk is. Wat zijn de assets waar je je op wilt richten? Doe niet alles, maar kies risico-gebaseerd.

Eefje van der Harst: Zorg voor bewustwording bij de business, waarom het belangrijk is I&AM goed in te richten en te onderhouden. Het is heel eenvoudig om heel veel rechten uit te delen, zodat je heel veel kan, maar houd dat tegen het licht of het echt nodig is en zorg ook dat rechten op tijd afgenomen worden. Die bewustwording is vaak nog onvoldoende aanwezig.

Als je kijkt naar de toekomst, naar I&AM in de cloud, dan is het gebruik van open standaarden heel belangrijk om de interoperabiliteit met andere systemen voor elkaar te krijgen. Er zijn in het verleden al te veel gesloten systemen en suites opgetuigd als technische oplossing, werkend binnen de organisatie maar moeilijk naar buiten te brengen.

I&AM is nooit af, zorg dat het regelmatig tegen het licht wordt gehouden en continu wordt verbeterd. Laat in rapportages zien hoe het zich ontwikkeld en in hoeverre bijsturing nodig is. ●

Referenties

[1] SURFconext - http://www.surfnet.nl/nl/Thema/coin/whatis/Pages/default.aspx
[2] Three Lines of Defence - http://www.eciia.eu/about-us/news/whats-hot

COLUMN

ZULLEN WE GEWOON EENS OPNIEUW BEGINNEN?

Patiëntenprivacy blijft in Nederland doorlopend een hot topic. En ik noem dat nu wel patiëntenprivacy, maar eigenlijk gaat het gewoon om u en ik en om uw kinderen, ouders en vrienden. Op de één of andere manier lijken we het maar niet voor elkaar te krijgen dit goed te regelen. De voorpagina's van de kranten koppen – wederom – dat het EPD een privacylek kent. Blijkbaar zijn de gegevens uit de dossiers die voor onderzoek gebruikt worden toch niet zo anoniem als gewenst. Nu is anonimiseren ook erg lastig, omdat je al snel toch weer spreekt van herleidbaarheid tot de persoon. En is er sprake van herleidbaarheid, dan kun je de facto iemand identificeren en is de privacywet van toepassing.

Het College Bescherming Persoonsgegevens neemt wat betreft die herleidbaarheid een strikt standpunt in. Het is een harde lijn, die in de praktijk voor bedrijven en overheden nog weleens voor problemen zorgt. En dan niet altijd uit onwil, maar puur vanwege het feit dat door het schuiven met wat gegevens je al snel weer herleidbaarheid gevonden hebt. Om even bij dat EPD te blijven: voor het onderzoek wordt informatie uit consulten en contra-informatie verwerkt. Echter daarbovenop wordt een geboortedatum, het geslacht en de vier cijfers van het postcode meegezonden. Hoeveel vrouwen geboren op 27-07-1976 denkt u dat er wonen in postcodegebied 2562? Juist. Eentje. Ik. En dan zullen we het nog maar niet hebben over de informatie die dan meegezonden wordt uit het dossier.

Even terug naar die anonimisering dan. Want het kan wel. Het College heeft in 2009 aangegeven wat volgens haar de juiste weg naar Rome is. Ik schrijf het hier even voor u op, zodat u een spiekbriefje heeft:

Bij toepassing van pseudonimisering is geen sprake van de verwerking van persoonsgegevens, indien aan de volgende voorwaarden is voldaan:

1. er wordt (vakkundig) gebruik gemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens;
2. er zijn technische en organisatorische maatregelen genomen om herleidbaarheid van de versleuteling (replay back) te voorkomen;
3. de verwerkte gegevens zijn niet indirect herleidbaar;
4. in een onafhankelijk deskundig oordeel (audit) wordt voor aanvang van de verwerking en daarna periodiek vastgesteld dat aan de voorwaarden 1, 2, en 3 is voldaan;
5. de pseudonimiseringsoplossing dient op heldere en volledige wijze te zijn beschreven in een openbaar document, zodat iedere betrokkene kan nagaan welke garanties de gekozen oplossing biedt.

Goed, anonimiseren is dus te doen. Maar uiteraard is dit niet het enige privacyprobleem rondom het EPD. De dossiers van alle Nederlanders worden blijkbaar in de Verenigde Staten opgeslagen. En wie mijn columns zo nu en dan eens leest, weet wat ik nu ga zeggen: Patriot Act! Minister Schippers kreeg daar, zeer terecht, Kamervragen over. Dat mocht ook wel, want ze had eerder al gezegd dat het met die Patriot Act wel goed zou komen. Men had haar verzekerd dat in een contract afgesproken zou worden dat de gegevens niet gedeeld zouden worden met de Amerikaanse overheid, indien deze een verzoek daartoe zou indienen. Nu moet u begrijpen dat ik groot voorstander ben van het maken van heldere afspraken in een goed doortimmerd contract. Maar er zijn nu eenmaal zaken die niet te becontracteren zijn. Oh ja, je kunt het gerust opschrijven, maar het heeft weinig zin. Amerikaanse bedrijven zijn simpelweg verplicht gehoor te geven aan een dergelijke vordering op grond van de Patriot Act. Afijn, bij nader inzien moet minister Schippers dat ook bedacht hebben, want ze had (vooralsnog?) geen antwoord op de kamervragen daarover. Rest de vraag: is het dan erg dat de Amerikaanse overheid potentieel alle medische gegevens van alle Nederlanders kan opvragen? Misschien moet u deze vraag gewoon even voor uzelf beantwoorden. Mag ik u dan nog meegeven dat medische gegevens gevoelige gegevens zijn en dat daarvoor een verzwaarde beveiligingsplicht geldt? En ik denk dat ik er nog maar even het zwijgen toe doe wat betreft de prachtige data-analyses die je kunt maken met de medische dossiers van een heel land in je hand en hoe je dat vervolgens weer kunt inzetten. Misschien zou je op grond van iemands medische dossier wel kunnen voorspellen of de persoon in potentie een terrorist is? Dat lijkt me in ieder geval het onderzoeken waard!

Ik denk dat we een zero-tolerance beleid moeten voeren wat betreft de privacyinbreuken op medische gegevens. Ik heb hier slechts ruimte om 2 problemen te bespreken, maar betreffende het EPD zijn het er inmiddels veel meer. Terug naar de tekentafel. Alles wat bedacht is weggooien. Ergens is een afslag gemist. Zullen we gewoon eens opnieuw beginnen? ●

Mr. Rachel Marbus, @RachelMarbus op Twitter


STARREVELD KOMT WEER UIT DE KAST

ADMINISTRATIEVE ORGANISATIE ALS GENERIEK KADER VOOR ACCESS CONTROL

Drs. André Koot RE CISM is redacteur van het blad Informatiebeveiliging en directeur-eigenaar van i3advies. Hij heeft 15 jaar ervaring op het gebied van Informatiebeveiliging en is auteur van diverse artikelen rondom Identity Management en Access Control. Hij is te bereiken via meneer@tken.net

Drs. Maarten Stultjens is werkzaam als VP business development bij Hunite in Alkmaar. Hij heeft ruim 10 jaar ervaring op het gebied van Identity & Access Management en Role Based Access Control. Hij is te bereiken via stultjens.maarten@gmail.com

Het toekennen en beheren van toegangsrechten kent de nodige uitdagingen. De belangrijkste vraag is op grond waarvan, op grond van welke principes, autorisaties aan individuen worden toegekend en beoordeeld. Zijn er normen en is hiervoor beleid geformuleerd? Dat geldt zowel bij het toekennen van autorisaties op basis van functies en rollen (denk aan RBAC of workflow) als bij het beoordelen van autorisaties door een manager of een IT-auditor.

Dit artikel tracht een generiek kader/framework te bieden om autorisatieregels op te stellen. Generiek, omdat de ontwerpcriteria van toepassing zijn op iedere organisatie die haar eigen processen, objecten en risico's kent. Hiervoor grijpen we terug op de oer-Hollandse begrippen die Starreveld heeft gedefinieerd in de leer van de Administratieve Organisatie.

> Op grond van welke principes, worden autorisaties aan individuen toegekend?

Van Access Control naar Administratieve Organisatie en Starreveld

Organisaties streven naar het goed inrichten en controleren van autorisaties om reden van efficiency, beveiliging, voorkomen van fraude, goed kunnen ondersteunen van organisatieveranderingen enz... Voor veel organisaties is goed autorisatiebeheer zelfs een conditio-sine-qua-non, ze moeten voldoen aan wet- en regelgeving.

Het realiseren van autorisatiebeheer wordt in veel gevallen in één adem genoemd met het inrichten van identiteitenbeheer, Identity and Access Management, of I&AM. In de praktijk blijkt echter dat deze beide aspecten maar zelden gelijktijdig ingericht kunnen worden. Sterker, het is eigenlijk wel een beetje vreemd dat beide aspecten in één adem worden genoemd. Identiteitenbeheer richt zich op het lifecycle management van identiteiten die binnen een organisatie kunnen worden gebruikt en dat is in de regel een HRM verantwoordelijkheid (voor eigen personeel) of een CRM taak (voor klanten en andere relaties). Dat proces heeft maar weinig te maken met autorisatiebeheer – het bepalen 'wie wat mag'. Dat laatste is een verantwoordelijkheid van proces- en gegevenseigenaren. Je zou hooguit kunnen stellen dat iemand zonder een vertrouwde, geaccepteerde identiteit geen autorisaties zou mogen bezitten. Het beheer van identiteiten is daarmee dus wel een randvoorwaarde voor het kunnen inrichten van autorisatiebeheer, maar het is niet een onderdeel van autorisatiebeheer. In deze bespiegeling beperken we ons tot autorisatiebeheer, of Access Control.

> Een leidend principe is werkverdeling

Met Access Control wordt bedoeld dat iemand die verantwoordelijk is voor een object (denk aan informatie, maar ook aan een fysieke kantoorruimte) in staat is te bepalen wie toegang tot dat object mag hebben en die ook toeziet op het (blijvende) juiste gebruik van de toegang tot het object. Dat omvat dan ook het soort autorisatie en de periode waarbinnen die autorisatie gebruikt mag worden. '*Wie mag wat wanneer*'? Dat maakt echter al meteen duidelijk dat in ieder geval het eigendom van het te beveiligen object vastgesteld moet zijn. Iemand moet dit bepalen, afdwingen en controleren.

Waarom zou iemand autorisaties aan anderen toe willen kennen? Die laatste vraag is betrekkelijk eenvoudig te beantwoorden. Het leidende principe is werkverdeling en daarmee het beleggen van taken, bevoegdheden en verantwoordelijkheden bij iemand anders. Als iemand geen werk hoeft te verdelen, dan is er ook geen probleem, denk aan de eigenaar/ondernemer met een eenmanszaak. Die persoon is integraal verantwoordelijk en hoeft eigenlijk alleen aan zichzelf verantwoording af te

leggen. Zo gauw echter de hoeveelheid werk te veel is voor één persoon, moet het werk georganiseerd worden. Daarbij moet werk aan anderen worden toebedeeld en toevertrouwd (!) en ontstaat de noodzaak van het inrichten van beheersmaatregelen om de kwaliteit van het werk van die anderen te borgen.

Het invoeren van werkverdeling met beheersmaatregelen is niet nieuw. Het is bekend onder de noemer Administratieve Organisatie en Interne Controle en omvat onder meer het begrip Functiescheiding. Functiescheiding is een bekend begrip bij wet- en regelgeving, denk aan de beheersmaatregelen rond 'Segregation of Duties' in de Sarbanes Oxley traject. Het is een belangrijke factor geworden en het struikelblok waardoor menig organisatie bevindingen van toezichthouders heeft moeten wegwerken. In Role Based Access Control projecten bestaat dan ook veel aandacht voor inrichten van functiescheiding. Maar de bovenliggende vraag is: "*Op welke wijze kun je bepalen welke Taken, Bevoegdheden en Verantwoordelijkheden gescheiden moeten worden?*".

Starreveld

We grijpen op zoek naar een antwoord naar de boekenkast met onze studieboeken over de leer van Starreveld – die in de jaren '60 de grondlegger was van de moderne Administratieve Organisatie (AO) en Interne Controle (IC). Uitgangspunt is dat een baas wil voorkomen dat zijn personeel fraudeert en de volledigheid van omzet kan worden gegarandeerd. Hij zal daartoe proberen om zodanige maatregelen te treffen dat fraude wordt ontmoedigd of tegengegaan en -in het geval het toch plaatsvindt- tijdig wordt gedetecteerd en getraceerd. Het ontmoedigen en tegengaan van fraude gebeurt op verschillende manieren. Starreveld onderkent voor verschillende typologieën van organisaties, verschillende soorten beheersmaatregelen. Zo ontwikkelde Starreveld instrumenten voor verbandscontrole (denk aan standen-registers bij verhuurders van onroerend goed en aan goederenbeweging bij handelsbedrijven: BeginVoorraad + Productie – Verkoop = EindVoorraad). Voor dit artikel beperken we de scope tot financiële transacties.

Starreveld ontwikkelde het gedachtegoed van functiescheiding

Ook ontwikkelde Starreveld het

Voorkomen van Fraude en Verduistering

gedachtegoed van functiescheiding door het creëren van tegengestelde belangen. Door het splitsen van bevoegdheden wordt voorkomen dat één persoon zoveel macht krijgt, of zoveel faciliteiten heeft dat hij of zij de bestaande beheersmaatregelen weet te omzeilen. Door het creëren van belangentegenstellingen wordt samenspanning van medewerkers, het samenwerken om beheersmaatregelen te omzeilen (ook in een situatie van functiescheiding), zo veel mogelijk tegengegaan. Maar helaas stelt ook Starreveld vast dat je samenspanning het moeilijkst van alle bedreigingen tegengaat.

Onze onderzoeksvraag is of, en zo ja hoe, de criteria van Starreveld voor functiescheiding te gebruiken zijn als generieke ontwerpcriteria voor autorisatiebeheer?

Functiescheiding

Het stelsel van Controletechnische Functiescheiding zoals gedefinieerd door Starreveld onderkent de volgende vijf 'functies':

- *Beschikken*
  Beschikken impliceert dat je namens een bedrijf verplichtingen aangaat.
- *Registreren*
  Dit is het vastleggen van een feit en heeft door automatisering een nauwe relatie met uitvoeren, zoals hieronder beschreven.
- *Uitvoeren*
  Het uitvoeren van een taak conform de werkinstructie. Doordat veel systemen de processen geautomatiseerd ondersteunen, lijkt een strikte scheiding tussen uitvoeren en registreren niet meer helemaal van deze tijd.
- *Bewaren*
  De functie die verantwoordelijk is voor kwaliteitscontrole (voldoet een object aan de gestelde normen) en het handhaven daarvan. Te lezen als Operationeel Beheer van een informatiesysteem.
- *Controleren*
  Vaststellen of aan de vastgestelde normen wordt voldaan.

Stempelen en paraferen hielp vroeger

Starreveld geeft aan dat het borgen van de integriteit van informatie moet voldoen aan een aantal regels. Deze regels zijn kortweg als volgt: De controletechnische functie-scheiding houdt in dat een zodanige

functie- en taakverdeling wordt gecreëerd dat:

- iedere functionaris slechts een beperkt aantal stappen van een proceskringloop kan beïnvloeden, maar nooit twee opeenvolgende;
- beslissingen om over waardevolle objecten te beschikken niet worden genomen door bewarende functionarissen;
- functionarissen die verantwoordelijk zijn voor de uitvoering van processtappen niet belast mogen zijn met de bewaring van objecten;
- de bovengenoemde functionarissen geen bemoeienis hebben met de activiteiten van de registrerende of controlerende functionarissen.

In onderstaande matrix zijn deze ontwerpcriteria op grond van de AO regels geformuleerd:

	Beschikken	Bewaren	Uitvoeren	Registreren	Controleren
Beschikkende functie	+	-	+	-	+
Bewarende functie	-	+	-	-	-
Uitvoerende functie	+	-	+	-	-
Registrerende functie	-	-	-	+	+
Controlerende functie	+	-	-	+	+

Autorisatieregels

De groene combinaties zijn de in de praktijk goed te combineren functies. De rode combinaties zijn de verboden combinaties. We hebben deze matrix op grond van de voorgaande regels symmetrisch ingericht, maar door toepassing van compenserende en aanvullende maatregelen (zoals het automatisch vastleggen van audit-trails en inrichten van een workflow) zijn andere combinaties wellicht toch acceptabel.

Automatisering

De leer van Starreveld is ontstaan voordat sprake was van automatisering. Een heleboel functies en beheersmaatregelen die hij beschreef, zijn binnen de geautomatiseerde bedrijfsprocessen eigenlijk niet meer als zodanig te onderkennen. Binnen de moderne geautomatiseerde systemen worden diverse functies geheel geautomatiseerd uitgevoerd. Met name de beschikkende en bewarende functies worden grotendeels geautomatiseerd uitgevoerd. Maar er zijn nog andere interessante ontwikkelingen. Daar waar vroeger een klant aan een loket verscheen of een brief stuurde, waarna een medewerker de relevante gegevens beoordeelde en registreerde in een dossier, neemt de klant nu zelf de registratie over in een webportaal en maakt de klant zelf al verschillende keuzes op grond van adviezen die een 'wizard' of intelligente assistent op de website presenteert. Hoe zit het dan met functiescheiding? Wie is dan nog verantwoordelijk voor de betrouwbaarheid van een transactie?

Starreveld kan ons hierbij toch wel helpen. De meeste door hem gedefinieerde functies kunnen we wel ergens onderkennen, al is het dan niet in een eenduidige vorm.

De beschikkende functie wordt bijvoorbeeld zichtbaar daar waar werkstroombesturing en kennisregels geautomatiseerd beslissingen nemen omtrent bijvoorbeeld acceptatie van een polis of een claim bij een verzekeraar. Of daar waar een wizard of een intelligente assistent een aantal keuzes voorlegt aan een klant. De kennisregels zijn feitelijk de geobjectiveerde beslissingspunten die uitmonden in een transactie, een feit waardoor een organisatie juridisch gebonden wordt. In die zin is een kennisregel (en de aan de beslissing ten gronde liggende parameters) eigendom van een iemand die een beschikkende functie moet vervullen. En die persoon is daarmee dan ook verantwoordelijk voor alle transacties die via deze kennisregels worden gerealiseerd.

De registrerende functie wordt ook steeds meer geautomatiseerd in portalen en wizards. De registratie gebeurt steeds meer aan de voorkant en dan noemen we dat 'data entry'. Het grootste risico is de integriteit van de ingevoerde gegevens, aangezien die in veel gevallen 'rücksichtlos' worden verwerkt in systemen. Verbandscontroles en plausibiliteitscontroles, evenals volledigheidschecks moeten zoveel mogelijk aan de voorkant worden ingericht. Daarmee wordt de proces-eigenaar verantwoordelijk voor de juistheid van de registratiefunctie. Willen we processen 'lean' inrichten, dan begint dat met juiste invoer.

De bewarende functie wordt in de regel door een systeem zelf uitgevoerd. Maar dat is natuurlijk al te simpel: de systeemeigenaar wordt hierdoor feitelijk de bewarende functionaris. Hij heeft tot taak de integriteit en vertrouwelijkheid, conform de eisen van de consumerende proces- en gegevenseigenaren te garanderen.

De kans op onbedoelde functie-vermenging zou in een geautomatiseerde omgeving kunnen ontstaan als een registrerende functionaris een geautomatiseerde beslissing initieert. Dus niet zozeer doordat hij zelf de beslissing neemt (dus beschikt) maar wel de gegevens invoert op basis waarvan een systeem een beslissing neemt!

> Door automatisering ontstaan nieuwe processen

Dit risico moet worden beperkt door bij het ontwerp en realisatie van de werkstroom en de kennisregels expliciet vast te stellen welke gegevens


©Wikipedia

Oogtoezicht kan nu niet meer

op welke wijze de beslissing hebben beïnvloed en door die beslissing in een audit-trail (wie heeft wat wanneer gedaan) vast te leggen voor controle achteraf. En bovendien: wie heeft de kennisregel goedgekeurd, wie is dus feitelijk 'accountable' voor de genomen beslissing?

Preventief en detectief autorisatiebeheer

Voordat we kunnen bepalen wat de waarde van 'Starreveld' is voor autorisatiebeheer, onderscheiden we allereerst twee methoden: preventief en detectief beheer van autorisaties. Preventief betekent dat uitsluitend op basis van vooraf gedefinieerde bedrijfsregels autorisaties worden toegekend. Preventief autorisatiebeheer wordt veelal ingericht met een combinatie van rollen (verzameling van autorisaties), regels (condities waaronder een rol kan worden toegewezen aan een gebruiker), context (eventuele veranderende omgevingsomstandigheden) en workflow (handmatige goedkeuring). We bekijken het voorbeeld van een medewerker op de afdeling debiteurenadministratie. Deze medewerker krijgt een standaard set autorisaties op grond van een 'rol' die past bij zijn functie. Als hij door zijn manager belast wordt met een specifieke taak binnen de afdeling, krijgt hij hiervoor via een workflow extra autorisaties toegewezen voor een bepaalde tijd. De daadwerkelijke uitvoering van het autorisatiebesluit in autorisatieregels heet in IT-termen provisioning en kan handmatig of via automatische interfacing worden gedaan. Voor preventief autorisatiebeheer wordt vaak verwezen naar Role Based Access Control (RBAC).

Detectief beheer van autorisaties is post-factum, dat wil zeggen dat het zich richt op het controleren van de huidige autorisaties tegen actueel geldende bedrijfsregels. Verkeerde autorisaties worden vervolgens opgeschoond of er wordt expliciete toestemming gevraagd om af te wijken van de geldende regels (certificatie of management verificatie). Als een als onjuist gesignaleerde toegekende autorisatie toch juist blijkt, dient de bedrijfsregel te worden aangepast. Voor detectief autorisatiebeheer wordt vaak verwezen naar Access Governance (AG). AG richt zich niet op het operationele proces van het uitdelen van autorisaties. Access Governance richt zich ook niet op het toetsing van de juistheid van de uitgevoerde transacties ten opzichte van een baseline.

Hoewel preventief beheer vanuit vele oogpunten te prefereren is, blijkt het invoeren ervan een lastig traject omdat de organisatie de autorisatieregels vooraf moet definiëren en ze ook correct moeten zijn. Verkeerde regels leiden tot verkeerde autorisaties die bovendien vaak niet achteraf gesignaleerd kunnen worden en daarmee zouden kunnen leiden tot een onwerkbare situatie, denk aan strakke preventieve autorisaties op een medisch dossier dat voor een spoedgeval toch geopend moet worden. Daarbij laten ongestructureerde omgevingen, zoals bestandssystemen of data in SharePoint, zich lastig structureren als onderdeel van een autorisatieproject.

Doordat detectief autorisatiebeheer minder impact heeft op de bestaande processen en IT-componenten is, is het ook sneller in te voeren. Met name organisaties die autorisatiebeheer snel onder controle moeten krijgen en snel moeten kunnen aantonen dat ze voldoen aan wet- en regelgeving kiezen voor deze AG-methode. IT-auditors passen bij audits eveneens AG-methoden toe. Door toepassing van deze methode worden niet alleen autorisaties opgeschoond, maar ontstaat tevens kennis over de rollen en regels. Deze kennis vergemakkelijkt de latere invoering van preventief autorisatiebeheer, bijvoorbeeld door 'normaal gedrag' uit te werken in een Role Mining project ten behoeve van RBAC.

Starreveld's waarde voor autorisatieregels

Een groot voordeel van de huidige tijd is wel dat we kunnen automatiseren. En dat kan omdat we steeds meer gaan standaardiseren. Daar waar Starreveld bijvoorbeeld handmatige controles moest uitvoeren, kunnen we dat nu grotendeels automatiseren. Het wordt nu zelfs mogelijk om realtime te controleren op afwijkingen van de gestelde norm. We kunnen realtime de juistheid en volledigheid van transacties controleren en dus vaststellen of de transactie door

en namens de juiste persoon is uitgevoerd en of de juiste autorisaties werden gebruikt. Het detectieve autorisatiebeheer levert in de huidige landschappen een goed instrument op om de verantwoordelijke functionaris de waarborg te bieden dat processen lopen zoals ze moeten lopen.

Door automatisering ontstaan wel nieuwe processen. Denk aan het toekennen van autorisaties en het ontwikkelen van autorisatieregels en -matrices. Het toekennen van autorisaties op basis van autorisatieregels is te beschouwen als een beschikkende functie. Het aanbrengen van wijzigingen in de autorisaties (provisioning) is een uitvoerende taak. Voor identiteiten-beheer onderkennen we met name registrerende en bewarende functies. Als ook op dat vlak de juiste beheers-maatregelen worden getroffen, is het ook beter mogelijk om op dat vlak 'in control' te zijn.

Aanbeveling

Dat alles betekent dat voor elk proces onderzocht moet worden welk soort functie door welk soort functionaris (of door welk proces) wordt uitgevoerd en dat de autorisatieregels conform de beslistabel moeten worden vast-gelegd. Dat geldt niet alleen voor de bedrijfsprocessen, maar ook voor de autorisatie- en provisioning processen. Het eenduidig vastleggen van deze beleidslijn en de afzonderlijke regels is een belangrijk onderdeel van Access Governance.

Access Governance blijkt in de praktijk een effectieve en efficiënte methode om inzicht te verkrijgen in de juistheid van de aanwezige autorisaties en daarmee te voldoen aan wet- en regelgeving. De binnen de methode ontwikkelde kennisregels bieden ook het inzicht om enerzijds een uitspraak te doen over de autorisatiestructuur en anderzijds om zo nodig te komen tot een herontwerp van autorisatieregels en -matrices.

Administratieve organisatie

(Bron: http://nl.wikipedia.org/wiki/Administratieve_organisatie)

Administratieve Organisatie (AO) houdt zich bezig met het functioneren van de organisatie, de informatie die hieruit voortkomt en het complex van maatregelen om het functioneren en informeren naar wens te laten verlopen. Een deugdelijke AO is van belang om op de juiste wijze financiële verantwoording te kunnen afleggen en daardoor een goedkeurende accountantsverklaring te verkrijgen.
Functiescheiding wordt toegepast om te voorkomen dat er, door bovenmatige autorisaties, misbruik of oneigenlijk gebruik van gegevens of processen plaatsvindt, waardoor het resultaat van de organisatie negatief wordt beïnvloed. Controletechnische Functiescheiding vindt plaats door bepaalde 'risicovolle' handelingen af te splitsen en bij verschillende functionarissen onder te brengen. Dat geeft meteen de grens van controletechnische functiescheiding aan: tegen samenspanning is vrijwel geen kruid gewassen.

Access Governance

(Bron: KPMG Compact 2010_03)

Access Governance (AG) is een efficiënt proces waarbij op regelmatige basis met behulp van analytische tooling toegang binnen, tot en over applicaties en IT-platformen periodiek wordt beoordeeld.

Conclusie

De ontwerpregels van Starreveld bieden een generiek kader voor het vaststellen van autorisatieregels voor de uitvoering van bedrijfsprocessen. En daarmee zijn deze regels bij uitstek geschikt als basis voor het formuleren van het autorisatiebeleid. De vraag waarom iemand welke autorisaties krijgt, is op grond van de aloude leer van de AO te beantwoorden. En het is mogelijk om de AG business rules te modelleren op basis van de functiescheidingsprincipes van Starreveld.

Wat we daarnaast kunnen vaststellen is dat ook Identiteiten- en Autorisatie-beheer te beschrijven is in termen van functies zoals ontwikkeld binnen de AO-theorie.

Een nadere concretisering van de theorie van Starreveld naar moderne informatieverwerking zou voor de opstellers van autorisatieregels een nog beter handvat kunnen geven. Maar tot die tijd raden we aan om het oude boek toch weer uit de kast te halen.

Bronvermelding

- *KPMG 2: Compact 2010_3 'Facts to value, beyond application security' van Francken, Hermans, Schreurs*
- *CoBiT 4.1, www.isaca.org*
- *Bestuurlijke informatieverzorging Deel 1: algemene grondslagen (druk 5, 2002, ISBN-13: 9789020730524) - R.W. Starreveld, O.C. van Leeuwen, H. van Nimwegen*
- *Bestuurlijke informatieverzorging deel 2a (druk 5, 2004, ISBN-13: 9789020730531) - R.W. Starreveld, O.C. van Leeuwen, H. van Nimwegen*
- *Bestuurlijke informatieverzorging deel 2B (druk 5, 2008, ISBN-13: 9789020733105) - R.W. Starreveld, O.C. van Leeuwen, H.B. de Mare*
- *KPMG 1: Afweging tussen business-flexibiliteit en controle via functie-scheiding - Gerben de Roest en Maarten de Rooij (KPMG Compact, 2008-3, http://www.compact.nl/artikelen/C-2008-3-Roest.htm)*

INTERVIEW MET JUUSO PESOLA

ENCRYPTION WITH A TWIST

Juuso Pesola is medeoprichter en vicepresident van research en ontwikkeling bij Envault Corporation, een bedrijf dat data-protectie oplossingen levert. Envault is gevestigd in Vantaa, Finland. Juuso is te bereiken via Juuso.Pesola@envaultcorp.com. Opmerkingen of vragen naar aanleiding van dit interview kunnen worden gestuurd naar Lex Borger, hr@pvib.nl.

Eind vorig jaar hoorde ik over een mij onbekende manier om data te vercijferen. Deze methode heet envaulting en ligt ten grondslag aan de producten die het bedrijf in de markt zet. Om hier meer over te weten te komen, had ik een aantal gesprekken met Juuso Pesola, die de R&D van het bedrijf overziet. Deze gesprekken waren in het Engels.

In the Dutch market, we are not yet familiar with Envault, its solutions and its products. To start with, I ask Juuso how they position Envault in the market. Is it a data encryption/ protection tool or is it a secure content management system?
"We position our solution as a data protection tool. The target segment is big corporate customers who have many end-users and end-user devices and need to follow and control the flow of their sensitive data, for example due to compliance or regulatory reasons."
When you read about Envault, it is quickly obvious that everything revolves around the method of **envaulting**. I ask Juuso to define and describe what envaulting is.
"Envaulting is a data protection method, in which the data to be protected is first encrypted and then divided into two parts. The bigger part, approximately 99% of the original data, is stored where the system directs it, for example locally on the hard drive. The smaller part (the fragment) is stored in a special server, the Fragmentvault-server, located at a trusted location in the network. This server is typically located in the corporation's intranet.
Envaulting starts with encrypting the data. The encryption algorithm used in the process can be freely chosen, but typically standard AES–256 (CBC mode) is used, with randomly generated 256-bit secret keys. The division of data in two parts is done in such a way that the removal of a little bit of the data affects all the remaining data, effectively making it impossible to decrypt. The smaller part, the fragment, in fact has become a 'technical' password for that processed data. Keep it separated from the remaining data and you can use it for access control.

> The division of data is done in such a way that the remaining data cannot be decrypted

This division is the key step in the method. Before a fragment can be separated, a preceding diffusion step ensures that enough entropy is created that each bit in the fragment is required to be able to decrypt the data. When the fragment is removed from data, the data can no longer be successfully decrypted. The size of the fragment selected is large enough to prevent brute-force guessing of the fragment. It is set to 128 bits at this moment. It has properties of a hash,

and it uniquely identifies the data from which it is created (and that is stored)."

My understanding of the envaulting method grows as the interview progresses. So the fragment is required to decrypt the data and can be used to identify the data. However, if you remove the fragment and store it elsewhere, you take away the ability to use it for identification. When a user wants to access the original data, how is the corresponding fragment found in the central Fragmentvault-server?

"There is a mapping database that links the fragment to its originating file. Each file in the map is unique, even though it might be a duplicate of data stored elsewhere. As our software intercepts write and read operations, a copy and move generates a new file from Envault's point of view. Renaming a file is just an update to the fragment's metadata. The fragments are stored in the server's file system, not in the database, and the mapping information actually provides a direct link to the file containing the fragment. This makes operating system features like data roaming, back-ups, and synchronization transparent to envaulting. They can be done with basic services provided by the OS. Envaulting is efficient because it divides data into blocks, so in fact there is a fragment produced for each block of data. As a result, editing an envaulted document changes only part of the fragments, not all files need to be re-envaulted. It also adds to the protection, because unauthorized knowledge of fragments and/or encryption keys does not automatically open the newest versions of the files, because the encoding of the fragment is different."

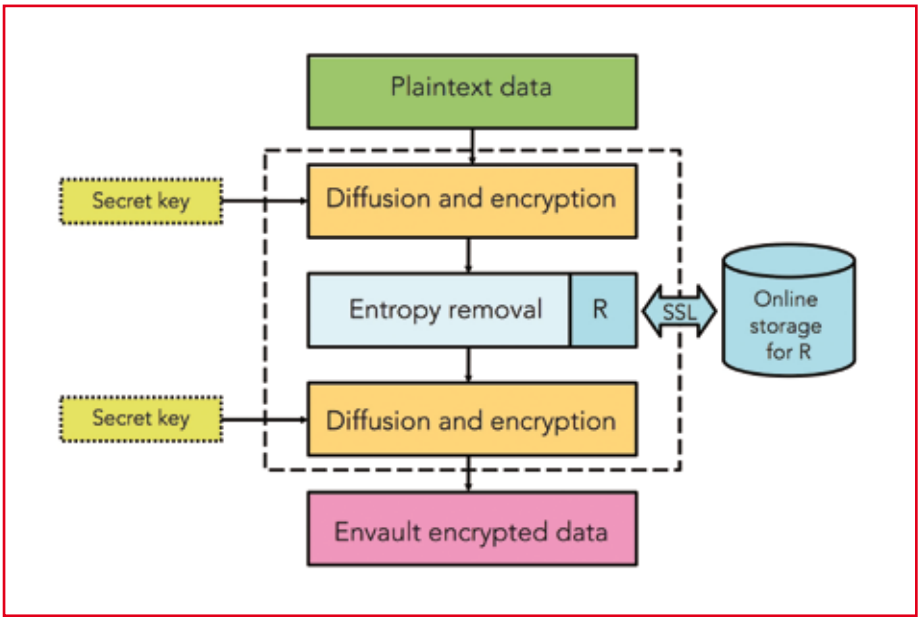


Figure 1 - The Envault Method

Password-free data-protection

We proceed to talk about the benefits that the envaulting method brings.

"The envaulting method is used to provide very easy-to-use, password-free data protection products for end-users in corporation environments. The method actually creates a very simple but efficient key management system, which enables automatic protection of data, without needing any information, like a password, from the end-user. Actually, the whole process is totally transparent to the user: he is actually unaware that the data is encrypted and decrypted. I could add that it brings an additional layer of security on top of the encryption algorithm used, but when you use AES–256, that does not add any relevant encryption strength."

So, envaulting is like encryption with a twist. I wonder what the advantage of this is, since there are comparable encryption products out there using standard encryption. Envault is not a standard crypto solution, even though components of it use standard crypto. So I ask how the Envault products distinguish themselves from other data encryption solutions.

"The difference between mainstream encryption products and Envault's data protection is that encryption products are based on a password that is provided by the end-user and thus needs to be managed by the end-user. They have an end-user centric solution, while Envault's products are corporation-centric. Envault works in the context of an established security session, like a login to the Microsoft Active Directory. If a smart card login is used by the organization, it applies to all envaulting activity. If the user's account is reset, envaulting keeps working. And not in the least: if an administrator has access to the user's files, he cannot access the data because he has no access to the fragments. Yet, backup/restore mechanisms will work fine.

The whole process of envaulting is thus transparent to the end-user. He has no passwords to choose. The control over and the protection of the data are managed centrally by the organization using Envault products. As such, fragments are stored in the Fragmentvault-server. For this reason we adopted user-friendliness and high-usability as our most important design principles, next to data protection and company control."

I remark that there are corporation-centric encryption solutions that do not burden the user with password creation and management. "What is the benefit of envaulting in this case", I ask.

"Envaulting gives an additional layer of security on top of the used encryption.

OS features like data roaming, back-ups and synchronization are transparent to envaulting

During my research I ran across the name of a security expert who I know: Hannu Kasanen. He participated in the evaluation of a collection of security products for Secproof [3]. I was able to get a personal reaction from him – I should note that he is no longer with Secproof. He was positive about Envault, but with a critical note.
"Envault's ability to retain control over data stored on various types of removable media is its unique selling point. With Envault, the enterprise is able to control how the data can be used after it has left the building. For example, storing confidential information onto a USB memory stick is a smaller risk if the data is properly encrypted.
One critical point: that doesn't prevent me from accessing the data after I've been terminated. Envault is supposed to address that issue. I also remember being annoyed when it came to offline and off-site data usage. After all, there are plenty of legitimate reasons for sharing data using, say, USB memory sticks. Having the Envault solution in place meant that I had to store the data to the Airlock and whoever received the memory stick had to execute "airlock.exe" to access the files. I hardly call that a transparent solution."

"An Expert's View"

Some of our customers consider this to be the main advantage. They presume that AES (or its implementation) might have a backdoor or will eventually get broken. These risks are eliminated by our products."

Offline operation

Envaulting is a method that requires online access to the Fragmentvault-server. But I know from reading the product descriptions that it can also work offline. In offline mode, recent fragments are still available for the user, using his company PC. That means that fragments are then cached on the end-user's device. How does this work?
"The user can be given controls to download all of his fragments, or remove all the locally cached fragments. He even gets those by default. We could implement more detailed controls, but our customers have not requested that yet. The organization maintains control over the fragments by setting the lifetime for the fragments, so that they are cached only for a limited time. This timespan is very flexible, from 1 second to unlimited. Also, an organization can remotely remove all fragments, combined with an 'anti-theft' feature that, if enabled, forces the device to check in at a specific internet-facing server. This server contains rules to disable stolen laptops. If the contacting device is on the list, it empties its cache. All offline accesses are reported to the central server once the device comes back online."

The device checks in to validate it is not stolen. If it is listed, it empties its cache

Another feature that I had picked up was the ability to share data with other parties - outside of the control span of the organization, for example on storage devices (like USB-sticks). This sounds like an interesting feature. Does it require extra software?
"The envaulted files and fragments are stored encrypted with AES256 on the storage device, together with a special program, called Airlock. The AES keys are also stored in the Airlock and protected by a key generated from the user password with PBKDF2. The outsider with whom data is shared needs to run this program. It is a simple Windows .exe, installed on every protected storage device. All data put into the Airlock is encrypted and password protected.
The only way to access data on the storage device is to launch Airlock. When it is launched, it checks the local time and acts accordingly by either decrypting the data or destroying the data. Airlock generates log from all the user actions on the storage device, which is sent to the Fragmentvault-server when the Airlock is attached to an Envault client. There are some additional controls to limit the ability of an attacker to tamper with the time on the remote workstation; the Airlock notices any illogical jumps in time. In this case a warning is given and logged. We decided against automatic removal, to make availability prevail in this case.
Any time you apply a twist to cryptography, you run the risk that you introduce a vulnerability. So I ask if there was any formal cryptanalysis performed on the envaulting process.
"Envault did not implemented its own crypto library; instead we use the well-known FIPS 140–2 certified OpenSSL crypto library. The key generation and management as well as the overall security of the Envault products are currently awaiting approval in the national acceptance process, during which the National Communications Security Authority NCSA-FI together with Finnish Defense Forces has been evaluating the technology thoroughly. The process is expected to result into National and EU acceptance during the first quarter of 2013."
Other vulnerabilities can be introduced in the software development process. I am a software developer; I know how problems can just sneak in. So how is the software QA done on all envaulting code?

"Envault uses Quality Assurance processes derived from the common standards and modified to better serve Envault's requirements. All the core libraries as well as the products are continuously tested: we perform code reviews, unit tests, module tests and release tests. Most of the testing is automated with manual analysis of the results. Still, the code reviews and many of the use cases require manual interaction in order to provide meaningful results. Testing activities are the most laborious tasks in our R&D work."
I think that with all this attention, envaulting might even be considered to become a recognized cryptographic method. At this point it is intellectual property of Envault and there is a patent pending. I ask Juuso if he foresees that envaulting might become a standard at some time in the future.
"We have considered publishing the so far confidential parts of the Envaulting method as open source, but so far it has not been done. However, there are no specific reasons why it could not be done, and the overall security of the method does not rely on anything that should be kept proprietary or in secret. Still it is a whole other story to make it standard, even if it would be published."
I thank Juuso for his information. It has helped me to understand the underpinnings of the envaulting method. ●

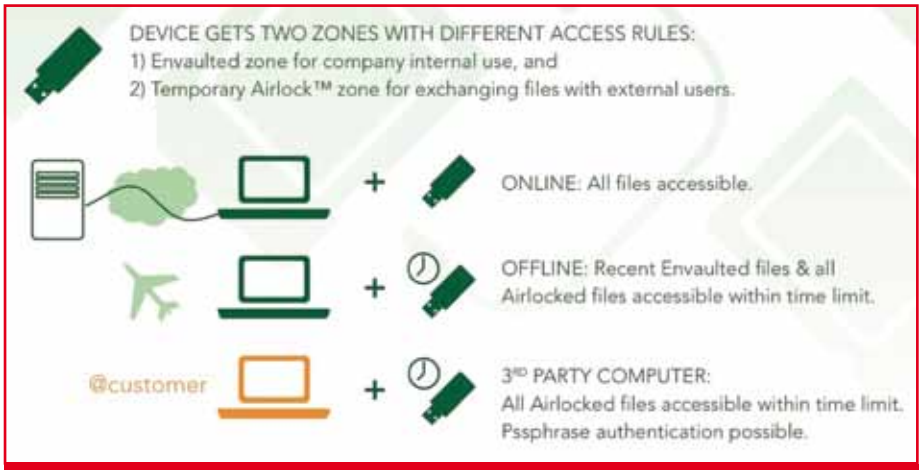


Figure 2 - Overview of Removable Media Protection

Testing activities are the most laborious tasks in our R&D work

Links

[1] Corporate web-site: http://www.envaultcorp.com/

[2] Envault management team: http://www.envaultcorp.com/about-us/people

[3] Report of Secproof: http://www.envaultcorp.com/wordpress/wp-content/uploads/Secproof_RESEARCH_RemovableMediaProtection_2009.pdf

FOX IT

for a more secure society

FOX-IT voorkomt, onderzoekt en beperkt de meest serieuze cyberdreigingen met innovatieve oplossingen voor overheid, defensie, politie, vitale infrastructuur, banken en grote bedrijven wereldwijd. Onze aanpak combineert slimme ideeën met technologie om hiermee innovatieve oplossingen te bieden die zorgen voor een veilige maatschappij. We ontwikkelen producten en maatwerkoplossingen om de beveiliging van gevoelige overheidssystemen te garanderen, industriële netwerken te beschermen, online bankiersystemen te verdedigen en strikt vertrouwelijke data te beveiligen.

FOX-IT.COM

Fox zoekt nieuwe Foxers

FOX-IT groeit en bloeit. Om deze reden zijn wij over de volle breedte van ons werk op zoek naar hackers, Forensic Experts, Pentesters, Developers (Python / C++), Hardware Engineers en Fraude analisten. Een Foxer is nieuwsgierig, kritisch en talentvol.
Je draagt bij aan de missie van FOX-IT: having fun in making technical and innovative contributions for a more secure society

Interesse om bij ons te komen werken?
Bel of mail Walter Doorduin 06 41901011 of doorduin@fox-it.com.

MAN IN THE BROWSER

YOUNG PROFESSIONALS SESSIE

Cor Verkoelen is security scientist bij TNO.
Hij is te bereiken via cor.verkoelen@tno.nl

Op 26 september is de sessie van de Young Professionals "Man-in-the-browser" gehouden. Voor deze sessie is SNS REAAL bereid gevonden om een achtergrond, werkwijze, en inzicht in tegenmaatregelen te geven. Om 18:00 werden de leden van PvIB en NOREA welkom geheten op de locatie van SNS REAAL in Utrecht. De presentaties werden verzorgd door twee enthousiaste Security Specialisten van de afdeling Informatiebeveiliging van SNS REAAL, Martijn Veken en Joris Kuijper.

In deze presentatie werden de deelnemers aan de hand meegenomen door de tijd, waarin duidelijk werd gemaakt dat de tijden veranderen van traditionele bankroof naar een man-in-the-browser aanval. Daar waar banken zich goed wapenen tegen een fysieke bankroof, ligt er op dit moment nog een uitdaging voor de bescherming van een bank tegen een logische aanval. Ook werd duidelijk dat er verschillende initiatieven zijn genomen om in deze wedloop aan kop te blijven door, onder andere, verschillende (internationale/sectorale) samenwerkingsverbanden en een overzicht van mogelijk te nemen maatregelen.

Zo is tijdens deze informatieve avond een compleet beeld gegeven van context tot en met de technische analyse van een daadwerkelijke besmetting van een systeem met malicious software, wat resulteerde in een man-in-the-browser aanval. Het is tijdens deze avond duidelijk geworden dat er een race is tussen de aanvallers en de beveiligers, waar aan beide kanten steeds nieuwe ontwikkelingen plaatsvinden. Wat hierbij de rol van de burger is en hoe deze betrokken kan worden, of juist niet, in het voorkomen van de steeds complexer wordende aanvallers, is verder toegelicht.

Joris Kuijper

Martijn Veken

Vanuit de Young Professionals willen we via deze weg nogmaals SNS REAAL, en in het bijzonder Marijn en Joris, bedanken voor deze informatieve avond en het enthousiasme waarop deze beide Security Specialisten het onderwerp hebben toegelicht aan de leden van PvIB en Norea. ●

Link

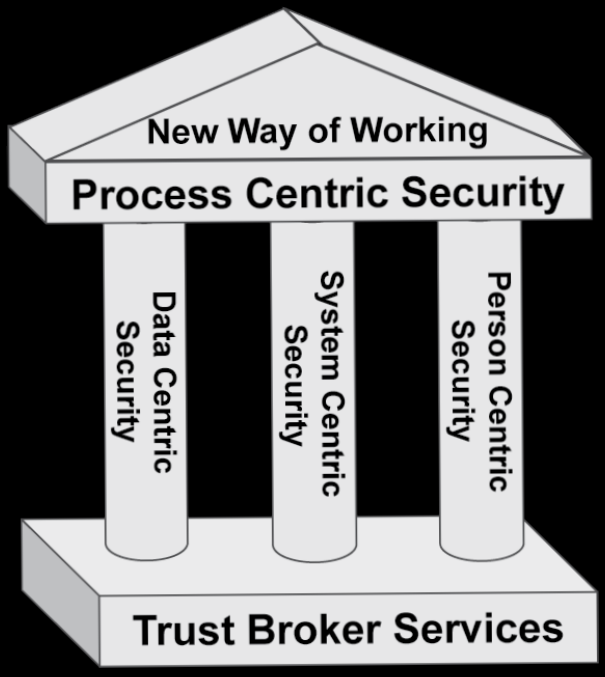
PvIB Young Professionals:
http://www.pvib.nl/yp-algemeen

COLUMN

FUTURE READY

In this issue we take another Business Attribute from the SABSA Business Attributes Taxonomy, looking this time towards the future. What kind of security architecture shall we need to align with new and upcoming business models as they evolve? How shall we be ready for the future? In the previous issue we pointed to the emergence of 'everything as a service', the changing attitudes of 'Generation Y', the need to be more business-process centric and what is commonly referred to as 'The New Way of Working'. Now we examine some of the specific developments and how we should address them.

It is helpful to list the current trends: cloud services; smart personal hand-held devices, green IT driven by the desires of society to conserve both energy and materials (by moving to more home working with fewer office buildings and less use of transport), massive roll-out of Wi-Fi including 4G (enabling mobility on a scale never before possible), and a high demand for 'bring your own device' (BYOD).



Traditionally 'security architecture' has been based on a system-centric view.
The aim has always been to secure a series of systems, and the very concept of a system implies a boundary between the system and its environment – in the majority of cases a physical boundary. Even when we began to deal with 'distributed systems' this physical notion of the system was sustainable because then we had a series of physical sub-system islands interconnected by networks that could be secured by logical means. The main characteristic was that we still knew where everything was to be found.
The introduction of 'service oriented architecture' meant that this physical visibility was removed to a lower layer in the stack, but nevertheless we could still draw a series of physical diagrams that would locate every component of our architecture. That is what is changing.

In the cloud you no longer know where your data is being stored and processed. In the Wi-Fi environment with portable devices you no longer know where your users are situated. All physical control disappears and all you have left is logical control. That means that the security and assurance policies to be applied to your data must travel with it and must be applied to it wherever it lands. Similarly user security and assurance policies must be bound to the people and their mobile devices, irrespective of where they travel. So as well as a system-centric view of security architecture (yes, we shall still need that) we must now also conceive of a data-centric view and a person-centric view, with detailed mobile security profiles that will be articulated in the form of Business Attribute Profiles that travel with the data and the person/device. This three-pillar conceptual security architecture is shown in the diagram.

There remains one more major issue – trusted execution. In the end there must be an execution platform that is trusted to abide by and enforce these mobile policies, and we no longer know where it is or who owns it. Anyone, any time, any place is our new mantra. So how will this work? We predict the emergence of a new market place for trust services, offered by trust brokers who fulfill the role of the traditional 'trusted third party' and who arrange for our services to be provided by a global network of trusted service providers. 'Trust-as-a service' (TaaS) will be a major new component of the services market place and the foundation stone of our future security architecture. It is immature at present but without this development it is difficult to see how the present trends will be sustained.
It remains to be seen who will be the leading players in this new market, but one thing is for sure – we shall need the Business Attributes profile as means to communicate our detailed requirements for securing and assuring our data and its use in a common, machine readable, XML-based language. ●

The Attributer

NOMINATIES VOOR ARTIKEL VAN HET JAAR 2012

Van de redactie

Het wordt de vijfde keer dat het PvIB een prijs uitlooft voor artikel van het jaar. In deze jaarlijks terugkerende activiteit worden opnieuw drie prijzen uitgereikt. De eerste prijs zal een waarde hebben van vijfhonderd euro. De meest belangrijke reden om een prijs uit te reiken aan onze auteurs is om waardering uit te spreken en ze te bedanken voor de goede artikelen die ze ons bezorgen.

De jury is samengesteld uit drie gekozen ledenvertegenwoordigers. De redactie heeft een voorselectie gemaakt van twaalf artikelen, waaruit de jury drie winnaars kiest en haar keuze in een juryrapport onderbouwt.

In de jury zitten dit jaar:
Leo van Koppen van de Haagse Hogeschool
Remco Bakker van CQure
Lambrecht Nieuwenhuize van BNG

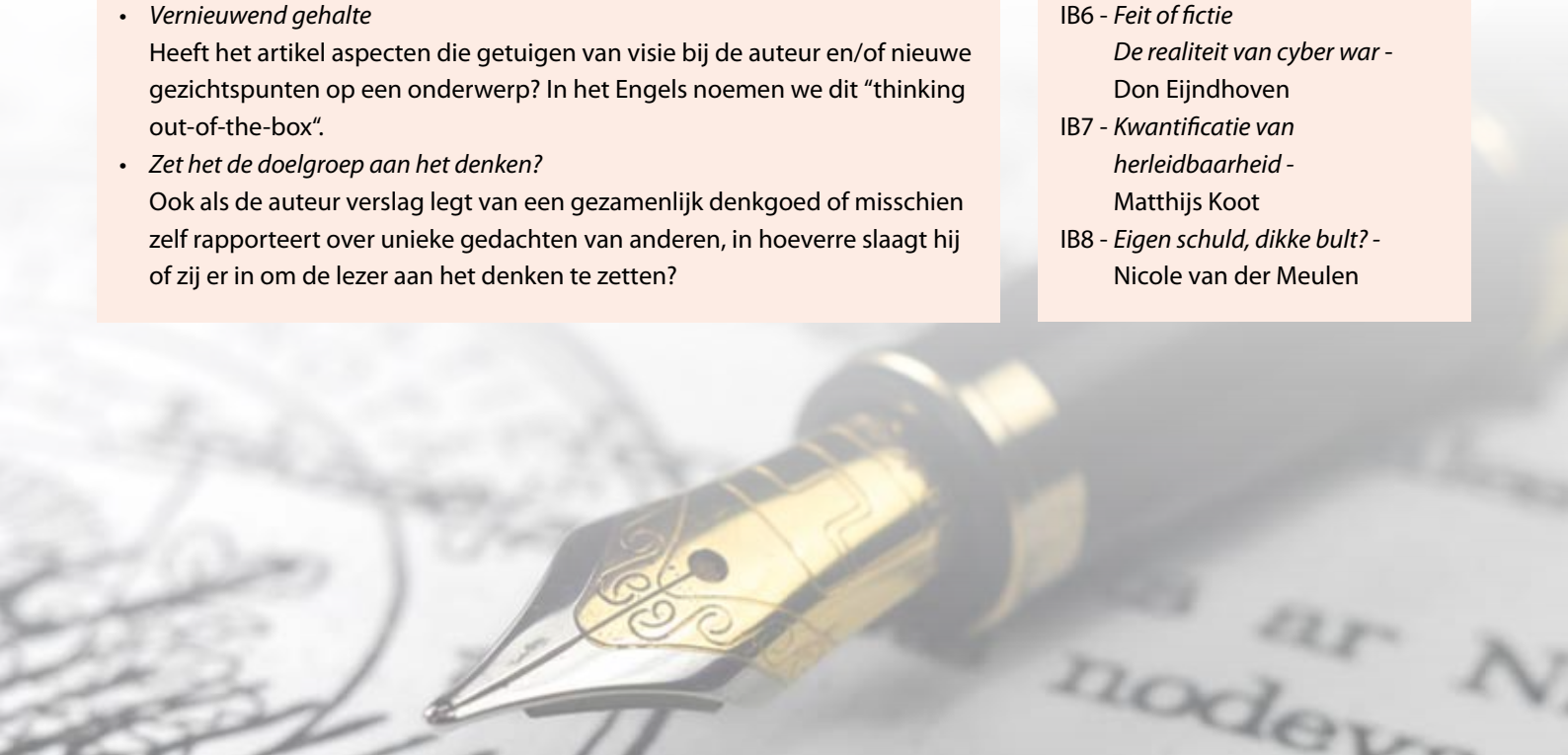
Vaste rubrieken en artikelen van redactieleden dingen niet mee. De criteria die we de jury meegeven zijn ongewijzigd en van oplopend belang. De redactionele begeleiding helpt bij de eerste drie criteria. De laatste twee criteria gaan over de creatieve inbreng van de auteur en zijn dus van speciaal belang.
Uitreiking van de prijzen wordt opgenomen in het programma van de ledenvergadering en bijeenkomst op 14 mei a.s. ●

Beoordelingscriteria:

- *Opzet artikel*
  Is de opzet van het artikel juist voor de soort (inhoudelijk of opiniestuk)?
- *Leesbaarheid*
  Is het artikel helder en begrijpelijk geschreven, met passende illustraties? Is de stijl consistent, zoals serieus of satirisch? Of het nu een praktijkbeschrijving is of een wetenschappelijke beschouwing betreft, is de leeservaring prettig?
- *Benadering van de doelgroep*
  Is het duidelijk wat de doelgroep is voor het artikel? Is het artikel te volgen voor een lezer buiten de subgroep?
- *Vernieuwend gehalte*
  Heeft het artikel aspecten die getuigen van visie bij de auteur en/of nieuwe gezichtspunten op een onderwerp? In het Engels noemen we dit "thinking out-of-the-box".
- *Zet het de doelgroep aan het denken?*
  Ook als de auteur verslag legt van een gezamenlijk denkgoed of misschien zelf rapporteert over unieke gedachten van anderen, in hoeverre slaagt hij of zij er in om de lezer aan het denken te zetten?

Genomineerde artikelen (op chronologische volgorde):

IB1 - *Virus in je noodstroomgenerator* - Jeroen Aijtink en Jan Wiersma
IB2 - *De impact van BYOD* - John Grüter
IB3 - *Het lekken van data* - Johan Pater
IB4 - *Lean Business Continuity* - Management bij VGZ - Thérèse van Vliet
IB4 - *Hebt u ze op een rijtje?* - Rob van Gansewinkel en Aaldert Hofman
IB5 - *Vergeten gegevensrisico's* - Ronald Koorn en Jeroen van Kerkhof
IB5 - *Pincode voor je pacemaker* - Jules Prast
IB6 - *Schaap of Herder* - Jurgen van der Vlugt
IB6 - *Open Einde* - Henk-Jan van der Molen
IB6 - *Feit of fictie De realiteit van cyber war* - Don Eijndhoven
IB7 - *Kwantificatie van herleidbaarheid* - Matthijs Koot
IB8 - *Eigen schuld, dikke bult?* - Nicole van der Meulen



In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever, of van PvIB. Vragen en/of opmerkingen kunt u sturen naar ibmagazine@pvib.nl.

RESPONSIBLE DISCLOSURE

Begin januari presenteerde minister Opstelten 'Een kader voor het verantwoord melden van beveiligingslekken'. Het kader, waaraan diverse beveiligingsspecialisten meewerkten, beoogt goedwillende hackers structuur te bieden voor het verantwoord onderzoeken en melden van kwetsbaarheden. Maar biedt dit kader hackers ook daadwerkelijk juridische bescherming? En krijgen publiciteitszoekers hiermee niet juist een vrijbrief om bedrijven ongevraagd te testen? Met als gevolg dat een hardwerkende systeembeheerder 's-nachts om twee uur door het IDS uit zijn bed wordt gepiept, omdat een hackende student zijn pizza nog niet op had en het "met alle goede bedoelingen" op zijn systemen heeft gemunt? Onze redacteuren bogen zich over dit vraagstuk en komen met een aantal interessante invalshoeken.

Aart Jochem

Hacken *leeft* in Nederland. Met de publicatie van 'Een kader voor verantwoord melden van beveiligingslekken' beantwoordt minister Opstelten een vraag aan hem gesteld door de Tweede Kamer. Ook voormalig minister Spies van BZK heeft desgevraagd al eens een lans gebroken voor de ethische hackers. Hacken werd even synoniem met klokkenluiden, het aan het licht brengen van misstanden, toen in 2011 een maand lang dagelijks beveiligingsissues werden gepubliceerd.

Lang voordat E.L. James zijn bestseller schreef, wisten hackers en beveiligers al dat er meer schakeringen zitten tussen white en black hats. Voor organisaties die geconfronteerd werden met meldingen door hackers is deze nuance vaak moeilijk te zien. Sommige reageren direct door alle communicatie met de melder te stoppen en aangifte te doen bij de politie. Andere organisaties, die de internetcultuur beter kennen, gaan het gesprek aan en belonen zelfs de onderzoekers. XS4All geeft al lange tijd duidelijkheid over wat wel en niet mag, Google is genereus met het belonen van onderzoekers en Marktplaats heeft sinds een jaar een helder beleid op het melden van kwetsbaarheden.

Met de Leidraad voor Responsible Disclosure biedt minister Opstelten een handreiking hoe organisaties kunnen omgaan met meldingen van hackers en beveiligingsonderzoekers. Het idee is dat organisaties aan de slag gaan, voorbereid zijn op een melding en een hacker weet hoe hij moet melden. Opstelten biedt ook een uitweg als het niet loopt: het NCSC kan bemiddelen. De leidraad is een startpunt waarmee organisaties aan de slag kunnen.

De reactie uit de hackerswereld is wisselend. Hackers die dachten dat ze aan de slag kunnen zonder het risico dat er aangifte wordt gedaan of dat het OM eigenstandig een onderzoek instelt, zijn ernstig teleurgesteld. Hacken blijft strafbaar, maar als aan bepaalde voorwaarden wordt voldaan, zal een organisatie besluiten om geen aangifte te doen. Deze voorwaarden moet de organisatie helder communiceren en een hacker in acht houden. Een lek aantonen kan bijvoorbeeld ook zonder een groot deel van de database te downloaden of extra software te installeren. En een hacker die de grenzen overschrijdt, kan zich altijd nog achter de bronbescherming van een journalist verstoppen. Helaas heeft de gehackte organisatie niet zo'n troefkaart.

Met het publiceren van de Leidraad is de discussie rond responsible disclosure nog niet klaar. Er zullen in de praktijk nog belangrijke lessen geleerd kunnen worden, tussen beveiligingsonderzoekers en organisaties. Onderzoeker Floor Terra heeft via *responsibledisclosure.nl* een voorbeeld van een policy gegeven. En de community van internetorganisaties, hackers en overheid heeft sterke behoefte aan goede voorbeelden. Maar er is een duidelijke start gemaakt.

André Koot

Complimenten voor de minister, dat 'ie de richtlijnen voor ethisch hacken heeft omarmd. Hij kan helaas weinig met die complimenten, want daar blijft het bij. Het is natuurlijk wel een heftige ontwikkeling, want door de

richtlijnen wordt feitelijk een gat geschoten in de wetgeving rondom computercriminaliteit. Sommige strafbare feiten worden gedoogd, maar wel met een boel mitsen en maren en nog meer slagen om de arm. En daar ligt dan ook de beperking van mijn loftuiting: daar had de minister (en het NCSC) wel een stap verder kunnen gaan. De grootste zorg is voor mij dat er onvoldoende vrijwaring voor justitieel ingrijpen wordt toegezegd voor onderzoekers die zich houden aan de richtlijnen (die overigens te beperkt zijn voor hackers) en die overduidelijk met de goede intenties een onderzoek uitvoeren en de resultaten melden. Dat had voor mij wel wat beter gekund. Hoe dan? Zonder hacken aan te moedigen? Vooropgesteld, ik ben een voorstander van het *responsiblediscloure.nl* initiatief van Floor Terra. Maar ook dat concept mag wat mij betreft een stap verder gaan: als 'hacker' en slachtoffer beiden dezelfde uitgangspunten onderschrijven, dan is er geen enkele reden voor het OM om in te grijpen. Als een onderzoeker zich heeft gehouden aan de richtlijnen en als hij/zij daarmee de intentie aangeeft om een bijdrage te leveren aan het beveiligen van een organisatie, dan hoeft er geen aangifte te volgen. Dat laat ruimte voor ingrijpen als blijkt dat de onderzoeker zich niet aan de gedragscode heeft gehouden. In dat geval moet het OM dus wel ingrijpen. Maar er is een andere kant aan de huidige RD: alleen de hacker wordt aangepakt. Onachtzaamheid door organisaties blijft onderbelicht. Om die reden hebben we het CBP gevraagd om onderzoek te doen naar Diagnostiek voor U, dat mijns inziens nalatig was bij het beveiligen van gevoelige medische gegevens. Alleen de hacker (Henk Krol...) aanpakken levert geen bijdrage.

Maarten Hartsuijker

Terwijl ik de inleiding voor deze 'Achter het Nieuws' schreef, merkte ik hoe lastig dit onderwerp eigenlijk is. Ik weet dat er veel organisaties zijn die weinig tot geen aandacht aan beveiliging besteden. En dat deze organisaties slordig met persoonsgegevens omgaan en af en toe best wat goed bedoelde hacker-aandacht kunnen gebruiken. Hoewel ik er daardoor van overtuigd ben dat het verschrikkelijk belangrijk is om goedwillende hackers handvatten en bescherming te bieden, zit ik er als security officer eigenlijk niet op te wachten dat Jan en alleman op onhandige tijden in mijn domein gaat lopen testen. Toegegeven: een onschuldig incidentje op zijn tijd is geweldig voor de awareness sessies en het beveiligingsdraagvlak. Maar security analisten en systeem-beheerders zijn ook gewoon gek op hun nachtrust.

Tegelijk is het zo dat waar mensen werken, fouten worden gemaakt. Geen enkel bedrijf zal zijn hand ervoor in het vuur steken dat zijn infrastructuur volledig foutvrij is. En klanten die je op een integere en constructieve manier op een fout wijzen, zijn natuurlijk goud waard. Zij helpen je om je eigen gegevens en die van klanten nog beter te beschermen.

En hier zit, denk ik voor vele beveiligingsbewuste organisaties het dilemma. Terwijl je blij bent met meldingen die je kunnen helpen om jezelf te verbeteren, wil je niet elke technische student die op internet een paar leuke tools heeft gevonden, uitnodigen om daar op jouw infrastructuur proef mee te draaien. Hoewel ik graag schouderklopjes en beloningen geef, vind ik omgevingen waar bedrijven hun geld verdienen eigenlijk geen speeltuin.

Misschien zouden we landelijk een nationale testdag moeten organiseren waarop goedwillende hackers vrij zijn om websites te testen. En als we met z'n allen op zo'n dag (of elke andere dag) dan wat minder opletten, omdat we er vanuit gaan dat de hackers wel het beste met ons voor zullen hebben, kunnen de echte cybercriminelen mooi via een #0day met de ruis mee naar binnen. ●

COLOFON

Informatiebeveiliging is het huisorgaan van het Platform voor InformatieBeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

Redactie
Lex Borger (hoofdredacteur, werkzaam bij Ideas to Interconnect), e-mail: hr@pvib.nl
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

Redactieraad
Tom Bakker (Allianz)
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Maarten Hartsuijker (ANWB)
Aart Jochem (NCSC)
André Koot (i3advies)
Rachel Marbus (NS, IT Advisory)
Bart van Staveren (UWV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl;
of neem contact op met MOS (Motivation Office Support)
T (033) 247 34 00
ibmagazine@pvib.nl

Vormgeving en druk
VdR druk & print, Nijkerk
www.vdr.nl

Uitgever
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
T (033) 247 34 92
F (033) 246 04 70
E-mail: secretariaat@pvib.nl
Website: www.pvib.nl

Abonnementen 2013
De abonnementsprijs bedraagt 115 euro per jaar (exclusief btw), prijswijzigingen voorbehouden.

PvIB abonnementenadministratie
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
e-mail: secretariaat@pvib.nl

ISSN 1569-1063

COLUMN

SNOEP VERSTANDIG, GEBRUIK EEN APPLE

Ook dit jaar had ik weer een aantal goede voornemens die eigenlijk allemaal al een beetje verbroken zijn. Ondanks de beloften aan mijzelf ga ik weer te laat naar bed en zo kan ik nog wel een aantal voornemens noemen die ik niet meer na kom, jammer! Nu sta ik op het punt weer een goed voornemen de nek om te draaien, namelijk om weer eens iets te schrijven over Apple en Samsung. Deze twee clubs hebben inmiddels de gehele markt van tablets en smartphones overgenomen en inmiddels iedere rechtbank ter wereld van binnen gezien. Samsung zou patenten van Apple hebben gestolen en die zonder toestemming hebben gebruikt. Samsung zou bovendien de modellen van Apple ordinair kopiëren en op die manier een graantje meepikken van deze markt, die sinds een aantal jaren volledig op zijn kop staat en waar de gevestigde orde niet meer weet hoe ze hun producten op de markt kunnen wegzetten. In een Amerikaanse rechtszaak werd Samsung veroordeeld tot een boete van 1.049 miljard dollar, een schijntje vergeleken met de winsten die Samsung haalde de afgelopen periode. Nu heeft de rechtbank een hele pikante uitspraak gedaan, namelijk dat Samsung niet met opzet heeft gehandeld bij het kopiëren van de Apple producten. De boete blijft wel staan, maar Samsung heeft het echt niet expres gedaan. Ik weet niet of jullie wel eens een tablet van Samsung naast die van Apple hebben gelegd, maar neem van mij aan dat de overeenkomsten ook wel bijzonder zijn. Totdat je de tablet aandoet, want dan gaan de grote verschillen ontstaan.

Als de machines aangezet worden, zie je een grote verscheidenheid aan apps die ook niet direct het verschil maken. Veel apps zijn gewoon vergelijkbaar met elkaar dus gaan we nog een niveau dieper graven. Het besturingssysteem van een tablet of een smartphone zijn onderling niet te vergelijken. Android heeft ontegenzeggelijk de mooiste namen bedacht voor het besturingssysteem. Namen als Cupcake, Donut, Gingerbread, Honeycomb en Jelly Bean spreken natuurlijk veel meer aan dan iOS 4, of iOS 5 of iOS 6. Nee, op dat gebied ligt Android toch wel een groot aantal punten voor. Naast de vele versies van het Android besturingssysteem zijn we er nog niet, omdat iedere fabrikant zich wil onderscheiden is Jelly Bean op een HTC anders als op een Samsung of een Sony, nog sterker deze versies zijn onderling niet uitwisselbaar. Waarom zou iemand zich druk maken over het besturingssysteem van een telefoon? Ten eerste hebben we het niet meer over een telefoon, maar over een smartphone. Dit lijkt een miniem verschil, maar als je prijs en functionaliteit vergelijkt, merk je de verschillen echt wel. Een smartphone is gewoon een computer die vergelijkbare zaken kan als een laptop of tablet en dus ook de vergelijkbare risico's met zich mee brengt. De foto's van de kinderen, je mail, documenten, creditcardgegevens, je mobiele bank gegevens, eigenlijk staat je hele hebben en houden op je device. Toch is het wonderlijk dat het laatste besturingssysteem van Android slechts op 10 procent van alle devices staat, dat betekent dat er op 90 procent van alle Android devices een verouderde versie van het besturingssysteem staat. Een versie die malware niet kan tegenhouden en die het device geschikt maakt om te kraken en te misbruiken. Ga naar een willekeurige elektronica winkel en vraag of ze je even willen helpen met het plaatsen van de nieuwste software. In eerste instantie wordt je wat glazig aangekeken en vervolgens gaan ze tientallen redenen opnoemen waarom je dat niet moet doen. De telefoon wordt traag, veel kans op problemen en de rest bespaar ik jullie.
iOS heeft dan weliswaar niet de meest in het oog springende naam, maar de updates gaan gewoon automatisch. Je wordt vriendelijk gewezen op het feit dat er een nieuwe iOS is en even later staat die op je device, die daarmee weer beschermd wordt tegen de allerlaatst bekende gaten in de software. Zolang je iOS device wordt ondersteund door Apple zal deze methodiek werken, een gebruiker zal deze updates ook installeren, omdat er vaak extra functionaliteit meekomt in de update. Dit is dan ook de reden dat iOS 6 in oktober 2012 binnen 6 weken op meer dan 200 miljoen iOS devices was geïnstalleerd. Blijkbaar ben ik dan toch niet de enige die behoefte heeft aan een robuust en veilig besturingssysteem. Misschien zou Samsung dat eens moeten kopiëren van Apple! ●

Berry

Data Leakage

Bring Your Own Device

Security As A Service

Compliance & Auditing

SECURITY

geen keuze, maar noodzaak!

De toepassingsmogelijkheden van Bring Your Own Device, Security As A Service, Data Leakage en Compliance & Auditing ontwikkelen zich in hoog tempo. Daarmee nemen ook bedreigingen toe in de vorm van Cybercrime, Hacking en Identiteitsfraude. Ook worden deze bedreigingen steeds geavanceerder. Adequate beveiliging van werkomgevingen, data en identiteitsgevens zijn inmiddels geen keuze, maar noodzaak geworden. Security vereist nu ervaren, betrouwbare en loyale partners. CRYPSYS is toonaangevend op het gebied van security analyse, advies en installatie bij overheden, semi-overheden, gemeenten, grote bedrijven en organisaties.

CRYPSYS
secure computing

CRYPSYS Data Security BV Edisonweg 4 4207 HG Gorinchem **tel** +31 (0)183 62 44 44 **fax** +31 (0)183 62 28 48 **mail** sales@crypsys.nl **web** www.crypsys.nl

CRYPSYS is officieel distributeur van: Sophos. Lumension. Norman. Cryptzone. Cryptshare. Adyton. Tenable. Kanguru