04/2012

INFORMATIE BEVEILIGING

PvIB Platform voor InformatieBeveiliging

Huisorgaan van het Platform voor InformatieBeveiliging

Nummer 4 - 2012

ONBEWUST ONVEILIG

LEAN BUSINESS CONTINUITY MANAGEMENT BIJ VGZ

BCM MET EEN FOCUS OP BEDRIJFSPROCESSEN

DE ERFENIS VAN HET DIGINOTAR DRAMA

BEKENDMAKING ARTIKEL VAN HET JAAR 2011

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.

VOORWOORD

Disclosure.
We hebben de afgelopen tijd in het nieuws een aantal publieke meldingen gehad van vervelende tot erge kwetsbaarheden in systemen gekoppeld aan het internet. Nieuwsprogramma's publiceren dit kennelijk graag en ontdekkers van kwetsbaarheden vinden de weg naar de nieuwsleveranciers ook eenvoudig.
Zo'n publieke melding heeft gevolgen voor de eigenaar en beheerders van de systemen in kwestie. Een kwetsbaarheid moet onderzocht worden en opgelost worden, zo snel mogelijk - en dat terwijl het systeem (zo mogelijk) ook stabiel moet blijven werken. Een prachtrecept om fouten en ongelukkige keuzes te maken. En dan rol je van het ene probleem in het andere.
Directe publieke meldingen zijn bij deze partijen niet populair. Het liefste krijgen zij de kwetsbaarheden gemeld en wordt er nooit iets in de publiciteit gebracht. Ze stoppen het dus graag in de spreekwoordelijke doofpot, los van het feit of ze het probleem oplossen en in welk tempo.
Dus voor de ontdekker is het tijdstip van publieke melding zijn machtsmiddel tegen dit 'in de doofpot stoppen'.
En hier kunnen we de helden onderscheiden van het gewone volk en de boeven. Hoe ga je met dat machtsmiddel om? Een held zal uit altruïstisch gevoel de kwetsbaarheid eerder melden aan de systeemeigenaar en die dan een redelijke tijd geven voor hij de kwetsbaarheid publiek maakt. Responsible disclosure.
De boeven bewandelen een heel ander pad: zij zullen alles geheim willen houden en indien mogelijk misbruiken - of het hier nu om financiële uitbuiting gaat of het uitvoeren van geruchtmakende activiteiten. Hun machtsmiddel is om de kwetsbaarheid een "zero-day" te laten zijn die zij kunnen exploiteren.
En dan komen we bij de overgebleven groep ontdekkers, die geen held zijn en ook geen boef, maar zich wel kunnen laten verleiden tot actie - zij het dan meer vanuit een persoonlijk gevoel van gewin. In responsible disclosure profiteert de systeemeigenaar vooraf, maar zit het gewin voor de ontdekker pas wanneer de publieke melding gedaan wordt - dan kan hij de roem opeisen voor zijn ontdekking. En omdat de kwetsbaarheid opgelost is, is eigenlijk de angel er al uitgetrokken: alle spanning rondom de afwikkeling van de oplossing is dan al voorbij.
En hier zie ik een interessante ontwikkeling opkomen: De definitie van responsible disclosure lijkt wel aangepast te worden. Wat eerst een protocol van gunning omschreef voor de systeemeigenaren, wordt nu uitgebreid met verwachting van publieke erkenning voor de ontdekking bij de oplossing, of zelf de verwachting een geldelijke beloning voor de ontdekker. Ik begrijp dat dit komt doordat bedrijven als Google en Facebook - als eigenaar van vele publieke systemen ook de veelvuldige ontvanger van kwetsbaarheden in die systemen - specifieke beloningsprogramma's instellen.
Maar is het nu zo dat, omdat er partijen zijn die zo'n programma hebben, iedereen met een publiek systeem nu een beloningsprogramma behoort te hebben? En dat bij gebrek aan zo'n programma bij een partij kwetsbaarheden niet meer voorgemeld gaan worden? Wellicht wel nuttig, maar het is nog geen uitgemaakte zaak, ik verwacht hier nog wel wat maatschappelijke discussie over. Eén ding is zeker voor mij: dit gaat niet meer over het originele begrip responsible disclosure - de heldendaad, dit gaat over de business ervan - de persoonlijke beloning.

INHOUDSOPGAVE

ONBEWUST ONVEILIG

Eric Luiijf is principal consultant bescherming vitale infrastructuur bij TNO en is als expert beveiliging procescontrolesystemen en Smart Grids verbonden aan het Nederlandse Centre for Protection of National Infrastructure (CPNI.NL). Eric is bereikbaar via eric.luiijf@tno.nl en eric.luiijf@cpni.nl

Uw organisatie of bedrijf heeft een risicoanalyse van de eigen ICT-faciliteiten en -diensten uitgevoerd, informatiebeveiligingsmaatregelen getroffen en houdt nieuwe dreigingen in de gaten. U denkt het ICT-risico volledig te beheersen. De kans is dan groot dat uw organisatie of bedrijf, net zoals zo vele andere organisaties en bedrijven, onbewust onveilig is. Dit artikel gaat in op enkele recente incidenten en de onderliggende oorzaken. Een gedegen oplossing vereist de samenwerking van de hele keten van aanbieders, opdrachtgevers, inkopers en opleidingen.

U bent verantwoordelijk voor de informatiebeveiliging in organisatie of bedrijf. Na een risicoanalyse, het treffen van maatregelen en het continu in de gaten houden van nieuwe dreigingen bent u in een beheerste fase terecht gekomen. Bent u niet iets vergeten?
U bent facilitair manager of hoofd technische dienst. Om de haverklap moest u vroeger 's nachts de regenjas over de pyjama aan trekken om te reageren op een storingsmelding via de semafoon. Tegenwoordig hoeft u alleen de tablet aan te zetten en het reservecircuit in te schakelen.
U bent onderhoudsmonteur van een bedrijf in luchtbehandelingen of gebouwbeheersing. Vroeger reed u heel Nederland en Vlaanderen af om diep de kelders in te duiken van organisaties en bedrijven. Nu, telewerkend, controleren u en uw collega's de werking van de systemen. Volgens afspraak is het wachtwoord NL_organisatie resp. BE_organisatie. De klanten zijn blij, de onderhoudskosten zijn door onderhoud op afstand met 30% gedaald.

Monitoring en besturing van steeds meer technische apparatuur, zowel lokaal als op afstand, gaat met computers, de zogenaamde procescontrolesystemen. Iedereen denkt dan aan de besturingssystemen van onze vitale sectoren zoals onze energie- en drinkwatervoorzieningen, wissels en seinen van trein en metro, raffinaderijen, containeroverslag, bagagebanden en afvulinstallaties van zuivelproducten. Dergelijke procescontrolesystemen in vitale infrastructuren en andere sectoren in binnen- en buitenland zijn in de afgelopen jaren ten prooi gevallen aan hackers en malware (virussen, wormen en Trojans). Incidenten die in de media terecht zijn gekomen omvatten nucleaire centrales, elektriciteitsnetwerken, gas- en oliewinning, trein- en tramwissels, chemische fabrieken en havensystemen. De publiek gemaakte incidenten vormen slechts een klein topje van de ijsberg.

Minder gauw wordt gedacht aan besturingssystemen van riolering, straatverlichting, pomp-, sluis- en brugbedieningen, gebouwbeheersing, luchtbehandeling, liften en toegangsbeveiligingssystemen. Geheel buiten de ICT-afdeling om, wordt de bediening van deze apparatuur door een installatiebedrijf gekoppeld met publieke netwerken zoals het internet. Dat geeft de mogelijkheid van bediening op afstand en/of "onderhoud of afstand". Onderhoudskosten worden zo aanzienlijk gedrukt en het aantal manuren om monteurs te begeleiden is ook lager. Bij oplevering of derde partij onderhoud worden eenvoudige wachtwoorden gebruikt.

> De bediening van deze apparatuur wordt door een installatiebedrijf gekoppeld met het internet

Niemand in de hele keten van fabrikant tot eindgebruiker maakt zich druk om beveiliging: de hele keten is onbewust onveilig.

Recente incidenten laten zien dat systeemeigenaren als gemeenten, organisaties en bedrijven geen flauw benul hebben van het risico. De verantwoordelijkheid hiervoor ligt op papier bij de systeemeigenaar. Echter inkopers, fabrikanten, systeemleveranciers, systeemintegrators, installatie- en onderhoudsbedrijven en opleidingen treffen ook blaam dat de informatiebeveiliging onvoldoende geborgd is. Wat incidenten steeds zichtbaarder maken is dat, bij gebrek aan kennis en beveiligingsbewustzijn, de bediening van vitale fysieke processen zonder na te denken over enige vorm van informatiebeveiliging gekoppeld wordt met publieke telecommunicatienetwerken zoals mobiele netwerken of het internet. Het grootste probleem ligt bij de verantwoordelijken voor het proces die denken aan de meest efficiënte en gebruiksvriendelijke besturing van de processen als airconditioning, riolering, straatverlichting zonder zich ook maar een moment af te vragen of het wel veilig is. Dit artikel legt uit wat er in Nederland al aan de beveiliging van procescontrolesystemen gebeurt.

Daarna wordt aangegeven waar de kern van het probleem zit en hoe dit aangepakt kan worden.

Incidenten

Op 14 februari jongstleden liet het TV-programma Een Vandaag zien dat de verwarming in een pand van het Leger des Heils vanaf het internet was te regelen [1]. De toegang was simpel. Er was geen wachtwoord nodig. Ook technische systemen van gemeenten zijn gekoppeld aan het Internet. Systemen van de Gemeente Veere bleken voorzien te zijn van het wachtwoord Veere. Dat kwam prominent in beeld omdat het twee weken en een aantal telefoontjes duurde voordat de installateur/externe onderhoudspartij aangaf actie te gaan nemen. De burgemeester vertelde dat de gemeente uiteindelijk "de stekker uit het systeem getrokken had". Niet direct in beeld waren de bediensystemen bij een aantal andere gemeenten die met eenzelfde 'gemeentewachtwoord' bloot aan het internet aangetroffen zijn. Ook de pompen van een zwemparadijs waren via het internet te manipuleren [9].

Nederlandse aanpak

Dat informatiebeveiligingsproblemen met procescontrolesystemen zich in steeds sterkere mate voor zullen doen, is iets waar deskundigen al tien jaar voor waarschuwen. Begin 2006 schreven TNO/KEMA een rapport voor de overheid over de organisatorische en technische aspecten van de onveiligheid van SCADA-systemen [2]. Sindsdien wordt er hard gewerkt aan het nog strakker op orde brengen van de beveiliging van de procescontrolesystemen in onze vitale sectoren. Dit binnen het thematische kader van het Informatieknooppunt Cybercrime van het Nederlandse Centre for Protection of the National Infrastructure (CPNI.NL). Een voorbeeld hiervan is de start van het programma 'Nationale Roadmap voor veilige procescontrolesystemen', waaronder diverse activiteiten zijn en worden ontplooid.

De verwarming in een pand van het Leger des Heils was te regelen vanaf het internet

Naast benchmarks in de drinkwater- en energiesectoren zijn SCADA Good Practices [3] en een bewustwordingsboekje [4] ontwikkeld. Drie groepen van ieder zo'n veertig medewerkers van Nederlandse vitale infrastructuur- en andere bedrijven ondergingen een red-blue team training in de VS. Ze leerden daar over het inbreken en verdedigen van processystemen. Ze keerden steeds vol overtuigd terug over de kwetsbaarheid van de systemen en de noodzaak om de beveiliging goed in de greep te houden. Verder werken multinationals en leveranciers voor high-end procescontrolesystemen samen aan de ontwikkeling van standaarden voor inkoop, certificatie en installatie van veiliger procescontrolesystemen [5]. Voor andere activiteiten op dit gebied, zie [6]. In de wereld loopt Nederland hiermee voorop. Waarom gaat het dan toch fout bij de niet als vitaal aangemerkte bedrijven en lagere overheden?

Andere werelden

Het bewustzijn over de ICT-kwetsbaarheid en cybercriminaliteit is inmiddels stevig doorgedrongen tot de ICT-afdelingen van bedrijven, organisaties en overheden. De ICT-dienstverlening en de interne informatiesystemen worden om die reden beveiligd en op aangeven van de leveranciers worden systemen, netwerkcomponenten en firewalls gepatcht. De ICT-afdeling is daar dagelijks mee bezig, al gaat het daar ook wel eens mis.

Vitale infrastructuurbedrijven en overheidsorganisaties worden door het Nationale Cyber Security Centrum (NCSC) op de hoogte gehouden van nieuwe kwetsbaarheden en oplossingen. Dat werkt prima voor de 'kantoor-ICT' en internetuitingen. Probleem is dat de meeste ICT-afdelingen geen enkele affiniteit hebben met kleppen, motoren, pompen en 24/7 operaties. Dergelijke technische systemen vallen onder de facilitaire dienst of de vaak diep in de kelder weggestopte technische dienst. ICT heeft dan ook geen zicht op welke technische systemen met ingebouwde ICT geïnstalleerd zijn. Ze zijn ook niet betrokken bij het opstellen van informatiebeveiligingseisen, de verwerving, de installatie, het gebruik en het onderhoud.

De wereld van hoofden gemeentewerken, facilitair managers en hoofden technische afdelingen heeft andere zaken dan informatiebeveiliging aan het hoofd. Zij zijn verantwoordelijk voor de aanschaf, installatie, werking en het

onderhoud van technische systemen. Denk bijvoorbeeld aan systemen voor beheersing van luchtvochtigheid, overdruk en temperatuur in ziekenhuizen en bedrijven (gebouwbeheersing), sturing van liften, beveiligingssystemen als slagbomen, deurtoegangen en camerabesturingen, in- en uitschakelen van de openbare verlichting, riolerings- en afvalwatersystemen, brug- en sluisbediening op afstand, polderpompen en -schuiven. Het belangrijkste voor hen is dat deze systemen ongestoord werken. Nog niet zo lang geleden waren deze systemen en de processen die ze bedienen zeer specifiek ontworpen en maakten gebruik van specialistische techniek. Een ware revolutie is gaande. De procesbesturing draait steeds vaker op 'gewone' ICT. Met een gebruiksvriendelijke bedieninterface in de vorm van een webtoepassing (of zelfs al een app) monitort en bedient men op afstand de werking van brug, riolering, airconditioning, enz.. Weinig tijd is meer nodig voor opleiding en dagelijks beheer. Dat hierbij essentiële fysieke processen gekoppeld zijn aan GSM, telefoonnetwerk of het internet zonder na te denken over enige vorm van informatiebeveiliging komt niet in de gedachten op. De reclame van Essent, waarbij de verwarming op afstand hoger gezet wordt, zorgt voor de perceptie dat bediening op afstand doodgewoon en inherent veilig is. De begrippen veilig en beveiligd worden hierdoor niet versterkt bij systeemeigenaren.

Het onderwerp informatiebeveiliging staat bij de meeste fabrikanten, leveranciers en systeemintegrators niet op de voorgrond. Procescontroleapparatuur zoals getoond in de uitzending van Een Vandaag wordt geleverd met een korte installatiehandleiding van enkele pagina's en een CD met uitgebreide documentatie. De korte installatiehandleiding vertelt niets over het aanbrengen van een wachtwoord en hoe sterk dat moet zijn, wel hoe je het systeem koppelt met een LAN en de 220V. Bladzijde 52 van de uitgebreide handleiding beschrijft in drie regels hoe je een wachtwoord instelt en dat kunt verwijderen (!). Een aantal pagina's later staat waar je het wachtwoord moet intypen als je een slotje ziet. Niet vreemd dat systeemintegrators en installatiebedrijven geen of slechts een simpel wachtwoord aanbrengen dat iedere onverlaat kan raden.

Het onderwerp informatiebeveiliging wordt ook niet naar voren gebracht door inkoopafdelingen en bij openbare aanbestedingen. De technische afdeling richt haar focus op de pompen, motoren, sensoren, kleppen en schuiven: de functie, niet op informatiebeveiliging. Er worden zelden informatiebeveiligingseisen gesteld. Informatiebeveiliging hoort bij Internetbankieren, niet bij de bediening van de riolering vanuit thuis uit. "Iedereen vindt rioolwater vies, dus is er geen enkele hacker geïnteresseerd." En als er eisen gesteld worden, worden ze vaak als eerste geschrapt als dat extra kosten met zich meebrengt. Bij de aanschaf van de systemen geldt namelijk zo min mogelijk franje en zo efficiënt mogelijk, iets dat zich vaak vertaalt in 'de goedkoopste aanbieder'. Met het aanbieden van (extra) informatiebeveiliging ben je als aanbieder duurder en val je af.

> De meeste ICT-afdelingen hebben geen enkele affiniteit met kleppen, motoren, pompen en 24/7 operaties

Tenslotte de bedrijven die onderhoud op afstand uitvoeren, iets dat steeds vaker gebeurt omdat de eigen technische afdelingen steeds vaker tot een minimum teruggebracht zijn. De kosten voor een extra internetaansluiting of GSM-abonnement zijn nihil op de kosten van het totale onderhoud.

Afbreukrisico

Recent sprak ik een directeur van een installatiebureau. Die had geen informatiebeveiligingsprobleem meer: de gehele administratie was in handen van een extern bedrijf. Toen ik vernam dat zijn personeel onderhoud op afstand pleegt aan airconditioning-, luchtbehandeling-, en andere technische systemen bij ziekenhuizen en grote bedrijven, vroeg ik hem hoe hij de beveiliging van informatie over deze achterdeuren bij derden borgde en hoe veilig de wachtwoorden waren. Hij werd bleek toen hij zich het afbreukrisico realiseerde.

De aansluiting gaat om de beveiligingsmaatregelen van de ICT-afdeling heen. En om snel ondersteuning te bieden worden simpele onderhoudswachtwoorden ingesteld met daarin de klantnaam, eventueel voorafgegaan met NL_ als het een internationaal opererend onderhoudsbedrijf betreft.

Verantwoordelijkheid?

Minister Opstelten legde in de Kamercommissie Veiligheid en Justitie de verantwoordelijkheid voor de incidenten neer bij de systeemeigenaren. In principe heeft hij gelijk. Anderzijds zijn de incidenten nauwelijks te verwijten aan de systeemeigenaren. Niemand heeft ze over het risico verteld; ze leven in een andere wereld! De proceseigenaren zijn daardoor onbewust onveilig.

> Om snel ondersteuning te bieden worden simpele onderhoudswachtwoorden ingesteld met daarin de klantnaam

Actie gevraagd

Aanpak van deze problematiek vergt een krachtdadige samenwerking van alle betrokkenen. Dit werkt alleen als er een breed bewustzijn van de problematiek is en een sterk gevoel van urgentie ontstaat. Dit betekent dat

Een waterschap, 2003
'Als hele volksstammen hun financiën via internet regelen, dan moet je op die manier een waterzuivering kunnen aansturen'

systeemeigenaren verantwoordelijk zijn en eigenaarschap tonen. Ze moeten op basis van een gedegen risicoanalyse gepaste maatregelen treffen om hun kritieke processen te beschermen. Daarvoor moeten ze wel beschikken over kennis over het beveiligingsprobleem en over handelingsinformatie. Ze moeten heel hard nadenken over of het echt noodzakelijk is dat bediensystemen aan openbare telecommunicatienetwerken gekoppeld worden. Leveranciers, systeemintegratoren en installateurs hebben hier een 'zendelingsfunctie'. Het boekje [4] (een nieuwe editie is gepland), CPNI.NL activiteiten [6] en de NCSC factsheet [7] vormen een eerste hulp. Voorbeelden van maatregelen zijn het trainen en opleiden van het personeel dat de kritieke systemen beheert als ook het voeren van een verantwoord wachtwoordbeleid. Eisenpakketten bij de verwerving/openbare aanbesteding van technische systemen en onderhoudscontracten waar enige vorm van ICT, zoals procescontrole, deel van uit maakt, dienen altijd een hoofdstuk informatiebeveiliging te bevatten. Inkoopafdelingen dienen in te grijpen in het verwervingsproces als blijkt dat informatiebeveiliging onvoldoende aandacht krijgt. Een good practice handleiding daarvoor zou in publiek-private samenwerking ontwikkeld kunnen worden. De basis hiervoor is al gelegd in het eerder genoemde document dat door de WIB [6] is opgesteld en dat op dit moment tot een officiële IEC standaard wordt ontwikkeld. Certificering van de leverancier is onderdeel van dit proces. De overheid kan afdwingen dat, net als grote bedrijven als Shell dit doen, de leveranciers van systemen die kritieke functies in de samenleving aansturen verplicht gecertificeerd worden tegen deze IEC 62443-2-4 standaard [8]. Fabrikanten van procescontrolesystemen moeten – liefst Europees – gedwongen worden om het onderwerp informatiebeveiliging prominent en uitgebreid in hun handleidingen te behandelen.
Installatiebedrijven, systeemintegrators, installatie- en onderhoudsbedrijven moeten aansprakelijk zijn voor onveilig opgeleverde (toegang tot) procescontrolesystemen. Bij oplevering en onderhoud moeten zij daarom de systeemeigenaren onderwijzen in veilig gebruik voordat zij ontslagen zijn van de aansprakelijk.
Opleidingen facilitair management en opleidingen gerelateerd aan procescontrole bediende systemen moeten aandacht besteden aan informatiebeveiliging van technische systemen.

> De samenleving zal nog een reeks aan informatiebeveiligingsincidenten met procesbesturingen beleven

Als u als ICT-er al met de beveiliging van deze systemen bezig bent, vergeet dan ook niet de beveiliging van de telefooncentrale, de ICT-systemen in de bedrijfsauto's, draadloze medische apparatuur, enzovoorts.

Conclusie
Vooralsnog moeten we echter bang zijn dat de samenleving nog een reeks aan informatiebeveiligingsincidenten met procesbesturingen, mogelijk zelfs met ernstig gevolg voor gezondheid en goederen, zal beleven. Procesbesturingen bij lagere overheden en veel bedrijven zijn nu onveilig gekoppeld met publieke communicatievoorzieningen. Eigenaren zijn zich onvoldoende bewust van de onveiligheid. Actie is nodig. Laten we snel van onbewust onveilig gaan naar de status van bewust veilig of misschien nog beter naar onbewust veilig.

Referenties

[1] *EenVandaag 14-02-2012, Sluizen, gemalen en bruggen slecht beveiligd: kinderlijk eenvoudig van thuis uit te bedienen, on-line: http://www.eenvandaag.nl/binnenland/39770/sluizen_gemalen_en_bruggen_slecht_beveiligd*

[2] *Ir. H.A.M. Luijif en Ir. R. Lassche, SCADA (on)veiligheid: een rol voor de overheid?, TNO-KEMA rapport, april 2006.*

[3] *H.A.M. Luijif, SCADA Good Practices for the Dutch Drinking Water sector, TNO DV 2008 C096, maart 2008, on-line: https://www.cpni.nl/publicaties/scada-security-good-practices-for-the-drinking-water-sector.*

[4] *Luijif, H.A.M., "Process Control Security in het Informatieknooppunt Cybercrime", NICC, december 2009, on-line: http://www.cpni.nl/publications/PCS_brochure-NL.pdf*

[5] *WIB "Process Control Domain-Security Requirements for Vendors": www.wib.nl*

[6] *Activiteiten en publicaties rondom de beveiliging van procescontrolesystemen: volg www.cpni.nl*

[7] *Factsheet SCADA-systemen, NCSC, on-line: https://www.ncsc.nl/binaries/nl/dienstverlening/expertise-advies/kennisdeling/factsheets/beveiligingsrisicos/1/Beveiligingsrisicos%2Bvan%2Bonline%2BSCADA%2Bsystemen.pdf*

[8] *IEC 62443-2-4: Security for industrial process measurement and control - Network and system security - Part 2-4: Certification of IACS supplier security policies and Practices.*

[9] *http://webwereld.nl/nieuws/109573/attracties-van-zwembad-door-hackers-te-beheren.html*

SECURITY AWARENESS

We vragen auteurs in de LinkedIn-groep voor IB-auteurs om een korte reactie. Zes auteurs reageren op de volgende vragen:

Security Aware zijn houdt in dat je begrijpt dat er een mogelijkheid is dat sommige mensen met opzet of per ongeluk gegevens stelen, schade veroorzaken of misbruik maken van de gegevens die zijn opgeslagen, of terwijl ze verwerkt of verzonden worden en dat het verstandig is om te proberen dat niet te laten gebeuren.

Hoe meer mensen om ons heen security aware zijn, hoe beter dat is voor de omgeving waarin we zitten. Dit gaat op voor onze woon- en werkomgeving, en ook voor onze cyberactiviteiten. Het vergt dat we op de hoogte zijn van de manieren waarop schade veroorzaakt wordt en dit vroegtijdig kunnen herkennen.

Als dit zo'n alom aanwezige noodzaak is, wiens taak is het om te zorgen dat we collectief security aware zijn?

De besloten LinkedIn groep voor IB Auteurs is te vinden via http://www.linkedin.com/groups?gid=4188826.
Wij heten aspirerende auteurs graag welkom.

Rashid Niamat

Op het gevaar af een open deur in te trappen en daarmee een beginnende uitwisseling van ideeën te frustreren... Ik pleit ervoor dat het begrip "security aware(-ness)" standaard wordt opgenomen in elk handboek arbeidsvoorwaarden. Daarmee worden tenminste twee zaken duidelijk:

- de werkgever erkent het belang van "security awareness"
- de werknemer ziet dat de werkgever hier serieus mee omgaat

Dat gezegd hebbende: dit moet dan uiteraard ook vertaald worden voor de situaties waar externen de rol van werknemers vervullen.
Ik wijs dus naar de HR / P&O functionarissen - en hoe zij aan de benodigde kennis komen, dat is bijna een special op zich waard.

Wouter Zwiers

Ik mis een beetje de voorbeeldfunctie van het management in organisaties of de overheid in het dagelijkse leven in bovenstaande opmerkingen. Te vaak worden audits uitgevoerd waarna de directeur toch maar besluit om net die onveilige (maar wel coole natuurlijk) laptop in het netwerk te hangen. Of hoger overheidspersoneel gaat weer ergens de fout in. Anders gezegd: het is ook een kwestie van voorbeeldgedrag vanaf boven (zonder het hier al teveel te simplificeren..;)) Die laatste Postbus 51-spot met al die vissers op de daken is in die zin een goed begin.

Ed Bronner

Ja, voorbeeld en echt gevoeld handelen van het MT. Belang van organisatie (van oudsher organisatiedoel!) en medewerkers. Ergo primaire waardeketen en sturende en ondersteunende processen met hun "mapgood" (dank Ernst) benodigdheden, die het belang

conform regelgeving en beleid waarborgen. En wie weet zonder bonussen en hedgefunds sturen, kaderen van het gedrag...in werk en privé voor het gezamenlijk belang. Het MT is de reisleider op een gevaarlijke bergtocht. Ultieme sanctie is daar de dood...ietsje minder mag, maar iedereen moet dit belang helder hebben....en er naar handelen.

Thom Schiltmans

Security awareness is geen project, het is een mindset van boven naar onder en van onder naar boven, en vooral in de breedte. Op het moment dat iemand ingrijpt als een blinde man vlak voor een auto wil oversteken vinden we dat een heldendaad omdat die persoon dat doet zonder eigenbelang. Daarom is het des te vreemder dat mensen in een organisatie niet ingrijpen (hard of zacht) als zij risico's zien (voor die organisatie of voor een project etc.) die het voortbestaan in gevaar kunnen brengen van diezelfde organisatie of project, waar die individuele persoon zelf ook hinder van heeft. Het management heeft vaak het best overzicht en kan misschien beter beoordelen in welke mate het voortbestaan van de organisatie in gevaar is, maar ook de individuele medewerker levert een bijdrage aan het signaleren van risico's en het voorkomen van de gevolgen daarvan.
Security awareness is dus een continue bewustzijn bij mensen van potentiele risico's die de organisatie en zijn omgeving in gevaar kunnen brengen en daar proberen zo goed mogelijk naar te handelen. (fouten zijn menselijk).

John Grüter

Security awareness is in onze huidige maatschappij verschrikkelijk moeilijk, los van het feit of je dat betrekt op organisaties, de maatschappij of op personen. Tot 20 jaar geleden was de maatschappij en (bijna) alles wat er plaatsvond 'werkelijk' (of 'analoog'). Ik denk (ben bang) dat 80% van de inwoners van Nederland geen idee heeft op welke houtje-touwtje manier nu onze maatschappij aan elkaar hangt en wat de impact is van die digitale verknoping.
Omdat het fundament van onze maatschappij ondertussen digitaal is, is het voor 99.99+% van de mensen volstrekt onzichtbaar welke gegevens door wie, over wie, wanneer en waarom worden uitgewisseld! We hebben een traditie van honderden jaren, gebaseerd op 'zintuigelijk waarneembaar' vertrouwen in onze medemens, onze bestuurders, onze werkgevers, etc. Nu kunnen onschuldige handelingen door burgers, medewerkers of familieleden (of het laten daarvan) zeer grote gevolgen hebben, ook voor wat betreft security, omdat de gevolgen niet kort-cyclisch (zintuigelijk) waarneembaar zijn. Zittrain (http://futureoftheinternet.org/) laat zien dat Big Brother niet de overheid is, niet de Corporates, maar wijzelf. Foto, post op Facebook, gezichtsherkenning en zie: John is op maandag 9 april 2012 om 14:32 in Vijfhuizen geweest. Vanuit de ene context volstrekt onschuldig, vanuit een andere misschien wel uitermate gevaarlijk omdat we geen idee hebben hoe en waarmee dat 'feit' wordt gecombineerd, buiten onze waarneming.
Zo lang de informatiestromen zich onttrekken aan onze waarneming, en mensen (burgers, medewerkers, managers, politici) er niet van doordrongen zijn hoe zeer wij afhankelijk zijn van een evolutionair ontstaan netwerk van informatiesystemen en de fouten die daarin (kunnen) voorkomen, verwacht ik niet dat security awareness 'zomaar' toe zal nemen. Ik denk dus dat security awareness pas aan de beurt komt wanneer we bewust zijn van de (on)mogelijkheden en risico's van onze digitale

maatschappij. Dat neemt overigens niet weg dat we dan maar achterover moeten leunen, maar dat we heel duidelijk over security awareness moeten praten en daarnaar moeten handelen, maar zeker ook over de digitale maatschappij die de noodzaak van security awareness zoveel groter maakt.

Michiel Perdeck

Ik kan me volledig vinden in de observaties van John Grüter. Awareness is geen rationele maar een emotionele toestand. IT systemen hebben nog steeds (en misschien wel altijd en misschien is dat zo slecht nog niet) een grote afstand tot ons gevoel. Het vervelende is natuurlijk dat ze toch grote gevolgen kunnen hebben. Deze afstand tussen gevoel en gevolgen is typisch voor veel van de techniek en de organisaties in onze hoogontwikkelde samenleving. Noch de voordelen noch de nadelen van wat wij dagelijks doen in onze kantoren is erg duidelijk. Ja, we krijgen een salaris, zijn lekker bezig met interessante problemen maar wat die nou werkelijk bijdragen aan het geluk van de mensheid is tamelijk wazig.... ik dwaal af.... Hoewel, daar zit hem toch de kneep denk ik. Het is duidelijk dat je je lange haar in een knotje moet doen als je met een cirkelzaag werkt maar dat je je wachtwoorden regelmatig moet veranderen is veel minder logisch voor ons gevoel. En temeer, dat komt er nog bij, als we het gevoel hebben dat die techniek ons het leven vaak ook nog erg moeilijk maakt (30 wachtwoorden moeten onthouden…). Dus, Security Awareness ja maar bezie wel de problematische relatie tussen mens en techniek.

LEAN BUSINESS CONTINUITY MANAGEMENT BIJ VGZ

Thérèse van Vliet is Business Continuity Officer bij de Coöperatie VGZ. Hiervoor was zij werkzaam bij het UWV en is een aantal jaren beroepsmilitair geweest. Thérèse is fulltime werkzaam als Risk & Compliance officer en vervult daarmee de rol van BCO op parttime basis. Zij is te bereiken via t.vanvliet@vgz.nl

De Coöperatie VGZ heeft 4,2 miljoen verzekerden en een omzet van 10 miljard euro (2010) en is daarmee de tweede zorgverzekeraar van Nederland. Bij de Coöperatie VGZ werken ca. 3000 medewerkers, verdeelt over 5 vestigingen en 8 servicepunten. Deze geografische spreiding biedt kansen maar heeft ook zorgpunten vanuit het oogpunt van bedrijfscontinuïteit. Aan de ene kant beschikt de Coöperatie VGZ over voldoende locaties om medewerkers met een belangrijke functie (bijv. afhandelen van declaraties) een alternatieve werkplek aan te bieden. Aan de andere kant moet de Coöperatie VGZ er continue voor zorgen dat de verschillende locaties zijn aangesloten op het centrale netwerk en wat gebeurt er met de medewerkers waarvoor geen werkplek meer is?

De situatie

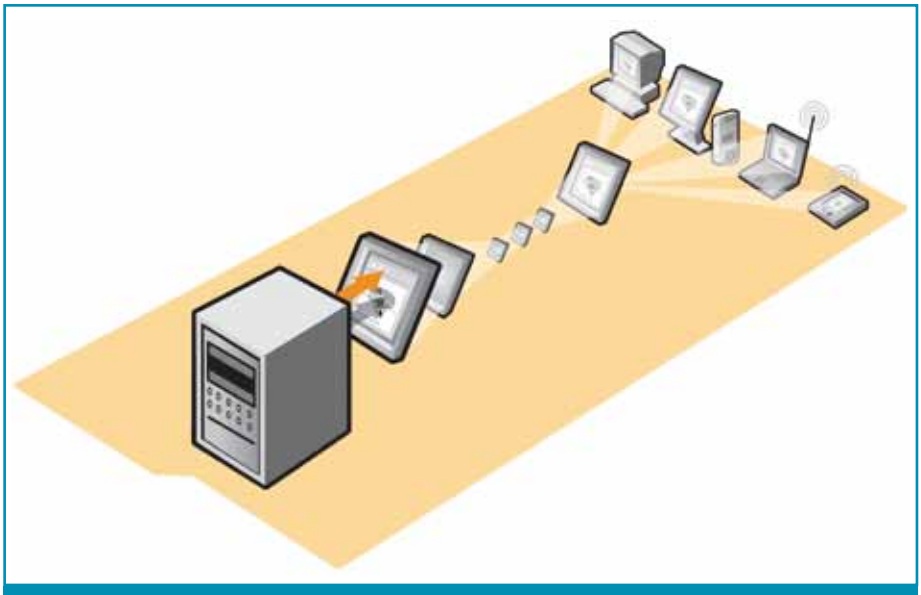
Een aantal jaren geleden constateerde de Coöperatie VGZ dat BCM nog niet optimaal was ingericht. Zowel vanuit de eigen bedrijfsvoering als in overleg met de toezichthouder was het belangrijk om BCM verder te verbeteren. Als zorgverzekeraar heeft de Coöperatie VGZ immers een belangrijke rol in het slimmer organiseren van de zorg in Nederland.

Voor goede zorg zorg je samen

Deze dienstverlening valt of staat bij een goed werkende IT-infrastructuur, maar ook dat er voldoende medewerkers hun werkzaamheden kunnen uitvoeren. Meestal wordt er bij bedrijfscontinuïteit alleen gedacht aan IT-uitwijk. Maar een crisis is meer dan alleen het falen van IT; zeker zo belangrijk zijn de gebouwen en de mensen van een organisatie. Denk aan een uitslaande brand of een ernstige griepepidemie waardoor een groot deel van de medewerkers thuis is (als zieke of als verzorgende). Deze oorzaken staan daarbij los van een functionerende IT-infrastructuur.

> Bij een crisis zijn de gebouwen en de mensen van een organisatie zeker zo belangrijk als IT

Met ingang van september 2009 is Het Nieuwe Werken gefaseerd uitgerold bij de Coöperatie VGZ. Dit stelt medewerkers in staat om tijd en plaats ongebonden te werken. Medewerkers kunnen hierdoor ook elders werken, zolang ze maar beschikken over een internetverbinding en een token om in te kunnen loggen. Hiermee stuit de Coöperatie VGZ bij een crisis direct op performanceproblematiek: kunnen de medewerkers die nu ergens anders moeten werken ook tegelijk inloggen op het netwerk? Het antwoord hierop is positief, mits het inloggen maar gecontroleerd gebeurd. Door het toewijzen van inlogperioden aan afdelingen wordt de server niet overbelast en kan men de belangrijkste activiteiten blijven uitvoeren.



Citrix Server-based Computing

En toen

Aanvankelijk is VGZ in projectvorm van start gegaan volgens de traditioneel beproefde methode conform de Britse standaard BS 25999. Een methode die voorziet in het opstellen van impactanalyses, dreigingsanalyses en risicoanalyses, omgeven met een scala aan plannen en uitgevoerd door een BCM-organisatie. Deze organisatie zou – in onze situatie – een omvang hebben

Lange termijn visie nodig

van minste 30 voltijdse medewerkers. Na het eerste jaar had het project wel veel informatie verzameld op het gebied van min of meer kritieke applicaties, maar een goed doordachte BCM strategie om tijdens een calamiteit te kunnen overleven ontbrak nog steeds. Dit werd ondermeer veroorzaakt doordat er veel aandacht was voor de continuïteit van de IT-infrastructuur maar niet voor de continuïteit van de uitvoering zelf, inclusief de medewerkers en gebouwen.

In het najaar van 2009 heeft de Coöperatie VGZ daarom een opdracht voor het opzetten van BCM neergelegd bij VKA in Zoetermeer.
Bij VKA was een nieuwe opzet van BCM (lean BCM) ontwikkeld die nadrukkelijk aansluiting zoekt bij de bestaande activiteiten en de directie en managers de ruimte geeft om zelf met werkbare oplossingen te komen.
De basis van deze aanpak is vrij eenvoudig en bestaat uit 3 pijlers: uitgaan van de flexibiliteit en improvisatievermogen van de directie en de vakkennis van de medewerkers. En niet meer plannen schrijven dan nodig.
Een crisis laat zich niet dwingen in een van te voren beschreven scenario. Het gaat immers in de praktijk altijd net even anders dan verwacht.

Deze aanpak is succesvol gebleken bij de Coöperatie VGZ. Door uit te gaan van de competenties van onze medewerkers lijkt het inderdaad niet nodig om de plannen in detail uit te werken. Men heeft vooral stil gestaan bij de uitwijkmogelijkheden en het prioriteren van de belangrijkste activiteiten (impliciete business impact analyse).

Het resultaat
Binnen een half jaar na de start van lean BCM was er voor de Coöperatie VGZ een Strategie en Beleidsdocument opgesteld. In dit document is vastgelegd wat de prioriteiten zijn voor ons bedrijf, hoe de taken en bevoegdheden zijn ingericht en welk (communicatie) protocol er gevolgd moet worden.
In de maanden daarop volgend is er aan elk bedrijfsonderdeel een workshop gegeven waarin de strategie en beleid en de principes van lean BCM is toegelicht. Vervolgens zijn er per locatie en per bedrijfsonderdeel continuïteitsplannen gemaakt en is er een crisis communicatieplan opgesteld.

Als zorgverzekeraar is de Coöperatie VGZ grotendeels afhankelijk van een goedwerkende IT-infrastructuur. Het is daarom dat de IT-afdeling een eigen crisismanagementplan heeft. Dit plan bevat de procedures die uitgevoerd moeten worden bij uitval van één of meer applicaties. Afhankelijk van de prioriteit van een applicatie wordt een specifiek protocol (uitwijk) uitgevoerd, waardoor er voldaan kan worden aan de afgesproken hersteltermijn.

Na iets meer dan een jaar was BCM ingericht en geïmplementeerd bij de Coöperatie VGZ en werden de plannen getest. Vanaf 2011 worden alle plannen ten minste één keer per jaar getest, zowel per locatie als per bedrijfsonderdeel. Eventueel in combinatie met een ontruimingsoefening met de BHV.
Het meeste succes heeft de Business Continuity Officer (BCO) met het type oefening waarbij de directeur wordt "ontvoerd" naar een locatie buiten het kantoor en geconfronteerd wordt met een indrukwekkende crisis. De oefening begint dan met de vraag: "wat ga je nu doen?"

Door jaarlijks scenario's te oefenen blijft de directie en management bewust van het nut en de noodzaak om de plannen actueel te houden. Tijdens die oefeningen blijkt immers onmiddellijk wat er niet klopt aan het plan. Aan het eind van iedere oefening wordt directie en management gevraagd of ze vertrouwen hebben in de noodoplossingen.

> Na iedere oefening geeft management aan of ze vertrouwen hebben in de noodoplossingen

Daarnaast wordt "spelenderwijs" het protocol bij de Coöperatie VGZ doorgenomen: wanneer bel ik nu met onze communicatieafdeling en wie bepaalt ook al weer of de coördinatie bij een crisis overgenomen gaat worden door de Raad van Bestuur.

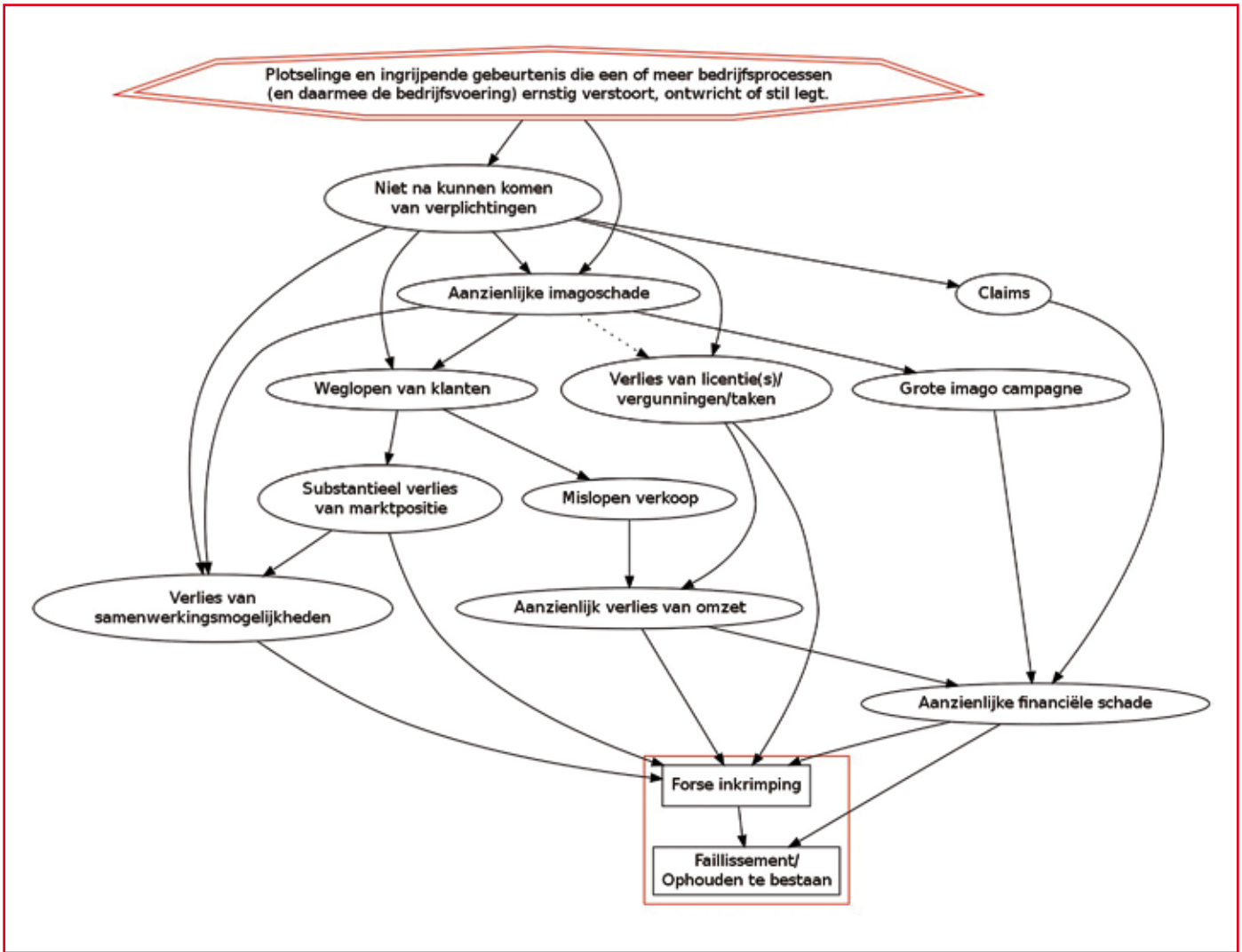
Tot slot
Voor onze organisatie is lean BCM succesvol gebleken. Door de bestaande competenties van de directieleden en managers aan te spreken, hebben zij wezenlijk invloed in het snel in de hand krijgen van een chaotische situatie, waardoor onze core business voortgezet kan worden. En ze vinden de oefeningen leuk.
Als BCO van de Coöperatie VGZ is het dan ook een plezier om op deze manier (samen) te werken en vertrouw ik op een goede afloop mocht er in de toekomst zich toch iets voordoen.

BCM MET EEN FOCUS OP BEDRIJFSPROCESSEN

Rein de Vries is directeur en mede-eigenaar van LBVD Consultancy en adviseert opdrachtgevers met betrekking tot de onderwerpen bedrijfscontinuïteit en informatiebeveiliging. Zijn focus ligt daarbij met name op statusonderzoek en het komen tot een praktische maar toch doeltreffende invulling.
Rein is te bereiken via rein.de.vries@lbvd.nl.

Informatiesystemen nemen een belangrijke plaats in binnen bedrijfsprocessen: zonder informatiesystemen staat tegenwoordig immers bijna alles stil. De vraag is nu: in hoeverre begin je iets in het geval van een calamiteit? Hoe erg is dat? Wat doe je er aan? Hoe voorkom je dat processen grotendeels of geheel stilvallen? Hoe houd je de ellende zo beperkt mogelijk als, ondanks alle preventieve maatregelen, toch een calamiteit plaatsvindt? Bedrijfscontinuïteitsmanagement (BCM) moet hier een adequaat antwoord op formuleren.

Waarom ook al weer?
Behoud van positie en groei staan bij veel organisaties hoog in het vaandel. De ultieme gebeurtenis die BCM tracht te voorkomen is het tegenovergestelde: een forse inkrimping van de organisatie of faillissement. Deze zijn vrijwel altijd terug te voeren op een plotselinge en ingrijpende gebeurtenis die een of meer bedrijfsprocessen ernstig verstoort of zelfs geheel stil legt (zie Figuur 1). BCM moet zich op de eerste plaats richten op het voorkomen en bestrijden van ernstige ontwrichting van bedrijfsprocessen. Indirect zal BCM zich richten op de onderliggende oorzaken en daarmee op de kritischer bedrijfsmiddelen.



Figuur 1: Causaliteit Calamiteit - Verstoring van continuïteit

Robuustheid van processen

Bedrijfsprocessen zijn afhankelijk van bedrijfsmiddelen zoals gebouwen, machines, informatiesystemen, medewerkers, et cetera. Als middelen niet in de vereiste mate voorhanden zijn stokt het proces. Voorts bepaalt hoe het proces specifiek is ingericht hoe kritisch middelen zijn. Je kunt daarbij spreken van de robuustheid van het proces: naarmate een proces robuuster is, is het beter bestand tegen uitval van specifieke middelen en zijn de middelen zelf minder kritisch.

Neem bijvoorbeeld logistieke processen. In dit soort processen is het aanhouden van voorraden en geografische verspreiding van voorraden een mogelijkheid. Indien het proces hierin voorziet kan de afhankelijkheid van productiesystemen en de logistiek kleiner zijn, al naar gelang de grootte van de voorraden. Maar ook: als in het logistieke proces bij langdurige stroomuitval duimendraaiende medewerkers het logistieke systeem vervangen, kan het proces mogelijk productief blijven zonder dat investeringen nodig zijn, zoals een mogelijk kostbare noodstroomvoorziening.

De kunst is om onder gegeven vaste omstandigheden - de kaders - een balans te vinden tussen de inrichting van het proces en middelen (beiden variabel), zodanig dat de continuïteit van productie en levering optimaal gewaarborgd is. Bij een dergelijk optimalisatievraagstuk speelt voortdurend de vraag: als bepaalde middelen haperen of uitvallen, is het dan toch niet mogelijk om het proces op alternatieve wijze voort te zetten?

De specifieke omstandigheden zijn hierbij bepalend voor het optimum. Het aanhouden van voorraden kan een kostbare aangelegenheid zijn. Het beleid zal zijn om een zo klein mogelijke voorraad aan te houden. "Just In Time" productie en uitlevering is het gevolg. Dit maakt zowel het productie- als uitleveringsproces kritischer, de afhankelijkheid van productie- en logistieke middelen kritischer en daarmee de beschikbaarheidseis hoger.

Rampzalig - Orkaanschade

Voorbeelden van andere omgevingsfactoren die een stempel op de inrichting van logistieke processen drukken zijn het concurrentieniveau, de verkoopbaarheid van goederen en de inschikkelijkheid van de markt. Als de concurrentie groot is, maakt kwaliteit, prijs en service het verschil, is logistiek een middel om te concurreren, zal de druk op het logistieke proces groot zijn en beschikbaarheidseisen hoog. Als het om waar gaat die kan bederven, is de druk op het logistieke proces groot om op het juiste tijdstip de juiste hoeveelheid op de juiste plaats te leveren en is tevens een hoge beschikbaarheidseis voor ondersteunende informatiesystemen van kracht. Als de afnemer in zekere mate afhankelijk is en het product toch wel koopt, is het logistieke proces wellicht minder kritisch en de claim die dit proces op middelen legt ook.

Scopebepaling

Welke processen vallen binnen de scope van BCM? Wat zijn de kritische stappen in deze processen? Het is zaak om bij het selecteren van te behandelen processen kritisch te zijn. In organisaties zijn vaak niet zo veel processen die echt kritisch zijn. Welke nadelige gevolgen wil je echt voor zijn of minimaliseren? Welke gebeurtenissen zijn echt een ramp? Maak onderscheid tussen omstandigheden die lastig of vervelend zijn en rampzalige of desastreuze gebeurtenissen.

Een selectierichtlijn kan zijn dat een verstoring zo min mogelijk moet resulteren in een verstoring van bedrijfsprocessen van de klant. Dit zou immers leiden tot ontevreden klanten en daarmee tot het weglopen van klanten en aanzienlijke omzetderving. Het bevoorraden van klanten kan bijvoorbeeld cruciaal zijn. In dat geval moet de aandacht vooral uitgaan naar het goed ingericht hebben van de logistieke processen.

Alternatieve middelen en werkwijzen

Na kritische processen te hebben geselecteerd volgt de vraag hoe je de kritische delen van deze processen - ondanks het uitvallen van informatiesystemen of andere middelen - voor kortere of langere duur voldoende productief kunt houden. Voor processen die verregaand geautomatiseerd zijn kan het zijn dat het opnieuw beschikbaar hebben van dezelfde als de normale informatiesystemen via uitwijk of herstel de enige mogelijkheid is om de kritieke delen gaande te houden. Deze conclusie moet je niet te snel trekken. Probeer eerst creatief te zijn.

Zo kon bijvoorbeeld tijdens de omvangrijke storing in het Vodafone-netwerk in april 2012 een taxibedrijf doordraaien door terug te schakelen naar het oude radiosysteem dat nog niet was ontmanteld. Als het e-mailsysteem het laat afweten kan een fax of telefoon uitkomst bieden. Mocht elektronisch betalen ergens in het proces een ernstig probleem kunnen vormen, zorg ervoor dat er op een alternatieve manier kan worden betaald, bijvoorbeeld via cash geld. Probeer al bij het ontwikkelen van informatiesystemen - indien mogelijk - de afhankelijkheid van techniek te beperken. Laat bijvoorbeeld bij een landelijk opererende winkelketen het kassasysteem niet geheel afhankelijk zijn van netwerkverbindingen, maar zorg er voor dat - indien nodig - kassa's of winkels lokaal kunnen doordraaien. Bij het creatief zijn kan het de moeite lonen om goed na te denken wat je kunt bereiken met pen, papier en mensen. Bijvoorbeeld, welke productiviteit is mogelijk als je zou beschikken over prints met gegevens? Het achter de hand hebben van actuele prints kan al een hoop mogelijk maken, waardoor de techniek 'dunner' uit te voeren is: geen dubbel maar enkel systeem. Wat ken je bereiken met de inzet van extra menskracht? Hebben we het over handwerk dat in vijf minuten uit te leggen is? Zo ja, dan kan het wegtrekken van medewerkers uit andere delen van de organisatie, een belronde onder medewerkers die normaal in shifts werken of een beroep doen op een uitzendbureau uitkomst bieden. Het is beter om medewerkers niet dubbel op te leiden. Bij het overschakelen naar alternatieve werkwijzen is het zaak om zo laat mogelijk over te schakelen. Het kan de moeite lonen om te proberen tijd te rekken om zo laat mogelijk over te gaan. Een relevante vraag is hoe lang de verstoorde situatie te tolereren is. Het antwoord kan afhankelijk zijn van de factor tijd, bijvoorbeeld het tijdstip op de dag. Het is een dooddoener, maar vergeet niet periodiek te oefenen bij het hebben van alternatieve procedures of een backupplan. Keer op keer blijkt dat onbekendheid leidt tot veel verlies van tijd. Creativiteit en out-of-the-box denken zijn vaak ook vanuit een andere optiek

Classificatie

De mate, waarin de waarborging van Beschikbaarheid, Integriteit en Exclusiviteit/Vertrouwelijkheid belangrijk is voor informatiesystemen en/of gegevensverzamelingen, is op de volgende wijze te duiden:

	Behoud van Beschikbaarheid (B): In hoeverre is verlies van beschikbaarheid desastreus? Ofwel: in hoeverre is beschikbaarheid belangrijk?	**Behoud van Integriteit (I):** In hoeverre is verlies van integriteit van informatie of het niet correct functioneren van het informatiesysteem desastreus? Omgekeerd: hoe belangrijk is (het waarborgen van) integriteit?	**Behoud van Exclusiviteit (E):** In hoeverre is het desastreus als je niet zelf exclusief over de informatie of het informatiesysteem beschikt? Ofwel: hoe belangrijk is behoud van exclusiviteit?
0. Beperkt belangrijk (prettig)	Uitval is (in enige mate) te dulden; het zorgt wel voor enige overlast en extra kosten.	Integriteit is niet van grote invloed; het niet geheel foutloos zijn c.q. functioneren zorgt voor enige overlast.	Onbevoegde toegang tot de informatie of het informatiesysteem is niet rampzalig. Openbaring heeft geen vervelende gevolgen.
1. Belangrijk (nodig)	Uitval van het systeem en/of het niet beschikbaar zijn van informatie zorgt voor aanzienlijk productieverlies, het in enige mate niet kunnen nakomen van verplichtingen, overlast en extra kosten.	Integriteit is belangrijk. Verlies van zorgt voor ongemak, extra kosten en het in enige mate niet kunnen nakomen van verplichtingen.	Onbevoegde toegang tot de informatie of het informatiesysteem is pijnlijk. Het bekend worden van gegevens, werkwijzen, et cetera heeft nadelige gevolgen.
2. Vitaal	Het systeem/de informatie is onmisbaar. Uitval resulteert in het grotendeels of geheel stilvallen van (werk)proces(sen) en daardoor zeer beperkte tot geen productie, met directe, ernstige gevolgen voor het kunnen nakomen van verplichtingen.	Correct zijn c.q. functioneren is vitaal. Afwijking resulteert in het grotendeels of geheel stilvallen van (werk)proces(sen) en daardoor zeer beperkte tot geen productie, met directe, ernstige gevolgen voor het kunnen nakomen van verplichtingen.	Onbevoegde toegang tot de informatie of het informatiesysteem is rampzalig. Het aan onbevoegden bekend worden van gegevens, werkwijzen, et cetera en/of het niet 100% eigenaar zijn van het systeem, doordat het systeem is gecompromitteerd, is desastreus.

hard nodig: bij calamiteiten zoals de storing in het Vodafone-netwerk in april 2012 gebeurt vaak wat voor onmogelijk wordt gehouden. Er doen zich situaties voor die je vooraf amper had kunnen voorzien. Als je wel een goede administratie voorhanden hebt hoe de bekabeling afgemonteerd is, maar geen toegang tot het gebouw, dan heb je een serieus probleem. Bekabeling elders opgraven kan in dat geval een oplossing zijn, maar dan moet je wel op een of andere manier weten wat wat is, welke kabel waar naar toe gaat!

Eisen

Gegeven de omgevingsfactoren en de grenzen aan alternatieven, zal op enig moment in het belang van bedrijfscontinuïteit specifieke eisen aan de beschikbaarheid van middelen moeten worden gesteld. En als het specifiek om informatie gaat, moeten ook concrete eisen worden gesteld aan het waarborgen van de integriteit en exclusiviteit (vertrouwelijkheid) van belangrijke informatie. Het is aan te raden om dit expliciet te doen via een standaard classificatiesysteem, zodat de organisatie wat betreft dit soort bedrijfseisen geheel op één lijn zit (zie kader "Classificatie").

Op wiens bord?

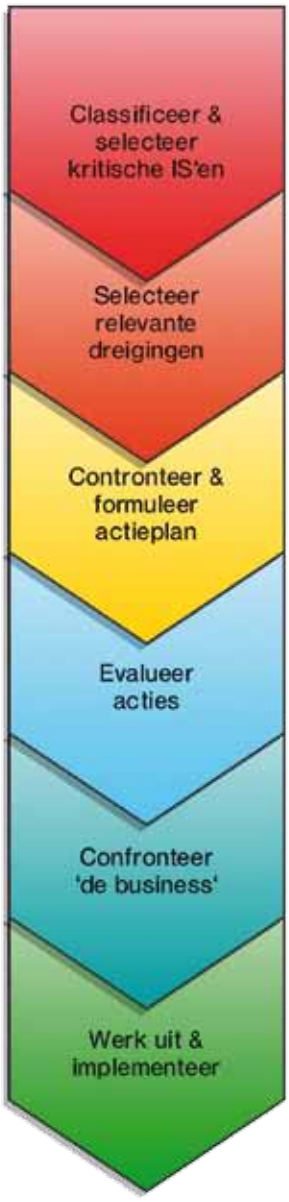
In veel organisaties staat de afdeling ICT er tamelijk alleen voor wat betreft het "regelen" van continuïteit. De business gaat er vaak van uit dat ICT haar mannetje staat en het op orde heeft op dit gebied. Immers, ICT weet toch hoe je zorgt voor robuuste systemen die door blijven draaien, hoe je deze systemen beschermt tegen stroomuitval, brand, oververhitting, et cetera. Menig ICT-afdeling krijgt de bal terug als zij bij de business aanklopt om eisen helder te krijgen: daar zijn we jullie toch voor? Als de ICT-afdeling bemerkt dat zij als probleemhouder wordt gezien, kan zij via de plus-min methode zichtbaar maken wat het actuele continuïteitsniveau van de ICT-voorzieningen is (zie kader "Plus-min methode"). Zo kan de ICT afdeling voorbereid de dialoog met de business aangaan om te komen tot het werkelijk vereiste niveau.

Conclusie

Bedrijfscontinuïteit is een lastig vraagstuk. Veel organisaties hebben geen pasklaar antwoord. Logistieke processen behoren zeer zeker tot scope, met name vanwege de directe merkbaarheid van het niet nakomen van verplichtingen jegens andere partijen en de omvang van de schade die al snel het gevolg is. Voor het verkrijgen van bedrijfscontinuïteit is het niet altijd nodig om middelen dubbel uit te voeren. Probeer creatief te zijn en analyseer wat mogelijk is met alternatieve middelen en/of werkwijzen, zoals desnoods met pen, papier en menskracht.

Plus-min methode

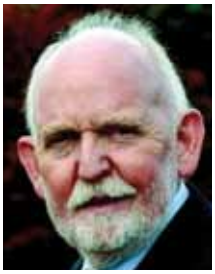
Via de hieronder beschreven plus-min methode kan een ICT-afdeling bepalen hoe zij er wat betreft continuïteit voor staat . De methode geeft inzicht in de punten waarop men tekortschiet en op welke punten het prima voor elkaar is. Of men zelfs te goed presteert en geld kan besparen door maatregelen te schrappen. De methode bestaat uit zes stappen, zie figuur 2.



Figuur 2: Stappenplan plus-min methode

Over het algemeen is het echter wel zo dat met pen, papier en extra menskracht alleen de minder zwaar geautomatiseerde processen voort te zetten zijn.

BRITSE STANDAARD BELEMMERT EFFICIËNTE INVOERING VAN BCM



Jacques A. Cazemier is Principal Consultant bij VKA voor de onderwerpen Informatiebeveiliging en BCM.
jacques.cazemier@vka.nl

Een reservewiel in de kofferbak van de auto is een goed voorbeeld van Business Continuity Management (BCM). Een lekke band komt maar eens in de zoveel jaar voor, maar als dat gebeurt – zeker op een regenachtige avond – dan is het heel plezierig een mogelijkheid te hebben om de situatie te verhelpen. Als de reserveband een zogenaamd thuiskomertje is, waarmee niet sneller dan 80 km/u gereden kan worden, zal niemand een bezwaar vinden. Thuis kunnen komen is immers belangrijker.

Inrichting van BCM is een investering. Zoals bij iedere investering dient daarvoor een kostenafweging gemaakt te worden. Omdat een crisis bij voorkeur helemaal niet en in het ernstigste geval over een aantal jaren voor komt, is het slecht te verdedigen daarvoor een eigen organisatie met een gesloten managementsysteem in te richten. Dat zou betekenen dat er continue aandacht is voor een fenomeen dat voorlopig niet gebeurt.
Nu wordt in sommige organisaties BCM ook gebruikt voor het oplossen van operationele crises – zoals het netwerk dat het niet doet, onderbroken telefonie of een weggevallen internetverbinding. In dat geval fungeert BCM als hoogste escalatieniveau van support. In dit artikel beschouwen we BCM als redmiddel van crises die – als het ongelukkig uitvalt maar eens in een carrière gebeuren.

De Britse standaard BS25999 over Business Continuity Management is een van de weinige standaarden op het gebied van BCM. De daarin beschreven aanpak levert weliswaar uitgebreide inventarisaties en analyseresultaten op, maar het verzinnen van noodoplossingen wordt daardoor niet vereenvoudigd. Het tegendeel is waar: door alle analysedetails wordt het steeds moeilijker de grote lijn te bepalen die richting geeft bij het oplossen van een crisis.
In dit artikel wordt aangegeven hoe het

CC by Andy Beecroft

Lekke band

mogelijk is sneller en goedkoper BCM in te richten met werkbare noodoplossingen en volledige acceptatie van het management.

Huidige situatie
Voor het inrichten van BCM wordt op dit moment voornamelijk de Britse standaard BS25999 ingezet. Er is ook een Duitse standaard 100-4 over Notfallmanagement (zie www.bsi.de), die is in Nederland minder populair. Er wordt hard gewerkt aan het omzetten van die tekst naar een ISO standaard en er zijn (voornamelijk Britse) organisaties bezig met het opzetten van certificering. Daarvoor wordt dan – net als bij ISO 9001 en ISO 27001 – gebruik gemaakt van het universele managementsysteem dat ISO voor dergelijke onderwerpen kent.

Inrichting van BCM volgens die standaard is een kostbaar, langdurig traject. Dat begint met uitgebreide procesinventarisaties door de hele organisatie om vast te stellen wat de RTO's en RPO's zijn. RTO staat voor Recovery Time Objective: de maximale uitvalsduur van het betreffende proces, en RPO betekent Recovery Point Objective: het maximale productieverlies. Deze begrippen worden voornamelijk binnen IT gebruikt; in productie en logistiek heeft men het over MUD – maximale uitvalsduur – en productieverlies. Dat zijn andere namen voor dezelfde begrippen.

De inventarisaties van (kritieke) processen vormen al meteen de eerste uitdaging: een Interne Controle afdeling zal zijn werk van groot belang vinden voor in stand houden van aantoonbare compliance en risicomanagement praktijken en zal daardoor het belang van de auditprocessen en de systemen die dat ondersteunen hoog inschatten. Hoger dan de algemeen directeur dat zal doen, want die vindt klantcontact het belangrijkst: de klant moet altijd (telefonisch) in contact kunnen komen met de organisatie. Daarbij is het acceptabel dat de ondersteunende systemen die de klantinformatie leveren niet direct beschikbaar zijn. In geval van nood werkt potlood en papier nog steeds, zolang er maar een boodschap doorgegeven kan worden – de klant kan altijd later worden teruggebeld.

> Thuis kunnen komen is belangrijker

Een ander probleem dat direct zichtbaar wordt is dat van eigenaarschap. De term eigenaar wordt gebruikt voor de functionaris (meestal een manager) die de bevoegdheid heeft de functionele eisen voor de betreffende toepassing te bepalen. De eigenaar is ook degene die aangeeft hoe groot RTO en RPO zijn. In veel organisaties kost het onevenredig veel moeite de eigenaars vast te stellen en de BCM eisen te laten goedkeuren door de business. Ervarig leert dat zelfs nadat BCM vorm gekregen heeft, er discussie is over de BCM eigenaars.

> Door alle analysedetails wordt het steeds moeilijker de grote lijn te bepalen

Vervolgens worden dreigingenanalyses uitgevoerd om na te gaan welke ongelukken kunnen gebeuren, wat de oorzaken zijn en hoe groot de kans is dat een dergelijke ramp ook werkelijk gebeurt. Daarbij wordt zichtbaar dat er altijd dreigingen zijn die nooit zijn verzonnen. Neem de overvloedige sneeuwval van een paar jaar geleden, waardoor in de buurt van Utrecht een rekencentrum ontruimd moest worden omdat het platte dak de hoeveelheid sneeuw niet meer kon dragen. Deze dreiging was helaas niet meegenomen in de dreigingenanalyse.

Tenslotte volgen Business Impact Analyses (BIA) om de effecten van het wegvallen van processen voor de bedrijfsresultaten vast te stellen. Op basis van die analyseresultaten wordt vervolgens – volgens de standaard – een continuïteitsstrategie opgesteld. Nadat die strategie uitgewerkt is naar acties en activiteiten, worden plannen opgesteld om vast te leggen wat er bij het uitbreken van een bedrijfscrisis of calamiteit moet gebeuren om te kunnen overleven.

Bij bijna alle organisaties worden processen ondersteund door IT systemen met applicaties die gebruik maken van databases. In een aantal van de organisaties worden de medewerkers ondersteund door processystemen die werk en informatie verdelen over de afdeling. IT speelt een vergelijkbare rol als de elektriciteitsvoorziening: bij onderbreking stagneren meteen de bedrijfsprocessen.

Onhandig is dat IT en business verschillende werelden zijn die van nature niet goed aansluiten. In dit artikel pleiten we voor scheiding van die werelden en het apart inrichten van BCM voor de IT, los van de inrichting van BCM voor de business. Bij dat eerste horen termen als redundantie van infrastructuur, uitwijk en datareplicatie.
Door IT zijn eigen BCM te laten inrichten wordt mogelijk betrouwbare IT dienstverlening te organiseren die voldoende crisisbestendig is.

Omdat het tegenwoordig als organisatie niet meer te verdedigen is niets aan BCM gedaan te hebben en omdat in sommige sectoren toezichthouders strikte normen hanteren, wordt met name in de financiële sector veel aandacht besteed aan het inrichten ervan. Er zijn geautomatiseerde hulpmiddelen beschikbaar om in korte tijd nog meer inventarisatie uit te voeren en geautomatiseerd plannen te genereren met actiepunten gebaseerd op de ingevoerde gegevens. Daarmee wordt het helaas nog makkelijker om meer inventarisaties en analyses uit te voeren en meer details in plannen op te nemen.

> Inrichting van BCM volgens de standaard is kostbaar

Samenvatting van het probleem
Met de op de standaard gebaseerde inrichting van BCM vallen de volgende zaken op:
het kost erg veel inspanning om de inventarisaties en analyses uit te voeren; inspanning en doorlooptijd. Dat betekent dan niet zelden de inrichting wordt gestopt omdat er nog geen resultaat is en de kosten te hoog worden.
de verzameling resultaten is erg gedetailleerd en maakt de businessstrategie voor het afhandelen van en crisis niet zichtbaar. De mate van detail veroorzaakt uitgebreide discussie in de organisatie die niet bijdraagt aan het snel bepalen van een BCM oplossing.
het inrichtingsteam stelt noodoplossingen op die vervolgens geaccepteerd moeten worden

Tornadoschade

door de business. In de praktijk blijkt dat moeizaam te verlopen; business kan zich niet altijd vinden in de oplossingen of de goedkeuring blijft om andere redenen achterwege.
Niet zelden wordt een aparte BCM organisatie opgetuigd. De koppeling tussen de BCM organisatie en business vergt acceptatie, oefening en onderhoud.

> Het is als organisatie niet meer te verdedigen niets aan BCM gedaan te hebben

Het inrichten van BCM vergt in het algemeen teveel tijd. Dat betekent dat het te lang duurt voordat BCM op orde is, de plannen goedgekeurd zijn en de organisatie weet dat bij een crisis er goed gereageerd gaat worden.
Omdat het inrichtingstraject zoveel tijd in beslag neemt, zijn de kosten hoog. Als dan de noodoplossingen ook nog eens niet geaccepteerd zijn, is het twijfelachtig of dat werkt tijdens een calamiteit. Er is dan geen tijd om nog te schaven aan de oplossingen. Van te voren moet management voldoende vertrouwen hebben dat het mogelijk is de crisis te overwinnen.

De oorzaak van het probleem
De Brits BCM standaard is een ontwikkeling van een 'best practice' van The BCI, the business continuity institute. Dat document is omgezet naar een publicatie van het British Standards Institution (BSi) PAS56 en vervolgens opgenomen als British Standard BS25999. Op dit moment zijn er acties gaande om de standaard op te nemen in de ISO bibliotheek van standaarden.

> Management moet vertrouwen hebben dat de crisis overwonnen wordt

The BCI is een Engels commercieel adviesinstituut, dat sinds 1994 werkzaam is om over inrichting van BCM te adviseren, leden te voorzien van titels (achter hun naam) en dat uit te voeren. "Promoting the art and science of business continuity management worldwide".
Helaas ontbreekt in de standaard de optimalisatie naar de klantsituatie; het lijkt of er sprake is van maximalisatie van adviesdiensten.
We zien dan ook dat organisaties halverwege blijven steken omdat terecht gezien wordt dat er op korte termijn geen verbetering is van de crisisbestendigheid.

De oplossing: Lean BCM
Ervaringen tijdens grote calamiteiten in binnen- en buitenland leert dat goed werkende crisismanagement noodzakelijk is voor het overleven van een crisis. Dat is zichtbaar geworden na calamiteiten als 9/11 in New York, Katrina in New Orleans, maar ook bij de brand bij de faculteit Bouwkunde van de TU/Delft of de helikopteraanvaring met de hoogspanningsmast in de Bommelerwaard.

Overstroming

Uitslaande brand

Als we er van uit gaan dat ieder management team van iedere organisatie van nature in staat is om (business) problemen op te lossen, dan hebben we in iedere organisatie het team te pakken dat in geval van calamiteit de situatie kan gaan regelen. Vervolgens kent ieder management teamlid binnen zijn eigen afdelingen de medewerkers die in tijden van tegenwind het best in staat zijn de bedrijfsactiviteiten voort te zetten. Vakkennis, flexibiliteit en improvisatievermogen zijn de ingrediënten waarmee – met goede aansturing – het mogelijk moet zijn de business weer op de rails te krijgen. Zodat in principe iedere calamiteit overwonnen kan worden.
Het is daarbij noodzakelijk dat de basisvoorzieningen die nodig zijn om activiteiten ongestoord uit te voeren aanwezig zijn. Dat kan variëren van de noodvoorraad briefpapier tot reservevoorzieningen voor het telewerken.

> Ieder management team is van nature in staat om problemen op te lossen

De beste manier om na te gaan of een willekeurig management team in staat is een calamiteit te overleven is het simuleren ervan. Door een calamiteit zoals het voorlopig niet beschikbaar zijn van de locatie als oefenscenario uit te voeren, wordt duidelijk of het mogelijk is een werkende noodoplossing te vinden. Als dat het geval is, is documenteren van die oplossing voldoende om het Bedrijfscontinuïteitsplan (BCP) te vullen. Acceptatie mag daarna geen probleem zijn. Een volgende keer, bij een volgende simulatie, is het mogelijk dat de omstandigheden anders zijn, waardoor er een andere oplossing opgesteld wordt. Dat biedt dan de mogelijkheid het BCP aan te passen.

Nu is het niet beschikbaar zijn van de locatie maar een van de mogelijke scenario's. Een andere kan zijn die van het langere tijd niet beschikbaar zijn van de IT infrastructuur. Daarbij is het belangrijk wat de oorzaak is van de calamiteit. Het maakt voor de oplossing niet echt uit waardoor de locatie niet beschikbaar is, als maar bekend is hoe lang het gaat duren.
Welke scenario's gehanteerd worden, hangt af van aard en locatie van de betreffende business.

Indien er geen adequate noodoplossing gevonden wordt, moet het management team in staat zijn aan te geven welke elementen van de oplossing gewijzigd moeten worden om wel de crisis te overleven.
Door de focus bij het vinden van de oplossing te richten op het team dat het werk moet gaan doen, wordt bereikt dat in korte tijd een werkende oplossing ontstaat, acceptatie van de oplossing automatisch is en er niet meer ingericht wordt dan werkelijk nodig is. Daarbij geldt als rode lijn door de inrichting dat niet meer plannen worden geschreven dat noodzakelijk ios. Globale gedachte daarachter is dat tijdens een calamiteit er geen tijd is om dikke plannen door te werken. Aanbevolen wordt zelfs om de checklist met de eerste vijf acties op de omslag van het plan te zetten.

Deze vorm van inrichten is Lean BCM genoemd. Het is tot tevredenheid uitgevoerd bij een aantal organisaties.

DE ERFENIS VAN HET DIGINOTAR DRAMA

Auteursgegevens: André Koot is redacteur van het blad Informatiebeveiliging.
Hij is bereikbaar via pvib@tken.net

Wat kregen ze er van langs, de auditors en toezichthouders die betrokken waren bij het Diginotar drama. Ondanks allerhande goedkeurende verklaringen en rapporten bleek er heel wat mis te zijn en het vergde een technisch onderzoek van maar een paar dagen om dat allemaal duidelijk te maken. Hoe kan het bestaan dat er zo'n verschil zat tussen het opgebouwde vertrouwen en de trieste werkelijkheid?

Redactioneel commentaar
In dit het artikel wordt getracht vanuit een historisch perspectief aan te geven hoe complex de vertrouwensbusiness is ingericht en worden diverse knelpunten toegelicht. We plaatsen in de regel nooit zo'n lang artikel, maar we vonden het gezien het belang niet verstandig om het in meerdere afleveringen te plaatsen.

DEEL 1, VERTROUWEN IS GOED

Elektronische Handtekening
Om deze vraag over de betrouwbaarheid van vertrouwen te beantwoorden moeten we ver terug gaan in de tijd. Public Key Infrastructure[1] was zo'n 15 jaar geleden een nieuw concept in de beveiligingswereld. De mogelijkheden voor toepassing van certificaten als digitaal paspoort, het gebruik voor het plaatsen van elektronische handtekeningen en het gebruik voor server authenticatie, zijn vrij snel duidelijk geworden. Maar even snel bleken ook de problemen die ontstonden vanwege de complexe materie (cryptografische techniek, security, sleutelbeheer). Inmiddels blijkt dat in ieder geval de grootste zorg bestaat rondom het begrip 'Vertrouwen'. De toegevoegde waarde van certificaten bestaat namelijk juist daarin dat je een certificaat van een andere partij kunt vertrouwen, ook al ken je die externe partij niet, als je het digitale paspoort, het certificaat maar kunt vertrouwen. Je hoeft dus niet allerhande bilaterale relaties met andere partijen aan te gaan en te onderhouden om met elkaar zaken te kunnen doen, digitaal te kunnen factureren of te communiceren en om digitaal contracten te kunnen sluiten.

> Wegnemen van belemmeringen voor elektronische handel

De wens om elektronische handtekeningen te kunnen gebruiken werd breed gevoeld en dat betekende dat internationale regelgeving noodzakelijk werd. Europa kwam al snel met regelgeving rondom de elektronische handtekening. De EU was partij omdat de EU enerzijds de elektronische handel tussen bedrijven van de verschillende lidstaten wenste te stimuleren door het wegnemen van belemmeringen voor elektronische handel en anderzijds handelsbarrières wilde voorkomen door het gelijkstemmen van de juridische regelgeving in de verschillende lidstaten. Duitsland liep bijvoorbeeld al voor met eigen wetgeving rondom de elektronische handtekening.
Europa definieerde in de regelgeving het onderscheid tussen de 'gewone'

elektronische handtekening, de geavanceerde elektronische handtekening en de gekwalificeerde elektronische handtekening (zie kader).
PKI was in ieder geval het noodzakelijke en betrekkelijk kostbare instrument om gekwalificeerde elektronische handtekeningen mogelijk te kunnen maken.
In dit historisch perspectief moeten we overigens niet vergeten vast te stellen dat het gebruik van certificaten werd gereguleerd ten behoeve van het gebruik van de elektronische handtekening onder contracten. Het gebruik van certificaten ten behoeve van SSL kwam pas veel later in zwang.

In Nederland 'Marktwerking' uitgangspunt

Normenkaders
Het onderbouwen van vertrouwen is een zorg van alle tijden en plaatsen. Ook buiten Europa vonden ontwikkelingen plaats om trust te borgen. Met name op het gebied van certificaten werden al snel diverse standaarden in het leven geroepen. Belangrijk was de Amerikaanse ANSI standaard rondom inrichting en beheer van Certificate Authorities (CA's), X9.79:2000, 'PKI Practices and Policy Framework'. Hierin worden 3 specifieke aandachtsgebieden onderkend: Certificaatbeheer (uitreiken en intrekken van certificaten), Sleutelbeheer (uitvoeren van cryptografische bewerkingen en de procedures daaromheen) en Security Management.

Twee belangrijke gebruikers van dit ANSI framework waren de AICPA, de beroepsvereniging van accountants in Amerika en de American Bar Association, de Amerikaanse beroepsvereniging van advocaten. Dat geeft al aan dat er veel draagvlak bestond voor het hanteren van dit kader. De ANSI standaard vormde dan ook de basis voor het WebTrust initiatief van AICPA, het control en audit framework voor CA's. WebTrust is inmiddels door alle beroepsverenigingen van auditors overgenomen, maar ook de meeste andere relevante technische partijen, zoals browserleveranciers, hebben WebTrust omarmd als het referentiekader voor het kunnen vertrouwen van CA's en daarmee bijvoorbeeld als basis voor het vertrouwen in certificatenleveranciers, die op grond daarvan in de browsers zijn opgenomen!

In Europa werd het European Telecommunications Standards Institute (verder ETSI) aangewezen als partij om het normenkader voor CA's te ontwikkelen en beheren. Ook ETSI hanteert feitelijk het WebTrust kader als basis voor het eigen certificatieschema, ETSI Technical Specification TS101456.

TTP.NL
Uitvoering van de Europese regelgeving is een verantwoordelijkheid van de afzonderlijke lidstaten. Nederland koos voor het uitgangspunt van zelfregulering onder meer vanwege het

Elektronische handtekening
De Nederlandse wetgeving [2], gebaseerd op Richtlijn 99/93/EG onderkent 3 soorten van elektronische handtekeningen:

1. De gewone elektronische handtekening bestaat uit elektronische gegevens die zijn vastgehecht aan of die logisch geassocieerd zijn met andere elektronische gegevens. Deze handtekening wordt gebruikt als middel voor verificatie van de authenticiteit van de ondertekenaar. Denk aan een scan of fotokopie van een geschreven handtekening. Een ander voorbeeld is het gebruik van je RSA token, dat je gebruikt voor remote access, dat je ook zou kunnen gebruiken voor elektronische ondertekening van interne formulieren.
2. De geavanceerde elektronische handtekening is een elektronische handtekening die voldoet aan de volgende 4 eisen:
   - Zij is op unieke wijze aan de ondertekenaar verbonden;
   - Zij maakt het mogelijk de ondertekenaar te identificeren;
   - Zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
   - Zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.
     Denk aan een sleutelpaar bestaande uit een private en publieke sleutel. In bron [1] wordt het begrip Public Key Infrastructure (PKI) uiteengezet. Maar ook PGP (Pretty Good Privacy) certificaten voldoen aan deze eis.
3. De gekwalificeerde elektronische handtekening is een geavanceerde elektronische handtekening (dus conform 2) die bovendien:
   - Is vervaardigd met een certificaat, uitgegeven door een bij de Opta ingeschreven Certificatiedienstverlener (TTP);
   - Welk certificaat door de TTP in het certificaat zelf is aangemerkt als "gekwalificeerd";
   - Is gemaakt met een "veilig middel" (bijv. goedgekeurde smartcard, usb token);
   - Bij de afgifte aan de toekomstige gebruiker zelf visueel is gecontroleerd op diens identiteit. Dat moet fysiek gebeuren met een originele officieel identiteitsbewijs.

Alleen als een handtekening gekwalificeerd is, is de bewijslast omgekeerd: de partij die de ondertekening in twijfel trekt moet aantonen dat de handtekening niet juist is. Daarmee komt de juridische waarde van de elektronische handtekening overeen met de geschreven handtekening.

uitgangspunt dat de markt zelf verantwoordelijk is voor de goede naleving en uitvoering. En daarbij was op grond van het beleid van Economische Zaken 'Marktwerking' uitgangspunt. Dat impliceerde dat bij het implementeren van de richtlijn de volgende uitgangspunten werden gehanteerd:

- Toezicht op Certificate Service Providers (CSP's) (die gekwalificeerde elektronische handtekeningen mogen verstrekken) is wettelijk geborgd;
- Er is sprake zijn van een vrijwillig certificatieschema;
- Vergunning zijn verboden, er is geen drempel om als CSP op te mogen treden.

Dat levert wel direct een interessante spagaat op: Wat is de relatie tussen marktwerking (vrije toetreding) en trust (kwaliteitsborging door wettelijke inkadering). Vrije toetreding is natuurlijk strijdig met automatische beperking door wettelijke kaders.

ECP (tegenwoordig ECP-EPN), een samenwerkingsverband tussen overheid en bedrijfsleven, ontwikkelde het initiatief TTP.NL (TTP staat voor Trusted Third Party, een ruimer begrip dan CSP. In dit artikel wordt verder de term CSP gehanteerd vanwege de focus op het certificaatbeheer proces). Een van de belangrijkste activiteiten van TTP.NL was het opstellen van het certificatieschema en een daarbij passend accreditatieschema. Daarbij was het uitgangspunt dat vrijwillige certificering van CSP's zou gaan plaatsvinden, er is formeel dus geen wettelijk afgedwongen certificering van CSP's.

Accreditatie en Certificering
Accreditatie (uit het Latijn ad+credere, "te geloven"): Een procedure waarbij een derde partij een geschreven garantie geeft dat een product, proces of dienst beantwoordt aan specifieke vereisten. Het is een prospectieve erkenning, naar de toekomst toe. Het is een formele erkenning van een Inspectie-instelling of een Certificatie-instelling. De structuur van accreditatie is beschreven in internationale normen (ISO/IEC 17000, ISO/IEC 17025, ISO/IEC 17020, ISO/IEC 17021)
Certificering: Het door een onafhankelijke derde laten vaststellen dat een managementsysteem van een organisatie voldoet aan gepubliceerde normen en eventueel aanvullende documentatie (waarop het betreffende kwaliteitssysteem gebaseerd is). Certificerende instellingen verkrijgen hun accreditatie bij de Raad voor Accreditatie, die toezicht houdt op de uitvoering van de audits.

In Nederland is de OPTA namens de overheid de aangewezen toezichthouder die het register beheert waarin de TTP's staan vermeld die certificaten ten behoeve van de gekwalificeerde handtekening mogen verstrekken. Zonder een OPTA registratie is een certificaat van een CSP niet geschikt om als elektronische handtekening met wettelijke bewijskracht te kunnen fungeren. Een partij kan in Nederland zonder OPTA registratie wel als CSP optreden, maar de afgegeven certificaten zullen niet kunnen worden geaccepteerd als gekwalificeerde elektronische handtekening.
De OPTA heeft het TTP.NL certificatieschema en het accreditatieschema geaccepteerd als basis voor de registratie. Conformeert een CSP zich aan het ETSI kader, dan wordt daardoor vermoed dat de CSP aan de wettelijke eisen voldoet. OPTA voert geen inhoudelijke toets uit.

Het TTP.NL Accreditatieschema
Het accreditatieschema dat door TTP.NL werd ontwikkeld bevatte eisen die gelden om als certificerende partij (de auditor dus) voor TTP audits te mogen optreden. Het schema omvat de competenties, taken, bevoegdheden en verantwoordelijkheden van de auditor die een audit op een TTP mag uitvoeren. Het schema is zo stringent, dat een gewone RE of CISA niet zo maar zelfstandig een audit uit mag voeren, dat mag alleen een ervaren TTP auditor doen. Er zijn dan ook maar enkele auditors die dergelijke audits mogen uitvoeren. Inmiddels is het accreditatieschema vervangen doordat ISO/IEC 17021:2011, Conformity assessment, van toepassing is. Deze ISO standaard beschrijft de eisen ten aanzien van certificerende instanties, die management systemen auditen. Daarbij is de Raad van Accreditatie verantwoordelijk voor uitvoering.
Overigens gebeurt accreditatie in Nederland op vrijwillige basis[3], al kan zonder accreditatie een auditor niet optreden als partij om TTP audits in het kader van de OPTA regeling te mogen uitvoeren.

Het TTP.NL Certificatieschema
Het certificatieschema bevat een verwijzing naar de beheersmaatregelen uit de ETSI Technische Specificatie. Het is daarmee ook feitelijk het controleprogramma om een audit uit te voeren inclusief de bijbehorende normatiek. Het kader is op grond van internationale regelgeving grotendeels gemodelleerd naar de internationale standaarden (ANSI, WebTrust).

Het certificatieschema is inmiddels wel een complex verhaal. Waarom bestaat er nu nog een apart TTP.NL certificatieschema en wat is de relatie tussen bijvoorbeeld de (verschillende) ETSI normen, WebTrust, ISO 211XX, ISO2700x, ISO3200x? Is hier geen sprake van 'not invented here'? In ieder geval geeft het bestaan van zoveel normenkaders aan dat niet alleen de techniek en de processen complex zijn, maar dat ook de regelgeving en toezichtstructuren niet eenvoudig te doorgronden zijn.

Vrijwillig gebruik certificatieschema
Het gebruik van het certificatieschema is in Nederland feitelijk dus niet verplicht. Een CSP kan zelf besluiten om te willen voldoen aan het kader. Binnen deze systematiek kan een CSP een auditor een specifieke auditopdracht geven, maar een CSP kan ook zelf verklaren te voldoen aan de beheersmaatregelen (de Eigen Verklaring).

Om te voldoen aan de eisen voor het verstrekken van een gekwalificeerde handtekening conform de Europese regelgeving is formele toetsing conform het TTP.NL certificeringsschema in Nederland feitelijk óók niet verplicht. Als er geen auditverklaring is, kan een CSP zelf een aanvraagformulier van de OPTA invullen. Het aanvraagformulier invullen vergt wel bijna een audit door de aanvrager zelf, het is daarmee eigenlijk een soort Eigen Verklaring. Een CSP met een TTP.NL certificering wordt in ieder geval makkelijker toegelaten tot het OPTA register: de OPTA is binnen Nederland verplicht om de verklaring van een (ttp.nl) auditor te vertrouwen, de registratie is daarmee niet meer dan een formaliteit.
In het geval van een Eigen Verklaring zal de CSP bij de registratieaanvraag zelf alle evidence rondom implementatie, beheer en de vereiste waarborgen bij de OPTA moeten overleggen, aangezien de OPTA een compleet informatiedossier moet opmaken. Of en hoe de OPTA vaststelt of een dergelijk CSP geregistreerd mag worden, is mij op dit moment niet duidelijk. Gezien het wettelijke vermoeden is de aanvraag met alle evidence al voldoende basis voor registratie en zal de OPTA als toezichthouder steekproefsgewijs onderzoek doen. Voor zover mij bekend hebben alle Nederlandse CSP's met OPTA registratie in ieder geval wel een ETSI certificeringstraject doorlopen en beschikken ze dus over een verklaring van een geaccrediteerde auditor. In enkele gevallen is het certificaat afgegeven door een buitenlandse auditor, hetgeen onder het oude regime van het TTP.NL accreditatieschema niet mogelijk was.

In de ETSI standaard wordt gerefereerd aan ISO 17799-2000

Voorbeeld van een ETSI audit verklaring door auditor
Certificaat-/licentienummer:
ETS xxxx
Status:
Active
Schema/norm:
ETSI TS 101 456: v1.4.3
Bereik:
Certification Authority processes and services (as defined by ETSI TS 10 1 456) in accordance with the statement of applicability version 25th June 2009: Registration Service, Revocation Management Service, Certificate Generation Service (*), Revocation Status Service (*), Dissemination Service (*), Subject Device Provision Service. The services marked (*) are provided with the support of a third-party service provider, under the final responsibility of [naam verwijderd door auteur].

ETSI, ISO 27001/2, WebTrust, TTP.NL
Voor Nederland is in ieder geval de ETSI standaard van belang. De standaard omvat de volgende onderdelen (zie kader met auditrapport):
- Certificaatmanagement
- Sleutelbeheer
- Security Management

ETSI pretendeert zelf niet om een security baseline te zijn. In de standaard wordt voor het onderdeel security diverse malen gerefereerd aan ISO 17799-2000. Het gaat specifiek om de onderdelen Security Management (d.w.z. de security management processen, met name rondom security incidenten en continuïteit), Personele aspecten, Fysieke beveiliging en IT Security.

Als je de ETSI, WebTrust en ISO2700x kaders goed beschouwt, dan is het aantal overeenkomsten treffend.
Qua terminologie zijn er verschillen, maar qua inhoud is er eigenlijk alleen een verschil in een aantal in ETSI wel, maar in ISO niet beschreven normen. En die normen gaan logischerwijs over certificaatbeheer en sleutelbeheer.
En daar waar ETSI rept over security management zou je eigenlijk moeten denken aan ISO27002, het management system. ETSI refereert aan de ISO standaard, maar houdt op dit punt toch ook nog een eigen normenkader in stand. ETSI meldt dat het hanteren van Best Practices voor security management door het toepassen van de ISO standaard ook mag. Dat is wel een beetje raar omdat ETSI zelf ook niet meer dan een Best Practice is...

SSL, HTTPS en EV certificaten
Het verstrekken van een elektronische handtekening is omgeven met allerhande waarborgen. Denk aan de wettelijke inkadering om de elektronische handtekening gelijk te kunnen stellen aan de fysieke handtekening op papier. Toen Netscape in 1994 het

SSL-protocol ontwikkelde, werd in eerste instantie gebruik gemaakt van Kerberos[4]. Doelstelling van SSL was beschermen van de communicatie tussen de browser en de webserver tegen afluisteren. In SSL versie 2 werd heel slim de publieke sleutel in een servercertificaat gehanteerd om de communicatie te coderen. Oogmerk was dus om het afluisteren van de communicatie te voorkomen. Authenticatie van de server was niet een expliciet doel, eerder een soort bijkomstigheid, maar een bijkomstigheid die wel noodzakelijk was om vast te stellen dat uitsluitende de bedoelde servers met elkaar kunnen communiceren. Daar waar voor de geavanceerde en gekwalificeerde elektronische handtekening allerhande eisen werden gesteld ten aanzien van de vaststelling van de identiteit van een aanvrager, gold dat eigenlijk helemaal niet voor servercertificaten. Dat betekent dat CSP's die geen gekwalificeerde handtekening kunnen verstrekken omdat ze bijvoorbeeld geen OPTA registratie hebben, wel (SSL) servercertificaten conform de X509.3 standaard kunnen verstrekken. In het verleden was dat ook geen probleem, omdat de certificaten feitelijk alleen voor versleuteling van het communicatiekanaal of voor afzonderlijke berichten (denk aan belastingaangiften) gebruikt hoefden te worden. Het als authentiek waarmerken van een server door een certificaat is heel iets anders: zonder echte verificatie en goede governance bij de CSP, is er onvoldoende waarborg voor de authenticiteit. Maar dat herken je niet als je een certificaat bekijkt (denk aan de bekende 3x kloppen campagne van de vereniging van banken). Maar de laatste jaren wordt er, mede doorallerhande security incidenten in diverse publiciteitscampagnes, wel steeds meer aandacht geschonken aan het vertrouwen op grond van juist die functie van servercertificaten![5]

Dit probleem is natuurlijk ook onderkend in de security branche. En dat resulteerde onder meer in het ontwikkelen van de EV-certificaten (extended validation) standaard [6].
EV-certificaten worden verstrekt onder condities die in de 'Baseline Requirement' zijn vastgesteld door het CA/Browser Forum [7]. Dit Browserforum is het consortium van softwareleveranciers die de browsers ontwikkelen. Het belang is hierin gelegen dat deze browsers ons, als gebruikers, helpen bij het identificeren van vertrouwensproblemen. Als een CSP volgens de (leverancier van de) browser vertrouwt wordt, dan krijgen we dat te zien doordat de adresbalk in de browser dat toont. Alleen als een certificaat is verleend door een CSP die voldoet aan de baseline, dan zal de browserleverancier dat certificaat opnemen in de browser die wij gebruiken. Het belang van deze baseline en het vertrouwen dat wij daaraan ontlenen is dus aanzienlijk!
In de CA/Browser baseline gaat één hoofdstuk over de audit requirements ten aanzien van CSP's. Het forum refereert hierin aan een viertal standaarden: WebTrust, een nationaal schema conform ETSI TS 101 456 v1.2.1 of later, dan wel ETSI TS 102 042 V1.1.1 of later, of een schema conform ISO 21188:2006. Daarnaast mogen overheids CSP's een eigen schema hanteren. De Baseline stelt ook eisen aan de auditors. Het mag duidelijk zijn dat dergelijke certificaten kostbaar zijn. De vraag is of de markt in staat is om deze extra waarborgen te betalen...
De eerste versie van de Baseline Requirement zal medio 2012 formeel van kracht zijn.

Gevolg van menselijk falen

Soorten servercertificaten
Er bestaan verschillende soorten betrouwbaarheidsniveaus van servercertificaten:
Domain validated: controle over aanvraag domeincertificaat op basis van email verificatie
Organisation validated, via een whois lookup verificatie op basis van bij kvk geregistreerd telefoonnummer
Qualified: afgeleide fysieke verificatie mbv een token, dat wordt verstrekt aan een aanvrager op basis van visuele verificatie, maar nadien wordt vertrouwd op die initiële verificatie van de aanvrager.
EV: visuele verificatie aanvrager voor elke aanvraag afzonderlijk.

DEEL 2, TOEZICHT KAN BETER

Waar ging het nu fout in de Diginotar case?
Misschien moeten we eerst maar eens vaststellen waar het niet fout ging. Ten aanzien van de rol van de auditor ging het eigenlijk niet in letterlijke zin fout. De aan de auditor verstrekte opdracht was, conform het TTP.NL schema, een onderzoek naar het "management system". Maar wat houdt dat in? Wat is dan de scope van de audit?

TTP.NL illustreert de scope van de term 'Management System' met de afbeelding in figuur 1.

In deze afbeelding is te zien dat de scope van een management system audit beperkt is tot het linker deel van het schema. TTP.NL beschrijft de audit als een toets van opzet en implementatie van de beheersmaatregelen, waarbij feitelijk aan het ETSI toetsingskader wordt voldaan. Het rechterdeel van het schema, de product audit, omvat twee andere type audits, namelijk een audit van de Cryptomodules en een EDP-audit naar Trustworthy Systems op grond van CWA 14716-1. Dat onderdeel is een TPM-audit: de CWA is het normenkader ten aanzien van de technische specificaties van de specifieke high security infrastructuur, denk daarbij aan 'hardenen' van een operating system en aan het gebruik en beheer van firewalls.

Wat houdt deze inrichting van het audit framework concreet in? Het onderzoek dat werd gericht op het toetsingskader van ETSI is expliciet niet gericht op een beoordeling van de feitelijke werking van de technische beheersmaatregelen.
Dat impliceert dus meteen het enorme risico dat we lopen bij het hanteren van deze systematiek van toezicht. Stel de volgende situatie voor:

> Er geldt een wettelijk vermoeden van betrouwbaarheid

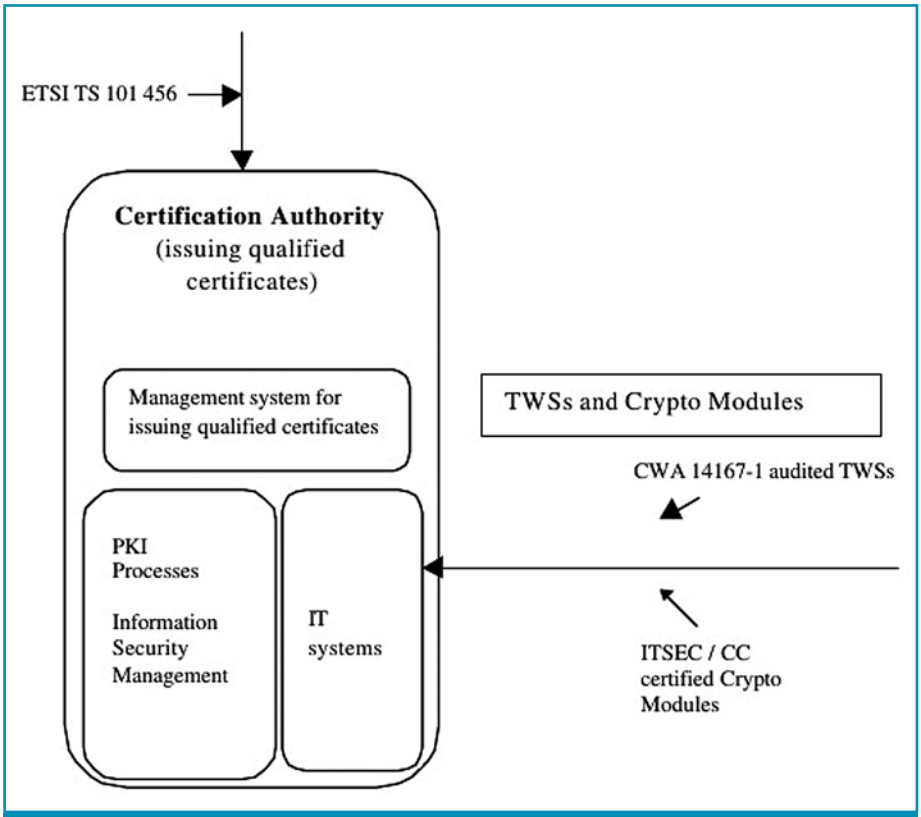
Een CSP (die gekwalificeerde handtekeningen wil verstrekken) vraagt bij de OPTA een registratie aan op grond van een auditrapport conform het TTP.NL schema. De OPTA voert zelf geen eigen onderzoek uit, maar vertrouwt op het auditrapport (de OPTA is overigens wettelijk verplicht zo'n rapport te vertrouwen, er geldt een wettelijk vermoeden van betrouwbaarheid). Als de CSP geregistreerd wordt, is een periodieke herbeoordeling verplicht, tenminste als de CSP zich vrijwillig houdt aan het TTP.NL schema. Maar die audit is identiek van inhoud en vorm aan het initiële onderzoek. Het resultaat van de audit zal dan dus, ceteris paribus, identiek zijn.

Zwakheden in het stelsel
De opdracht aan de Diginotar auditor was dus feitelijk of het Management System voldeed aan ETSI. En volgens het PWC auditrapport (indirect online beschikbaar via [8]) was dat het geval. Maar deze audit had even feitelijk dus een beperkte scope, je zou kunnen zeggen dat sprake was van een toets conform ISO 27001 (management system) en niet ook conform ISO 27002 (security controls).

De eerste zwakheid van het hele stelsel is daarin gelegen dat OPTA registratie automatisch verkregen kan worden door het TTP.NL schema op basis van vrijwilligheid toe te passen. En voor een CSP is het betrekkelijk logisch om zich te willen houden aan het schema, omdat het geen diepgaand onderzoek op werking impliceert en wel een vorm van transparantie voor derden biedt.

De tweede zwakheid bestaat daarin dat voor het kunnen toepassen van certificaten ten behoeve van SSL, het browserconsortium zich eveneens baseert op de landelijke regels. Een vrijwillige TTP.NL verklaring is dus extra waardevol, omdat zo'n verklaring in de meeste gevallen blijkbaar afdoende is om in browsers opgenomen te worden als (door de browser) vertrouwde root-CA[9].

Interessant is ook de rol van de browserleveranciers die zijn verenigd in het



Figuur 1: Scope van de term 'Management System'

browser-forum. In het verleden namen ze zonder feitelijk eigen toezicht iedere CA op als vertrouwde partij in de browser, hetgeen resulteerde in een volstrekt onoverzichtelijke browserlijst met meer dan 600 vertrouwde certificaatleveranciers. Microsoft en Mozilla hebben zelf, zonder enig overleg met wie dan ook, de Diginotar certificaten uit hun producten gesloopt. Achteraf bezien was dat natuurlijk volkomen terecht, maar het besluitvormingsproces en het wijzigingsproces waren volstrekt niet transparant en dat betekent dan wel een enorm risico: de browserleveranciers bepalen dus feitelijk wat op internet vertrouwd kan worden, toezicht bestaat niet en enige verantwoording leggen ze niet af. Schadeclaims voor onterecht intrekken lijken dan ook nergens te kunnen landen...

Een volgende zwakheid ligt besloten in de wijze waarop het toezicht in ons land is ingericht. Zo heeft de toezichthouder blijkbaar niet vastgesteld of het audit-rapport afdoende was om te voldoen aan de materiële eisen van de registratie. De initiële vergunning van Diginotar dateert van circa 2000 en sindsdien heeft de CSP uitsluitend de certificeringsgegevens aan OPTA hoeven doorsturen. Ik denk niet dat de toezichthouder ooit steekproefsgewijs zelf waarnemingen heeft gedaan, of laten doen (wat een toezichthouder binnen de wettelijke taak mag doen) of inhoudelijk een herbeoordeling heeft gedaan. En dat dan nog los van de vraag of het certificatieschema in de tussentijd niet inhoudelijk gewijzigd was. Ook de wettelijke beperkingen pleiten niet voor het vertrouwen in effectief toezicht.

OPTA wordt gefinancierd door de branche waarop hij toeziet

De daadkracht van de OPTA wordt natuurlijk niet in het minst ook geschaad doordat de toezichthouder voor het overgrote deel gefinancierd wordt door de telecombranche waarop hij toeziet[10], de OPTA is een kostenpost voor de branche. De OPTA bezit dan ook onvoldoende capaciteit om kwalitatief voldoende energie in de certificatenbranche te stoppen.

Dat levert bij eventuele overtredingen ook onvoldoende middelen op om de toezichthouderstaak te kunnen financieren. De Business Case voor effectief toezicht op de certificatenbranche is onvoldoende...

En voor mij is de hele complexiteit van normenkaders, baselines en betrokkenheid van diverse partijen een enorme zwakheid in het stelsel. Ik vind het ook bijzonder waarom een telecom instituut (ETSI) een certificaten framework ontwikkelt. Dat kan niet te maken hebben met de deskundigheid op het gebied van (juridische) gekwalificeerde elektronische handtekeningen, dat moet te maken hebben met de kennis en gebruik van de techniek om veilige communicatiekanalen te reguleren. Als dat zo is, is dat framework (met als achtergrond een security technische behoefte) dan wel geschikt om te dienen als framework voor een juridisch-technologische faciliteit? Wellicht zijn de kaders vergelijkbaar, maar de uitgangspunten zijn dat beslist niet. Ik denk dat met name op het aspect van Trust andere eisen gesteld worden aan elektronische handtekeningen dan aan X509.3 certificaten voor inrichten van VPN's...

En niet in het minst bestond er ook een aantal flinke zwakheden bij Diginotar zelf. Los van de vraag of er afdoende werkende technische beheersmaatregelen zijn getroffen, is mede gezien het resultaat van het onderzoek van Fox-IT bij Diginotar[11] duidelijk dat in het geheel niet werd voldaan aan de WebTrust/ETSI standaarden als het aankomt op certificaatmanagement, sleutelbeheer en incidentmanagement (meldingspicht bij incidenten!) en al helemaal niet aan de eisen aan Trustworthy systems, zoals vastgesteld in CWA.

Conclusies en aanbevelingen

De complexiteit van inrichting en toezicht leidt bijna tot de constatering dat falen in het systeem lag opgesloten.

De techniek is het probleem niet, maar wel hoe ermee wordt omgegaan.
Het hele toezichtstelsel biedt feitelijk geen enkele zekerheid op basis van afdoende risicomanagement bij de betrokken partijen. En zolang registratie zonder een daadwerkelijke technical audit mogelijk is, blijft een latent Diginotar-risico bestaan. Daar komt bij dat het niet handig is om zoveel verschillende normenkaders te hebben die vanuit verschillende optieken zijn opgesteld. Dat staat bijna borg voor inconsistenties en witte vlekken.
De trieste werkelijkheid is dat het gewenste en bestaande vertrouwen niet gestoeld is op afdoende eenduidige normen en adequaat toezicht en dat menselijk falen op alle niveaus dus wel onopgemerkt moest blijven. Deze knelpunten moesten onvermijdelijk wel leiden tot de ontstane situatie. En ik heb (buiten enkele high-level aanzetten) in de praktijk nog geen idee van verbetering waargenomen...
Het gebruik van EV certificaten zal een aanzienlijke verhoging van het niveau van Trust kunnen opleveren, ware het niet dat ook de CA/Browser Forum een paar vreemde keuzes heeft gemaakt.
Het hoofdstuk over audits meldt dat er niet een enkel auditschema hoeft te worden gehanteerd. Met alle respect voor de opstellers... handhaven van een vrijheid-blijheid situatie pleit niet voor duidelijkheid en eenduidigheid, laat staan dat dit bijdraagt aan een meer wenselijk gevoel van vertrouwen.

Misschien is dit dan ook wel een goede plek om een discussie over de toekomst aan te slingeren met een stel aanbevelingen.

- Laten we al die kaders maar eens op een hoop gooien. We hanteren ISO 2700x als basis en gooien er wat ANSI bij ten aanzien van certificaatmanagement en sleutelbeheer en indien en voorzover dat nodig is, enkele EV-eisen vanuit de CA/Browser-forum baseline. En dat kan misschien maar het beste een ISO standaard worden.
- Een baseline is een normenkader, maar niet automatisch een toetsingskader. Dat betekent dat de security gemeenschap, auditors en toezichthouders samen moeten nadenken over een beter audit framework.
- Toezicht kan niet meer zo vrijblijvend zijn als nu. Het verkrijgen van een registratie en het verlengen daarvan, vereist een inhoudelijke beoordeling en periodieke herbeoordeling van de certificering op grond van de normen die onder 1) zijn genoemd.
- Laten we dan ook meteen maar pleiten voor een toezichthouder die niet afhankelijk is van de nukken van de branche zelf. Laat de overheid de financiering regelen als ze Trust zo belangrijk vindt. Als OPTA dat niet kan, laat dan TTP.NL dat dan maar doen. Vertrouwen is iets anders dan digitale communicatie.

Lijkt me een leuke start. Wie pakt de handschoen op? Welke minister neemt verantwoordelijkheid voor vertrouwen?

Noten en Bronnen:

[1] *PKI, zie artikel in IB 2011 nr 7*

[2] *http://wetten.overheid.nl/BWBR0015046*

Tekst: http://www.opta.nl/download/wet-en-regelgeving/Wet%20Elektronische%20Handtekeningen.pdf

[3] *https://www.opta.nl/nl/tsl/vrijwillige-accreditatie/*

[4] *http://www.sslcertificatereviews.net/blog/ssl-certificates-history-background.html*

[5] *http://www.darkreading.com/authentication/167901072/security/news/232500346/is-ssl-cert-holder-id-verification-a-joke.html?*

[6] *zie Informatiebeveiliging 2007-6 "Extended Validation SSL Certificates" door Jacob Moehn*

[7] *http://www.cabforum.org/Baseline_Requirements_V1.pdf*

[8] *http://files.gendo.nl/Documenten/Certificaat_Diginotar_ETSI%2010-0020.pdf*

[9] *Er zijn diverse certificatieprogramma's bij browserleveranciers, maar die zijn niet alle even transparant. CACert, een web of trust dat X509.3 certificaten levert, heeft uitgebreide security policies, die voldoende garanties bieden voor authenticiteit van certificaten. Maar het lukt Cacert niet om als root-CA erkend te worden. Je neigt te denken aan het ontbreken van commerciële bijkomstigheden.*

[10] *90% van het OPTA budget wordt gefinancierd door de branche zelf: http://www.opta.nl/nl/hoe-werkt-opta/opta-is-een-zbo/*

[11] *http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html*

Nuttige website College van Belanghebbenden TTP.NL: http://www.ecp.nl/college-van-belanghebbenden-ttpnl

Met dank aan de reviewers, Frank, René, Aart, Lex, Cordny en Bart.

COLUMN

WINDMOLENS, PRIVACY EN EEN VERHOOGDE STAAT VAN BEWUSTZIJN

Bewustzijn is een thema waar filosofen zich al jaar en dag mee bezighouden. "*Bewustzijn is een toestand van de geest die gekenmerkt is door een besef van het eigen ik en de omgeving*". Een omschrijving waar ik me als wetenschappelijk onderzoeker naar privacy en identiteit wel in kan vinden. Ik weet wie ik ben online, offline en daartussenin. Ik ken de habitat, weet wat er leeft op Twitter, Facebook en binnen andere online omgevingen. Maar, wat betekent het nu eigenlijk voor mij en voor mijn vakgebied 'privacyrecht'? Wanneer is voor mij de staat van 'privacybewustzijn' nu echt gerealiseerd? Als iedereen in Nederland weet wat zijn rechten zijn? Als we sterke handhaving van privacywetten hebben? Als bedrijven en overheden samen de letter van de wet naleven? Of als de krant bol staat van privacyschendingen en het maatschappelijke en politieke debat ten volle losbarst?

Mijn bewustzijnswereld is gekleurd. Ik hou me dagelijks bezig met privacyzaken. De wet, grondwet, problemen, oplossingen, compliance en nieuwe wetsvoorstellen. Volg via Twitter de wereld op de voet, zie het privacynieuws aan me voorbij razen. In mijn werk zie ik bedrijven en overheden die het vooral goed willen doen en hulp nodig hebben in het oerwoud aan regels. In de politiek zie ik vernieuwde vitaliteit na het zoveelste ICT-debacle en de nieuwe voorgestelde verordening van de EU. Mijn wereld is privacy. Ik ken de wet. Ik weet doorgaans hoe het zit. Ik zoek naar werkbare oplossingen. Constateer problemen die de wet niet dekt. Maar altijd, leef, eet en adem ik privacy. Soms gaat de arrogantie met me op de loop en vooronderstel ik dat anderen ook wel weten hoe dat zit met privacy en veiligheid. En dat zijn nu juist de momenten… dat ik weleens voor een verassing kom te staan.

Ik ontving pas geleden een email. Een verzoek of ik als privacyexpert meewilde naar een meeting. Om uit te leggen wat er nu allemaal gaande is, waar de pijnplekken zitten en wat er op stapel staat. Graag! Als ik privacybewustzijn kan vergroten, dan ben ik met liefde van de partij. Een email later wordt me gevraagd of ik mijn BSN wil sturen. Dat is makkelijk want dat scheelt dan bij de legitimatie bij binnenkomst. Ik lees de mail nogmaals door. Is dit een test? Of ik wel een echte expert ben? Of is het een social engineeringtrucje? (U snapt, na jaren werkzaam te zijn op het gebied van privacy en informatiebeveiliging ben ik lichtelijk paranoide geworden). Mijn aluhoedje stond vol te blinken. Het was echt. En dus, privacybewust als ik ben, stuurde ik mijn antwoord terug: "Nee, u krijgt mijn BSN niet via e-mail. Dat is onveilig. Daarnaast geef ik alleen mijn BSN in persoon af aan instanties die op grond van de Wet BSN gerechtigd zijn dat BSN aan mij te vragen". De persoon aan de andere kant van de e-mail had er alle begrip voor, het was een onbewuste onbekendheid geweest met de wet. En even arrogant als ik privacybewust ben, was ik stiekem ook wel blij. Weer iemand erbij die weet wat zijn rechten zijn en die hopelijk zelf ook de volgende keer kritisch zal reageren als hem iets gevraagd wordt te onthullen over zichzelf!

Zolang ik nog steeds op deze manier verrast kan worden, heb ik nog genoeg missiewerk te doen. Hup! Op de barricades. Schrijft u even mee?

- Op 11 juni is het Nationaal Privacydebat, www.nationaalprivacydebat.nl
- Bits of Freedom kan altijd hulp en donaties gebruiken, www.bof.nl en
- Op 20 juni organiseert PvIB een set prachtige lustrumlezingen die allen over 'Awareness' gaan.

En als u nu vanavond naar bed gaat, wilt u dan iets voor me doen? Vraag uw partner of hij/zij uitlogt als het Facebooken weer gedaan is. Dan heeft u dubbel winst. Het is een stuk beter voor de beveiliging van het account en u komt niet in de verleiding om de privacy van uw partner te schenden door de Facebookpagina te lezen ;-). Deze Don Quichotte gaat ondertussen vrolijk voort met het verhogen van het algehele privacybewustzijn in Nederland!

mr. Rachel Marbus, @rachelmarbus op Twitter

LOCKED AND LOADED: A DECADE OF DATA SECURITY TRENDS

Samenvatting: In dit artikel beschouwt Joe Sturonas de beveiligingstrends van de afgelopen tien jaar: hoe we van perimeter-, apparaat-centrisch en communicatiebeveiliging naar data-centrische beveiliging zijn gegaan.

By: Joe Sturonas. Joe Sturonas is Chief Technology Officer for PKWARE. PKWARE offers software solutions to critical IT problems, namely the explosive growth of data, the need to secure data, and the emergence of data in the cloud. He can be reached at Joe.sturonas@pkware.com.

There is one thing that has not changed in the last ten years in data security…and that is security professionals are still kept up at night by something. That something is the harsh realization that security is not Boolean. You can never say that you are secure, because what is deemed secure today is not secure tomorrow.

Think back to the security systems in place ten years ago, try to reconcile them with the threats that exist in today's world. Certainly none would pass modern day scrutiny and no one would endorse them to provide adequate security. The threat vectors contributing to those sleepless nights have become far more sophisticated over the last decade; security professionals are forced to grapple with incredibly complex scenarios as well as computing systems that now extend up… into an environment known best as "the cloud".

Most experts agreed that the perimeter of the corporate network was a safe place

Although security was more centralized ten years ago, trends were moving quickly to a more decentralized model. However, most experts agreed that the perimeter of the corporate network, whether physical or virtual, was a safe place. Everyone was focusing on the network perimeter and making sure that it was fortified and able to keep threat vectors at bay. You could almost hear the mantra… thou shall not penetrate the inside of the network. The good news? If you were inside the network, then you were most likely trusted.

REGULATION AND COMPLIANCE A DRIVING FORCE

Regulation and compliance have had, and continue to, significantly impact data security trends and IT behavior. The following are some of the most instrumental policies and their influence on security operations.

Directive 95/46/EC ("Data Protection Directive")

At a European level, sets up a regulatory framework and strict limits on the collection and use of personal data in an effort to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU).

PCI Payment Card Industry Compliance

PCI regulations went into effect in 2005. By design, the compliance regulation protects vendors, employers, employees, and consumers from unprotected network systems that result in loss of personal data and revenue.

BASEL II

Basel II, initially published in June 2004, includes recommendations on banking laws and regulations issued by the Basel Committee on Banking Super-

vision (BCBS). In the simplest terms, the greater risk to which the bank is exposed, the greater the amount of capital the bank needs to hold to safeguard its overall financial stability and economic soundness.

Health Insurance Portability and Accountability Act (HIPAA)
HIPAA seeks to establish standardized mechanisms for electronic data interchange (EDI), security, and confidentiality of all healthcare-related data.

Hague Conference
Preliminary Document No 7 of April 2000, "Electronic Data Interchange, Internet and Electronic Commerce", acknowledged the groundbreaking work of a number of international organizations with regard to the protection of privacy in connection with trans-boundary data flows and suggested some avenues for future Hague Conference work.

AND THE WALLS COME TUMBLING DOWN
Data that is stored is usually thought of as data-at-rest. It is typically protected by the operating system access controls designed to permit access to only those intended and approved to access the data. Diana Kelley, of SecurityCurve, explains that the myth of the "trusted insider" assumed that internal users could always be trusted.

According to Kelley, while this model was a bit dubious even in the 90s, it is clearly no longer viable in the current reality of de-perimeterization. De-perimeterization refers to the fact that single gateway perimeters do not adequately protect data that is shared and transmitted by an organization in today's IT architecture.

Data in motion is data that is moving across the network. Such data is typically very vulnerable before it leaves and is vulnerable when it arrives. Destination systems are different operating system with different access controls and do not have the same protection for the data as the originating system.

> The theory predicts that regulation is actually lowering the bar for security rather than raising it

Kelley states that placing security into applications emerged as an interim model when the perimeters began breaking down, but it does not adequately address the total data security problem. She concludes that there is no simple "inside" and "outside" – there are, in fact, many complex zones.

Recent research published by IDC claims that only two-thirds of EMEA manufacturers are confident that their data is protected from external and internal attacks. And, of the security threats faced by manufacturers, the greatest is employee error or accidental loss of sensitive information.

A MAJOR SHIFT IN TRENDS
As IT environments evolve and the plethora of data is unleashed, the methods of security responses shift in light of the changes. Here's a quick review of how popular trends are reacting to a decade of transformation.

Trend: Perimeter Security
The true realization with protecting data is that the perimeter is almost meaningless. That is not to say that perimeter security is no longer needed, but insider threats are real and growing. The perimeter is no longer thought of as a safe place, because close to 50% of recent security breaches have been insider attacks, not someone breaching the perimeter. Thus, insider attack threat vectors are moving security professionals toward a data-centric approach to protecting data.

Trend: Device-centric Security
Data in motion is converting device-centric security more towards data-centric security. Device-centric security

can safeguard the data while it is on the device, but once the data leaves, the device that was protecting it can no longer do so.

The trend away from device-centric security was accelerated with the growth of virtualization and cloud. As a result, it is much less about the device protection and more about the data, and how to provide data-centric protection without device dependency.

Trend: Transport Layer Security
Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. TLS ensures that no third party may eavesdrop or tamper with any message. However, protecting data-in-transit via 128-bit SSL encryption only provides security during transit not at its origin or destination.

BEYOND BASIC COMPLIANCE IS BEST
There is a common myth that regulation and compliance, such as PCI and Basil II, benefits data security. In other words, thanks to these mandates data is more secure …where it otherwise would not be. In reality, it quite possibly could make some organizations much less secure.

How could a regulation that defines how data should be more secure, and companies that comply with this regulation, be less secure? The theory predicts that regulation is actually lowering the bar for security rather than raising it. Since the regulation only focuses on the minimum amount of security required to enforce the regulation across all companies, it in fact, promotes the lowest common denominator.

There are organizations that were in compliance of a regulation but still suffered a security breach

Organizations in compliance often believe that they are also secure. Not true, it only means that they are following the regulation. *Compliance* and *security* are not synonyms.

Compliance with any standard does not equate to an assessment whereby a company's security is automatically appropriate. Standards do not necessarily commensurate with the size and complexity of the business environment or the type, and amount of data involved. It is highly recommended that security measures go well beyond the well intended parameters of required mandates.

REAL REASONS WHY
There are numerous examples of organizations that were in compliance of a regulation but still suffered a security breach.

The most notable example, Heartland Payment Systems--found to be in PCI compliance yet lost millions of credit card data records because they were not secure. Deemed the largest credit card crime of all time, hackers had broken into the computers used to process about 100 million transactions each month for 175,000 merchants. Card issuers flagged suspicious transactions which revealed a masterminded scheme underway to steal more than 130 million credit and debit card numbers as well as personally identifying information (PII). Heartland has paid out millions to settle claims over the breach.

If organizations fear the auditor more than they fear the bad guys, then they are NOT secure. Worse yet, the bad guys know the regulations, and the vulnerable areas not covered by regulation and that's where you might lack necessary attention.

Failure to protect information can also allow unsophisticated, yet successful access to sensitive information. Newswire reports state that a history student-turned-hacker penetrated the company responsible for publishing the Netherlands government's budget, accessed the secret unreleased 2012 budget and tweeted out the details on Twitter.

In other news following the wake of last year's security breaches at the government-sanctioned DigiNotar certificate authority, Dutch Security Minister Ivo Opstelten recently opened

a national cybersecurity center. The Hague center joins expertise from various governmental organizations and agencies to offer expertise, advice, aid in response to cyber threats or incidents, and support to strengthen crisis management.

Can you outrun the bear?
Because security is not Boolean, how do you know if you are secure? If regulation and compliance are not measures of whether you are secure or not, then how do you measure if your data is secure? Security is very gray, and very complicated. But, consider this simple story for some perspective:

If a boy and his friend are in the forest, and they come upon a bear, the boy does not have to run faster than the bear, he just has to run faster than his friend.

Security is analogous to the bear, to say that you are absolutely secure means that you want to be able to run faster than the bear. That could be very expensive. Ideally, your main goal is not to escape the bear, just stay faster than most organizations, those that will be overcome by the bear.

CONCEPTUALIZE THESE PARALLEL TRIANGLES

Project management triangle

Projects need to be completed and delivered under certain constraints. Traditionally, the three constraints have been referred to as the *Project Management Triangle***.** One side of the triangle cannot be changed without affecting the others and each side represents a constraint as follows:

- Time constraint - amount of time available to complete a project.
- Cost constraint - budgeted amount available for the project.
- Scope constraint - what must be completed to produce the project's end result.

Security triangle

In the context of the *Project Management Triangle*, one could describe a *Security Triangle*. The concepts and legs of the triangle are very similar. Again, each side represents a constraint so one side of the triangle cannot be changed without affecting the others. The *Security Triangle* includes a:

- Usability constraint - how useable the security will be once implemented.
- Cost constraint - the amount of money available for the task.
- Security constraint - how secure the tasks end result will be.

These are often competing, i.e., increased security typically means decreased usability and increased cost.

If an organization wants to write their own security system to protect all their sensitive data to make it as secure as possible without sacrificing usability, it would cost them a very large amount of money.

Constraints Fuel Compromise
There are the organizations that merely want to be compliant, and have less concern for real security. Those organizations fear the auditor, not the bad guy. They are the organizations that will most likely be breached and hacked, even unknowingly.

There are also organizations that want to be secure, and will spend a significant amount of money to become secure, because they fear the bad guy. They always want to be faster than the bear.

Rule #1
Encrypt data at the file-level before it leaves a trusted zone.

Then there are the organizations that fall into the middle…they are very judicious with their security spend. They want to be more secure than compliant. However, they don't want the high cost required to be faster than the bear, just faster than those that will be eaten by the bear.

TODAY'S TREND: DATA-CENTRIC SECURITY
Based on independent research by the Ponemon Institute, a 2011 multi-national survey concludes that "encryption and key management have become strategic business issues to address compliance and manage risk." Findings suggest that the importance of encryption is growing globally. There is more deployment of encryption within an overall data protection strategy and for the first time, there are more organizations with an encryption strategy than without.

One of the best ways to ensure that sensitive information is always secure, is to employ data-centric, file-level encryption that is portable across all computing platforms and

operating systems and works within a private, public or hybrid cloud computing environment.

Choose a security solution that encrypts the data at the file-level before it leaves a trusted zone. A quality data-centric solution protects data, is portable across all computing platforms and operating systems, and works within any computing environment—giving you control over your data. Used properly, data-centric encryption security prevents unauthorized access and tampering regardless of the state of your data and regardless of where the data travels.

Data-centric protection through encryption renders the data unusable to anyone that does not have the key to decrypt it. No matter whether the data is in motion or at rest, it remains protected. The owner of the decryption keys maintains complete control over the security of that data and determines access to that data. Encryption procedures can easily be integrated into the existing workflow, i.e., a procurement manager could encrypt a private customer contract before sending it to a collaborative worksite.

WHAT IS YOUR TREND?

Where are you … where will you be in ten years?

A number of important issues and trends have been explored, but only you can assess your path to success and minimized risk. Recognize that computing environments have changed drastically during the last ten years, and security requirements have shifted dramatically. A big safe, powerful wall around your data center data just won't suffice any longer. Data is on the move, and needs protection in any and every state, any time and any place. So as you contemplate your security strategies consider these questions and that huge bear fast on your tail.

Choose a security solution that encrypts the data at the file-level before it leaves a trusted zone

What type of organization are you?
Are you an organization that merely fears the auditor?
Are you an organization that always wants to run faster than the bear?
Or, are you the type of organization that is changing, improving, faster than the organizations around you so they will be overcome by the bear while you survive?

VISIE: NIEUWE VORMEN TELEWERKEN INTRODUCEREN RISICO'S

Bart Verhaar, Business Developer bij Motiv (bart.verhaar@motiv.nl)

De stortvloed aan nieuwe mobiele apparatuur bezorgt IT-beheerorganisaties aardig wat kopzorgen. Iedereen met een mooie nieuwe smartphone of tablet wil natuurlijk zijn zakelijke e-mail lezen en het liefst ook andere zakelijke taken uitvoeren. Maar een toenemend extern gebruik van bedrijfstoepassingen en -informatie betekent ook meer risico's, zo betoogt Business Developer Bart Verhaar van Motiv: "beveiliging en beheersbaarheid van alle apparatuur geschikt voor telewerken wordt nog belangrijker." Waar beheerorganisaties eerder gecontroleerd toegang konden verlenen voor thuis-pc's en zakelijke pc's op afstand, hebben ze nu moeite om met de apparatuur van deze tijd mee te gaan. Maar moeten ze dit dan? Steeds vaker zien we dat het management van organisaties deze vraag met een stevige 'Ja' beantwoordt. Sterker nog; de adoptie van mobiele apparatuur wordt veelal aangewakkerd vanuit het management.

Gecontroleerde toegang

De uitdaging om mobiele apparaten te adopteren in het bedrijfsnetwerk zit niet zozeer in het verbinden van het apparaat met het netwerk. Het zit meer in het gecontroleerd toegang verlenen van mobiele apparatuur. Je ziet dan ook steeds meer leveranciers van beveiligingsproducten hierop inspelen. Opmerkelijk is dat veel partijen een deel van de uitdaging aanpakken. Waar de ene leverancier sterk is in het beveiligen van mobiele apparatuur is de andere leverancier juist sterker in het beheren en weer een ander kan perfect voor een verbinding zorgen.

Gebruiksvriendelijkheid

Wat we ook zien, is dat gebruikers voor een groot deel van het telewerken nog steeds graag een zakelijke laptop of pc gebruiken, naast de smartphone en tablet. De gebruiksvriendelijkheid van telewerken is altijd één van de belangrijkste factoren geweest voor succesvol gebruik. Eenduidigheid is hierbij essentieel. De verwachting is dat telewerken de komende jaren steeds meer gaat lijken op werken op kantoor, en vice versa. Het is daarbij niet ondenkbaar dat organisaties in de toekomst alleen nog een internetverbinding aanbieden aan medewerkers op kantoor. De zakelijke applicaties en informatie zijn dan binnen de kantoormuren te benaderen via een vorm van telewerken. Voor de gebruiker worden de handelingen binnen en buiten de kantoormuren dan gelijk en dat is wel zo gebruiksvriendelijk. Beveiliging en beheersbaarheid van alle apparatuur geschikt voor telewerken wordt nog belangrijker, want meer extern gebruik van bedrijfstoepassingen en -informatie betekent ook meer risico's. Op deze punten moeten organisaties grip krijgen om op een veilige manier alle nieuwe vormen van telewerken te adopteren.

> De adoptie van mobiele apparatuur wordt veelal aangewakkerd vanuit het management

Mobile Device Management

De komende jaren zien we meer Mobile Device Management-oplossingen ontstaan die alle uitdagingen rondom het gebruik van mobiele apparatuur aanpakken. Hierbij ontstaat een combinatie van traditioneel telewerken met laptops en desktops en allerlei mobiele apparatuur. De kunst voor de leveranciers van deze oplossingen is om bij te blijven met alle mobiele platformen. Leveranciers gaan daarom op zoek naar oplossingen waarbij het onderliggende platform of de aanwezigheid van software, bijvoorbeeld de nieuwste Java-versie, niet meer uitmaakt. Of dit laatste lukt is de vraag, maar het zou beheerorganisaties in ieder geval enorm ontlasten en daarmee kosten besparen.

COLUMN

AGILE

In this newly launched, but soon to be regular column (that is, if the Editor likes it) we shall examine Business Attributes from the SABSA Business Attributes Taxonomy one by one, looking at them from new perspectives and especially looking for topical applications of each attribute as we meet it. In this issue we shall look at the attribute 'agile'.

This topic arose during discussions with the analyst community during briefings about the launching of the Open Group white paper on TOGAF-SABSA Integration, the one that was published last October 2011. What's that you say? You haven't read it? Well then you must go to the Open Group's home page on their web site where you'll find an item called 'Popular Downloads'. On that list is 'White Papers'. Click on it and look for white paper W117.

Now let's get back to the analyst briefings. One industry analyst in particular asked us about how this work might fit into the 'Agile' movement with regard to software development. The point is that the white paper describes how TOGAF in its next iteration (due in 2013 and currently being worked upon) will enhance its strong emphasis on Requirements Management in the ADM (architecture development method) by importing and integrating the Business Attributes Profiling method straight from SABSA. As it happens, when you look at the standard taxonomy of attributes described in the SABSA 'Blue Book' (Enterprise Security Architecture: A Business Driven Approach), 'agile' is missing from the list, although it is an obvious candidate for inclusion.

This omission emphasizes several points regarding Business Attributes Profiling. First, the method is a concept, not a recipe. The taxonomy, whilst quite extensive (more than 80 attributes) is neither definitive nor complete. It is merely a set of examples that demonstrate the concept of Business Attributes Profiling as a method. You can pick and choose standard attributes from the list, but you should make sure that you redefine each one in the specific context of your business environment, customizing each one as you go. Secondly, you will find that not all the attributes given in that standard list apply to your business – so miss them out. You will also, when you get the hang of the method, realize that you can invent new attributes that are conceptually similar to those given, but which do not appear in the standard list. That's the point – it's a framework and a method but not a recipe – not all the ingredients are specified and you can invent your own recipes to fit your business needs. SABSA is not a cookbook – more a framework that enables you to become a *chef de cuisine* that can write new cookbooks for new situations.

'Agile' in the software development world means escaping the tyranny of traditional 'waterfall' development lifecycle methods, in which the first stages are used to discover the business requirements for a new system. Once these requirements are fixed they are followed through with the rigorous sequential steps of the lifecycle until the system is accepted (by testing against the requirements) and put into live production. This all seems very logical and sensible, but experience tells us that in projects that span any substantial time period, the requirements are constantly changing. What the stakeholders said that they wanted when we started has matured, moved on, changed. Sometimes it has changed so much that the project is no longer relevant to the business need and it has to be scrapped, killed, and abandoned. The investment is wasted. Business stakeholders find that the aftertaste is rather bitter and so do the developers, since all their hard work came to nothing. That's not great for anyone's morale.

Whose fault does this turn out to be? Why, it's the software developers of course. They were not able to keep up with the changing world. Didn't they realize that nothing stands still in business? This was, after all, a 'change programme'. Which part of 'change' did they not understand?

So, now we talk of 'agile developments', in which it is expected that the requirements will change constantly. There are many 'agile' methods out there and we shall leave it you to use your favorite search engine to research them. However, one thing emerged from the analyst discussions on TOGAF-SABSA integration – that one of the most likely tools to enable agile developments, especially those for large-scale projects, is Business Attributes Profiling itself. One of the key concepts of agile development is to keep a constant dialogue going between the business stakeholders and the developers – planning small steps, delivering working components and reviewing the requirements frequently, building up investments and changing direction as the requirements evolve. The SABSA approach to Requirements Management proves its value once again.

The Attributer

HEBT U ZE OP EEN RIJTJE?

Ir. Rob van Gansewinkel CISSP is gecertificeerd TOGAF9 en werkt bij Capgemini op de vakgebieden infrastructuur en security. Hij is bereikbaar via rob.van.gansewinkel@capgemini.com.
Ir. Aaldert Hofman CISA CISSP is gecertificeerd TOGAF9 architect en werkt bij Capgemini op de vakgebieden architectuur en security. Hij is bereikbaar via aaldert.hofman@capgemini.com

Nee, wij twijfelen niet aan uw geestelijke vermogens. U weet dat informatiebeveiliging belangrijk is. Architectuur is dat ook. Maar weet u ook hoe informatiebeveiliging geadresseerd wordt in architectuurmethoden en raamwerken als TOGAF, SABSA, IAF en O-ESA? Dit artikel zet dat voor u op een rijtje.

Introductie

Het idee voor dit artikel ontstond een paar maanden geleden, naar aanleiding van een discussie tussen de auteurs over security architectuur. We constateerden dat we behoefte hadden aan een overzicht van hoe informatiebeveiliging geadresseerd wordt in de verschillende architectuurmethoden die we kennen. Uiteindelijk resulteerde dit in een presentatie voor Capgemini collega's en het resultaat delen we graag met u in dit artikel.
We veronderstellen dat de lezer voorkennis heeft zowel op het gebied van informatiebeveiliging als van architectuur. We gaan ook niet in op nut of noodzaak van security architectuur. Dat leidt af van het eigenlijke onderwerp en ligt buiten de scope van dit artikel.
In dit artikel hanteren we bewust de term security architectuur. Ten eerste is dat de term die in de literatuur van genoemde architectuurmethoden gebruikt wordt en ten tweede is een goede vertaling naar het Nederlands lastig. Discussie over terminologie is niet het doel van dit artikel.

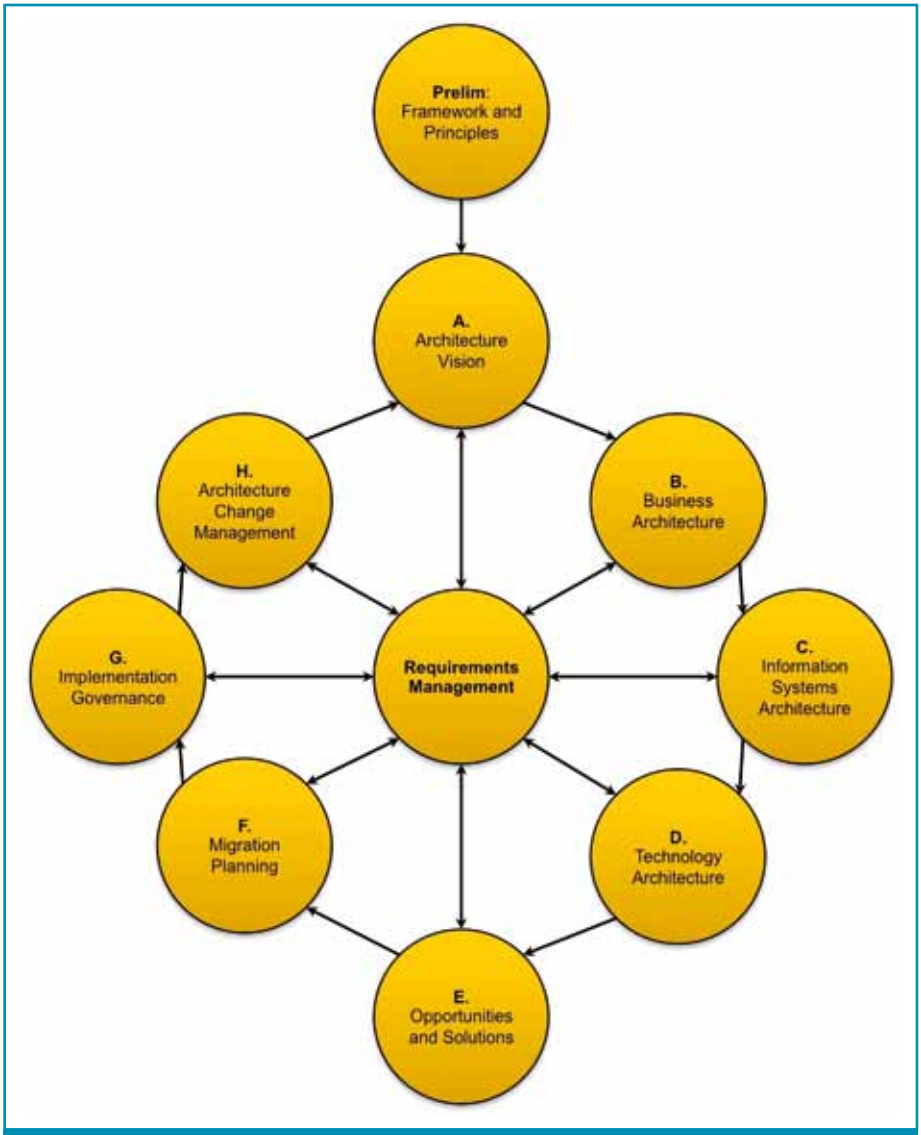
Het referentiekader

Dit artikel zet op een rijtje hoe informatiebeveiliging geadresseerd wordt in TOGAF, SABSA, IAF, Zachman en O-ESA. Dit zijn de voornaamste architectuurmethoden die wij in de praktijk gebruikt zien worden.
Om een vergelijking te kunnen maken tussen deze methoden, is het nodig om een referentiekader te hebben. Daarmee scheppen we helderheid: waar hebben we het over en op welke punten vergelijken we.
Het referentiekader baseren we op TOGAF, waarin aangegeven wordt wat verwacht mag worden van een organisatie die op een volwassen manier omgaat met architectuur. TOGAF geeft aan dat het toepassen van architectuur op een volwassen niveau een formele taxonomie voor de diversiteit aan typen van artefacten, processen en hulpmiddelen vereist. Bij hulpmiddelen dient u overigens bijvoorbeeld te denken aan software voor de ondersteuning van zowel het proces als voor het vastleggen van artefacten.
Die formele taxonomie vereist een architectuur metamodel, dat in feite de organisatiespecifieke toepassing van architectuur beschrijft. Het metamodel dient zowel een methode als een raamwerk voor het vastleggen van de inhoudelijke architectuur te bevatten. De methode beschrijft wat de manier van werken is om een architectuur te maken (kortweg de architectuurmethode). Het raamwerk beschrijft uit welke artefacten de inhoudelijke architectuur moet bestaan, wat hun onderlinge relaties zijn en hoe deze worden vastgelegd (kortweg het architectuurraamwerk).
Architectuur kan worden toegepast op verschillende niveaus in een organisatie en ook dat is een aspect om op te letten bij het kiezen van een methode. Een architectuur kan de hele organisatie beschrijven (enterprise architectuur), een deel van de organisatie (domein architectuur) of een project binnen die organisatie (project architectuur). In de regel wordt het detailniveau groter naarmate het beschouwinggebied kleiner wordt.
Komende paragrafen gaan in op TOGAF, IAF, Zachman, SABSA en O-ESA. Voor elk van deze hanteren wij hetzelfde referentiekader: hoe wordt informatiebeveiliging geadresseerd in de architectuurmethode of het architectuurraamwerk.

TOGAF

Voor TOGAF baseren wij ons op The Open Group Architecture Framework, version 9, Enterprise Edition [1]. De kern van TOGAF is de Architecture Development Method (ADM), een stapsgewijze aanpak om een enterprise architectuur te ontwikkelen (illustratie 1). In TOGAF is er ook het Architecture Content Framework, een gestructureerd metamodel voor architectuur artefacten. TOGAF biedt dus zowel een architectuurraamwerk als een architectuurmethode, voornamelijk gericht op enterprise architectuur, hoewel projectarchitectuur ook mogelijk is. TOGAF biedt ook de ruimte om specifieke technieken of aanvullende aspecten op te nemen in methode of raamwerk.

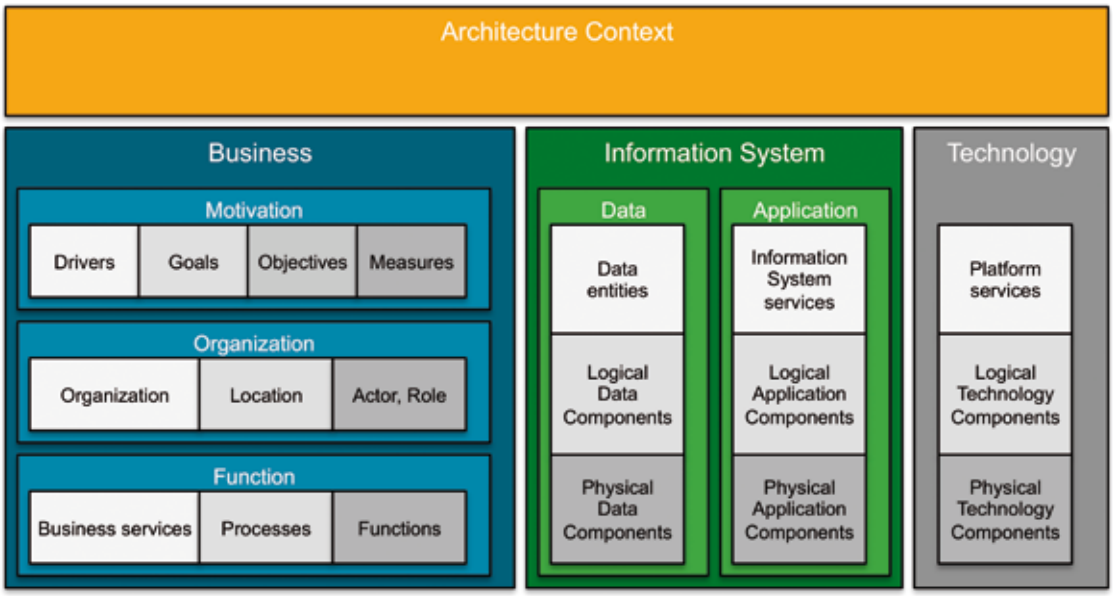
TOGAF9 adresseert zowel Business architectuur, Information Systems (Data & Applicaties) architectuur als Technology architectuur. Security architectuur komt nauwelijks aan de orde. De beschrijving van de ADM methode noemt het woord "security" slechts vier



Figuur 1 - TOGAF

keer in 160 pagina's. Hoofdstuk 21 is weliswaar getiteld "Security Architecture and the ADM", maar stelt vervolgens letterlijk dat dit hoofdstuk "is not intended to be a security architecture development methodology". Het doel van dat hoofdstuk is: "it is intended to inform the enterprise architect of what the security architect will need to carry out their security architecture work".

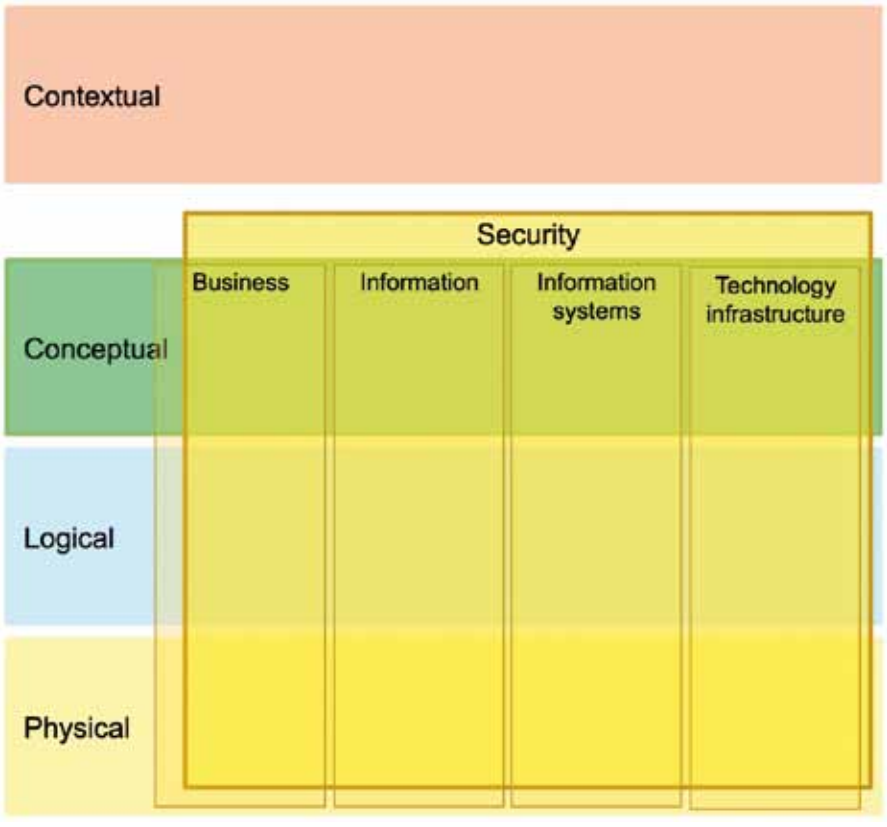
Het architectuurraamwerk van TOGAF (de Architecture Repository) biedt een formele structuur om het resultaat, de producten van de architectuur te plaatsen (illustratie 2, licht vereenvoudigde weergave). Daarin zijn geen specifieke security architectuur producten opgenomen, maar er zijn wel veel architectuur producten bruikbaar voor security architectuur (bijvoorbeeld Actor, Role, Data Entities). Het raamwerk onderkent een breed scala aan views, met daarin de Data Security View. Dat is helaas de enige specifieke security view.
Toch is het eerder genoemde hoofdstuk 21 zeer bruikbaar als het gaat om te komen tot zinvolle input voor de security architectuur. Zo wordt voor elke ADM fase expliciet gedefinieerd wat de security input en output dient



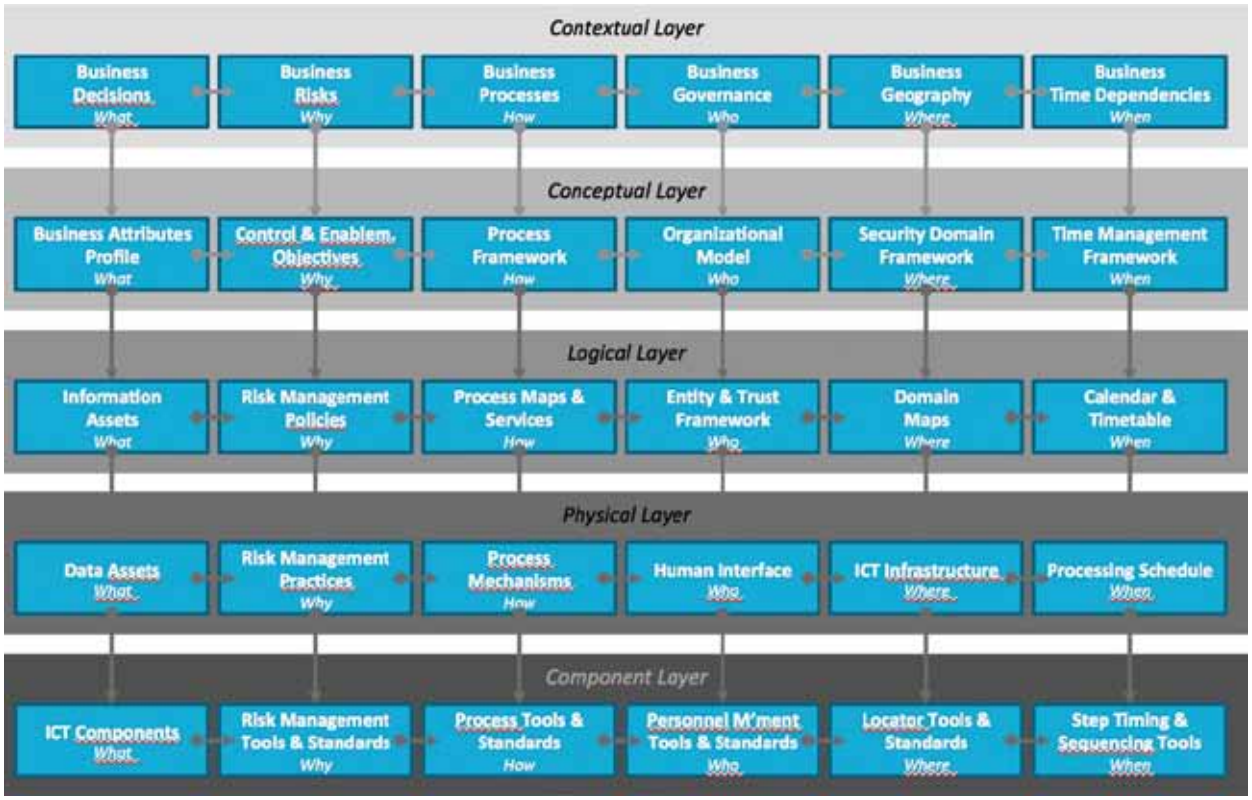
Figuur 2 – TOGAF Architecture Content Framework

te zijn, waarbij ook de activiteiten worden beschreven die nodig zijn om die input aan de security architect te kunnen leveren!
Ondanks hoofdstuk 21 herbergen zowel de methode als het raamwerk in TOGAF het risico dat security aangebouwd in plaats van ingebouwd wordt. Dat wordt het beste geïllustreerd door hoofdstuk 21: security is niet geïntegreerd in de overige hoofdstukken, maar heeft een afzonderlijk hoofdstuk gekregen. Een mooi begin, maar we zijn er nog niet.
In dit kader is het relevant te melden dat in oktober 2011 een "TOGAF-SABSA Integration white paper" is verschenen. Dave Hornford (Voorzitter van Open Group Architectuur Forum) heeft in de Open Group conferentie in San Francisco (januari 2012) toegelicht hoe het Architectuur Forum van plan is om deze publicatie te integreren in TOGAF.

Integrated Architecture Framework
Voor IAF baseren wij ons op het Integrated Architecture Framework, versie 4.5 [2]. IAF is wat de naam al zegt, een architectuurraamwerk, geïntegreerd over de architectuurdomeinen Business, Informatie, Informatiesystemen (IS) en Technology Infrastructure (TI) (illustratie 3). IAF beschrijft geen architectuurmethode, al wordt wel summier geadresseerd op welke wijze de architect welke onderdelen van het raamwerk kan toepassen, afhankelijk van de context van de opdracht. Het IAF raamwerk kan gebruikt worden voor enterprise architectuur, domeinarchitectuur en voor projectarchitectuur. Security is volledig geïntegreerd in de artefacten in het IAF raamwerk, heel concreet doordat security is opgenomen in de template van elk artefact. Dat gebeurt door per artefact de classificatie op te nemen voor Confidentiality, Integrity en Availability. Naast de artefacten waarin security geïntegreerd is, onderkent IAF meerdere specifieke Security views, maar geen specifieke Security Architectuur artefacten.
In de artefacten voor Business en Informatie architectuur specificeert de hiervoor genoemde classificatie in feite het niveau aan security dat voor dat specifieke artefact vereist is. In de artefacten voor IS en TI specificeert de classificatie juist het niveau aan security dat door dat specifieke artefact geboden wordt. Daarmee wordt nadrukkelijk de Demand (vanuit Business en Informatie) en Supply (vanuit IS en TI) in kaart gebracht. Kruistabellen zorgen voor de afstemming tussen wat gevraagd wordt en wat geboden wordt, waarmee traceerbaarheid van de vereiste requirements naar de geboden oplossing vastgelegd wordt.
Op basis van bovenstaande is de conclusie gerechtvaardigd dat het niet mogelijk is om met IAF een Business of Informatiearchitectuur te specificeren zonder daarbij nadrukkelijk de security requirements te benoemen. Op basis van die requirements kan de volledige geïntegreerde security architectuur opgesteld worden, bestaande uit IS en TI componenten waarbij traceerbaarheid naar requirements geborgd is.
Aan de andere kant biedt het raam-



Figuur 3 – Integrated Architecture Framework



Figuur 4 – SABSA Matrix

werk ook de mogelijkheid om een IS en TI security architectuur te specificeren onafhankelijk van specifieke business requirements, maar waarvan wel duidelijk is welk niveau van security geboden wordt. Een soort security baseline.

Zachman

Het Zachman Enterprise Architecture Framework is een bekend raamwerk, hoewel er weinig materiaal publiek beschikbaar is [3]. Het is een architectuurraamwerk waarin architectuur in de aspecten Data, Function, Network, People, Time en Motivation wordt beschreven. Zachman bevat geen architectuurmethode. Het Zachman raamwerk kent ook geen expliciete adressering van Security Architectuur. Zachman kan toegepast worden voor enterprise architectuur, domeinarchitectuur of voor projectarchitectuur.
Het Zachman raamwerk definieert wel een aantal artefacten die bruikbare informatie verzamelen en beschikbaar stellen voor security architecten. Die artefacten bevinden zich vooral in aspecten Data, Function en Network. De rijen in het Zachman raamwerk bieden verschillende perspectieven. In het bijzonder de perspectieven vanuit de Planner (Scope, Contextual), vanuit de Owner (Enterprise Model, Conceptual) en vanuit de Designer (System Model, Logical) bieden bruikbare inzichten voor de security architectuur.

SABSA

Voor SABSA baseren wij ons op het welbekende blauwe boek Enterprise Security Architecture waarin Sherwoods Applied Business Security Architecture (SABSA) beschreven staat [4]. SABSA is ontstaan in Engeland en de laatste jaren ook sterk in Nederland in opkomst. SABSA biedt een architectuurraamwerk (illustratie 4) en lijkt sterk geïnspireerd door het Zachman raamwerk. Naast het raamwerk, stelt SABSA nadrukkelijk een "business driven approach" te zijn. Hoofdstuk 7 adresseert een methode om SABSA als een praktische gids te gebruiken, maar het voert te ver om dat als een doorwrochte architectuurmethode te beschouwen.
In SABSA ligt een sterke nadruk op het vaststellen van de security requirements, waarvoor het artefact "business attribute profile"wordt gehanteerd. Daarmee wordt de link naar de business requirements en ook naar information risk management gelegd. Het SABSA raamwerk benoemt expliciet de artefacten van de security architectuur, maar beschrijft niet de artefacten van de Business, Data, Applicatie of Technology architectuur.
De kracht van SABSA ligt in het uitgebreide security architectuurraamwerk met daarin veel specifieke security artefacten. Daarmee is SABSA prima geschikt om een security domein of projectarchitectuur op te stellen. Een nadrukkelijk risico is dat het lastig is om de security architectuur te integreren met Business, Data, Applicatie of Technology architectuur, vooral ook doordat SABSA enkele termen (bijvoorbeeld het begrip "services") op een an-

dere manier hanteert dan bijvoorbeeld TOGAF of IAF. Dat kan tot miscommunicatie leiden.
Zoals bij de bespreking van TOGAF al gememoreerd, is in oktober 2011 door de Open Group een white paper gepubliceerd over hoe TOGAF en SABSA elkaar aanvullen. Een interessante ontwikkeling die zeker de moeite waard is om te monitoren.

O-ESA

Voor O-ESA baseren wij ons op de Open Enterprise Security Architecture (O-ESA) zoals door de Open Group gepubliceerd in 2011, als een opvolger voor de NAC 2004 ESA Guide [5]. Hoewel de naam anders doet vermoeden, biedt O-ESA geen architectuurmethode of architectuurraamwerk. O-ESA biedt wel een enterprise security program framework en template voor een policy-driven security.
Het O-ESA raamwerk positioneert wel een Security Technology Architecture, met daarin een expliciet uitgewerkte Identity Management Architectuur en een Border Protection Architecture. Deze architecturen zijn niet te vergelijken met de architectuurraamwerken die hiervoor besproken zijn; de O-ESA architecturen zijn eerder te beschouwen als blauwdrukken. O-ESA is een relatief nieuwe ontwikkeling die zich in de praktijk nog moet bewijzen, daarom kunnen we nog geen uitspraken over de bruikbaarheid doen.

Conclusies

Tabel 1 geeft een samenvattend overzicht van het voorgaande, waarbij wij aangeven hoe de verschillende methoden of raamwerken scoren op de aspecten van methode, raamwerk en de integratie van security. Alle methoden en raamwerken hebben hun specifieke voordelen en nadelen.
Het overzicht maakt ook duidelijk dat er geen eenduidig antwoord is op de voor de hand liggende vraag: wat is de beste architectuurmethode of architectuurraamwerk om te selecteren voor security architectuur?

	Architectuurmethode	Architectuurraamwerk	Security geïntegreerd?
TOGAF9	Ja	Ja	Nee
IAF	Nee	Ja	Ja
OESA	Nee	Beperkt	Ja
Zachman	Nee	Ja	Nee
SABSA	Beperkt	Ja	Focus

Tabel 1 - Architecture methods and content frameworks recap

Kijken we echter met meer nuance naar het overzicht, dan durven we wel enkele voorzichtige conclusies te trekken. Met nadruk 'voorzichtig', omdat we niet uit het oog mogen verliezen dat een opdrachtspecifieke context van de te maken security architectuur erg belangrijk is en niet in het overzicht opgenomen kan worden.
Een eerste conclusie: om een veilige architectuur (bijvoorbeeld een veilig project) te leveren is het meest belangrijke om een methode en raamwerk te gebruiken waar security volledig is geïntegreerd met alle andere architectuurdomeinen in het project. In deze context is bijvoorbeeld IAF goed te gebruiken.
Een tweede conclusie: om een gemeenschappelijk fundament aan security te leveren is het meest belangrijke om een raamwerk te kiezen met focus op een uitgebreide set aan security componenten. In dat geval is SABSA goed te gebruiken.
Maar zoals eerder genoemd, is de opdrachtspecifieke context ook zeker van belang. Die context kan bestaan uit organisatiespecifieke standaarden zoals de eerder genoemde organisatiespecifieke taxonomie voor architectuur. Vergeet ook niet dat het resultaat, de security architectuur, moet passen in de architectuurbeschrijvingen die al in de organisatie aanwezig zijn.
Dan is er ook nog de persoonlijke ervaring en voorkeur van de architect zelf. Natuurlijk dient de architect zich te conformeren aan een vastgestelde methode en raamwerk, maar binnen die kaders kan en zal de architect zijn ervaring en voorkeur hebben. Als een raamwerk gebruikt wordt zonder bijbehorende methode is de kennis en ervaring van de architect zelfs cruciaal om tot een coherent resultaat te komen.

Afsluitend

Dit artikel heeft u een overzicht gegeven van de wijze waarop security architectuur geadresseerd wordt in TOGAF, IAF, SABSA, Zachman en O-ESA. We hebben laten zien dat security architectuur op verschillende manieren in architectuurmethoden en raamwerken wordt geadresseerd. De conclusie is dat er geen eenduidig antwoord is te geven op wat de beste aanpak is zonder de specifieke context te kennen. Om maar te besluiten met een oude architectuurwijsheid: "it depends!".
Dan nog dit: wellicht is het u opgevallen, maar in dit artikel hebben wij geen omschrijving gegeven van wat volgens ons een security architectuur is, of welke typen security architectuur wij onderkennen. Voor het doel van dit artikel was dat niet nodig; mogelijk werken wij dat nog uit in een volgend artikel. Wilt u daar niet op wachten, neem dan contact op met ons.

Referenties

[1] *TOGAF Version 9, The Open Group, 2009, ISBN 978-90-8753-230-7*

[2] *The Integrated Architecture Framework Explained, Van 't Wout et al., 2010, ISBN 978-3-642-11517-2*

[3] *Informatie over het Zachman Framework kan gevonden worden op het internet, bijvoorbeeld via Wikipedia.*

[4] *Enterprise Security Architecture, Sherwood et al., 2005, ISBN 978-1-57820-318-5*

[5] *Open Enterprise Security Architecture (O-ESA), The Open Group, 2011, ISBN 978-90-8753-672-5*

BEKENDMAKING ARTIKEL VAN HET JAAR

Op 26 april vond de bekendmaking plaats van de winnaars van het artikel van het jaar. In het tijdvak tussen de algemene ledenvergadering van het PvIB en het avondprogramma maakte Kees Hintzbergen de uitslag bekend. Helaas waren geen van de winnaars aanwezig om de prijs direct in ontvangst te nemen. Inmiddels hebben wel alle winnaars hun bonnen ontvangen.

Foto's: Lex Borger

JURY RAPPORT ARTIKEL VAN HET JAAR 2011 VAN HET BLAD INFORMATIEBEVEILIGING

Namens de jury, Leo van Koppen

De jury heeft zich, alweer voor de vierde keer, gebogen en uitgesproken over de verkiezing van het artikel van het jaar.

Even voor uw herinnering een opsomming van de voorgaande winnaars:

2008	**Wolter Pieters**	**met**	***De monsterlijke trekjes van beveiligingsproblemen***
2009	**Said El Aoufi**	**met**	***De rol van audits (in beveiliging en architectuur raamwerken)***
2010	**Jan de Boer**	**met**	***De misleider te werk***

De jury is inmiddels ververst, John Rudolph heeft zijn plaats overgedragen aan Remco Bakker, maar continuïteit en ervaring is behouden in de personen van Kees Hintzbergen en ondergetekende Leo van Koppen.

Van hoofredacteur Lex Borger kregen wij dit keer in eerste instantie het verzoek om alle artikelen van 2011 mee te nemen in de beoordeling. Na enige onderhandeling was de redactie bereid om alsnog een lijst van negen genomineerden op te stellen. Op basis van deze shortlist en een enigszins aangepaste set van criteria is de jury aan de slag gegaan. Onafhankelijk van elkaar hebben we een oordeel opgesteld en dat vervolgens bediscussieerd, om vervolgens te komen tot een top drie.
Ook dit jaar weer een redelijke diversiteit in het aanbod. Divers in themakeuze, benadering ervan, maar ook in schrijfstijl en originaliteit. Zelf was ik wederom verbaasd dat je, onafhankelijk van elkaar, opvallend unaniem bent in het kiezen van een top 5. Hierbij de resultaten.

Op de 3e plaats is geëindigd het artikel *Facebook volgt iedere internetgebruiker: like this*! van Arnold Roosendaal.
Dit artikel moet zowel de voor- als tegenstanders van Facebook aanspreken en dat is op dit moment zo ongeveer iedereen. Geschreven dus voor een zeer grote doelgroep en het verdient daarom ook een publicatie in andere tijdschrift dan het lijfblad van informatiebeveiligers. Het geeft een scherp beeld van de slimme technieken die Facebook inzet om de dominante hegemonie uit te breiden c.q. te behouden. Voordat je er erg in hebt "ben je lid van de club"!
Het leest als een thriller, want langzaamaan sluit het net zich om het slachtoffer, facebookgebruiker of niet!
Het artikel voldoet naar de mening van de jury aan alle criteria van een opiniërende artikel, is daarbij goed geschreven in een vlot leesbare stijl.
De essentie van het artikel, de slimme technieken van Facebook, was ook voor de meeste juryleden een eyeopener. Wellicht dat details van de slimme technieken sommige lezers te ver gaan. Dat aspect maakt dat het artikel net niet tot de eerste plaats reikte.
Samenvattend een goed leesbaar artikel voor een breed publiek met een hoge actualiteitswaarde.

Op de 2e plaats is geëindigd het artikel *De volgende stap in applicatiebeveiligingsonderzoeken* van Michiel van Veen
Applicatiebeveiliging is de achilleshiel van IT-beveiliging en mede daarom verdient dit artikel alle waardering en is een must read voor alle software engineers. Ook dit artikel verdient om die reden een veel breder publiek. Publiceren in andere bladen en media is dan ook een warme aanbeveling van de jury. Security incidenten die zo ongeveer wekelijks worden uitgemeten in de diverse media tonen telkens opnieuw aan dat veel beveiliggingslekken terug te voeren zijn tot enorme kwetsbaarheden in de applicaties. Dat heeft alles te maken te weinig controle, een te lage prioriteit en het ontbreken van harde eisen vanuit certificering of wetgeving. Kortom hier zijn meerdere instanties debet aan, waaronder tot mijn spijt, ook nog steeds

het hedendaagse informatica onderwijs. Het artikel voldoet naar de mening van de jury aan alle criteria van een goed leesbaar artikel , met een uitstekend opbouw en heldere modellen. Het brengt de applicatiebeveiliging daarmee naar een hoger niveau en is een must read voor software engineers.
Samenvattend een goed leesbaar artikel, weliswaar voor een selectief publiek, maar met een hoge actualiteitswaarde en dat ook iets extra toevoegt aan de bestaande opvattingen over applicatiebeveiliging.

Op de 1e plaats, en daarmee de winnaar van 2011, is geëindigd het artikel *Succesvolle integriteitsbeheersing door beïnvloeden menselijk handelen* van Peter Schimmel
Het is een zeer boeiend artikel over een essentieel aspect van het vakgebied, namelijk de integriteit van mensen. Dit artikel zal eveneens een breed publiek aanspreken. Ondanks verwijzing naar psalmen (of juist daarom, dat is me even ontgaan in de discussie) een zeer geloofwaardig artikel. Vertrouwen, integriteit en moreel besef zijn de sleutelwoorden bij informatiebeveiliging, het artikel stelt dit allemaal aan de orde. Nieuwe invalshoeken worden getoond en uitstekend uitgewerkt. Daarmee is het in essentie toepasbaar in een breed scala van organisaties en functies. Goed geschreven, leesbaar voor een grote doelgroep en zeer vernieuwend. Daarmee een terechte winnaar van het artikel van het jaar.
Samenvattend een, naar de mening van de jury, een uitstekend artikel geschikt voor een breed publiek en het geeft de lezer veel nieuwe gezichtspunten op principiële aspecten van het vakgebied, integriteit van mensen en organisaties. De terechte winnaar.

Dit jaar geen aanmoedigingsprijs en helaas ook geen vrouwelijke auteurs. Hopelijk is dit eenmalig. De oorzaak van dit feit is ons geheel onduidelijk, maar zien we wel als een verschraling van het aanbod. Overall kan je zeggen dat de artikelen stuk voor stuk zeer serieus van aard zijn en of dat komt omdat vrouwelijke auteurs ontbraken bij de genomineerden? Het blijft voor ons nog even duister. Wellicht kan een goed gesprek met de hoofdredacteur helpen voor een andere shortlist volgend jaar en daarnaast bij deze een oproep aan de vrouwelijke auteurs (in spe) onder u.
Ondanks deze kritische slotnoot deden we het weer met genoegen.

IN MEMORIAM: PAUL OVERBEEK

Op 9 mei jl. is Paul Overbeek volkomen onverwacht overleden. Hiermee is ons een groot informatiebeveiliger veel te vroeg ontvallen. Wat moet je zeggen over iemand die nog volop in het leven stond? Één aspect dat bij mij meteen naar boven komt als ik aan Paul denk, is zijn bereidheid om zijn kennis met anderen te delen. Altijd en overal. En speciaal was ook de manier waarop hij dat deed, hij gaf je het gevoel dat je zelf op het idee was gekomen. Dát is de ultieme leermeester.
Ook was Paul een veelgevraagd spreker en dagvoorzitter bij allerhande congressen en seminars. Wat ons naast zijn kennis rondom het vakgebied ook zal bijblijven is zijn grote gevoel voor humor waarmee hij zijn presentaties en optredens verluchtigde. Hij kon als weinigen relativeren en ons daarmee aanzetten tot nadenken.

Zo'n eigenschap is een grote gave. Paul was een meervoudig auteur in Informatiebeveiliging, en schreef ook (mee) aan andere publicaties voor het PvIB. In 2008 schreef hij een Questafette column over Iebeetopia, die ik nog regelmatig geciteerd zie. Als Paul schreef, dan klonk de echo ervan nog lang door.
Voor de informatiebeveiligingsprofessionals die hem gekend hebben, zal Paul altijd in gedachten bij hen zijn. Voor de komende generatie: profiteer van de kennis die hij aan geduldige media heeft toevertrouwd. En aan allen: Paul heeft jaren onzelfzuchtig zijn kennis gedeeld. Het is aan ons om kennis te blijven delen. Terugbetalen kunnen we niet, vooruitkijken wel...
Paul, bedankt voor alles wat je aan informatiebeveiliging gegeven hebt.

Namens de hele redactie,
Lex Borger

ACHTER HET NIEUWS

Het thema van dit jubileumnummer is *Vertrouwen*. Onze redacteuren mogen daar in de rubriek Achter het Nieuws hun zegje over doen. Maar niet nadat we hen enigszins voorzien van de nodige munitie. Want het onderwerp vertrouwen is natuurlijk te breed voor een eenvoudige beschouwing. Nee, om onze redacteuren iets beter uit te dagen, zullen we het thema meer expliciet moeten inkaderen en wat kunnen we dan beter doen dan het thema vertrouwen in een eenvoudig model te plaatsen:

	Bewust	*Onbewust*
Vertrouwen		
Wantrouwen		

Dit model bestond voor deze uitgave nog niet, dus we zijn benieuwd wanneer we het, gelardeerd met de kennis en ervaring van onze redacteuren voor het eerst elders gepresenteerd zien worden. Veel leesplezier!

Reactie Ronald van Erven:

	Bewust	*Onbewust*
Vertrouwen	Bewezen door eigen ervaring en daardoor eigen meningsvorming.	Ingesleten door jarenlange omgang en patronen - dit is de automatische piloot – dit krijg je mee van je ouders en slijt er in door wat je op scholen / opleidingen leert of wat in jou ogen de "experts"zijn en wat zij zeggen. (het gevaar van papagaaien & de "selffulfilling phrophecy") In ons vakgebied, of zelfs binnen de PvIB zie je dit verschijnsel ook. Je ziet heel vaak dezelfde mensen met dezelfde kapstokken iets vertellen of schrijven. En als je het maar vaak genoeg vertelt ga je als PvIB lid (lees: de klant) al gauw mee. De meeste leden gaan ervan uit dat wat deze experts vertellen klopt. Terwijl het ook propaganda kan zijn om "iets"(een methodiek / zichzelf) te promoten. Zeker als je ziet dat de meeste experts "consultant" zijn die 2 boodschappen brengen (vakinhoudelijk & zelfpromotie) en niet bij een eind-gebruikers-rol / klant werken is een gezond wantrouwen op zijn plaats.
Wantrouwen	Bewezen door eigen ervaring en daardoor meningsvorming.	Ontwikkelen Intuitie - Ingesleten door jarenlange omgang en patronen - automatische piloot – dit krijg je mee van je ouders en slijt er in door wat je op scholen leert. of wat in jou ogen de "experts"zijn en wat zij zeggen. (het gevaar van papagaaien & selffulfilling phrophecy) Door bepaalde triggers kan dit opeens naar bewust overslaan en kan het wantrouwen ongegrond blijken. (dan ben je bewust gemaakt) Gelukkig voor ons nuchtere Nederlanders kijken we eerst de kat uit de boom en willen we vooral bewijzen zien. Echter in andere culturen wordt er minder gekeken maar meer hoe een en ander gezegd word. Dit wordt al vanaf de lagere school getraind en intuïtief ontwikkeld. Kortom, de mate van onbewust vertrouwen en wantrouwen hangt af van de gevoeligheid van de persoon en cultuur.

Lex Dunn

Een nieuw model vraagt natuurlijk om invulling vanuit de praktijk, dus hierbij een poging mijnerzijds om met voorbeelden de matrix te vullen.

Onbewust wantrouwen: dit zit ingebakken in de menselijke soort als overblijfsel van ons leven in de fysieke wildernis. Alles, wat we niet kennen, vertrouwen we niet. Da's de meest optimale strategie om te overleven in een wereld van sabeltandtijgers en giftige bessen. Het is vermoedelijk ook onze "default" (maar ik ben geen psycholoog), die komt aardig overeen met het gezegde "de kat uit de boom kijken". Jammer genoeg lijkt het niet onze standaard instelling te zijn in de digitale wereld!

Bewust wantrouwen: dit is de toestand die we als securologen met al onze security awareness campagnes proberen te bereiken: niet op executable files klikken, geen emails openen van onbekenden, niet op links in emails klikken ….. en ga zo maar door. Maar het blijft natuurlijk jammer dat we op een negatief sentiment als wantrouwen sturen.

Onbewust vertrouwen: ook dit kennen we. Als je iets koopt in de supermarkt ga je er van uit dat het te eten is, en dat anderen er voor gezorgd hebben dat dit gecontroleerd wordt. Ik persoonlijk ken maar weinig mensen die een volledige chemische analyse uitvoeren van wat ze op hun bord krijgen ;-)

Bewust vertrouwen: in tegenstelling tot de variant inzake "bekwaamheid/onbekwaamheid" (waarbij het doel is te komen tot "ONBEWUST bekwaam" willen we in dit model nu juist aankomen in het kwadrant "BEWUST vertrouwen". Vertrouwen is goed, maar je moet wel weten WAAROM je iets vertrouwt. Daarom moet je er altijd over nadenken, en is dit (in mijn optiek) de ideale eindtoestand.

André Koot

Vertrouw het model

Wij zijn natuurlijk dol op modellen. Modellen verklaren en modellen helpen ons om richting te geven. En dit is nou typisch zo'n model waar we de komende jaren heel blij mee gaan worden. De opzet van dit model lijkt heel erg op dat van het leermodel dat op de assen bewustheid en bekwaamheid hanteert. Dat model laat zien dat er niet zo iets als een status quo als het gaat om ontwikkeling. Als je denkt dat je er bent, als je dus na heel veel leren en trainen Onbewust Bekwaam bent, volgt onherroepelijk Onbewust Onbekwaam. En dat gaat allemaal om jezelf. In het nieuwe model wordt dat helemaal geprojecteerd op jouw beeld van je omgeving. En het spannende aan dit model is dat ook daar de cyclus lijkt te worden aangegeven, het model toont daarmee aan dat ook vertrouwen niet een permanente status is, maar dat ook vertrouwen fluctueert.

Het model zegt in eerste niets over de externe partijen die jou vertrouwen. Vertrouwen is eenrichtingsverkeer. Maar wat het model ons wel leert, is dat we dus wel op moeten passen voor het doorlopen van deze cyclus door de partijen die òns vertrouwen. We moeten op onze hoede zijn om te voorkomen, of om in ieder geval tijdig vast te kunnen stellen, dat onze externe partner het vertrouwen in ons verliest. De mate van vertrouwen in ons wordt daarmee een kritische succesfactor van jewelste. En aangezien vertrouwen een eenrichtingsweg is, kunnen we de ander niet zomaar ertoe bewegen om ons te vertrouwen, maar moeten we dat vertrouwen constant waarmaken en moeten we dus constant bewijzen dat we betrouwbaar zijn, ook al zien we daar niet direct iets van terug, immers zolang de ander ons bewust of onbewust vertrouwt, is er een goede relatie. Levensgevaarlijk om die statuswijziging dus onopgemerkt te laten. Misschien moeten we het model dus ook zodanig inkleuren dat er ook een tegengestelde beweging mogelijk wordt: van onbewust vertrouwen naar bewust vertrouwen. En dat kan heel makkelijk, want onze uitdager heeft helemaal geen pijltjes in het model getekend...

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 Domus Technica),
e-mail: lex.borger@domustechnica.com
Motivation Office Support bv, Nijkerk (eindredactie)
e-mail: ibmagazine@pvib.nl

Redactieraad
Tom Bakker
Lex Dunn (Capgemini)
Ronald van Erven (GBF)
Maarten Hartsuijker (ANWB)
Aart Jochem (GOVCERT.NL)
André Koot (i3advies)
Rachel Marbus (KPMG, IT Advisory)
Gerrit Post (G & I Beheer BV)

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 2012
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

SNOEP VERSTANDIG, EET EEN APPEL

Ik stond laatst bij het koffieapparaat op ons hoofdkantoor toen ik werd aangesproken door mijn baas. De vraag was kort en simpel, er moet een nieuwe model telefoon worden uitgezocht die bij de standaarduitrusting van onze medewerkers gaat behoren, en of ik daar iets van vond. Mij kennende wist ze dat ik daar wel iets van vind en thuisgekomen maar eens aan het zoeken geweest op internet. De eerste marktsituatie plaatjes waren duidelijk. Ik hoef me maar op 2 types te richten. De Symbian (besturingssysteem van de Nokia) is eigenlijk helemaal weg, de BlackBerry is in een neerwaartse spiraal terecht gekomen en verliest dagelijks veel terrein. Microsoft heeft wel een aantal pogingen gedaan om de markt van de smartphones binnen te dringen maar dat is tot op heden niet gelukt. Het samenwerkingsverband met Nokia lijkt een goede keus maar deze toestellen zijn al aangeduid als toestellen voor consumenten en zullen niet geschikt zijn voor de zakelijke markt. Ik geloof Microsoft niet vaak maar in dit geval twijfel ik niet aan hun woorden. Dan blijven er eigenlijk maar 2 types over en dat zijn de Android telefoons en de IOS telefoons. Ik bestudeer een markt penetratie tabel en zie tot mijn verbazing dat Android wel heel erg veel verkocht wordt. Bijna vergelijkbaar met de iPhone maar tegelijkertijd zie ik dat de verkoopcijfers van de IOS telefoons zijn uitgesplitst in iPhones, iPads en zelfs iPods, maar even verder zoeken maar ik zie nergens de verkoopaantallen van de Android telefoons, altijd zijn deze gecombineerd met de tabletverkopen. Ik besluit maar eens mijn netwerk te bellen en kom erachter dat een Android tablet niet te onderscheiden is van een Android telefoon.

Een telefoon is wel leuk maar de apps zijn veel leuker en daar zit wel een groot verschil tussen de IOS en Android machines. Apple heeft in zijn app store ontelbaar veel apps staan en Google in de Android Market veel minder. Maar het verschil is dat Android nogal wat andere markets heeft. De officiële en de vele markets in Azië waar je de meest fraaie apps kunt krijgen, die echter op geen enkele manier gecontroleerd zijn en waar de malware welig tiert, er is op dat punt geen enkele controle. De grote diversiteit in Android versies en de wijzigingen die telefoonfabrikanten op het Operating system maken om het toestel een eigen touch te geven maakt het beheer van deze toestellen wel heel erg lastig. Android 2.3 (om één van de vele versies te noemen) bestaat dus feitelijk uit diverse versies waardoor patchen of beheren toch wel een zware klus moet zijn. Ik neig er naar om de Android het stempel "niet geschikt" te geven. Maar ja, de prijs is wel lager dan de IOS telefoons. Ik heb het dan niet over de prijs-kwaliteit verhouding maar meer over de out-of-pocket kosten.

Gaat die Berry weer een keus maken voor een Apple product?

Ik ben inderdaad een redelijke Apple fanaat en dat heeft zijn redenen. Mijn PC's en laptops dragen allemaal een Appel op de rug en ik vind ze geweldig, tot op heden heb ik nog nooit met malware te maken gehad tot begin april dit jaar toen een exploit van Java werd misbruikt. Antivirus software gebruik ik op de appels niet omdat dit echt niet nodig is, de exploit is verholpen en mijn machines zijn weer immuun. Een controle of de malware via de kier naar binnen was gekropen bleek gelukkig negatief uit te vallen. Een smetje op de jaren die ik al veilig heb kunnen werken.

iPhone is eveneens jaren mijn speeltje en ik behoor ook tot de groep die in de bus, in de trein en voor de winkel op zaterdagmiddag met zijn iPhone speelt. Geweldig ding maar ik sla weer door. Ik ga weer verder met mijn opdracht. Ik bel een paar mensen waarvan ik weet dat hun bedrijf is overgegaan op de iPhone om eens te vragen of ik inzage kan krijgen in de business case. Wonderlijk, ik heb drie bedrijven (groter dan 1000 medewerkers) gebeld en alle drie geen business case, met als motivatie dat het toch geen kwestie van kiezen is. Er is namelijk geen keuze, als je je medewerkers goed wilt ondersteunen en veilig zijn werk wil laten doen dan zal een telefoon aangeschaft moeten worden waar medewerkers intuïtief hun werk mee kunnen doen, waar ze alle apps mogen installeren die Apple heeft vrijgegeven, die goed te beheren zijn en waar ze eenvoudig mail kunnen binnenhalen, ook willen we onze beheerders goede instrumenten geven om de telefoons te beheren. Ik weet inmiddels wat er in mijn rapport moet staan en ik klap mijn laptop open.

Groetjes, Berry

SOPHOS

simple + secure

Individually great, altogether – better

Security products that cover every aspect of your business, individually great, but if you put them altogether – they're even better.

endpoint | web | e-mail | encryption | mobile | network

distributeur: CRYPSYS Data Security | 0183 - 62 44 44 | sales@crypsys.nl | www.crypsys.nl