oktober 2009 nummer 6

INFORMATIEBEVEILIGING

Cybercriminaliteit kost bedrijfsleven en overheid handenvol geld

De Leidraad voor de uitwisseling van gevoelige informatie van NAVI

Cybercrime trendrapport: geen verbetering van de veiligheid van internet

Voorkom schijnveiligheid door een veilig ontwerp

DEMO architectuur met security

ib

creative commons

PvIB
Platform voor InformatieBeveiliging

Voorwoord/colofon

Beste lezer,

Op het moment dat ik dit schrijf, ben ik druk in de weer met een verhuizing. Ons bedrijf sluit dit jaar een flink aantal kantoren, inclusief een paar hoofdkantoren, en dat betekent voor vrijwel iedereen een nieuwe werkplek. Voor ons is dat eigenlijk een 'werkvlek', want een vaste werkplek, dat zit er niet meer in. We gaan 'nieuw werken', plaats- en tijdonafhankelijk. De nieuwe hoofdlocatie in Arnhem is een toonbeeld van vernieuwing, met alles behalve gewone bureaus. We krijgen zitmeubilair in de vorm van poefjes, strandstoelen (zeegeluiden hebben we nog net niet), houten banken en wonderlijke amorfe zitdingen. En we hebben natuurlijk een bijpassend instrumentarium, bestaande uit een mobiel werkstation. Nou ja, het is een nieuwe laptop met een heel fraaie koffer met wieltjes. Al is de laptop eigenlijk te groot om in de trein echt te kunnen werken. En, dat zal ik misschien wel het meeste op prijs stellen, de koffiebar met echte koffie en wifi.
Het nieuwe werken lijkt me wel lekker.

En zo tussen het opruimen door kan ik jullie even door dit nummer begeleiden. Helaas niet zo'n dik nummer, maar wel met leuke artikelen over veel verschillende onderwerpen. Yuri Bobbert vult het Demo architectuurmodel aan met een security paragraaf en dat levert een interessante oplossing op. Matthijs van der Wel gaf dit voorjaar bij een themasessie een presentatie over cybercrime, het resultaat van een survey. Er waren veel leden, en dus lezers, aanwezig, maar het leek ons leuk om het verhaal ook in dit nummer te presenteren.
Ook Ton Slewe en Ella Broos van GOVCERT hebben het over cybercrime, op basis van een overheidssurvey. Hans Muller en Erwin van der Zwan gaan in op de Leidraad voor de uitwisseling van gevoelige informatie van NAVI, waarin overheid en bedrijfsleven samenwerken aan de bestrijding van risico's ten aanzien van de vitale infrastructuur, zoals nutsvoorzieningen en strategische installaties. Samenwerken betekent communiceren en hoe doe je dat met vertrouwelijke gegevens? Het PvIB heeft overigens in de klankbordgroep gezeten, mooi dat we daar een bijdrage hebben geleverd.
Kees Hogewoning gaat in op het verschil tussen echte en optische beveiliging in een artikel over schijnveiligheid. Tom Bakker heeft wederom een functionaris informatiebeveiliging geïnterviewd. Daarnaast hebben we natuurlijk de questafette, waarin Marcel Lavalette zijn visie geeft op security certificeringen. Scoop: we hebben nu al een verslag van de thema-avond over her EPD. Berry is weer terug van vakantie en daarmee besluiten we dit nummer.

Veel leesplezier,

André Koot
Hoofdredacteur

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

Redactie
André Koot (hoofdredactie, werkzaam bij Univé-VGZ-IZA-Trias),
e-mail: A.Koot@Unive.nl
Peter Westerling/Monique van Diessen (eindredactie, TOPpers Media bv, Berlicum)

Redactieraad
Tom Bakker (Delta Lloyd)
Mario de Boer (Logica)
Lex Borger (Domus technica)
Lex Dunn (Capgemini)
Rob Greuter (Secode Nederland)
Aart Jochem (GOVCERT.NL)
Renato Kuiper (HP)
Henk Meeuwisse (Sogeti)
Gerrit Post (G & I Beheer BV)

Advertentieacquisitie
e-mail: adverteren@pvib.nl

Vormgeving
Van Velzen Grafisch Ontwerp, 's-Hertogenbosch

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
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

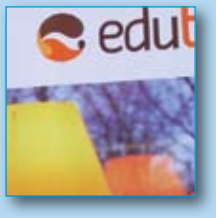
creative commons

PvIB
Platform voor InformatieBeveiliging

Inhoud







Waarom informatiebeveiliging goed is voor uw portemonnee

Auteur: Matthijs van der Wel > Matthijs van der Wel is manager Principal Forensics EMEA bij Verizon Business Security Solutions en bereikbaar via matthijs.vanderwel@verizon.nl.

Voor bedrijven wordt de uitdaging om informatieactiva veilig te stellen met de dag groter. De moderne zakelijke omgeving binnen de extended enterprise, oftewel de onderneming met al zijn vertakkingen, is ingericht om werkgevers, leveranciers, partners en klanten met elkaar te verbinden via één wereldwijd netwerk om de productiviteit en de prestaties te verbeteren. Omdat de besluitvorming een onlosmakelijk onderdeel van deze verspreide en dynamische omgeving vormt, liggen de kritische bedrijfsgegevens niet langer binnen een centrale locatie besloten. Bedrijfsgegevens stromen in en uit de onderneming en de concurrentiepositie van bedrijven is afhankelijk van de snelheid waarmee zij deze informatiestroom kunnen beheren.

Maar hoe meer informatie bedrijven verspreiden en beheren, en hoe groter het aantal locaties waarin deze informatie wordt ondergebracht, des te groter het risico dat onbevoegde partijen de kans zien zich toegang tot deze informatie te verschaffen. En nog belangrijker: dit gevaar is niet langer per definitie van buiten de organisatie afkomstig. Binnen de informatiestroom is er sprake van reële, tastbare bedreigingen, die afkomstig zijn van entiteiten binnen de toevoerketen van de onderneming, zoals partners, leveranciers en de gebruikers van de bedrijfsgegevens.

Bovendien gaan op internet enorme sommen geld om. Dit kan gaan om directe geldstromen, zoals in het geval van digitaal geld of creditcardtransacties, of items die indirect verband houden met logische gegevens, fysieke activa of waardevolle goederen. En uiteraard volgt de onderwereld deze geldstromen op de voet.
De georganiseerde misdaad wordt steeds vindingrijker in het uitbuiten van kwetsbaarheden. Desondanks kunnen bedrijven de meeste gegevenslekken op eenvoudige wijze voorkomen door een aantal uiterst simpele beveiligingsmaatregelen te treffen.

Groeiende cybercriminaliteit
Volgens het 2009 Verizon Business Data Breach Investigations Report (DBIR) vielen bedrijven in 2008 ten prooi aan enkele van de meest ingrijpende gevallen van cybercriminaliteit ooit. Deze tweede editie van het jaarlijkse onderzoeksrapport is gebaseerd op een analyse van gegevens van negentig door Verizon Business onderzochte gegevenslekken, waarbij 285 miljoen records bij betrokken waren. Volgens het rapport werden er in 2008 meer elektronische records geschonden dan in alle vier voorgaande jaren bij elkaar.
Deze groei was het gevolg van een sterke gerichtheid op de financiële dienstverleningssector en een nauwe betrokkenheid van de georganiseerde misdaad.
De financiële dienstverleningssector vertegenwoordigde 93 procent van alle gegevenslekken, en bij de diefstal van maar liefst 90 procent van deze records waren groepen betrokken die deel uitmaakten van de georganiseerde misdaad.

De belangrijkste bevindingen van dit jaar bevestigen de conclusies van het rapport voor het voorgaande jaar en bieden daarnaast nieuwe inzichten. In 2009 werden, net zoals in het jaar daarvoor, de meeste gegevenslekken door externe partijen veroorzaakt. Dit jaar waren externe partijen verantwoordelijk voor 74 procent van alle gegevenslekken, terwijl in 32 procent van de gevallen zakelijke partners betrokken waren. Volgens het onderzoek waren insiders voor slechts twintig procent van alle gegevenslekken verantwoordelijk, een bevinding die mogelijk indruist tegen de algemene opvattingen.

De meerderheid van de gegevenslekken was het resultaat van een combinatie van gebeurtenissen in plaats van een enkele handeling. In 64 procent van alle gevallen was er sprake van hackers die een combinatie van methoden gebruikten om het bedrijf in kwestie aan te vallen.
Dit jaar was er echter opnieuw sprake van een grote gemene deler. Bij de meest succesvolle aanvalspogingen maakten de aanvallers misbruik van een fout van hun slachtoffer. Als gevolg van deze fout wisten de aanvallers zich een weg binnen het netwerk te verschaffen en malware op een computer te installeren om informatie te verzamelen.

Detectie van gegevenslekken: compliance werpt vruchten af
De meeste bedrijven blijken er nog steeds grote moeite mee te hebben om gegevenslekken te detecteren op het moment dat deze zich voordoen. Of de fout nu aan de technologie of een bedrijfsproces is te wijten, het resultaat is hetzelfde.
De afgelopen vijf jaar waren relatief weinig slachtoffers in staat om het gegevenslek te ontdekken. In maar liefst 69 procent van alle gevallen werd het lek door een externe partij ontdekt.

De financiële dienstverleningssector kreeg het in 2008 hard te verduren. Deze sector vertegenwoordigde dertig procent van alle gegevenslekken, en meer dan negen van de tien van alle 285 miljoen gestolen records. Het aantal onderzoeken dat door het Investigative Response-team van Verizon Business buiten de Verenigde Staten werd uitgevoerd, steeg tot meer dan een derde van het totaal aantal onderzochte gevallen. Sterk getroffen regio's zijn onder meer de

Verenigde Staten, Canada en Europa, terwijl het aantal onderzochte gegevenslekken gestaag bleef groeien in Brazilië, Indonesië, de Filippijnen, Japan en Australië.

Ondanks alle, in brede kring gedeelde, zorgen over pc's, mobiele toestellen, draagbare media, enzovoort, had 99 procent van alle incidenten betrekking op servers en toepassingen. Voor een incident werden meerdere entiteiten of locaties afzonderlijk getroffen. Opvallend is dat de helft van alle gegevenslekken aan elkaar gerelateerde incidenten omvatten die vaak door dezelfde personen werden veroorzaakt.

Uit het rapport blijkt tevens hoe belangrijk is om aan de richtlijnen van de branche-normen te voldoen om gegevenslekken te voorkomen. Zo blijkt compliance met de PCI-norm van cruciaal belang. Maar liefst 81 procent van de getroffen bedrijven waarop de Payment Card Industry Data Security Standard (PCI-DSS) van toepassing is, bleek niet aan de richtlijnen van deze norm te voldoen op het moment dat het gegevenslek zich voordeed.

De onderneming beschermen

De onderzoekers van Verizon Business concludeerden dat een ongekend hoog percentage (87 procent) van alle gegevens-lekken in 2008 voorkomen had kunnen worden, als er simpele of directe controle-mechanismen waren geïmplementeerd. Het gaat in alle gevallen om standaard-praktijken waar bedrijven binnen de branche zich dagelijks mee bezig houden. In slechts dertien procent van de gevallen werd het gebruik van intensieve controle-mechanismen (wat betreft inspanning en kosten) aanbevolen.

De aanbevelingen die op basis van het nieuwe onderzoek gedaan kunnen worden, komen overeen met die voor 2008. De resultaten tonen opnieuw aan dat eenvoudige ingrepen, mits op accurate en consequente wijze uitgevoerd, grote voordelen kunnen opleveren.

Onze aanbevelingen moeten geenszins worden gezien als een uitgebreide strategie voor het beveiligen van bedrijfsgegevens, en al evenmin als een garantie tegen

gegevensdiefstal. Ze vormen echter een neerslag van de ervaringen die werden opgedaan op basis van honderden onderzoeken naar gegevenslekken. Deze aanbevelingen hebben ten doel specifieke probleemgebieden te identificeren waarvan sprake is bij veel van de bedrijven die door Verizon Business werden onderzocht.

- **Het wijzigen van de standaard aanmeldingsgegevens is een must**
  In 2008 wisten meer criminelen zich toegang tot bedrijfsactiva te verschaffen met behulp van standaard aanmeldings-gegevens, dan met behulp van welke andere methode dan ook. Bovendien waren de slachtoffers zonder uitzondering op de hoogte van het belang om gebruikersnamen en wachtwoorden te wijzigen. Ze verzuimden simpelweg dit voor een paar activa te doen (die de indringers uiteraard feilloos wisten te vinden), of gingen ervan uit dat de externe partij die voor het beheer ervan verantwoordelijk dit wel zou hebben gedaan. De lering die men hieruit kan trekken, is dat u er niet automatisch vanuit moet gaan dat uw personeel of dat van uw zakelijke partner alle beleidsregels en procedures opvolgt.

- **Deel geen aanmeldingsgegevens**
  Een ander overduidelijk, maar vaak over het hoofd gezien probleem waarvan vaak misbruik wordt gemaakt, is het delen van aanmeldingsgegevens. Bedrijven moeten niet alleen de standaard aanmeldings-gegevens wijzigen, maar er ook op toezien dat er unieke wachtwoorden worden gebruikt en dat wachtwoorden niet door gebruikers met anderen worden gedeeld of op verschillende computers worden gebruikt. In 2008 resulteerde het gebruik van gedeelde aanmeldingsgege-vens in een relatief aantal gegevens-lekken. Het ging daarbij niet langer om afzonderlijke incidenten, maar eerder om een reeks van incidenten. Dit probleem trad met name op bij activa die door een externe partij werden beheerd.

- **Neem de gebruikersaccounts onder de loep**
  Deze aanbeveling komt overeen met de eerdere twee punten, maar het is de moeite waard om hier afzonderlijk op in te gaan. Als gevolg van een analyse van standaard en gedeelde aanmeldings-gegevens, het groeiende tempo van het aantal gegevenslekken (en het enorme aantal gestolen records) en onze jaren-lange ervaring zijn wij ons sterk bewust van het belang van een regelmatige evaluatie van gebruikersaccounts. Deze beoordeling zou een formeel proces moeten omvatten dat garandeert dat alle actieve accounts geldig zijn, op de juiste wijze zijn geconfigureerd, en de juiste rechten (het liefst zo weinig mogelijk) zijn toegekend.

- **Evalueer toepassingen en code**
  Aanvallen op basis van de SQL-injectie, cross-site scripting, het omzeilen van de

Secure your business with

SafeStick®

“Met SafeStick wéét ik dat mijn data veilig is!”

De voordelen van SafeStick:

- *Altijd veilig*
  data beveiligd met wachtwoord en encryptie
- *Automatisch lockdown*
  automatische vergrendeling als USB stick niet wordt gebruikt
- *Opslagcapaciteit*
  verkrijgbaar van 512MB tot en met 64GB (!)
- *Gebruiksvriendelijk*
  geen software of andere toepassingen nodig

SafeStick®

kijk op www.safestick.info voor meer informatie.
mail naar info@safestick.info of bel 0183 - 62 44 44

CRYPSYS data security

authenticatie en het misbruik van sessievariabelen vertegenwoordigden bijna de helft van alle gegevenslekken, die door hackers en indringers werden veroorzaakt. Het is niet bepaald een publiek geheim dat aanvallers zich op een steeds hoger niveau binnen de stack richten. En waarom zouden wij onze beveiliging daar dan niet aan aanpassen? Zoals altijd moeten we beginnen met brandjes blussen: zelfs met een oppervlakkige test of een scan van internettoepassingen hadden de meeste problemen die tot gegevenslekken hebben geleid in een vroeg stadium kunnen worden geïdentificeerd. Vervolgens is het zaak om regelmatig evaluaties van de architectuur, de rechten en de broncode uit te voeren. Bedrijven worden eveneens aanbevolen een Security Development Life-Cycle (SDLC)-aanpak binnen het applicatieontwikkelingsproces te integreren. Ten slotte moet u uw ontwikkelaars helpen om de waarde van het schrijven van veiliger code in te zien.

- **Slimmere strategieën voor patchbeheer**
  Voor elke kwetsbaarheid die in 2008 door hacker- en malware-aanvallen werd uitgebuit, bleek er minimaal zes maanden voor het incident plaatsvond een patch beschikbaar te zijn, waarmee het incident had kunnen worden voorkomen. Op slechts één geval na waren al deze patches minimaal een jaar van tevoren beschikbaar. Hoewel de logische conclusie zou zijn dat bedrijven niet snel genoeg zijn met het installeren van patches, zou dit een verkeerde voorstelling van zaken zijn. Bij al deze bedrijven was sprake van patch-trajecten die ver onder de zes maanden lagen. Op basis van vijf jaar onderzoek blijkt dat dit probleem veel meer een kwestie van omvang, dan van snelheid is. Bedrijven zouden veel meer gebaat zijn met consistenter en uitgebreider patchen dan met snel patchen.

- **Afvloeiingsprocedures**
  De afgelopen jaren was er sprake van verschillende gegevenslekken die het resultaat waren van kwaadwillende handelingen van een recent ontslagen (of van ontslag op de hoogte gestelde) werknemer. Elk bedrijf zou over een uitgebreide afvloeiingsprocedure moeten beschikken die in kaart brengt wie verantwoordelijk is voor het afvloeiingsproces, die procedures en checklists voor vertrekkende werknemers uiteenzet, het terugverkrijgen van alle bedrijfseigendommen garandeert en - nog het meest belangrijkst - een proces biedt op basis waarvan gebruikersaccounts snel worden gedeactiveerd en toegangsrechten worden ontnomen.

- **Activeer applicatielogs en bewaak deze**
  De aanbeveling 'bewaak event logs', die we vorig jaar deden, herhalen we dit keer opnieuw. Hierbij moeten echter worden opgemerkt dat veel bedrijven deze activiteiten concentreren op netwerk-, OS-, IDS-, en firewall-logbestanden, en vaak geen oog hebben voor logbestanden voor remote access services, internettoepassingen, databases en andere bedrijfskritische toepassingen. Deze logbestanden kunnen een schat aan informatie bieden voor het detecteren, minimaliseren en onderzoeken van gegevenslekken.

- **Definieer wat 'verdacht' en 'ongewoon' is en zoek daar vervolgens naar**
  Toegegeven, deze aanbeveling klinkt ietwat vaag. Het geval wil echter dat het onmogelijk is hier een definitie van te bieden die op alle bedrijven van toepassing is. Volgens ons onderzoek is er sprake van een deelverzameling van kleine, doch uiterst gerichte, geavanceerde en schadelijke aanvallen. Deze aanvallen treffen normaliter bedrijven die grote hoeveelheden gegevens opslaan of verwerken, waaraan de onderwereld grote waarde hecht. Dergelijke bedrijven vormen uiterst gewilde doelwitten. Bedrijven die in deze categorie vallen, moeten zich goed voorbereiden om deze uiterst vastberaden, goed gefinancierde, professionele en gerichte aanvallen te kunnen detecteren en afweren. Ga na welke gegevens van kritisch belang zijn, identificeer vervolgens wat onder normaal gedrag wordt verstaan en implementeer vervolgens gerichte mechanismen die afwijkingen van het normale gedragspatroon kunnen identificeren en daarover waarschuwingen afgeven.

Ons 2009 Data Breach Investigations Report, dat op een analyse van 285 miljoen gestolen records is gebaseerd, geeft een duidelijk alarmsignaal af voor de informatiebeveiligingsbranche. Nu wereldwijd de hoeveelheid informatie groeit en van invloed is op alles dat we doen, wordt het een steeds grotere uitdaging om de informatieactiva binnen de onderneming met al zijn vertakkingen veilig te stellen. Hoewel de meerderheid van de aanvallen een simpel karakter blijft houden, weten cybercriminelen zich aan de huidige beveiligingsstrategieën aan te passen en bedenken zij steeds weer nieuwe manieren om zich toegang te verschaffen tot de gegevens die voor hen van nut zijn.

Doordat we over steeds meer informatie beschikken, kan de branche werkelijke gegevens en werkelijke resultaten inzetten om bedrijven te helpen een beter inzicht te verwerven in de realiteit en ervoor te zorgen dat zij zich op de juiste aspecten richten. Ondertussen doen bedrijven er goed aan de hierboven uiteengezette simpele stappen te nemen, omdat deze van cruciaal belang zijn voor de beveiliging van hun informatieactiva.

Het volledige 2009 Verizon Business Data Breach Investigations Report kan worden gedownload via http://www.verizonbusiness.com/products/security/risk/databreach/.

Over Matthijs van der Wel
Matthijs van der Wel is de manager van de forensische praktijk binnen de EMEA-regio bij Verizon Business Security Solutions. In deze functie is hij verantwoordelijk voor het inspringen op en het uitvoeren van onderzoek naar incidenten. Verizon Business helpt klanten om zich voor te bereiden op incidenten waar mogelijk digitaal bewijs voor benodigd is en biedt diensten die klanten helpen een volledig onderzoek uit te voeren. Voorbeelden van incidenten waarnaar Verizon Business onderzoek doet zijn onder meer gegevensdiefstal, gehackte servers en toepassingen, anonieme bedreigingen via e-mail en fraude.
Matthijs is sinds 2001 werkzaam binnen de forensische en IT-beveiligingsbranche.

Uitwisseling van gevoelige informatie

Auteurs: Hans Muller en Erwin van der Zwan > Hans Muller en Erwin van der Zwan zijn senior adviseurs (security) bij het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) en ze zijn bereikbaar via Hans.Muller@minbzk.nl en Erwin.Zwan@minbzk.nl.

Informatie is essentieel voor, zo niet het meest belangrijke bezit van, veel organisaties. Veel bedrijven en instanties hebben een eigen informatie-beveiligingsbeleid. Dit beleid beperkt zich meestal tot interne procedures en maatregelen over hoe de medewerkers om moeten gaan met informatie. Regelmatig is het echter wenselijk of noodzakelijk dat gevoelige informatie wordt uitgewisseld met externe partijen. Samen met een klankbordgroep (waar ook het PvIB deel van uitmaakte) heeft het NAVI de Leidraad voor de uitwisseling van gevoelige informatie ontwikkeld.

Aan het verstrekken, het ter beschikking stellen of op andere wijze uitwisselen van gevoelige informatie zijn beperkingen en risico's verbonden. Zo is het slechts zeer beperkt en onder strikte voorwaarden mogelijk om gevoelige informatie van de rijksoverheid met bedrijven te delen. Ook bedrijven kunnen terughoudend zijn met het delen van gevoelige informatie aan de overheid. De op die manier in bezit van de overheid gekomen informatie zou met een beroep op de Wet openbaarheid van bestuur (Wob) mogelijk openbaar gemaakt moeten worden.

Bedrijven, overheid en instanties wisselen ook onderling gevoelige informatie uit, bijvoorbeeld tijdens bijeenkomsten over de kwaliteitsverbetering van de beveiliging van bedrijven binnen de vitale sectoren. Door bedrijven en instanties worden hierbij verschillende termen gebruikt om de gevoeligheid en de vertrouwelijkheid aan te duiden. Deze termen of de te nemen maatregelen zijn onderling niet altijd gelijkwaardig. Er is daarom behoefte aan helderheid over hoe en welke informatie op een veilige wijze gedeeld kan worden en welke maatregelen tussen betrokken partijen afgesproken kunnen worden.

Op verzoek van diverse bedrijven uit vitale sectoren organiseerde het NAVI in 2008 en 2009 enkele bijeenkomsten over de uitwisseling van informatie. De bedrijven stelden drie vragen centraal:

1 Hoe om te gaan met rubricering en informatiebeveiliging bij de vitale infrastructuur?
2 Hoe informatie te delen in multidisciplinaire en organisatieoverstijgende projectteams?
3 Hoe om te gaan met vertrouwelijke informatie in relatie tot bijvoorbeeld een vergunningaanvraag en/of in relatie met de Wet openbaarheid van bestuur?

De deelnemers aan de bijeenkomsten gaven aan dat er bij vitale bedrijven grote behoefte bestaat aan meer duidelijkheid en afspraken over hoe om te gaan met intersectorale en publiekprivate informatie-uitwisseling en tevens de noodzakelijke vertrouwelijkheid van de informatie te borgen. Ofwel, hoe kunnen we veilig communiceren zonder het risico te lopen dat informatie in verkeerde handen valt? Uitvoerig is gesproken over referentiekaders en een set van afspraken die daarbij behulpzaam zou kunnen zijn. In het bijzonder gaat het hierbij om de aspecten van rubricering van informatie en de bijbehorende afspraken en maatregelen voor wat betreft de uitwisseling van informatie met andere partijen.

Om bij het uitwisselen van gevoelige informatie dezelfde taal te spreken, heeft het NAVI in samenspraak met diverse vitale bedrijven, brancheorganisaties en overheden een leidraad opgesteld. Deze kan bijvoorbeeld uitgereikt worden bij platformbijeenkomsten of werkoverleggen. Het gebruik van de leidraad is vrijwillig, maar niet vrijblijvend. Van partijen die betrokken zijn bij een informatie-uitwisseling en die afspreken de leidraad te hanteren, wordt verwacht dat zij zich aan de voorgestelde afspraken en afgestemde beveiligingsmaatregelen houden. De leidraad gaat niet over het intern informatiebeveiligingsbeleid. Het NAVI heeft daar wel voorbeelden van beschikbaar.

Het indelen naar gevoeligheidsniveaus helpt het duiden van de informatie. De leidraad werkt met een kleuraanduiding voor de mate van gevoeligheid van de informatie:

Rood (geheim)
Geel (vertrouwelijk)
Groen (besloten)
Wit (openbaar)

Kleuren hebben als voordeel dat ze worden geassocieerd met een mate van exclusiviteit daar waar termen als 'geheim', 'vertrouwelijk' of 'intern' in verschillende bedrijfsculturen een geheel andere betekenis kunnen hebben. De leidraad sluit met deze kleuren aan op bestaande schema's zoals het *Traffic Light Protocol*. Om de mate van gevoeligheid extra te benadrukken, wordt naast de kleuraanduiding een generieke aanduiding van het gevoeligheidsniveau toegevoegd.

Het is van belang dat informatie alleen in bezit is van en toegankelijk is voor bevoegde personen. Een principieel uitgangspunt bij de verstrekking van informatie is dat de informatie-eigenaar of -verstrekker beslist binnen welke kaders de informatie gedeeld mag worden. Hierbij geeft de verstrekker aan welke gevoeligheidswaarde de informatie heeft en welke voorwaarden hij aan de verstrekking stelt. De ontvanger beoordeelt vooraf of hij/zij de aangeboden informatie wil en kan ontvangen.
De ontvanger verplicht zich tegenover de

verstrekker om de informatie vervolgens op de overeengekomen wijze te behandelen. Bij de verschillende gevoeligheidsniveaus zal ten minste moeten worden aangegeven wie mag kennisnemen van de informatie (het verspreidingsgebied), de wijze van verstrekken en de te treffen beveiligingsmaatregelen.

De beperkingen voor de gevoeligheidsniveaus zijn als volgt:

- **Rood:** De informatie is uitsluitend toegankelijk voor geselecteerde personen (op basis van noodzakelijkheid) die zijn aangewezen door, of bekend zijn bij de informatie-eigenaar. De informatie wordt in principe mondeling gedeeld. Indien de informatie-uitwisseling schriftelijk of elektronisch plaatsvindt, worden er expliciet afspraken gemaakt over de beveiliging van de informatie. Hierbij worden afspraken gemaakt over de borging dat de geadresseerde ook de juiste en enige ontvanger is.

- **Geel:** De informatie is alleen toegankelijk voor een selecte groep van direct betrokken personen, bijvoorbeeld voor deelnemers aan de specifieke besprekingen. Zij mogen de informatie ook delen met mensen binnen hun organisatie die deze informatie nodig hebben, hetzij om maatregelen te treffen of om een bijdrage te kunnen leveren aan de discussie en meningsvorming van de deelnemer.

- **Groen:** De informatie is alleen toegankelijk voor een bepaalde (besloten) groep van personen. De informatie mag worden gedeeld met andere organisaties, informatiefora of personen werkzaam in beveiligingsfuncties. De informatie mag niet openbaar gemaakt worden door publicatie of plaatsing op openbare internetsites.

- **Wit:** De informatie is specifiek gemaakt om openbaar te maken. Informatie is (op aanvraag) vrij toegankelijk of is vrijgegeven voor publicatie via openbare bronnen zoals internet en de pers.

Maatregelen waar de verstrekker en ontvanger afspraken over kunnen maken, zijn onder andere de wijze van (de-)

classificeren, het verwerken en opslaan op computersystemen (versleuteling), fysieke maatregelen, toegangscontrole (fysieke en ICT), verzenden per post of e-mail (onweerlegbaarheid), transport en duiden van gevoeligheidsniveau op documenten en gegevensdragers of personele maatregelen (zoals een geheimhoudingsverklaring en screenen).

De leidraad geeft per gevoeligheidsniveau aan wat het verspreidingsgebied is, maar laat het maken van specifieke afspraken over verstrekking en te nemen maatregelen over aan de verstrekker om te bepalen. Het voert te ver om in de leidraad dergelijke specifieke maatregelen op te nemen. Diverse deelnemers aan de gehouden bijeenkomsten gaven bovendien aan dat dit bedrijven zou kunnen weerhouden de leidraad te volgen omdat het dan ingrijpt in het eigen interne beveiligingsbeleid. Om dezelfde reden legt de leidraad bovendien geen directe koppeling tussen verschillende bestaande classificatieschema's en bevat de leidraad geen transformatietabel. Wel is een toelichting beschikbaar, waarin suggesties voor maatregelen zijn opgenomen.

In de leidraad zijn verder enkele aanbevelingen voor regels tijdens besprekingen en bijeenkomsten opgenomen. Daarnaast besteedt de toelichting onder andere (kort) aandacht aan de verstrekking van gevoelige informatie aan de overheid met het oog op de Wet openbaarheid van bestuur.

Deelnemende partijen aan een uitwisseling van (gevoelige) informatie wordt geadviseerd om vooraf altijd duidelijke afspraken te maken en verwachtingen af te stemmen. Organisaties worden aangemoedigd om de leidraad te hanteren en deze af te stemmen met een eigen informatiebeveiligingsbeleid.

De leidraad en de toelichting zijn te downloaden van www.navi-online.nl/producten.

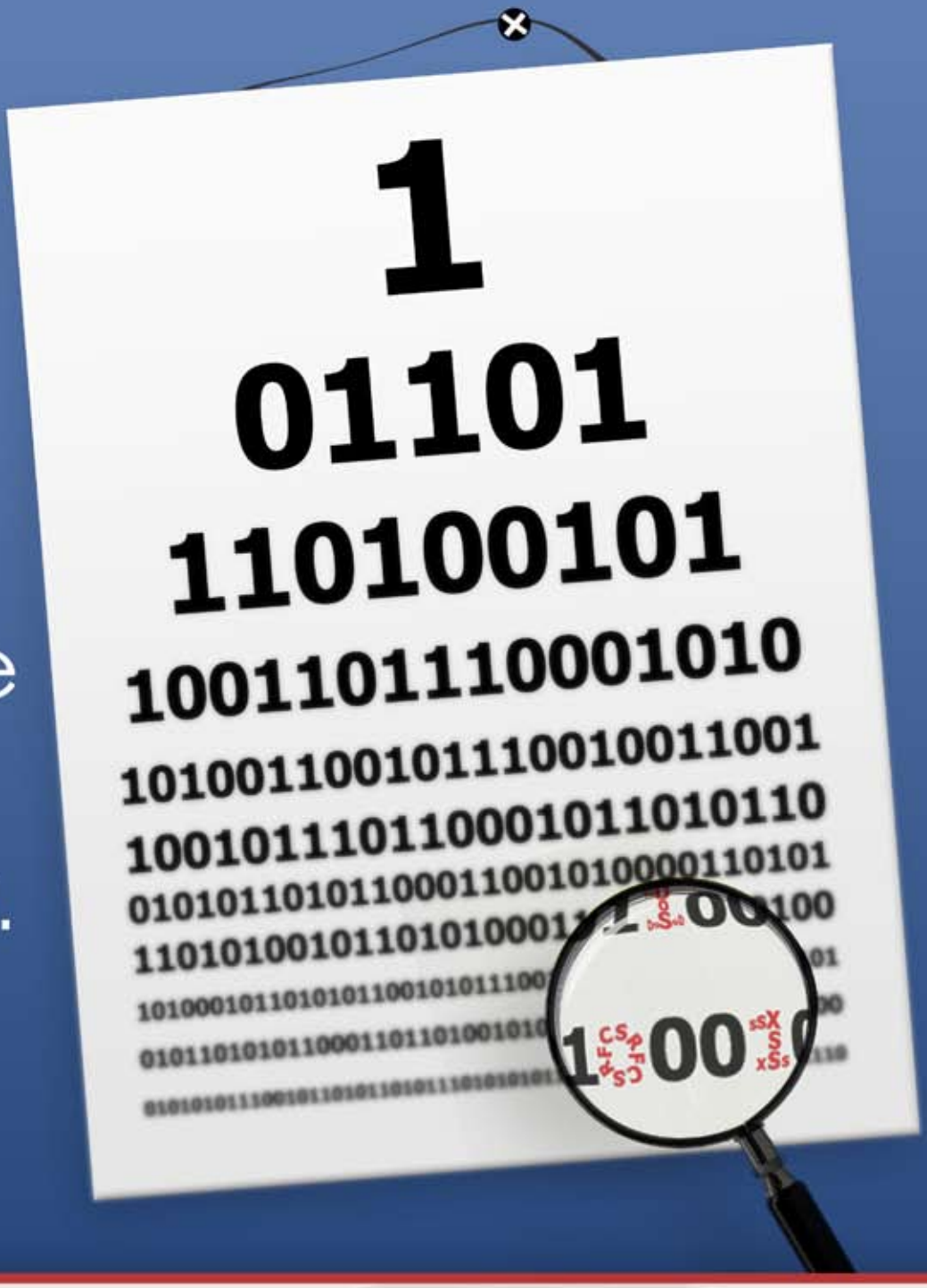
Wat is het NAVI?
In het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) werken overheid en bedrijfsleven samen aan de verbetering van de bescherming van de vitale infrastructuur in Nederland tegen moedwillig menselijk handelen (security). In haar activiteiten richt het NAVI zich op fysieke, personele, organisatorische en digitale dreigingen.

Het NAVI ondersteunt beheerders en eigenaren van de vitale infrastructuur door het bieden van een veilig platform voor informatie-uitwisseling, kennis & expertise en een (inter)nationaal contactpunt.

Met een serie handreikingen ondersteunt het NAVI thematisch de beveiligingspraktijk bij vitale bedrijven. Een deel van deze handreikingen zijn door het NAVI zelf ontwikkeld, zoals een Risicoanalyse, een Beveiligingsafstemming Vitaal en Overheid, een Operator Security Plan, Security Awareness en Informatie-uitwisseling. Het NAVI levert daarnaast een bijdrage aan andere publicaties en heeft ook internationale uitgaven geschikt gemaakt voor de Nederlandse markt.

Alle handreikingen zijn beschikbaar via www.navi-online.nl

What you can't see **CAN** hurt you.



CODEFEND™, the unique fusion of leading technologies with human expertise is an innovative, ***outsourced Security Code Review Service***.

Flexible. Accurate. Efficient.

Incorporate **CODE**FEND™ into your software development lifecycle.

A Service by

COMSEC Consulting
Information Security

CODEFEND™
Your Software SECURED.

Comsec Consulting BV | www.codefend.com www.comsecglobal.com | Tel: +31-10-2881010 | info@comsecglobal.com

Functionarissen in de informatiebeveiliging

Auteur: Tom Bakker > Tom Bakker is werkzaam bij de Delta Lloyd Groep als Group Security Officer en is lid van de redactie van Informatiebeveiliging. Hij is te bereiken via tom_bakker@deltalloyd.nl.

Als tweede in de reeks Functies in de informatiebeveiliging in de praktijk een interview met Jeroen van Duuren, Information Security Officer bij Edutel.

Wat heb je zoal gedaan in de informatiebeveiliging en wat doe je nu?
"Ik ben gefascineerd geraakt door IT- en informatiebeveiliging door een stageplaats als IT Security Engineer bij Simac. Ik ben daarna bij Edutel begonnen als IT Security Engineer, opgeklommen tot Information Security Engineer en ik ben nu Information Security Officer. De engineering functies waren voornamelijk technisch, maar ik ben nu bijna exclusief op tactisch en strategisch niveau bezig. Omdat Edutel nog niet zo groot is, ben ik ook nog deels bezig met de technische kant."

Hoe kijk je tegen security aan?
"Security is een breed begrip. Ik ben zelf een generalist en ik vind dat heel prettig omdat ik de link kan leggen tussen techniek en management. Ook is het erg interessant om inzicht te krijgen in hoe een complete organisatie eigenlijk werkt en hoe informatie door een organisatie beweegt. Je ziet zo ook het grote geheel van beveiliging en niet enkel meer de IT-technische kant."

Welke rol heb jij met betrekking tot security in jouw organisatie en de relatie naar aanverwante functies?
"Mijn rol is het beheersen van informatiebeveiliging en het managen van de fysieke beveiliging voor de gehele organisatie. Dit betekent het overzicht houden over de operationele securityprocessen, het schrijven en invoeren van beleidsstukken, interne standaarden, procedures en richtlijnen. Het (laten) uitvoeren van risicoanalyses en business continuity management. Ook word ik ook betrokken door de netwerk- en software-engineers bij de ontwerp- en testfases van hun projecten. Verder hanteren wij de ISO 27001-standaard en we hopen in 2010 ons daarvoor te certificeren. Naast de toezichthouder Agentschap Telecom doen wij zelf interne audits en laten wij een externe organisatie frequent audits uitvoeren."

Op welke plek binnen een organisatie hoort security thuis (positionering)?
"Formeel valt security bij Edutel onder IT als staffunctie, ik rapporteer dan ook aan de IT-manager. De IT-manager wil ook één aanspreekpunt voor security. Hij maakt deel uit van het managementteam. Vanuit de directie en het kernteam is er veel support voor informatiebeveiliging en zowel de directeur, als de managers geven het goede voorbeeld aan de rest van de organisatie."

Kennen jullie de functie zoals genoemd in het studierapport?
"Nee, Edutel is nog klein en heeft pas sinds kort informatiebeveiliging als speerpunt in de organisatie opgenomen. Ik ben ook de enige fulltime security professional binnen de organisatie. Er is wel een securityteam dat bestaat uit mensen die zich parttime met informatiebeveiliging en incident-response bezig houden."

In hoeverre worden de functieprofielen toegepast?
"We hebben niet veel functies, dus dat is lastig aan te geven. De genoemde taakgebieden zijn vaak verenigd in één functie."

Wat vind je van de competenties? Herken je die in de praktijk?
"Voor de functie van CISO en ISM vind ik het een beetje raar dat het werk- en denkniveau die van master zou moeten zijn, terwijl het een toegepaste wetenschap is. Ik vind namelijk contact met de werkvloer belangrijk en vaak is het denkniveau van een master meer theoretisch. Maar voor de rest kan ik me goed vinden in de competenties zoals gesteld in het rapport. Zelf ben ik nu bezig met de CISM certificering."

Hoe kijk je aan tegen een carrièrepad in de informatiebeveiliging?
"Tot nu toe bevalt dit vakgebied mij erg goed omdat het zo breed is en je te maken krijgt met de technische kant, alsmede de organisatorische kant."

Interviewkandidaten
Wilt u na het lezen van dit interview ook geïnterviewd worden over uw mening over of over uw ervaring met functies in de informatiebeveiliging? Meldt u zich dan aan als interviewkandidaat bij Tom Bakker. Hij is bereikbaar via Tom_Bakker@deltalloyd.nl

Edutel is een telecomoperator die nu elf jaar bestaat en telefonie- en internetdiensten levert, voornamelijk op glasvezelnetwerken zoals de FttH (Fiber to the Home) initiatieven OnsBrabantNet en Ons Net Nuenen. Edutel heeft momenteel honderd medewerkers.
Edutel heeft te maken met de regelgeving vanuit het Agentschap Telecom. Toezicht op onder meer informatieveiligheid (BBGAT - Besluit beveiliging gegevens aftappen telecommunicatie), continuïteit en beschikbaarheid.

Europees betalingsverkeer:

Zekerheid

Auteur: Marcel Lavalette > Marcel Lavalette is Managing Consultant IT Risk Management & Compliance bij CompLions BV en is bereikbaar via m.lavalette@complions.nl.

Inderdaad, een mooie stelling van de vorige schrijver van de Questafette, Remco van Mook: 'De veelheid aan specifieke IT-security certificeringen (ISO27001, SAS70, PCI-DSS, NEN7510) doet eerder afbreuk aan het doel dan dat het daadwerkelijk wat toevoegt'. Vanuit de datacenter omgeving waarin hij werkzaam is, weet hij als geen ander dat klanten om zekerheid vragen. Het beschikken over één van deze certificaten of verklaringen geeft een duidelijk signaal af over een bepaalde mate van zekerheid die men kan verwachten. Dit signaal wordt mijns inziens niet altijd goed begrepen, waardoor er soms gevraagd wordt naar elkaar overlappende standaarden, normen of verklaringen.

Door middel van de interne en externe audits, die horen bij het certificatieproces, is immers aangetoond dat de organisatie werkt volgens de vastgestelde richtlijnen, procedures en werkinstructies die horen bij de standaard waarvoor men bijvoorbeeld al gecertificeerd is. Hierdoor verkrijgt men een bepaalde mate van zekerheid over de betrouwbaarheid. Desondanks wordt er gevraagd naar een additionele standaard, norm of verklaring, waardoor er feitelijk gevraagd wordt om zekerheid op min of meer dezelfde zekerheid. Onbekendheid met de 'andere' standaard speelt hierbij vaak ook een rol.

De probleemstelling

Remco's stelling zou betekenen dat de veelheid aan certificeringen niet bijdraagt aan de zekerheid die gevraagd wordt.
En hebben we het over zekerheid, dan gaat het al snel over zaken als SLA-management, informatiebeveiliging, beheersingsmaatregelen, compliance, betrouwbaarheid, risicomanagement, Governance en In Control. Allemaal aspecten die op één of andere wijze met elkaar verbonden zijn. Het is mijn ervaring dat deze zaken nog wel eens met elkaar verward worden of foutief gebruikt worden. Het maakt nogal een verschil om deze zaken te bespreken met een vakinhoudelijke security officer, een risicomanager, een IT-manager, een topmanager of het bestuur van een organisatie.
Hierdoor ontstaan misinterpretaties en onzekerheden over het juist toepassen of het bepalen van de mate van betrouwbaarheid die deze certificaten bieden of de zekerheid die we feitelijk eisen. Als we dan toch om zekerheid vragen en we weten het eigenlijk niet, dan wordt er al snel om een certificaat gevraagd of een SAS70 verklaring. Zonder dat we het ons realiseren, wordt zo meer zekerheid gevraagd dan nodig is of wordt er zekerheid op zekerheid gevraagd

en schieten we spreekwoordelijk met een kanon op een mug.

Daarnaast hebben de genoemde normen of standaarden veel overeenkomsten. De meeste van deze standaarden of maatregelen hebben zo elk hun eigen aanpak over het beheersen van risico's, activiteiten, verslaglegging, het voldoen aan wet- en regelgeving en het afleggen van verantwoording hierover. Fysieke beveiliging, logische toegangsbeveiliging, een informatiebeveiligingsbeleid, risicomanagement, et cetera, worden door de meeste van deze normen en standaarden in meer of mindere mate aangestipt en de overlap is vaak aanzienlijk.

Hier ontstaat dan ook het probleem dat de stelling beschrijft. Een financiële instelling met creditverwerkende processen richt zich vooral op de PCI-DSS standaard en zal van dienstverleners een PCI-DSS certificaat eisen om zaken met ze te kunnen doen. In het geval dat de dienstverlener al ISO 27001 gecertificeerd is, zou het zomaar kunnen dat men voor een groot deel al voldoet aan de PCI-DSS norm. Wordt er echter een PCI-DSS certificaat geëist in de RFP- of offertefase, dan zit er in het commerciële traject voor de dienstverlener vaak weinig anders op om dan maar het PCI-DSS certificaat te behalen. Certificerende instellingen voor een PCI-DSS certificaat zijn weer andere certificerende instellingen dan voor een ISO 27001 certificaat. Hierdoor betaalt de dienstverlener gewoon weer van voren af aan veelal het gehele certificeringproces en wordt zo geconfronteerd met dubbele audit- en (her)certificeringkosten en een extra aanslag op de interne kosten. Dit alles heeft als indirect gevolg dat de interne kosten van de dienstverlener alleen maar hoger worden. Om de eigen businesskansen op voorhand niet kansloos te maken in een RFP wordt er maar voldaan aan deze vraag.

Klanten of (keten)partners die zekerheid willen hebben, moeten zich realiseren dat deze zekerheid een prijskaartje heeft en dat er in het geval van een soortgelijk certificaat of verklaring ruimte moet zijn voor afstemming. Het is daarom veel beter eerst de zekerheidsaspecten goed vast te stellen in een eigen normenkader waaraan de dienstverlener moet voldoen of om de verschillen met een aanwezig certificaat vast te stellen.

Niet geheel tot mijn verrassing ontbreekt in de stelling van Remco dan ook de TPM, oftewel de Third Party Mededeling. Een veelal goedkopere oplossing dan een SAS70 verklaring, maar die mits goed vastgesteld, net zoveel zekerheid biedt. Hierbij wil ik niet de indruk wekken tegen een SAS70 verklaring te zijn, ik wil vooral benadrukken dat er ten aanzien van zekerheid meerdere wegen naar Rome leiden.

Als een organisatie al is voorzien van één van de genoemde certificaten of verklaringen dan zegt dit iets over een bepaalde mate van zekerheid. Om deze mate van zekerheid inzichtelijker te maken, dient er meer informatie over de scope en invulling gevraagd te worden. Vervolgens kunnen de verschillen in kaart gebracht worden. Er zijn verschillende mogelijkheden om zekerheid te krijgen over deze verschillen. Als beide partijen welwillend zijn, zal een pragmatische oplossing gevonden kunnen worden.

Het is beter om de verschillen in kaart te brengen en over het verschil een verklaring af te laten geven. Met een beetje pragmatische aanpak zijn deze verschillen weer onder te brengen in de scope van de reeds aanwezige standaard. Uit ervaring weet ik dat dit met ISO 27001 goed te doen is. Hierdoor weet de klant dat de beheersingsmaatregelen uit het verschil meegenomen worden in de reguliere interne- en externe audits en de (her)certificeringscope.

Dit zou in veel gevallen voldoende kunnen zijn. Het is tijd- en kostenbesparend voor alle partijen, waardoor de besparingen al snel oplopen in de tienduizenden euro's. Ik ken organisaties waar het al snel om veel meer geld gaat.

Ik ben het dus volledig met de stelling van Remco eens. De kneep zit hem echter vooral in het woord 'veelheid' uit zijn stelling. Organisaties die verschillende soorten klanten bedienen, met elk hun eigen wet- en regelgeving, zullen geconfronteerd worden met vragen naar specifieke normen of standaarden met de nodige zelfde mate van zekerheid. Deze organisaties doen er goed aan de grootste gemene deler te zoeken in één standaard. Met klanten en potentiële afnemers moet wel proactief naar aantoonbare zekerheid over het verschil in de additionele beheersingsmaatregelen gezocht worden. Organisaties horen zich dus niet blind te staren op een norm of standaard en zullen dienstverleners de ruimte moeten geven om met compenserende maatregelen als aanvulling op een aanwezige norm of standaard, eenzelfde invulling te kunnen geven aan de gevraagde zekerheid. Het bieden van een bepaalde mate van zekerheid is immers het doel. Een standaard of norm helpt hierbij dit aantoonbaar te maken. Ze moeten echter geen zekerheid op zekerheid vragen door overlappende normen of standaarden op te leggen. Hierbij snijden zij zichzelf in de vingers door hoger wordende kosten, zonder dat dit bijdraagt aan een hogere mate van betrouwbaarheid en zekerheid.

Ik geef estafettestokje door aan Alwin Hilberink, Forensisch ICT expert bij de Politie Academie, met de stelling: 'Levert een digitaal forensisch onderzoek op een systeem dat niet 'offline' is gegaan of mag gaan wel sluitend bewijs?'

GOVCERT.NL Cybercrime trendrapport 2009

Geen verbetering veiligheid internet

Auteurs: Ton Slewe en Ella Broos > Ton Slewe en Ella Broos werken binnen het KennisCentrum van GOVCERT.NL en zijn bereikbaar via ton.slewe@govcert.nl en ella.broos@govcert.nl.

In het Trendrapport Cybercrime 2009 dat GOVCERT.NL onlangs publiceerde, wordt geconstateerd dat het internet er niet veiliger op wordt. GOVCERT.NL onderbouwt deze constatering en doet aanbevelingen voor gezamenlijke inspanning van alle betrokkenen hierbij: internet service providers, softwareleveranciers, overheden, ontwikkelaars en eindgebruikers. Zowel techniek, als menselijk gedrag maken dat het internet nog steeds een bijzonder lucratieve werkomgeving voor internetcriminelen is.

Jaarlijks maakt GOVCERT.NL het trendrapport Cybercrime, met daarin de belangrijkste ontwikkelingen op het gebied van informatiebeveiliging en cybercrime. Op basis van vertrouwelijke en publieke bronnen en contacten met collega-CERT's wordt een beeld geschetst van de belangrijkste ontwikkelingen en aan de hand daarvan wordt een analyse gemaakt van de status van het internet én internetcriminaliteit. Deze trends worden uitgewerkt en toegelicht en tevens worden aanbevelingen gedaan aan organisaties en eindgebruikers over hoe gezamenlijk gewerkt kan worden aan een veiliger digitale wereld. GOVCERT.NL signaleert acht belangrijke trends, die in dit artikel aan de orde komen.

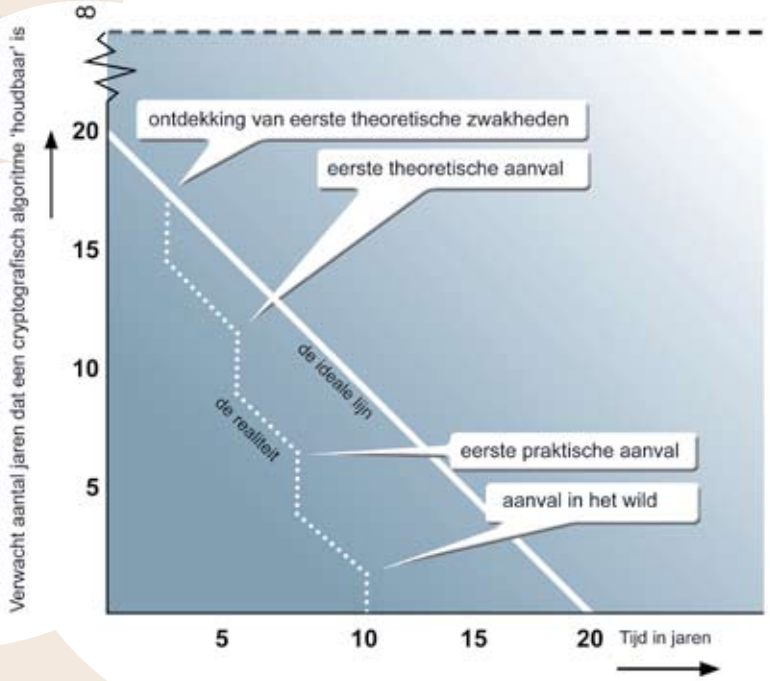
Kwetsbare eindgebruiker

In het Trendrapport van 2007 signaleerde GOVCERT.NL het al en dit geldt nog steeds: eindgebruikers, zowel thuis als op het werk, blijven een zwakke schakel in internetveiligheid. Zij zijn veelal slachtoffer van internetcriminelen, omdat hun computers met relatief gemak overgenomen kunnen worden door criminelen. Lekken in software worden misbruikt, omdat er onvoldoende gedacht wordt aan veiligheid: zelfs de simpele handelingen als antivirussoftware of een firewall installeren en updaten en het regelmatig en tijdig updaten van software blijven vaak achterwege. Ook wordt er ingespeeld op angst: grote groepen mensen gaan in op zogenoemde 'scareware': aanbiedingen van nep-antivirusproducten, waardoor mensen hun geld kwijtraken en hun computer alsnog wordt besmet. Met de overgenomen computers worden botnets gevormd, waarmee op grote schaal criminele activiteiten worden verricht. Het stelen en doorverkopen van persoonlijke informatie is er daar één van. Fraude met internetbankieren is er ook één, waar internationaal gezien een grote stijging te zien is.

Kwetsbare infrastructuur

Er zijn diverse kwetsbaarheden in de infrastructuur van het internet waarvan door criminelen misbruik kan worden gemaakt. Steeds duidelijker wordt het dat het web niet is ontworpen voor wat we er vandaag de dag mee doen. Zo zijn de protocollen die verantwoordelijk zijn voor een goede werking van het internet niet meer afdoende. Het gaat hier om BGP (Border Gateway Protocol), DNS (Domain Name System) en TCP (Transmission Control Protocol). De zwakheden in deze protocollen hebben bij de media de vraag opgeroepen of 'het internet stuk is'. Dat gaat ver, maar feit is dat met de toegenomen afhankelijk van het internet, voor zowel bedrijfsleven, overheid als samenleving, er met spoed aan gewerkt moet worden. Dat kan ook, want de beschreven kwetsbaarheden zijn niet nieuw. Ze bestaan al langer, maar de mogelijkheid om ze op grote schaal uit te buiten was nog niet bekend. Tevens zijn er oplossingen. In het geval van DNS bijvoorbeeld, is er al ruim tien jaar een veilig alternatief voorhanden. Dit wordt echter zelden gebruikt. Ook voor BGP zijn er betere alternatieven, maar die worden langzaam of niet in gebruik genomen. Het probleem is dat de eigenaren van netwerken wel de kosten van aanpassingen dragen, maar er op korte termijn zelf weinig voordeel bij hebben.

Geen verbetering veiligheid internet



Cryptografie

Een basismaatregel voor informatiebeveiliging is cryptografie. Het is belangrijk voor het garanderen van vertrouwelijkheid en integriteit van informatie en daarmee cruciaal voor veel zaken die wij in ons dagelijks leven doen. Cryptografie is niet alleen een wiskundige techniek. Het is een technische oplossing die alleen werkt wanneer deze regelmatig geëvalueerd wordt en goed gebruikt wordt, zowel in technische als in organisatorische zin.
Al in 2004 werd gewaarschuwd dat de bruikbaarheid van MD5-cryptografie ten einde liep. Rond de kerst van 2008 voerde een Nederlandse onderzoeker een aanval uit op de Public Key Infrastructure (PKI), die wordt gebruikt voor certificaten van beveiligde websites. De aanval was succesvol, wat betekent dat de onderzoekers een certificaat konden maken waarbij de handtekening van de Certificate Authority werd gebruikt om een eigen certificaat een geldige status te geven.
Zo kan een crimineel nieuwe certificaten aanmaken voor elk gewenst domein ter wereld, die door alle browsers vertrouwd worden. De crimineel heeft zo de mogelijkheid zich voor te doen als een ander.
Ook OpenSSL, een andere cryptografische toepassing, blijkt zwak. Door een, op zich kleine, fout van een programmeur heeft hierin anderhalf jaar een ernstige kwetsbaarheid gezeten, waardoor wereldwijd vele systemen onveilig zijn geweest door de generatie van zwakke sleutels met de toepassing. Ten slotte is ook een kwetsbaarheid in de versleuteling van draadloze netwerken aangetoond.
Het gaat om een kwetsbaarheid in TKIP (Temporal Key Integrity Protocol), gebruikt voor draadloze netwerken. De onderzoekers die de aanval uitvoerden, toonden aan dat het mogelijk was de versleuteling van een draadloos netwerk te doorbreken.

Cloud Computing

Meer en meer computertoepassingen verschuiven naar het web. Na toepassingen als e-mail, zijn nu ook tekstverwerking, foto- en videobewerking en relatiebeheer online beschikbaar. We noemen deze ontwikkeling 'cloud computing': het internet als een wolk waarin allerlei diensten beschikbaar zijn, inclusief virtualisatie, rekenkracht en opslag.
Samenwerking en andere 2.0 toepassingen zijn meer dan ooit aan de orde van de dag. Deze diensten bieden groot gebruikersgemak: zelf geen software meer installeren, gegevens altijd en overal kunnen benaderen en goede samenwerkingsmogelijkheden. De andere kant hiervan is dat er op het gebied van veiligheid het een en ander wordt ingeleverd. Een onlinedienst die kwetsbaar is, geeft misbruik van informatie vrij baan. Bij een geslaagde aanval op een dergelijke dienst krijgt de aanvaller ongeautoriseerd toegang tot gegevens en kan deze kopiëren, aanpassen of verwijderen. Ook schuilt er een risico in de gebruiksvoorwaarden van online diensten. Bijna alle aanbieders houden zich het recht voor de voorwaarden eenzijdig te wijzigen. Sommige voorwaarden bevatten bepalingen waarmee de dienstaanbieder een gebruikslicentie wordt verleend op alle online geplaatste informatie. Hiermee verliest de gebruiker voor een deel de controle over wat er met zijn informatie gebeurt.
Als gevolg van de verschuiving van desktopapplicaties naar webapplicaties, verschuift de aandacht van criminelen naar de browser in plaats van naar het besturingssysteem. Maar zelfs een up-to-date browser kan de risico's niet wegnemen. De dreiging zit veelal ook in alle plug-ins, toolbars, scripts en andere uitbreidingen die de eindgebruiker aan de browser toevoegt. In het afgelopen jaar zijn er in diverse plug-ins kwetsbaarheden ontdekt en ook misbruikt.
Sociale netwerken op internet zijn enorm populair, maar hiervoor geldt ook een risico. Netwerken als Hyves en MSN bijvoorbeeld zijn actief misbruikt en in het afgelopen jaar doken ook op LinkedIn nepprofielen op waarmee malware werd verspreid. Zelfs Twitter is een geliefd doelwit gebleken van hackers. En daar blijft het niet bij. Mobiel internet op de mobiele telefoon wordt steeds populairder. Over het algemeen heeft een mobiele internetter weinig mogelijkheden om zijn mobieltje te configureren. Updaten en veilig houden van software is dus niet zo gemakkelijk. Het is niet moeilijk voor te stellen wat een geslaagde aanval op een mobiel platform aan kan richten.

Deanonimisatie - verlies van privacy

Aan het verlies van privacy zitten twee kanten. Enerzijds maken internetcriminelen steeds meer persoonlijke gegevens buit, bijvoorbeeld door het inzetten van kwaadaardige software of door het omzeilen van de beveiliging van centrale systemen waarin persoonlijke gegevens zijn opgeslagen. Anderzijds geven internet-

gebruikers zichzelf steeds meer bloot door allerlei persoonlijke gegevens op internet achter te laten. Het vervelende voor hen is dat in het internet geen vergeetfunctie is ingebouwd. Wat men zich hierbij vaak ook niet realiseert, is dat internetcriminelen steeds beter in staat zijn de gegevens uit verschillende bronnen, bijvoorbeeld sociale netwerken, te koppelen. Zelfs als je op verschillende sociale netwerken een verschillende identiteit hebt, kan deze informatie worden gekoppeld.

Kwetsbare software

Kwetsbaarheden in software komen op grote schaal voor. Er moet veel tijd worden besteed aan het up-to-date houden van computers en systemen. Soft- en hardwareleveranciers integreren security steeds vaker in een veilig ontwikkelproces. Ook worden bij software steeds vaker automatische updatemechanismen ingebouwd, zodat het vrijwel geen moeite kost om updates te installeren. Uit een onderzoek van data die bij Google zijn verzameld, blijkt dat volledige automatisch bijgewerkte software veel meer up-to-date is: 97 procent na drie weken. Updates waarbij de gebruiker zelf initiatief moet ondernemen, werden in slechts 24 procent van de gevallen geïnstalleerd in dezelfde periode.

Ondanks de positieve ontwikkeling dat leveranciers meer aandacht besteden aan veiligheid, staat dit nog in de kinderschoenen. Het is vaak toch de verantwoordelijkheid van de gebruiker om veilig te werken en te surfen en die verantwoordelijkheid is te eenzijdig. Aansprakelijkheid voor fouten in een geleverd product wordt gewoonlijk uitgesloten in het End User License Agreement (EULA), het contract tussen de leverancier en de gebruiker. De Europese Commissie heeft een 'digitale agenda' opgesteld voor de consumentenrechten van morgen. Licentieverlening moet de consument van dezelfde basisrechten garanderen als wanneer hij een product koopt.

Hacktivisme

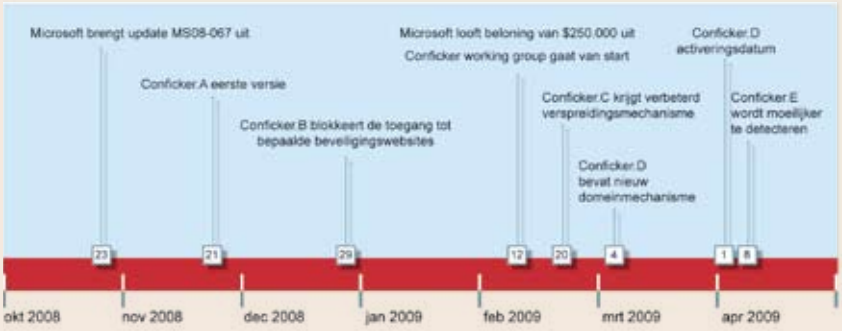
Geld is de belangrijkste drijfveer van de internetcrimineel. Een andere belangrijke drijfveer is hacktivisme, ofwel ideologisch gedreven aanvallen. We zagen aanvallen vanuit Rusland op Estland en van Rusland op Georgië. Het gaat niet zozeer om aanvallen vanuit de Russische overheid, maar in ieder geval door hackers vanuit Rusland en om een principieel conflict. Naast deze cyberoorlogen speelde zich ook een elektronisch conflict af tussen Israël en Hamas. Aanhangers van beide kampen werd opgeroepen malware te installeren waarmee websites van de tegenstander konden worden platgelegd. In Palestina wordt dit ook wel de Elektronische Intifada genoemd.

Positief

Twee positieve trends die worden gesignaleerd hebben betrekking op samenwerking en opsporing. De samenwerking in de strijd tegen cybercrime wordt steeds hechter én effectiever. Een sprekend voorbeeld is de strijd tegen Conficker, de worm die afgelopen jaar op grote schaal wereldwijd computers heeft geïnfecteerd. Vele partijen uit de hele wereld sloegen de handen ineen om de worm te keren en daardoor zijn de gevolgen van het virus beperkt gebleven. Andere voorbeelden zijn te vinden op het gebied van opsporing en berechting. Ook hier is samenwerking en intensief contact tussen onder andere CERT's, ISP's en het Team High Tech Crime van de KLPD en het Openbaar Ministerie uitgemond in succesvolle resultaten. Daarnaast heeft het spamverbod en het toezicht hierop door OPTA grote positieve gevolgen gehad.

Aanbevelingen

De aanbevelingen die GOVCERT.NL doet op basis van haar bevindingen zijn bedoeld voor eindgebruikers en beheerders en tevens voor de politiek, het beleid en de markt. Voor de eerste twee doelgroepen zijn ze praktisch (regelmatig updaten, awareness, patchmanagement, etcetera). Voor de derde partijen zijn ze verregaander. Een aanbeveling als het invoeren van DNSSEC, het uitfaseren van MD5 cryptografie en het stimuleren van automatische updates zijn geen acties die van de ene op de andere dag zijn uit te voeren. Desalniettemin zijn ze bijzonder belangrijk en moet er een begin gemaakt worden: er moeten besluiten genomen worden, zoals in de VS reeds is gebeurd. Daar moeten alle overheidspartijen voor het einde van 2009 verplicht DNSSEC ondersteunen. Juist met de groei van de e-overheid zijn dit soort besluiten van belang, om vertrouwelijkheid en integriteit van overheidsinformatie te kunnen waarborgen.



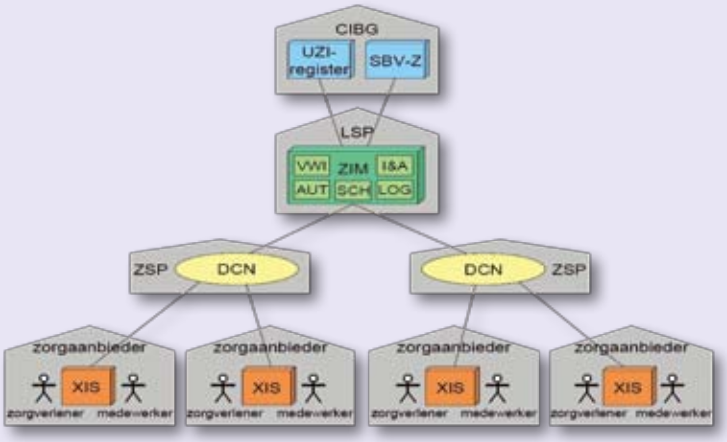
Het GOVCERT.NL trendrapport kan worden gedownload op www.govcert.nl/trends.

GOVCERT.NL is het Computer Emergency Response Team van de Nederlandse overheid. Het werkt aan het voorkomen en afhandelen van ICT-gerelateerde incidenten, 24 uur per dag, 7 dagen per week. GOVCERT.NL ondersteunt organisaties die een publieke taak uitvoeren, zoals overheidsinstellingen, en ze werkt samen met de vitale sectoren. Door middel van www.waarschuwingsdienst.nl wordt het publiek voorgelicht over maatregelen en actuele risico's die betrekking hebben op computer- en internetgebruik.

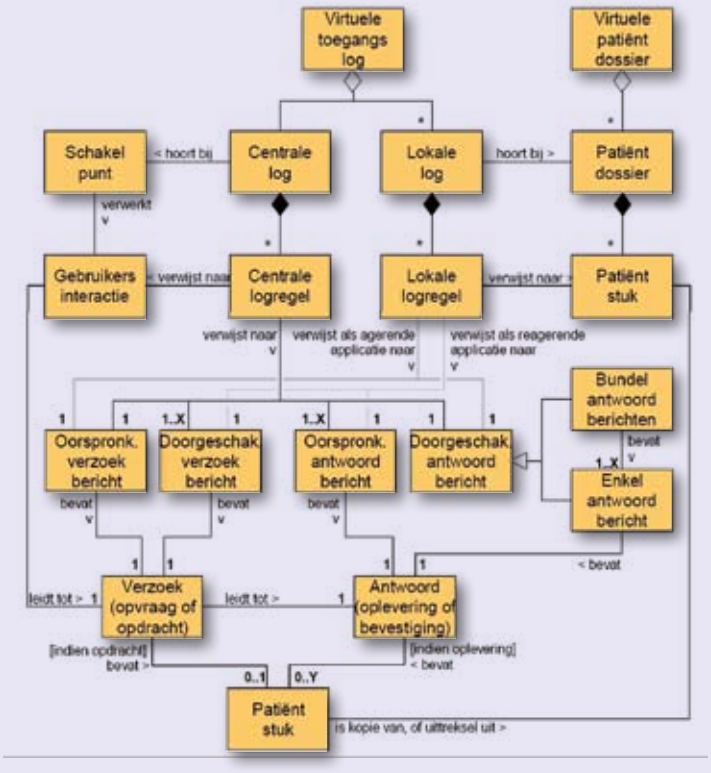
Interessante discussies over het Elektronisch Patiënten Dossier

Auteurs: André Koot (hoofdredacteur, a.koot@unive.nl) *en Erno Duinhoven* (activiteitencommissie, erno.duinhoven@capgemini.com)

Op 9 september jl. organiseerde de activiteitencommissie van het PvIB een seminar over het Elektronisch Patiënten Dossier (EPD). De setting was een nieuwe voor het PvIB, namelijk een debatvorm zoals dat van het televisie-programma Het Lagerhuis. In dat debat werd naar aanleiding van stellingen gediscussieerd over beveiligingsissues rond het EPD. Die debatvorm bleek een interessante oplossing, want het blijkt dat het EPD zorgt voor ophef, zowel op basis van rationele als emotionele gronden. Beide invalshoeken konden we waarnemen, en de overall conclusie luidde dan ook dat we beslist niet de laatste discussies rond het EPD hebben gevoerd.



Architectuur van het EPD



Logging is complex

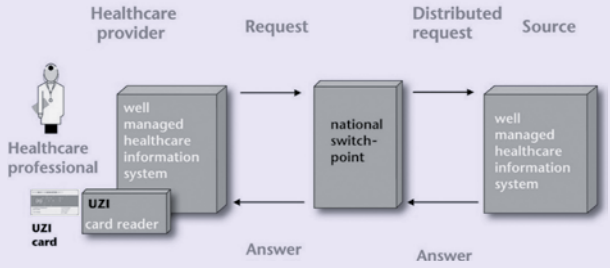
Voorzitter Henk Gomis (CJIB) leidde de hele sessie, die werd begonnen met twee presentaties, een mooi referentiekader voor het debat. De eerste presentatie werd door een 'bezorgde burger' gehouden. Bernhard van der Feen (van Microsoft Nederland, maar sprekend op persoonlijke titel) gaf aan waarom hij twijfelt aan het EPD, zoals dat nu ingevoerd wordt. Hij schetste de context, de aanleiding ervoor en stelde vervolgens een groot aantal vragen, waarachter we zijn zorgen konden aanhoren. En zorgen heeft hij genoeg.

Ten eerste zijn volgens Bernhard nut en noodzaak van het EPD onvoldoende aangetoond. De wens om het aantal medische missers terug te dringen en de wens om te kunnen besparen, zijn niet onderbouwd door onafhankelijk onderzoek. Het EPD zou medische missers door foutieve medicatie moeten terugdringen, maar er is niet onderzocht in hoeverre dat ook zal gebeuren. Niet elke medische misser ontstaat immers door onvoldoende informatie. Waar dan ook de besparing zit, is niet duidelijk.

De architectuur van het EPD baart ook zorgen. Er is gekozen voor een gedistribueerd model: geen centrale opslag van medische gegevens, maar opslag in de systemen van de lokale zorgverleners. Maar dat betekent dat er risico's zijn rond de beschikbaarheid van de lokale systemen (geen garanties…) en beveiliging van de lokale systemen (weet de gemiddelde huisarts daar ook maar iets van?).

Een probleem van een andere orde is de verantwoordelijkheid van de patiënt. Als hij zijn eigen gegevens kan inzien, is hij dan ook zelf verantwoordelijk voor de betrouwbaarheid ervan? En is hij verantwoordelijk voor het vaststellen van misbruik? Hoe gaan we daar mee om? Is een security monitoring proces wel voorzien en zo ja: van wie is dat dan? Hoe gaan we om met de logging?

Het systeem als geheel is zeer omvangrijk. De gelaagdheid van het model, maar ook de processen daarbinnen maken beheersing een flinke klus. Hoe zit het autorisatiemodel in elkaar? Ik, als patiënt, kan bepalen wie wat mag zien. Maar



< Gedistribueerd autorisatiemechanisme

hoe werkt dat? Kan ik ervoor zorgen dat mijn buurmeisje, dat doktersassistente is, mijn gegevens niet kan bekijken? En hoe weet ik dat zij niet werkt met het account van mijn huisarts?

Albert Vlug van NICTIZ liet een tegengeluid horen. NICTIZ is mede betrokken bij de invoering van het EPD. Hij ging vooral in op de vele autorisatiemechanismen binnen het EPD. Privacy en afscherming van medische gegevens is van vitaal belang en dus ook de beheersmaatregelen. Er zijn protocollen ontwikkeld en er wordt onder meer aangehaakt bij de UZI-pas om de identiteit van een raadpleger te kunnen vaststellen.

Daarbij komt dat de huidige functionaliteit van het EPD beperkt is tot een Elektronisch Medicatie Dossier en een Waarneemloket. Het mogelijk maken van datatransport en bijvoorbeeld fotodiagnose volgt later.
Wat Albert duidelijk maakte, was dat de menselijke factor een aandachtspunt is en blijft. Uiteindelijk zijn de zorgverleners verantwoordelijk voor zorgvuldig gebruik.

Helaas kon Albert geen aandacht besteden aan alle zorgen van Bernhard. De complexiteit van de architectuur en de waarborgen op dat gebied en de zorg over wie nu wat kan binnen het systeem bleef onbeantwoord. Voor ons ontstond de vraag wat nu eigenlijk het doel is van het EPD. Als het alleen zou gaan om het tegengaan van medische fouten door onjuiste medicatie, dus een EMD, dan is daar vast wel een goede legitimering voor te vinden.
Maar dan zou een andere dan de huidige architectuur wellicht handiger zijn. Minder gegevens nodig, minder te beveiligen. Maar de omvang van het EPD gaat verder. Hoe ver? Geen idee, en daardoor kunnen we eerder meegaan in de zorgen van Bernhard, dan in het vertrouwen van Albert…

Na de pauze werd gestart met het debatgedeelte van het Lagerhuis. De eerste stelling ging over de repressieve maatregelen die in het kader van misbruik van het EPD zouden kunnen gelden. Er werd gelijk op ingesprongen door de vraag te stellen hoe misbruik geconstateerd kan worden en wie dat doet. De zorgconsument kan dat niet zelf. Hieraan verwant is de discussie wie er eigenlijk eigenaar is van de gegevens. De 'custodian' is geregeld, maar het eigenaarschap niet. Belangrijk onderdeel in de detectie van misbruik is de centrale logging. Omdat het EPD een gedistribueerd systeem is, waarbij de afzonderlijke onderdelen in staat zijn onderling te communiceren, hangen de beveiligingsmogelijkheden af van de lokale inrichting.
Volgens Albert is door toepassing van technische middelen misbruik uitgesloten, met één uitzondering: een geneeskundige kan een behandelrelatie met een zorgconsument claimen en daarmee zijn gegevens inzien. De zorgconsumenten krijgen wel de mogelijkheid om bepaalde toegang in de autorisatiesfeer uit te schakelen. Op termijn kan misbruik via 'datamining' worden opgespoord, vergelijkbaar met het opsporen van creditcardfraude.
Er zijn twee instanties die sancties kunnen opleggen: het College Bescherming Persoonsgegevens (CBP) en de Inspectie voor de GezondheidsZorg (IGZ). De deelnemers aan het debat waren het er in grote lijnen mee eens dat de slachtoffers persoonlijk moesten worden geïnformeerd, het Californische model. Ook schadeloosstelling lijkt logisch, vergelijkbaar met creditcardfraude, om het vertrouwen van de zorgconsumenten te behouden.
Van vergaande sancties als ontslag na constatering van misbruik, wordt weinig verwacht, omdat dit ook maar zelden gebeurd bij medische fouten.

De tweede stelling ging over privacy. Privacy, zo wordt aangegeven door de deelnemers, is een grondrecht, maar het is sinds '11 september' geërodeerd. Bovendien is privacy geen absolute norm. De deelnemers vonden het EPD ondoorzichtig: wij weten niet wat er in het EPD staat en wat er met de gegevens gebeurd. Een deelnemer vroeg zich af of hij meer ziektekostenpremie moet betalen als hij gebruikmaakt van de opt-out regeling. Maar dat maakt geen verschil maakt ten opzichte van de huidige situatie, de zorgverzekeraar betaalt immers de rekeningen al en kan misschien al achterhalen wat hun cliënt mankeert. Het EPD is daarmee voor verzekeraars niet eens nodig. Dit werd later in de discussie genuanceerd, al had het statement 'Vertel mij uw medicatie en ik weet wat u mankeert' veel bijval.

De afsluitende stelling ging over de beveiliging van het EPD ten opzichte van de huidige situatie. Algemeen werd de schaalvergroting aangegeven als een probleem. Zeker als de zorgverlener nog een papieren dossier heeft. Een stapel dossiers van een huisarts neem je niet even mee onder je arm; een harddisk van 1TB wel.
Negenduizend zorgverleners kun je niet beveiligen. Negenduizend zorgverleners betekenen ook negenduizend potentiële lekken. Voor de kleine zorgverleners geldt zelfevaluatie tegen de NEN 7510 voor toelating tot het EPD. Deze vorm van evaluatie wordt door bijna iedereen als onvoldoende bestempeld.

Ten slotte werd er ingegaan op het idee van het introduceren van een logo voor een zorgverlener die zijn zaken op beveiligingsgebied op orde heeft. De voor- en tegenstanders van logo's wisselden elkaars pleidooien af, waarbij de tegenstander van een logo de meeste argumenten noemden. 'Een logo werkt niet', 'Kleine zorgverleners helpen certificering', 'Een logo wordt niet begrepen', 'Een logo is marketing', 'Een logo zegt alleen iets over het verleden'. Overeenstemming werd in ieder geval gevonden in de stelling dat een logo of keurmerk problemen zou veroorzaken: een huisarts is een vertrouwenspersoon en moet ik nu een andere huisarts zoeken, alleen maar omdat geen logo (meer) heeft?

De avond werd afgesloten met een netwerkborrel waar de discussie werd voortgezet. Vele positieve reacties waren te horen over de sprekers en de open discussie.

Bernhard van der Feen heeft aan het PvIB een uitgedaagd een werkgroep te starten waarin een advies over de beveiliging van het EPD kan worden gegeven aan zorgconsumenten, de gezondheidszorg, zorgverzekeraars en de overheid. Een mooie kans voor het PvIB? Laat uw mening horen op activiteiten@pvib.nl.

Voorkom schijnveiligheid door een veilig ontwerp

Auteur: Kees Hogewoning > Kees Hogewoning is Security en infrastructuur consultant bij Vanveen informatica en is bereikbaar via hogewoning@vanveen.nl.

Het doel van IT-beveiliging is om IT-middelen en het gebruik ervan veiliger te maken. Niet alle beveiligingsmaatregelen bieden ook relevante veiligheid. Sommige maatregelen lijken veiligheid te bieden, maar doen dit niet. Het gevolg is dat een beheerder, een eigenaar of een gebruiker denkt op een veilige manier bezig te zijn, terwijl dat niet zo is. Door deze schijnveiligheid kunnen aanvallers misbruik maken van de zwakke plekken die aanwezig zijn. Het toepassen van de juiste beveiligingsmaatregelen blijft door schijnveiligheid achterwege. Het herkennen en voorkomen van schijnveiligheid is dus belangrijk.

Schijnveiligheid, maar ook een goede beveiliging is niet gemakkelijk te herkennen. Een applicatie geeft bijvoorbeeld aan dat deze veilig geconfigureerd is, zoals dat bijvoorbeeld gebeurt met het slotje in de webbrowser (in de kaders bij dit artikel worden verschillende voorbeelden van schijnveiligheid aangegeven). Om te weten dat dit slechts schijnveiligheid is, zul je de techniek erachter moeten kennen. Als je weet hoe SSL werkt, dan kun je ook weten dat de weergave van het slotje niet aangeeft dat de website zelf te vertrouwen is. Een gezonde dosis achterdocht is nodig om schijnveiligheid te ontmaskeren.

Security through obscurity

Het meest bekende voorbeeld van schijnveiligheid is security through obscurity. Bij het toepassen van dit principe wordt geheimzinnigheid gebruikt als beveiligingsmiddel. Door zwakke plekken in de beveiliging geheim te houden, wordt gehoopt dat de zwakke plekken niet gevonden worden en dat er geen misbruik van gemaakt wordt. Maar volgens de bekende wet van Murphy zullen vroeg of laat de zwakke plekken gevonden worden. Wanneer dat gebeurt, is niet te voorspellen. Dat maakt het gebruikt van security through obscurity zo gevaarlijk. Je weet van te voren niet wanneer de zwakke plek gevonden gaat worden en wanneer er misbruik van gemaakt kan worden. Je loopt dus continu een risico. Security through obscurity is wel een geschikt aanvullend beveiligingsmechanisme. Waarom zou je het een aanvaller of hacker gemakkelijk maken? Het risico op een inbraak is klein wanneer de beveiliging in orde is. Hoe het beveiligd is, hoeft een hacker niet te weten. Dat is voor hem of haar immers extra informatie die gebruikt kan worden om alsnog een andere zwakke plek te vinden.

Openheid

Aan de andere kant geeft volledige openheid als tegenhanger van security through obscurity de mogelijkheid dat anderen de beveiligingsmaatregelen kunnen controleren. Van opensourcesoftware is bekend dat iedereen de broncode kan inzien, controleren en aanpassen. Een vaak aangehaalde uitspraak is: 'Given enough eyeballs, all bugs are shallow'. Hiermee wordt aangeven dat als er maar genoeg mensen (programmeurs, testers, enzovoort) naar de software kijken, alle bugs gevonden en opgelost kunnen worden. Volledige openheid suggereert dat er geen zwakke plekken zijn. Toch zitten er ook in opensourcesoftware ook veel fouten. De vele ogen die de broncode kunnen bekijken, maken de software niet foutloos. Er zijn verschillende redenen waardoor dit komt. De belangrijkste is dat weinig mensen de moeite nemen om naar de broncode naar kijken. Hoeveel procent van de Linux-gebruikers zou de broncode ervan bekeken hebben? Ik in ieder geval niet. De tweede reden is de kwaliteit van de broncode en de aanpassingen die daarin gemaakt worden. Als mensen de moeite nemen om de broncode te bekijken dan hoeven (complexe) fouten nog niet opgemerkt te worden. Ook aanpassingen die in de broncode gemaakt worden, kunnen ook weer fouten bevatten. Niet iedereen is tenslotte een goede programmeur.

Opensourcesoftware wordt vaak ontwikkeld door zogeheten communities. Dit is een groep programmeurs en andere betrokkenen die gezamenlijk aan een programma werken. Ze beginnen met het idee, schrijven de software, testen en distribueren dit. Daarnaast gebruiken ze de software ook zelf. De kwaliteit van het geleverde product staat of valt met de kwaliteit van de community. Hoe meer programmeurs, testers en gebruikers en hoe beter ze hun vak verstaan, des te beter kan de geleverde kwaliteit zijn. De beoordeling van opensourcesoftware is dus in belangrijke mate een beoordeling van de betreffende community.

Secure design

Naast openheid, zodat beveiligingsmaatregelen gecontroleerd en beoordeeld kunnen worden, is een veilig ontwerp (*security by design*) een belangrijk uitgangspunt om veilige systemen te maken. De term *security by design* en de daarbij behorende methoden worden vaak gebruikt bij software-ontwikkeling. Dit principe gaat echter veel verder, het is voor de volledige infrastructuur van toepassing. Secure design wordt toegepast om zwakke plekken in een infrastructuur te voorkomen.

Ongelaagde beveiliging

Een andere vorm van schijnveiligheid is het vertrouwen op één vorm van beveiliging. Helaas veel gehoorde argumenten zijn 'ik heb toch een firewall' of 'ik heb toch een virusscanner'. Hierbij is de gedachte dat alleen een firewall of alleen een virusscanner voldoende beveiliging is. Het beveiligingen een infrastructuur dient op verschillende niveaus te gebeuren. Alleen een virusscanner of firewall is niet voldoende. Het idee dat dit volledige veiligheid biedt, is een schijnveiligheid. Een virusscanner beschermt tegen virussen en een firewall bepaalt welk netwerkverkeer is toegestaan. Als er alleen een firewall gebruikt wordt en deze staat netwerkverkeer op tcp-poort 443 toe, dan kan een virus of malware door deze poort binnenkomen. Een virusscanner of firewall dekt alleen een deel van de bedreigingen af. Tegen andere bedreigingen zijn dan geen maatregelen genomen. Door het toepassen van secure design worden bedreigingen inzichtelijk gemaakt en kunnen passende maatregelen genomen worden.

Beveiligingsmeldingen
User account control (UAC) in Vista vraagt de gebruiker om toestemming om acties uit te voeren waarvoor administratorrechten nodig zijn. Als een gebruiker (te) vaak voor toestemming gevraagd wordt voor handelingen, zal het steeds makkelijker worden om op 'continue' te drukken zonder de dialogen te lezen. UAC geeft dan schijnveiligheid.
Het beveiligingsmechanisme is aanwezig, maar het gebruik ervan biedt geen veiligheid. In secure design zou dit gebruik van UAC als mogelijke bedreiging ervan vastgesteld moeten zijn. Een passende technische maatregel zou echt onderscheid tussen een administrator en een gebruiker kunnen zijn.

Voor het ontwikkelen van een secure design zijn de volgende stappen van belang:

1 Ontleden van de infrastructuur in de verschillende onderdelen waaruit deze bestaat. Hierbij wordt inzichtelijk gemaakt uit welke onderdelen de infrastructuur bestaat, wat ze doen en hoe ze met elkaar communiceren. Dit kan eenvoudig in een tabel en tekening worden weergegeven. In een tabel kan worden aangegeven welk onderdeel communiceert met welk ander onderdeel. Ook wordt aangegeven wat het doel is van de communicatie en welke protocollen gebruikt worden. In tekeningen worden de logische en de fysieke configuratie van de infrastructuur weergegeven. De tekening van de fysieke configuratie geeft aan welke apparatuur en andere tastbare onderdelen gebruikt worden. In een logische tekening wordt aangegeven welke services, software, databases en andere niet-tastbare onderdelen gebruikt worden en hoe ze aan elkaar gekoppeld zijn. Door het ontleden van de infrastructuur zijn de volgende stappen makkelijker uit te voeren. Ook voor het beheer kan dit een handig hulpmiddel zijn.
2 Bepaal de mogelijke bedreigingen. Hierbij worden de mogelijke bedreigingen bepaald die van invloed zijn op de beschikbaarheid, integriteit en vertrouwelijkheid van de infrastructuur en de informatie die in de infrastructuur wordt bewaard, bewerkt en getransporteerd.
3 Bepaal het risico van de bedreigingen. Hierbij wordt gelet op de mogelijke schade en andere gevolgen die kunnen ontstaan bij misbruik van een vulnerability. Ook de kans dat er misbruik gemaakt wordt van de vulnerability is een belangrijke factor. Deze kans kan onder andere door security through obscurity verkleind worden.
4 Bepaal maatregelen waarmee de bedreigingen verkleind of voorkomen kunnen worden. Naar aanleiding van de in de vorige stap bepaalde risico's is de prioritering van de op te lossen bedreigingen al bepaald.

Een hulpmiddel om een infrastructuur *secure by design* te laten zijn, is het maken van een security architectuur. In een security architectuur worden security principes vastgelegd. Deze principes zijn vaak erg high-level, maar ik ben voorstander van meer praktische principes. Architectuur is tenslotte een hulpmiddel en geen doel op zich. Op grond van deze security principes worden technische maatregelen ingevoerd. Zo kan standaard een groot deel van de bedreigingen voorkomen worden. Security principes zijn bijvoorbeeld:

- Gebruikers en processen mogen niet meer rechten hebben dan strikt noodzakelijk.
- Elke gebruiker heeft een eigen persoonlijke account. Hij/zij gebruikt alleen het eigen account en het gebruik wordt gelogd.
- Pas een minimale configuratie toe zodat niet meer applicaties, processen, protocollen en poorten gebruikt worden dan strikt noodzakelijk.
- De beveiligingsmaatregelen en de risico's worden periodiek gecontroleerd en daar waar nodig aangepast. De beveiligingsmaatregelen moeten relevant zijn (en dus ook geen schijnveiligheid creëren) en in verhouding staan met de waarde van wat beveiligd wordt.

En zo zijn er nog wel meer principes te bedenken.

Conclusie

Het herkennen van schijnveiligheid is belangrijk om beveiligingsmaatregelen op hun waarde te kunnen beoordelen. Zo kan bepaald worden of de beveiliging voldoende effectief is en of er geen gaten zitten in de beveiliging. Security through obscurity is bruikbaar als aanvulling op beveiligingsmaatregelen, maar het is niet iets om volledig op te vertrouwen. Openheid in de beveiligingsmaatregelen maakt dat de beveiliging te controleren is. Deze controle moet dan ook wel uitgevoerd worden en dan juist door iemand die weet wat de mogelijke bedreigingen en risico's zijn.
Een hulpmiddel om een veilig ontwerp te maken, is het toepassen van een security architectuur. Een praktische security architectuur fungeert als checklist van alle punten waaraan in het ontwerp gedacht moeten worden. Door met een veilig ontwerp te beginnen, kun je de hacker een stap voor zijn. Een veilige omgeving is secure by design.

SSL-certificaten

De banken proberen met de campagne '3x kloppen' het internetbankieren veiliger te maken. Op basis van drie regels moeten klanten controleren of de beveiliging klopt. Klopt uw pc-beveiliging, klopt de website en klopt uw betaling?

Eén van de geadviseerde punten waar een klant naar moet kijken om te bepalen of hij de juiste website gebruikt is het slotje in de webbrowser. Dit slotje geeft het gebruik van SSL aan. Het SSL-certificaat moet van de bank afkomstig zijn. In de praktijk blijkt dat een certificaat makkelijk aan te vragen is met vervalste gegevens. Het nabouwen van een website van bank is ook zo gebeurt. Het certificaat kan dan functioneel helemaal kloppen en toch is de website niet te vertrouwen. Het slotje in de webbrowser is alleen maar het bewijs dat er een versleutelde verbinding is opgezet. Of de communicatiepartner te vertrouwen is, staat of valt met het vertrouwen van de degene die het certificaat ondertekend. Dat is de certification authority. Deze CA hoort de identiteit van de aanvrager van een certificaat te controleren. Sommige CA's zijn niet zo nauwkeurig met deze controle.

Aan de hand van het rootcertificaat controleert de webbrowser of het certificaat ondertekend is door een vertrouwde CA. Wie bepaald nu welke CA's te vertrouwen zijn? Dat doet in eerste instantie de leverancier van de webbrowser. Deze bepaald welke rootcertificaten opgeslagen worden in de webbrowser. Een gebruiker kan ook zelf rootcertificaten toevoegen of verwijderen. Een hacker zou dus een gebruiker kunnen overhalen om een rootcertificaat van de hacker toe te voegen.
Het gebruik van certificaten is volledig gebaseerd op vertrouwen. Het vertrouwen op alleen een slotje in de webbrowser is dus schijnveiligheid. Het slotje in de webbrowser lijkt veiligheid te bieden maar doet dit niet.

Use of DEMO as a methodology for business and ICT security alignment

Auteur: Yuri Bobbert > Yuri Bobbert is Consulting Partner at B-Able, certified DEMO professional. Hij is per email bereikbaar via yuri.bobbert@b-able.nl. Co-author: Joop de Jong, Lector Extended Enterprise studies at Utrecht University of Applied Sciences and member of the Demo board.

In search of finding stronger methods to design a secure enterprise, DEMO[1] is underexposed. DEMO is a widely adopted international standard for designing and engineering 'extended enterprises'. The notation 'extended' indicates the broad variety of social interaction and interoperatibility between enterprises to accomplish a mutual benefit. Enterprises work together on all kinds of layers within the organization and therefore they cope with more and more extended inter(trans)actions that make use of information technologies –like the internet- to exchange business critical information. The exchange of critical information via the internet and the possible impact this may have on the confidentiality, integrity and availability of this information is rather unknown. The problem of the unawareness of security breaches that might occur during the information exchange between enterprises emphasizes the urge of examining the three mentioned areas of concern at the start of the design phase. In our opinion, it has to be embedded into the theory of design. The objective of this article is to determine the security aspects which are unique for each DEMO layer as well as the principles for implementing secure enterprises.

Background

To make this rather technology orientated paper readable for 'business' audience (target area) we would like to discuss a case about a fictional hospital. By using this case, business people have to abstract from all the details of this specific case to a more general way of working concerning exchanging data with third parties.
In particular, the effects of not exchanging data securely are exhibited. I chose the hospital case because every Dutch citizen was recently requested to authorize access rights to his or her medical records.
The main objective behind this request is to serve better healthcare in the Netherlands. With the electronic patient database (EPD) developments in mind and knowing that the data exchange infrastructure is far from ready to exchange this EPD securely, there was enough reason to examine this subject. Another reason why I chose this hospital case is due to the fact that commercial companies are developing health care applications (e.g. Google Health). With these applications it is possible to view records and exchange medical files. New web[2] technologies not only make it possible to exchange between hospitals but also between commercial companies, and even countries with other social ethics. For involving third parties into your own business process we consistently use the term 'extended enterprise'. So the example of a hospital that makes use of web technologies to exchange confidential medical records can be considered as an example of the extended enterprise.

The social impact of technology so far ahead of what we morally may want, makes it even more necessary to examine and to present a well considered way of modeling secure extended enterprises. The main reason for examining this topic is to find out if DEMO is suitable for the design of a secure extended enterprise.

What is DEMO?

DEMO is developed by Prof. Dr. Ir. J.L.G. Dietz at Delft University. DEMO has proven itself to be an effective methodology of decomposing the enterprise based upon the ψ-theory. The Greek letter is pronounced as PSI and stands for Performance in Social Interaction. This is the basic paradigm of this theory: the performance of the business in relation to the social interaction with itself and other systems. DEMO distinguishes three layers of critical essence: the business layer, the information layer and the data layer.

The business layer is the essential layer for enterprises to communicate and interact to establish business critical results. This layer consists of actors who initiate unique actions that lead to unique results. On this layer actors can interact with other social entities (actors) from other enterprises. For example a surgeon in hospital A requires a medical record to treat a just brought in car-crash patient whose medical records have been recorded in Hospital B. The treatment of this patient is the core business of the hospital and the responsible and competent actor who is authorized by hospital A is the surgeon (actor). The treatment of the patient leads to new and unique facts.

The information layer is the intermediate layer between business and data. The business actors need information to conduct their production acts. The information is the result of interpreting

1. DEMO Design and Engineering Methodology for Organizations (http://www.demo.nl).

2. In common literature this advanced way of exchanging data via the internet is called WEB 2.0.

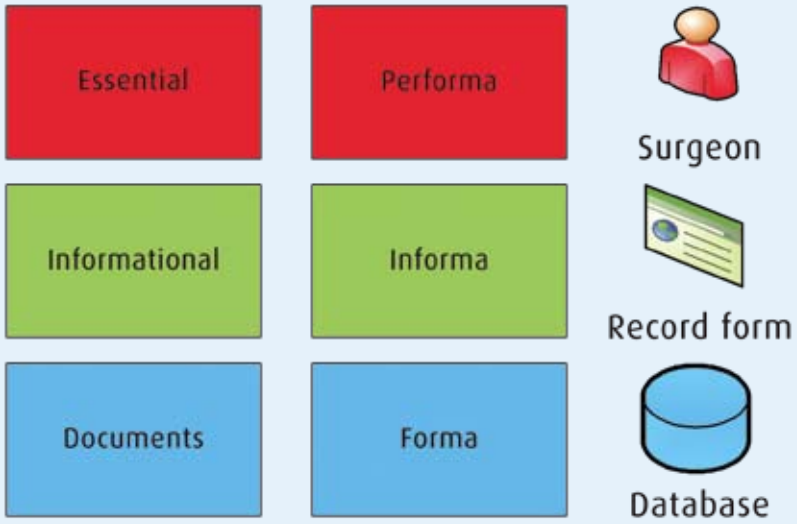


Figure 1: The three DEMO layers and their function

the data. The data initially is extracted from the data layer and is computed, reasoned, etcetera, by the information layer before it is offered to the business layer. In our example the surgeon reads the medical record (EPD) by use of information technology. The record is presented in a certain user interface. Before the data reaches the surgeon certain compatibility algorithms (protocol hand-shakes) need to be exchanged between both systems before the surgeon has privileged access to the patient's private records.

The data layer stores, copies or destroys all kind of documents (data). This layer distinguishes from the information layer in that it only concerns the form (forma) of the data and that it is not concerned in the content (informa) of the data. In the hospital case the surgeon approaches the medical records of the patient via the information layer. The medical records are stored in the data layer as static information in bits and bytes. This information could be blood type information and statistics or medical history to effectively threat the car-crash patient with the right type of blood and the right medication.

When we extend this data exchange to other enterprises the surgeon we had previously might need to extract several forms of data from several other enterprises.

Why DEMO-transactions?

Demo is used to visualize which layers within the organization serve the business function (conducting the business transactions), the information function (delivering information and storing original actions), and the data function (storing, retrieving and transmitting data that corresponds with original and derived actions). For each layer it has to be determined which transactions are critical and which security aspects are critical. For determining if security principles are suitable to embed into DEMO in this article we focus on the applicability to the Business and the Information layer only. Our special attention is to discuss where in the different DEMO models for both layers we have to introduce these principles. To determine which security principle to use in DEMO, we build on the three basic security principles Confidentiality, Integrity and Availability, CIA in short. I used these three basic principles to map them over the several DEMO models and derive them subsequently into principle scenarios.

On the business function (Performa) contextual influences, like corporate governance, and organizational political influences, like IT governance and security principles, have impact on business processes and might harm the confidentiality, integrity and availability of business transactions. By making use of the Transaction Result Table (TRT) we can quickly determine what breaches can occur on a specific business transaction and what their impact could be on the result.

With the help of the Information Use Table (IUT) and the Process Structure Diagram (PSD) we can determine where in the business transaction certain information is required. On these IUT and PSD the CIA principles are mapped to determine where security breaches might influence the transaction. In this example medical files can only be accessed by an authorized doctor, unauthorized individuals are not allowed to access these files. The identification and the claim to authorization are typical security aspects which have to be dealt with by actors at the Informa layer in the organization. By means of the data layer, the data that corresponds with original actions is stored to serve the above lying information layer. By separating static data (data at rest) from dynamic information (in motion) you can decide what CIA breaches can occur and what measures are required to mitigate risk or damage. For example you could store medical records at a Trusted Third Party on a high available storage cluster with strict separation of duties or you could store them in the cloud at Google.com. Both are ways to store data but with different CIA perspectives, the DEMO theory is a powerful method to distinguish data formats (Forma) and to determine where and when to implement certain security principles.

Because DEMO addresses business, information and data layers of the organization the DEMO theory ought to be more accepted across the enterprise departments. It provides insights in all organizational layers and therefore in possible information security issues. By

Initiator	Transaction	Result	Executor
CA01 Patient	T01 Treatment of Patient P	R01 Treatment of patient P has been completed	CA00 Treatment Handler
CA00 Treatment Handler	T02 Treatment by Medical Expert	R02 Treatment by Expert has been completed	A03 Expert
CA00 Treatment Handler	T03 Approve Medical File View	R03 File View has been approved	CA01 Patient

addressing each layer and making use of the SDEMO checklist (explained later on) it makes IT security 'readable' and therefore acceptable for business as well as IT people. It helps business and IT align by achieving mutual goals.

Understanding security breaches and possible risks help create awareness and is a necessity when it comes to allocating IT investment.

From DEMO transactions to security principles

To determine which principles to implement per layer we need to breakdown from ontology to construction. Dietz introduced DEMO and mainly focused on the business layer of the enterprise. De Jong focuses more in detail on distinguishing between information and data and how to construct architectural principles. When we introduce security principles in the design process of the extended enterprise it is necessary to address these principles during the design of these information (I) and data (D) layers. De Jong calls this the design of the D and I-organization. Based on the work of De Jong I will elaborate on some security principles by using the hospital case as an example of the extended enterprise.
To fully understand the essential need for DEMO I have followed the several DEMO modeling methods and made use of the basic notations[3]. Starting off with the Transaction Result Table where we state the essential transactions and their results (Facts).

After the TRT we graphically model these transactions and actors in a Global Actor Transaction Diagram (figure 2).

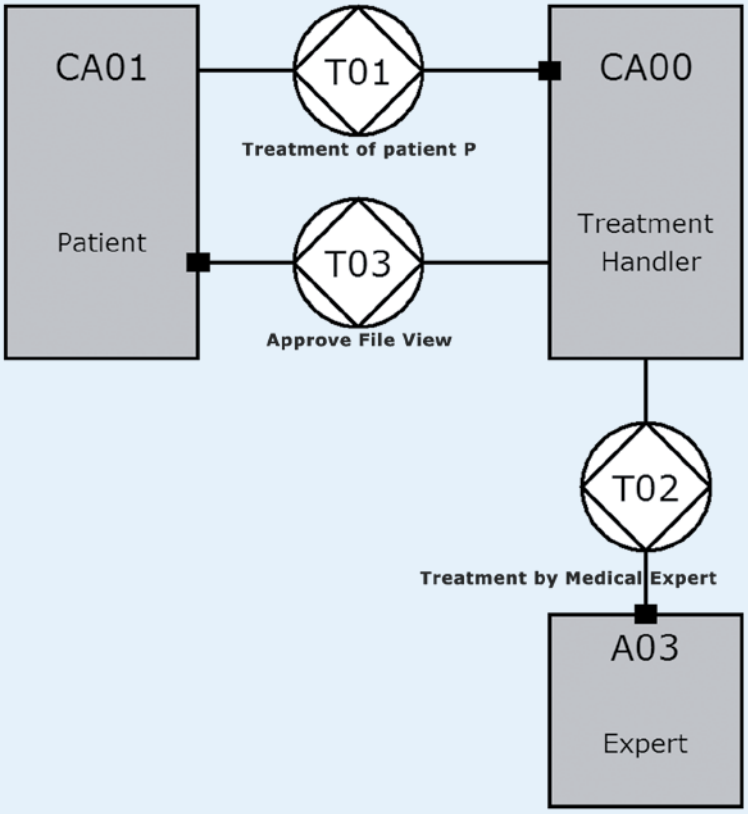


Figure 2: Global Actor Transaction Diagram Hospital Case (ATD)

In figure 3 the ATD is displayed, with Production Bank 'Medical File'. In this case the collective name for EPD and Production Bank is 'Security principles DB'. This is the external source where the hospital gets its security policy (best practices) information from.
It is necessary to determine where in DEMO security principles have to be introduced. Therefore it is important to distinguish the two actor roles in a basic transaction state that a specific transaction is in.
The requester is called the initiator and the deliverer is called the executor. The basic transaction pattern within DEMO is distinguished in three phases. The Order phase, Execution phase, Result phase. These OER phases are detailed by designing the transaction pattern according to the DEMO Process Structure Diagram (PSD), displayed in figure 4.

After detailing the transactions in DEMO we need to distinguish the variety of security threats that might arise during transactions. I therefore introduce a Secure Demo checklist (SDEMO) which can be used per layer of the organization to determine security measures.

From security principles to security investments

The DEMO Product Structure Diagram (PSD) is limited to the business layer. That means that the Security Code of Practice triad of Confidentiality, Integrity and Availability is only applicable for the business layer. The focus on the business layer neglects the layer where most of the CIA breaches arise.

3. For limitation purposes we narrowed down the number of Hospital Transactions to the basics.

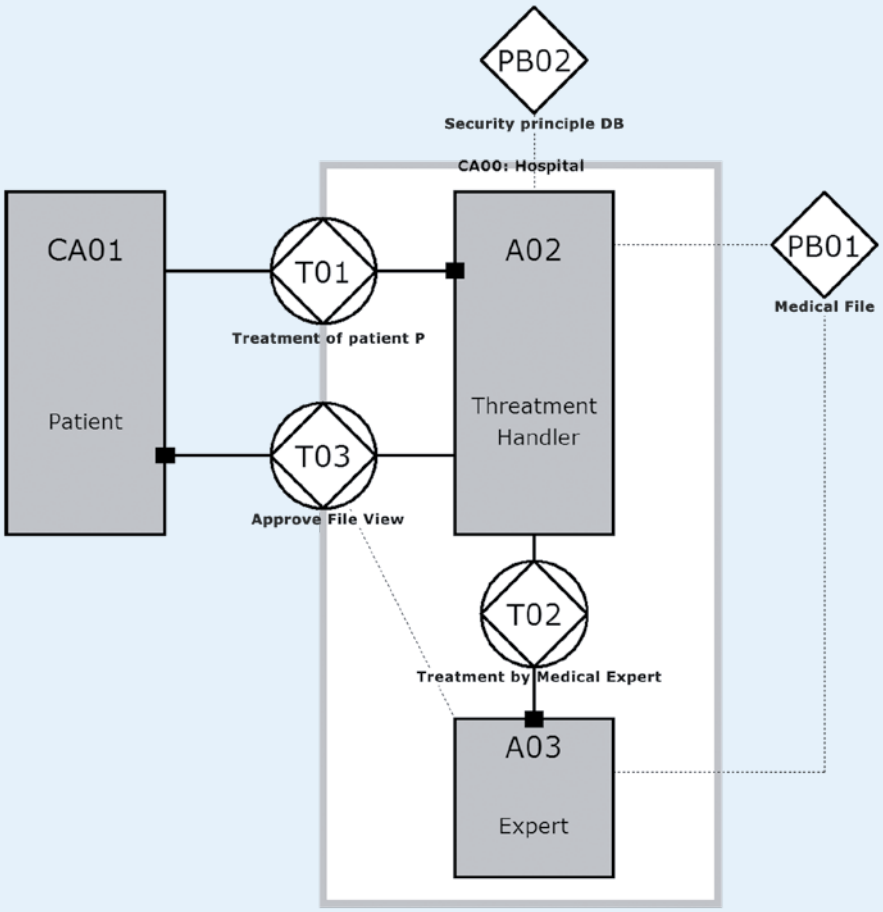


Figure 3: ATD with Production Bank 'Medical File'

Namely the I-layer and D-layer. When we go down into this I-layer of the organization and model the so called I-organization we explore all information transactions and informational actors[4]. Based upon these I-transactions we determine what CIA breaches these transactions reveal. It is here where the necessary principle scenarios need to be designed in order to take adequate measures to avoid negative impact. This is typically an exercise done by people with technical skills. After defining these principles the information (security) manager together with his business responsible people has to decide which principle to implement (and how much budget to allocate).

SDEMO Checklist

To align business and ICT people and fully benefit from the power by separation of B-I-D transaction layers of DEMO a checklist is developed. Business as well as technical people can use this checklist per layer of the organization and per transaction. This SDEMO checklist should have a dynamic character and is filled with the basic CIA security related questions that might arise during transaction

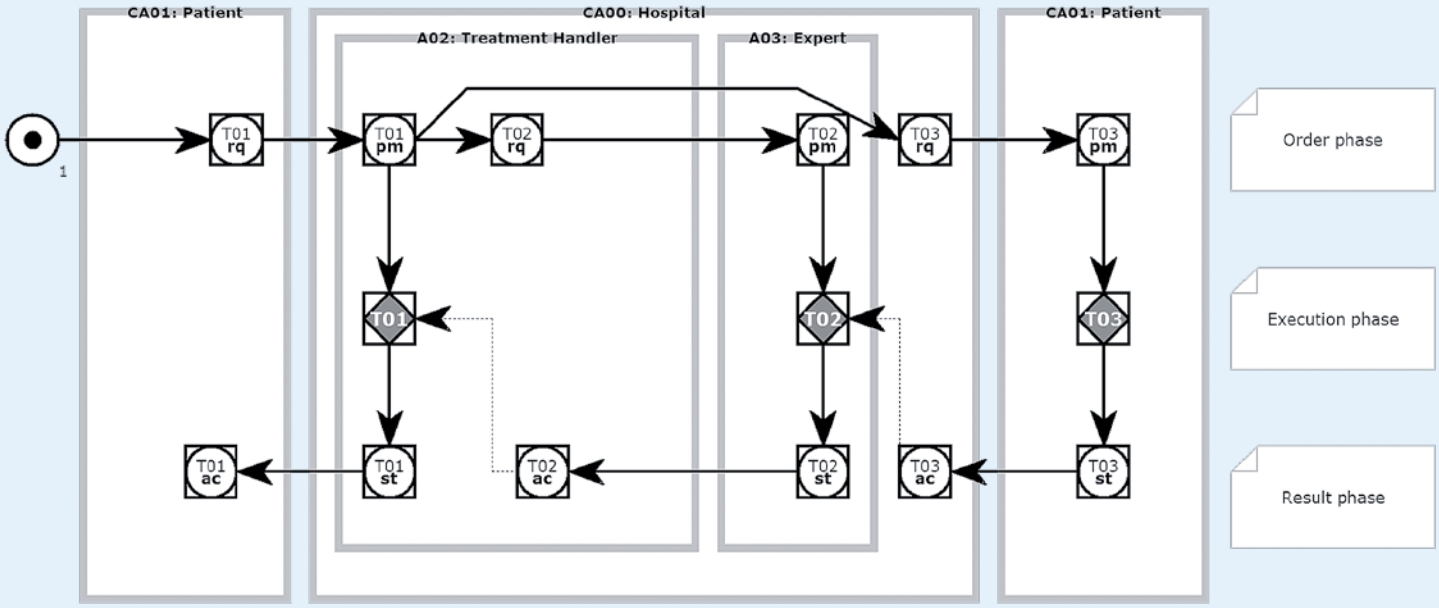


Figure 4: The DEMO process Structure Diagram displaying the state of a transaction

4. The specification of the I-layer according to DEMO with security principles is provided in the appendix

Demo layer	SDEMO Question
Performa (business)	1. Is this transaction business critical? 2. What if this transaction fails? 3. What if this transaction is not able to order, execute or request? 4. If transaction completed, what (information) result do I get and what's the criticality of this fact?
Informa (information)	1. Do I know all information actors involved in the transaction? 2. How are identification, authentication, authorization and administration handled? 3. What is the result, the impact on the business if information (during process) is stolen, manipulated or lost? 4. Is there an information handling procedure in place?
Forma (data)	1. Where is the data stored? Physical/virtual? 2. How can data be accessed? 3. Is there an access control policy and are control methods in place? 4. How is backup and restore handled?

handling.
We use the DEMO notation to effectively display all actors and transactions at an ontological level. After that we use the SDEMO checklist to address security issues that might arise. By using the combination of methods this method addresses (to stakeholders) the criticality of protecting the enterprise critical assets by interaction in a complex environment (extended enterprise). Most of the used DEMO basic modeling techniques like the construction model, process model, state model and action model have good starting points to extend the design with security principles. Either you use the CIA principles or you use standard baselines like BS, Cobit, ISO/IEC, HIPAA, NEN, SOx or other compliancy regulators, depending on the contextual influences (corporate governance) that effect the enterprise in question.

Rapidly changing technologies highly affect today's architecture principles. For example: implementation of security practice frameworks like ISO/BS or corporate governance guidelines like SOx might lead to separation of data and information flows in highly secure environments (financial data) on a physical level. For example, even though the introduction of virtualization already made his entrance in the enterprises construction level, the principles for network, server, storage virtualization of the data layer is embryonic. Therefore the D-layer needs further research as well as the transformation when information becomes data and vice versa.

Conclusion

Rapidly changing technologies serving the business require a swift way of re-modeling enterprises and their architectural principles. DEMO is a powerful methodology to design the essential layers by using different models. Implementing security principles into these models is limited due to the fact that I limited my research only to the business layer and the information layer. In practice I discovered that it is necessary to involve business people into principles implementation. Not only because they need to be aware of the business impact if they don't, but also because of the financial effects. The SDEMO checklist helps business people understand the possible security breaches and their impact on business transactions. More in-depth: overlaying the several business oriented models within DEMO with the security principles of Confidentiality, Integrity and Availability will result in an effective theoretical way of modeling. This can be done by using the Process Structure Diagram (PSD) combined with the information requirements diagram. This will not enlighten the necessary measures we need to take to avoid a security breach. This can be done by making use of the I-organization design together with the detailed transaction description. In this description we determine which CIA breach we might be facing. After the detailed description of these breaches and the possible principle scenarios stakeholders can make well argumented security principle decisions (investments). I found out that DEMO in itself was limited here by not involving the context in these decisions. Mainly because we are talking about extended enterprises I have searched for other techniques to add to DEMO and accomplish a fully integrated modeling technique. I therefore added the Extended Enterprise Framework of Dr. Martin Op 't Land to DEMO and initiated an ICT and business alignment security modeling technique. In my opinion it needs more research and practice on the data layer of the enterprise and also a better practice of distinguishing security process techniques (like ISO, ITIL) and security technology techniques (like segmentation, encryption, signing).

Also further research is needed to further sharpen the SDEMO questions and checklist. The objective should be to make sure checklist are formulated simple and brief in order to cover all possible breaches per layer. Further research also needs to be done to introduce checklists based upon compliancy guidelines or best practices. For example the practical implementation of SDEMO in combination with best practices (ISO/IEC27001) or practical implementations (ISO/IEC27002).

Literature

- Enterprise Ontology by Prof. Dr. Ir. J.L.G. Dietz. ISBN nr. 3-540-29169-5
- Rapid Enterprise Deployment by Prof. Dr. Ing. J.B.F. Mulder MBA , MSc.
- Applying architecture and Ontology to the splitting and allying of Enterprises by Dr. Drs. M. Op 't Land. ISBN nr. 978-90-71382-32-1.
- Informatiebeveiliging onder controle door Dr. Ir. P. Overbeek e.a. RE. ISBN nr. 90-430-0692-0 .
- Implementing Information Security based upon ISO27001/ISO17799 by management guide. ISBN 978-90-77212-783.

More info

- Official DEMO website: www.demo.nl
- Full research paper on: www.b-able.nl

Na een fijne vakantie kunnen we er weer tegenaan en ik kan de klus die ik al heel lang voor me uitschuif niet meer verder uitstellen. Mijn moeder heeft me gevraagd haar verzekeringsverzameling eens door te nemen. Ze heeft het idee dat ze iets te veel verzekeringen heeft. Mijn moeder (inmiddels de tachtig al gepasseerd) leeft in een hoog bejaardenhuis waar ze een wijds uitzicht heeft vanaf de tiende verdieping.

Het is die avond warm, maar afspraak is afspraak en om zeven uur zit ik aan de grote tafel (zo noemen wij de eettafel) met grote stapels papier om me heen. Ik schrok ervan en ik was blij dat ik bijtijds met deze enerverende klus was begonnen. De zorgpolis lag boven op de stapel, maar ik wilde niet met de moeilijkste beginnen. De fietsverzekering, die kon wel worden opgezegd. De fiets is inmiddels twintig jaar oud en staat al vijf jaar te verstoffen. De tuinverzekering kon er ook uit, want wat moet je op tien hoog met een dergelijke verzekering? Wat moet je überhaupt met een tuinverzekering? Wellicht je goudvissen of de rododendron verzekeren? Ik zal u verder maar niet vermoeien met de onzinnige en nutteloze verzekeringen die ik die avond vond.

Om kwart over elf stapte ik in de auto en trouwe lezers weten dat ik achter het stuur veel nadenk en mijmer. Blijkbaar is de auto een plek die uitnodigt om het leven en de obstakels daarin eens te overdenken.
Ik dacht aan een gesprek met één van onze leveranciers, die mij aangaf dat zijn producten en oplossingen ook een verzekering zijn tegen allerlei onheil van buiten. Onheil dat vaak niet te zien is, maar waarvan je weet dat je er wel mee te maken krijgt als je geen tegenmaatregelen neemt. Ik bedacht me hoe groot de stapel polissen op de grote tafel van mijn moeder zou zijn geweest als ik alle verzekeringen die ik voor mijn werkgever heb afgesloten uitspreidde. Antivirus, antispyware, intrusion detection en prevention systemen, firewalls, USB-beveiliging, legal hacking-contracten, enzovoort. De hoofdredacteur van dit onvolprezen magazine zou niet blij zijn als ik alle verzekeringen zou opnoemen, dus u moet maar van mij aannemen dat ik nog lang niet aan het einde ben van mijn opsomming.

Stilstaand voor het stoplicht bedacht ik me dat de investering in beveiligingsmaatregelen enorm is. Niet alleen in de onderhoudskosten, maar ook de beheersomgeving kost ieder jaar enorme bedragen, louter en alleen omdat er mensen op deze wereld rondlopen die het leuk vinden om andermans eigendommen te beschadigen of weg te nemen. Het aantal medewerkers dat volledig of zijdelings met verzekeringen (sorry, ik bedoel beveiliging) te maken heeft, wordt ieder jaar groter omdat de infrastructuur binnen ons bedrijf ieder jaar complexer wordt en de beveiligingsmaatregelen daardoor kostbaarder en complexer. Ik benoem hier dan niet de wrevel die bij de eindgebruiker ontstaat over deze maatregelen. De smartphone die iedere tien minuten in de schermbeveiliging springt als je om half negen 's morgens in Amsterdam met de navigatie op je telefoon je bestemming probeert te vinden, of de zeer complexe wachtwoorden die je iedere drie maanden moet verzinnen (en onthouden) om je mail op te halen.

Ik druk op de afstandbediening van de garage, die gelukkig doet waar hij voor gemaakt is, ik rijd mijn auto naar binnen en doe hem op slot. Misschien ben ik wel een beetje paranoïde aan het worden, want wie zet zijn auto in de garage nu op slot? Mijn vrouw zit aan de eettafel (wij hebben geen grote tafel) en ik vertel haar tijdens het inschenken van een glas witte bordeaux wat ik heb gedaan. Ze kijkt me aan en vraagt me wanneer ik voor het laatst onze verzekeringen kritisch heb bekeken. Ik bluf en zeg dat ik dat regelmatig doe, maar daar kom ik helaas niet mee weg. Ik nip aan mijn wijn en ik bedenk dat het bij onszelf ook een hele klus is. En dan te bedenken dat ik mijn moeder ook nog heb beloofd binnenkort alle garantiebewijzen en (verouderde) handleidingen door te spitten. Zal ik dat ook direct maar doen bij onze eigen handleidingen, want daar zitten ook oude en vergeelde exemplaren tussen. Zuchtend neem ik de laatste slok van mijn wijn en ik loop naar boven om te gaan slapen.
Ik hoop niet dat ik de hele nacht lig te woelen over de vele kleine lettertjes die ik vandaag heb gezien.

Groeten,
Berry

4 - 5 NOV 2009 JAARBEURS UTRECHT

VIER TOONAANGEVENDE VAKBEURZEN ONDER ÉÉN DAK

IT SECURITY
INFOSECURITY.NL

STORAGE
STORAGE-EXPO.NL

MAXIMIZE IT

LINUX-WORLD.NL
OPEN SOURCE

TOOLINGEVENT.NL
IT BEHEER

KEYNOTES | SEMINARS | CASE STUDIES | EXAMENS | RONDE TAFEL

GRATIS TOEGANG TOT ALLE VIER DE VAKBEURZEN NA VOORREGISTRATIE VIA:

WWW.INFOSECURITY.NL | WWW.STORAGE-EXPO.NL | WWW.LINUX-WORLD.NL | WWW.TOOLINGEVENT.NL

infosecurity.nl NETHERLANDS

STORAGE EXPO

LINUXWORLD CONFERENCE & EXPO

TOOLING EVENT

MEDIAPARTNERS

Automatisering Gids | informatie | beheer magazine

ORGANISATIE

Reed Exhibitions | IDG WORLD EXPO | marqit | Sdu UITGEVERS | vnu exhibitions europe