“Van IT audit naar Digital Trust en Digital Assurance”

Jan Matto, Mazars

ISACA, Round Table
Breukelen, 7 maart 2016

MAZARS

INHOUD

1) Introductie casusposities / “Setting the scene”

2) We doen de audit goed, maar doen we ook de goede audit?

3) Digital Trust en Digital Assurance

4) Drivers voor Digital Trust en Digital Assurance

5) Voorbeelden Digital Trust en Digital Assurance:
    a) Informatiebeveiliging
    b) Privacyvraagstukken

6) Rondvraag / discussie

Even voorstellen:

- **Partner Mazars (Management Consultants)**
  - Center of Excellence IT-audit & -advisory
  - <u>Andere professionele activiteiten</u>:
- Commissie Veilige Verbindingen, EZ,ECP,DHPA
- Commissie “Zeker Online”, Belastingdienst / ECP
- Publicaties over IT-audit en IT security
- Regelmatig spreker
- Colleges voor verschillende universiteiten
- Commissie van toelating / visitatie NOREA
- Stuurgroep Permanente Educatie Register-accountants IT en assurance, Veritas / VERA

Mazars wereldwijd

17,000
Professionals

950
Partners

Europe
→ 8,988

Asia
Pacific
→ 3,156

Americas
→ 2,185

Africa &
Middle East
→ 2,671

77
Integrated countries
International Reach

Global Coverage
260
offices

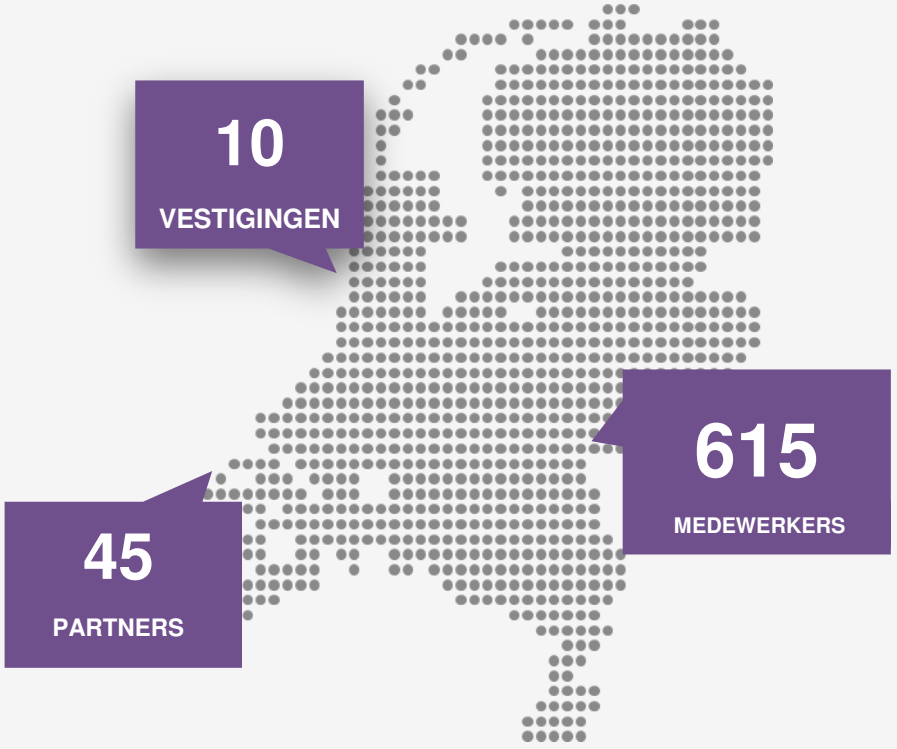
Growth
X 2
in size in 10 years

>100
Fortune 500 Global

1,25 bn€
Turnover

OVER MAZARS

Mazars Nederland



Winnaar 2012:
Human Rights assurance

Winnaar 2013:
Corporate culture audit

Incompany 100 - 2015
2e plaats klanttevredenheid accountancy

OVER MAZARS

Center of Excellence IT-audit en -advisory

Assortiment

- IT-audit support jaarrekeningcontrole
- IT-audit Third Party Memoranda (TPM, ISAE3000, ISAE3402, …)
- IT-audit / bijzondere onderzoeken
- Privacybescherming (audit, assessment, PbD, PET)
- Informatiebeveiligingsonderzoek en –advies
- Cyber security
- Penetratietesten
- Data analyse
- Onderzoek incidenten:
  - ➔ Data lekken
  - ➔ IT-projecten
  - ➔ Knelpunten informatievoorziening

INHOUD

1) Introductie casusposities / “Setting the scene”

2) We doen de audit goed, maar doen we ook de goede audit?

3) Digital Trust en Digital Assurance

4) Drivers voor Digital Trust en Digital Assurance

5) Voorbeelden Digital Trust en Digital Assurance:
    a) Informatiebeveiliging
    b) Privacyvraagstukken

6) Rondvraag / discussie

Enkele praktijkcasussen

- IT-sector/ Overheid: Onderzoek omvangrijke overheid ICT-projecten en integriteitissues
- Nederlandse Zorgautoriteit (NZa): Onderzoek datalek en informatiebeveiliging
- Ministerie BZK: Privacy en security audit Elektronische Nederlandse Identiteitskaart (eNIK)
- Ministerie BZK: Privacy Impact assessment identity management systemen (eID Stelsel 1.0 en Idensys)
- Central Bank of Ireland: Privacy Impact Assessment National Credit Register
- International “Human Genome Project”: Privacy en security risicoanalyse
- Ministerie VenJ / Defensie: Onderzoek robuustheid biometrische gezichtsherkenning-systemen grenscontrole (No-Q)
- Politie Nederland, WPG Audits / advies beveiligingsbeleid
- Mediation / calamiteiten / project recovery / second opinions

Het NZa-dossier: wanorde bij de toezichthouder

10 april 2014

Trending | Veel gedeeld

SOCIALE MEDIA
U twittert wel heel veel, zei de politie

SARAH PALIN
Kijken: actrice Tina Fey imiteert Sarah Palin

FYSIOLOGIE
Even rondje rennen voor het avondeten

BONNETJE
'Commissie-Oosting heropent onderzoek Teevendeal'

PVV-MOTIES
PVV in de ban sinds 'minder, minder'

informatievoorziening nogal instrumenteel is, waarbij het strategisch belang van deze onderwerpen in brede zin binnen de organisatie wordt onderschat; de ontwikkelingen op het gebied van ICT vinden op te grote afstand van de primaire processen plaats, waardoor het risico bestaat dat applicaties niet voldoen aan de behoeften van toekomstige gebruikers.

Uit de EDP-audit[4] die Mazars heeft uitgevoerd, komt de aanbeveling dat "*op het niveau van de IT-architectuur en IT-infrastructuur (de IT-werkelijkheid) aanvullende maatregelen noodzakelijk zijn. Het geplande informatie security management systeem (ISMS) is nog niet ingevoerd en geoperationaliseerd. Daarnaast is om gegevensverzamelingen intern te kunnen delen en hergebruiken een complex en moeilijk te beheersen autorisatiemechanisme ontstaan. Daarbij zijn de uitgangspunten niet gebaseerd op het 'need to know' principe.*"

De commissie Borstlap komt tot de conclusie dat de beveiliging op papier toereikend, is maar dat de normen onvoldoende leven. Daarom doet de commissie een drietal specifieke aanbevelingen:

- 1. Waarborg op alle niveaus de gedragsregels inzake ICT-gebruik met inbegrip van expliciete sancties bij overtreding van de regels.
- 2. Maak ICT-beveiliging expliciet onderdeel van de werving en beoordeling van managers bij de NZa.
- 3. Benoem krachtige, gezaghebbende security officers, die direct rapporteren aan de algemene leiding.

Overheid is verantwoordelijk voor een betrouwbaar identiteitenstelsel in de reële wereld én in de virtuele wereld.

Identiteitsfraude in Nederland:

- *Circa 5,6% van de burgers in de periode 2007 - 2011 (4 jaar) is slachtoffer van identiteitsfraude.*
- *In de jaren 2007 - 2012 (6 jaar) is dit circa 13,3 %.*
- *Van deze slachtoffers heeft een deel financiële schade geleden: naar schatting 9,5% van de gehele bevolking.*
- *Over 2012 is berekend dat tussen de 672.787 en 869.816 burgers slachtoffer zijn geweest, die gezamenlijk tussen de 393 en 508 miljoen euro schade hebben geleden.*
- *DigiD uiterlijk 2017 vervangen door nieuw systeem*

BRON: 2 april 2013, Brief minister Plasterk en bijbehorende rapportage over de Voortgang Toekomstbestendigheid Identiteitsinfrastructuur naar de Kamer.

https://www.rijksoverheid.nl/documenten/kamerstukken/2013/04/02/kamerbrief-voortgang-toekomstbestendigheid-identiteitsinfrastructuur

Proportionaliteits-issue Suwinet bij gemeenten

02
SEP

Privacy-overtredingen bij Suwinet waarschuwing voor medisch pull-dataverkeer

Het afgelopen half jaar is het niet correcte gebruik van het Suwinet herhaaldelijk in het nieuws geweest. Het programma Argos berichtte er uitgebreid over, in veel kranten(o.a. NRC-Handelsblad) werd er aandacht aan besteed. Eerder had het College Bescherming Persoonsgegevens (CBP) eind 2014 gerapporteerd, dat de gemeente 's-Hertogenbosch de zaken t.a.v. het Suwinet-gebruik totaal niet op orde had. In juni 2015 kondigde het CBP aan een lopend onderzoek naar het Suwinet-gebruik uit te breiden met acht gemeenten, nadat de Inspectie Sociale Zaken en Werkgelegenheid gemeld had dat het met het hanteren van de veiligheidsnormen slecht gesteld was. In de loop van anderhalf jaar was het aantal gemeenten dat aan de normen voldeed slechts gestegen van 4 naar 17%, een onbegrijpelijk laag percentage.

Suwinet

De grondvesten voor dit netwerk zijn gelegd in 2002 met als doel (persoons) gegevens van burgers tussen diverse overheidsorganisaties uit te wisselen in het domein Werk en Inkomen op basis van de Wet structuur uitvoeringsorganisatie werk en inkomen(SUWI). Het is een besloten netwerk dat ondersteund, beheerd

Type Here to Search

Meest recente berichten

Weer datalek door uitbestede werkzaamheden van ziekenhuizen

Autoriteit Persoonsgegevens schetst te rooskleurig beeld veilig gebruik Suwinet

KNMG wijst Eerste Kamer op falen van wetsontwerp 33509

Commissie Eerste Kamer buigt zich over wetsontwerp medische datacommunicatie

Zorgrobot Zora nu in NRC gehypet als wiskundeleraar

Recente reacties

Bas de Rooij,huisarts op Commissie Eerste Kamer buigt zich over wetsontwerp medische datacommunicatie

helder op Aanvalsvlak LSP voor indringers weer groter door PGD-LSP-koppeling

MAZARS

NU | NUzakelijk | NUsport | NUtech | NUentertainment | NUlifestyle | NUgeld | NUwerk | Inloggen

Maandag 25 januari 2016 | Het laatste nieuws het eerst op NU.nl

9 °C | 0 Files | 418,07 | TV gids | 3 Live

Voorpagina
Net binnen
Algemeen
Binnenland
Buitenland
Politiek
Economie
Geld
Ondernemen
Beurs
V&D
Sport
Voetbal
Schaatsen
Australian Open
Meer Sport
MijnTeam
Tech
Internet
Gadgets
Games
Mobiel

NU.nl › Tech › Internet

Datalek ziekenhuizen treft ruim 200.000 patiënten

Gepubliceerd: 25 januari 2016 11:36
Laatste update: 25 januari 2016 16:34

De gegevens van zeker 200.000 Nederlandse en Belgische patiënten van het Sint Anna Ziekenhuis in Geldrop en het Canisius-Wilhelmina Ziekenhuis in Nijmegen zijn door een datalek ruim een maand lang toegankelijk geweest voor onbevoegden.

Volgens de ziekenhuizen zijn er geen medische gegevens gelekt. Wel waren de geboortedata, dossiernummers en de vermeldingen van het specialisme toegankelijk voor kwaadwillenden.

Net binnen | Meest gelezen

20:53 - Centraal station Rome ontruimd vanwege... ›
20:32 - Racetalent Beitske Visser ook dit jaar in F... ›
19:50 - 'Zoeken naar bonnetje Teevendeal van h... ›
19:48 - Debat kandidaat-voorzitters FIFA met Eur... ›

Meer nieuws ›

Videoreviews

MAZARS

Illegaal gebruik tracking cookies Yieldr (cookie-wetgeving)

ONDERWERP Last onder dwangsom
OPENBARE VERSIE

Samenvatting

1. Het College bescherming persoonsgegevens (CBP) heeft ingevolge artikel 60 van de Wet bescherming persoonsgegevens (Wbp) ambtshalve onderzoek gedaan naar de verwerking van persoonsgegevens door YD Display Advertising Benelux B.V. (verder: Yieldr) voor *online behavioural targeting*. Naar aanleiding van dit onderzoek heeft het CBP besloten om op grond van artikel 65 van de Wbp in samenhang bezien met artikel 5:32, eerste lid, van de Algemene wet bestuursrecht (Awb) een last onder dwangsom op te leggen.

2. Het CBP heeft geconstateerd dat Yieldr in strijd handelt met artikel 8 van de Wbp doordat zij persoonsgegevens verwerkt voor het tonen van gepersonaliseerde advertenties op grond van eerder surfgedrag zonder dat de betrokkenen voor de verwerking hun ondubbelzinnige toestemming hebben verleend.

3. De last bestaat uit een maatregel die binnen de in dit besluit genoemde begunstigingstermijn dient te zijn nageleefd. Bij niet naleving is Yieldr een dwangsom verschuldigd van € 25.000,-- voor iedere week of een gedeelte daarvan dat de maatregel niet geheel is uitgevoerd, met een maximum van € 500.000,--.

MEDINOVA
Kliniek Zestienhoven

8 februari 2016

Geachte mevrouw Matto,

U ontvangt deze brief omdat u patiënt bij ons bent of geweest bent.
Een laptop van een van onze medewerkers is gestolen. De laptop is beveiligd met een wachtwoord. Op de laptop zijn in het verleden gegevens van klanten verwerkt. Daardoor kunnen we niet helemaal uitsluiten dat er persoonsgegevens, met name gebruikt voor declaratiedoeleinden, op de laptop zijn achtergebleven. We hebben aangifte gedaan van de diefstal. Bovendien hebben wij dit gemeld bij de Autoriteit Persoonsgegevens en de Inspectie voor de Gezondheidszorg.
Wij willen nogmaals benadrukken dat het niet zeker is dat er persoonsgegevens van u of andere klanten op de laptop zichtbaar waren. Wij willen u uit zorgvuldigheid hierover toch persoonlijk informeren.

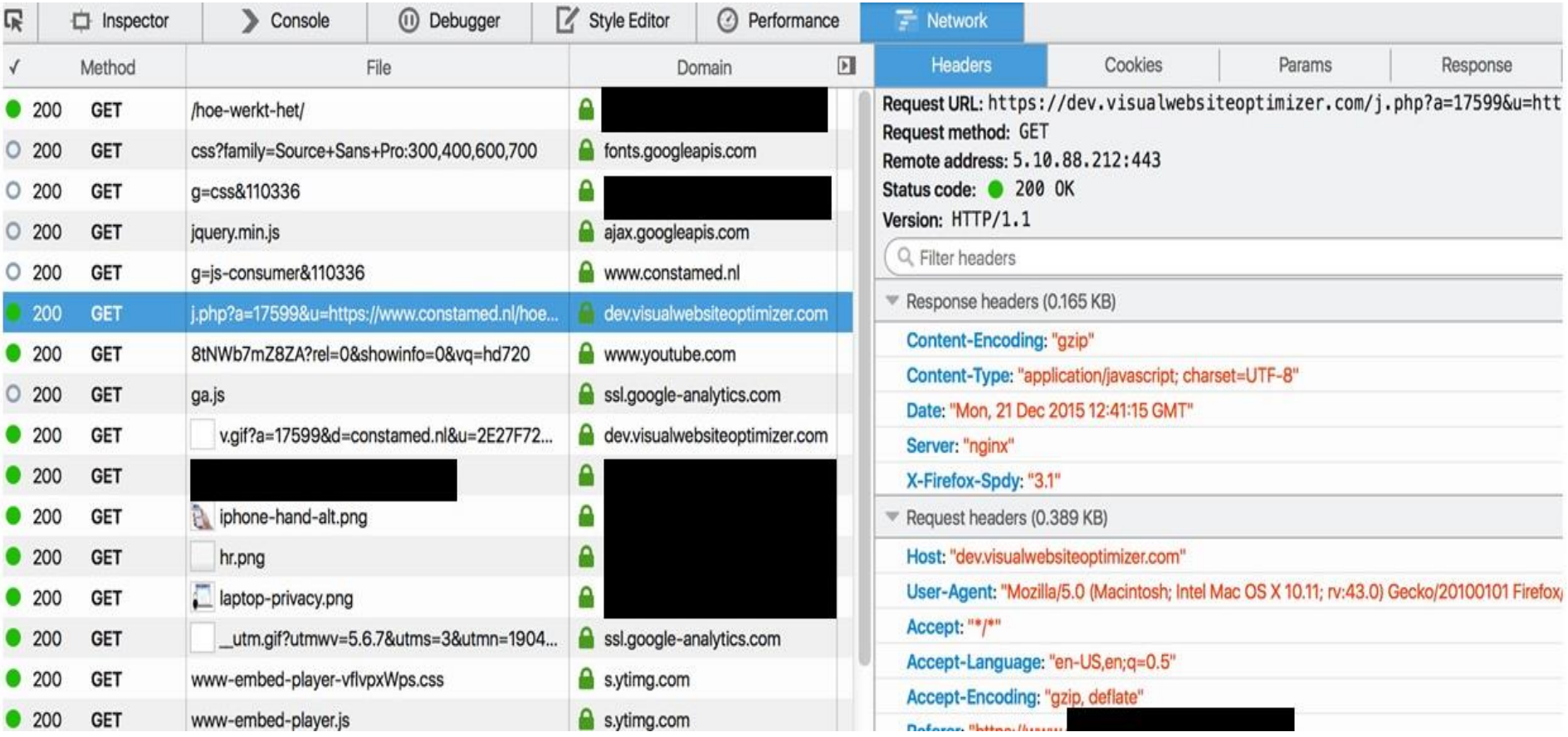
Hebt u vragen naar aanleiding van deze brief dan kunt u ons op werkdagen tussen 09:00 en 17:00 uur gratis bellen via: 050-5855801. Wij zien op dit moment geen noodzaak voor u om zelf actie te ondernemen.

Wij betreuren dit voorval zeer en bieden u hiervoor onze welgemeende excuses aan.

Met vriendelijke groet,

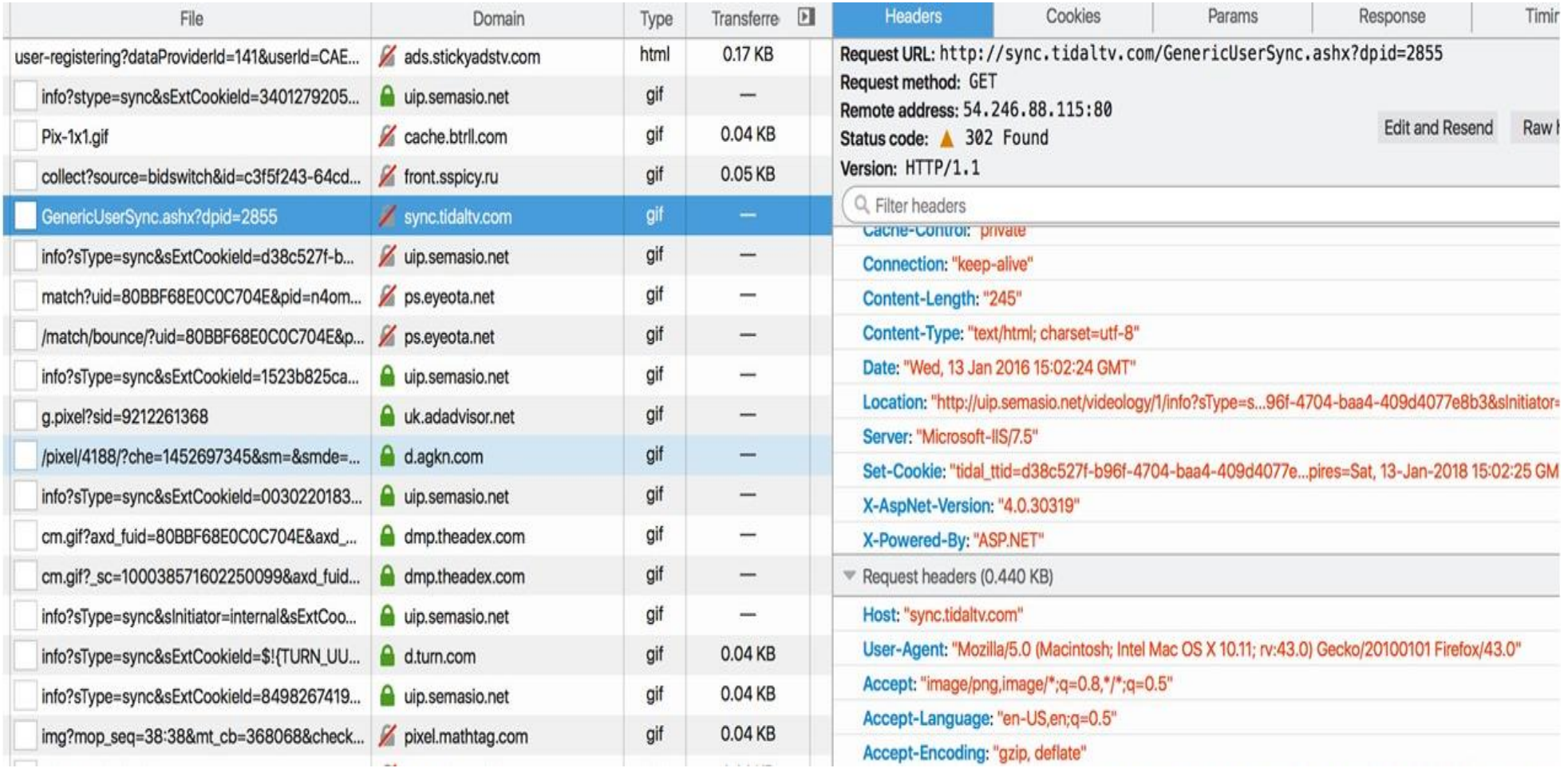
Renée Wilke
Algemeen directeur
Kliniek Zestienhoven

Bedrijf XYZ2



MAZARS

Bedrijf XYZ2



File	Domain	Type	Transferre
user-registering?dataProviderId=141&userId=CAE...	ads.stickyadstv.com	html	0.17 KB
info?stype=sync&sExtCookieId=3401279205...	uip.semasio.net	gif	—
Pix-1x1.gif	cache.btrll.com	gif	0.04 KB
collect?source=bidswitch&id=c3f5f243-64cd...	front.sspicy.ru	gif	0.05 KB
GenericUserSync.ashx?dpid=2855	sync.tidaltv.com	gif	—
info?sType=sync&sExtCookieId=d38c527f-b...	uip.semasio.net	gif	—
match?uid=80BBF68E0C0C704E&pid=n4om...	ps.eyeota.net	gif	—
/match/bounce/?uid=80BBF68E0C0C704E&p...	ps.eyeota.net	gif	—
info?sType=sync&sExtCookieId=1523b825ca...	uip.semasio.net	gif	—
g.pixel?sid=9212261368	uk.adadvisor.net	gif	—
/pixel/4188/?che=1452697345&sm=&smde=...	d.agkn.com	gif	—
info?sType=sync&sExtCookieId=0030220183...	uip.semasio.net	gif	—
cm.gif?axd_fuid=80BBF68E0C0C704E&axd_...	dmp.theadex.com	gif	—
cm.gif?_sc=100038571602250099&axd_fuid...	dmp.theadex.com	gif	—
info?sType=sync&sInitiator=internal&sExtCoo...	uip.semasio.net	gif	—
info?sType=sync&sExtCookieId=${TURN_UU...	d.turn.com	gif	0.04 KB
info?sType=sync&sExtCookieId=8498267419...	uip.semasio.net	gif	0.04 KB
img?mop_seq=38:38&mt_cb=368068&check...	pixel.mathtag.com	gif	0.04 KB

Headers | Cookies | Params | Response | Timir

Request URL: http://sync.tidaltv.com/GenericUserSync.ashx?dpid=2855
Request method: GET
Remote address: 54.246.88.115:80
Status code: 302 Found
Version: HTTP/1.1

Edit and Resend | Raw

Filter headers

Cache-Control: private
Connection: "keep-alive"
Content-Length: "245"
Content-Type: "text/html; charset=utf-8"
Date: "Wed, 13 Jan 2016 15:02:24 GMT"
Location: "http://uip.semasio.net/videology/1/info?sType=s...96f-4704-baa4-409d4077e8b3&sInitiator=
Server: "Microsoft-IIS/7.5"
Set-Cookie: "tidal_ttid=d38c527f-b96f-4704-baa4-409d4077e...pires=Sat, 13-Jan-2018 15:02:25 GM
X-AspNet-Version: "4.0.30319"
X-Powered-By: "ASP.NET"

Request headers (0.440 KB)

Host: "sync.tidaltv.com"
User-Agent: "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:43.0) Gecko/20100101 Firefox/43.0"
Accept: "image/png,image/*;q=0.8,*/*;q=0.5"
Accept-Language: "en-US,en;q=0.5"
Accept-Encoding: "gzip, deflate"

INHOUD

1) Introductie casusposities / “Setting the scene”

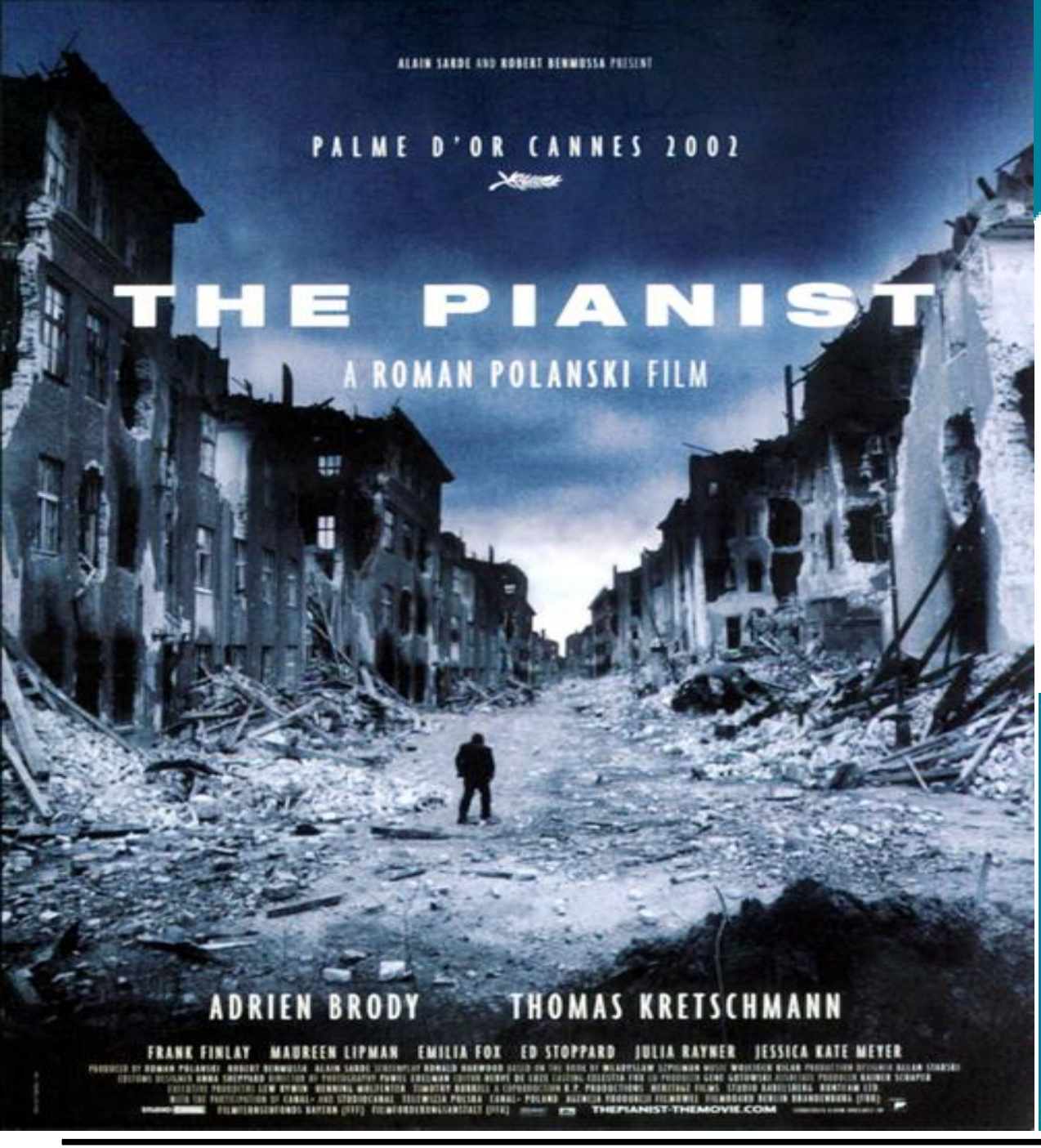
2) We doen de audit goed, maar doen we ook de goede audit?

3) Digital Trust en Digital Assurance

4) Drivers voor Digital Trust en Digital Assurance

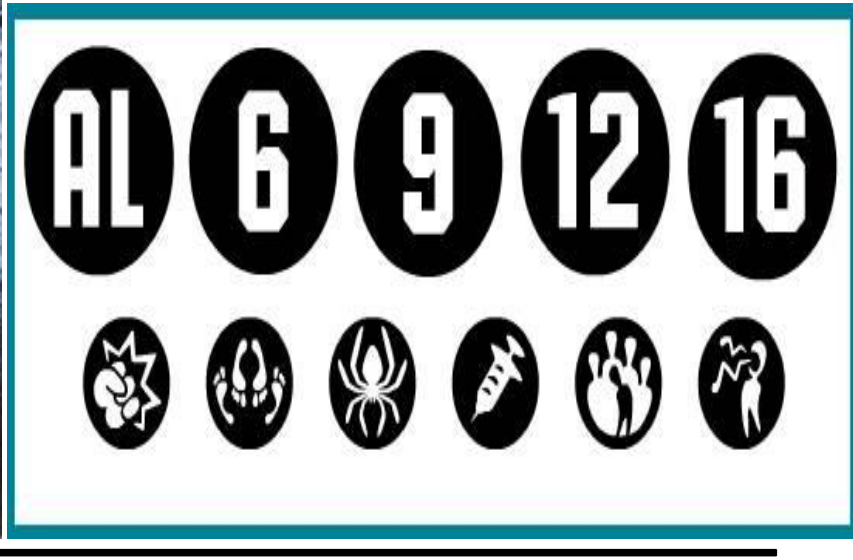
5) Voorbeelden Digital Trust en Digital Assurance:
    a) Informatiebeveiliging
    b) Privacyvraagstukken

6) Rondvraag / discussie



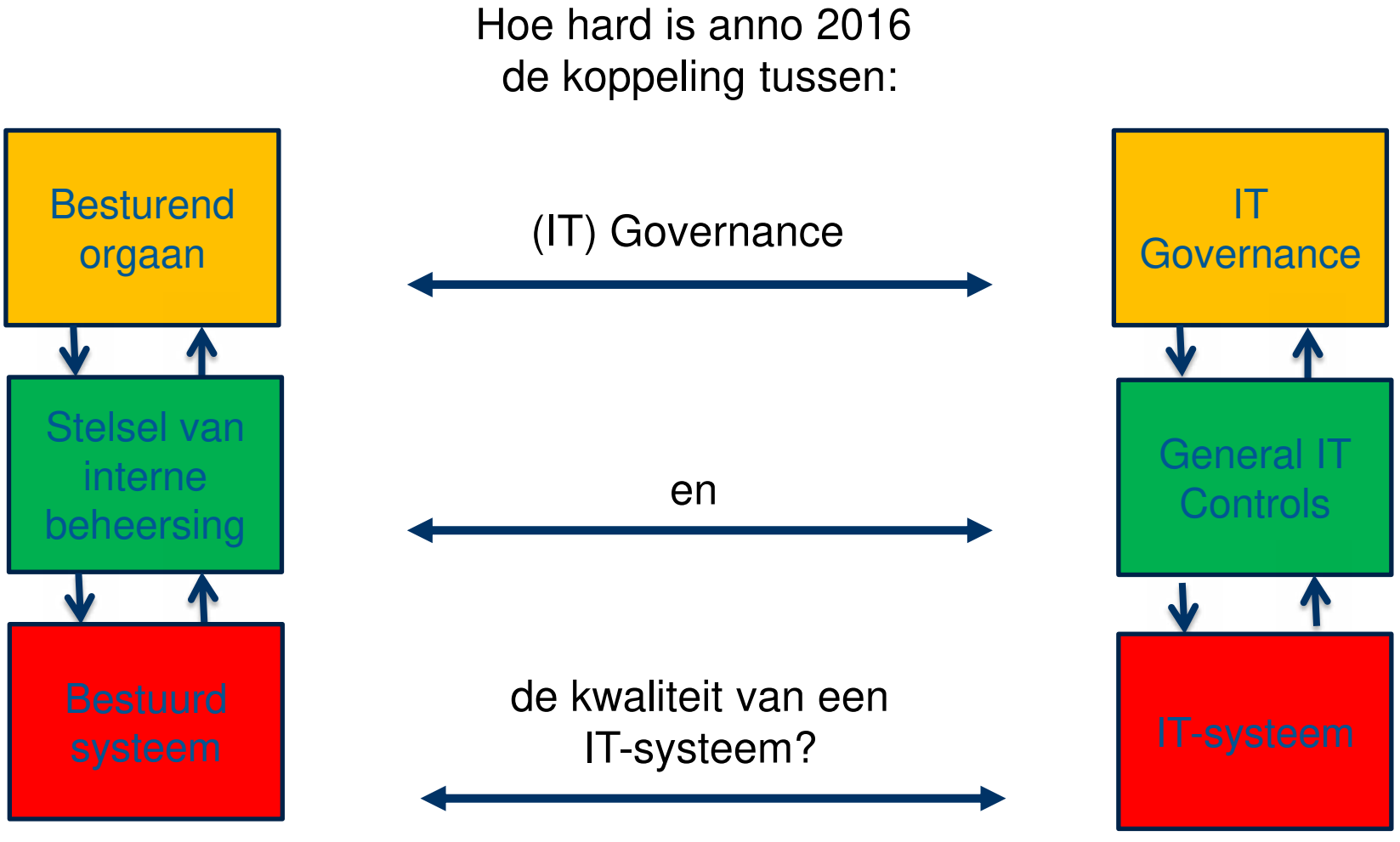
KIJKWIJZER

This presentation could include shocking visions



MAZARS

We doen de audit goed, maar doen we nog wel de goede audit?



MAZARS

INHOUD

1) Introductie casusposities / “Setting the scene”

2) We doen de audit goed, maar doen we ook de goede audit?

3) Digital Trust en Digital Assurance

4) Drivers voor Digital Trust en Digital Assurance

5) Voorbeelden Digital Trust en Digital Assurance:
    a) Informatiebeveiliging
    b) Privacyvraagstukken

6) Rondvraag / discussie

Wat beoogt Digital Trust & Digital Assurance ?

- Geeft inzicht in de toestand van het reële ICT-systeem: “De IT-werkelijkheid”;
- Via waarnemingen in de IT-werkelijkheid;
- Waarnemingen vinden plaats op verschillende systeemniveaus / -lagen
  - Architectuur, inclusief ketens, cloud en onderliggende systeemlagen (onderkent dat systemen veelal via netwerken gekoppeld zijn / vervaagde systeemgrenzen)
  - Uitrusting en inrichting;
  - Events en violations in systemen;
  - Transacties, reguliere processen, data.

- Inzet van tooling is daarbij belangrijk;
- Gaat meer in de richting van monitoring, detectie en respons;
- Normen te ontlenen uit de actuele context van het IT-systeem;
- Rapportage / transparantieverslag over systeem functioneren

INHOUD

1) Introductie casusposities / “Setting the scene”

2) We doen de audit goed, maar doen we ook de goede audit?

3) Digital Trust en Digital Assurance

4) Drivers voor Digital Trust en Digital Assurance

5) Voorbeelden Digital Trust en Digital Assurance:
    a) Informatiebeveiliging
    b) Privacyvraagstukken

6) Rondvraag / discussie

Drivers: Aanscherpingen in wet- en regelgeving die IT-audit raken

Algemeen privacy:

- Europees Verdrag Rechten van de Mens
  (EVRM: privacy, zelfbeschikking, vrije nieuwsgaring)
- Realisatie van een IT-systeem met verwerkingen van persoonsgegevens impliceert meestal een inbreuk op grondrecht van de bescherming van de persoonlijke levenssfeer
- Voortgaande digitalisering van maatschappij en economie vergroot de risico's

Maar er zijn ook andere maatschappelijke ontwikkelingen en risico's:

- Identiteitsdiefstal / -fraude
- Wantrouwen in digitale en eGovernment services
- Risico voor economische groei
- Verstoringen van marktwerkingen
- Politieke en Bestuurlijke risico's
- ……..

Drivers voor Digital Trust & Assurance: nieuw gedrag door stakeholders ten aanzien van IT

Journalists

Autoriteit Consument & Markt

Regulators

Government

Privacy regulators

Politics

Citizens, Consumers, Society

Civil rights & privacy protectors

Hackers

ANONYMOUS

Bits of Freedom

MAZARS

Drivers voor digital assurance komend decennium

- Aanhoudende stroom aan ICT- en security incidenten
- Toenemende maatschappelijke en economische relevantie van ICT
- Toenemende maatschappelijke bewustwording van ICT-risico's
- Wet- en regelgeving inzake privacy, data protectie en mededinging
- Toenemende ICT-interdependentie ondernemingen en instellingen
- Toenemende behoefte assurance en transparantie over IT bij uitbesteding
- Ontstaan van nieuwe normen op IT-systeemniveau
- Ontstaan van nieuwe initiatieven voor IT assurance en gerelateerde diensten
- Toenemende juridisering en aansprakelijkheidsdenken
- Zichtbare beperkingen van traditionele IT-audit benaderingen / conflicten en fricties

Drivers: "The Loss of IT Governance

Toenemende Complexiteit / distributie

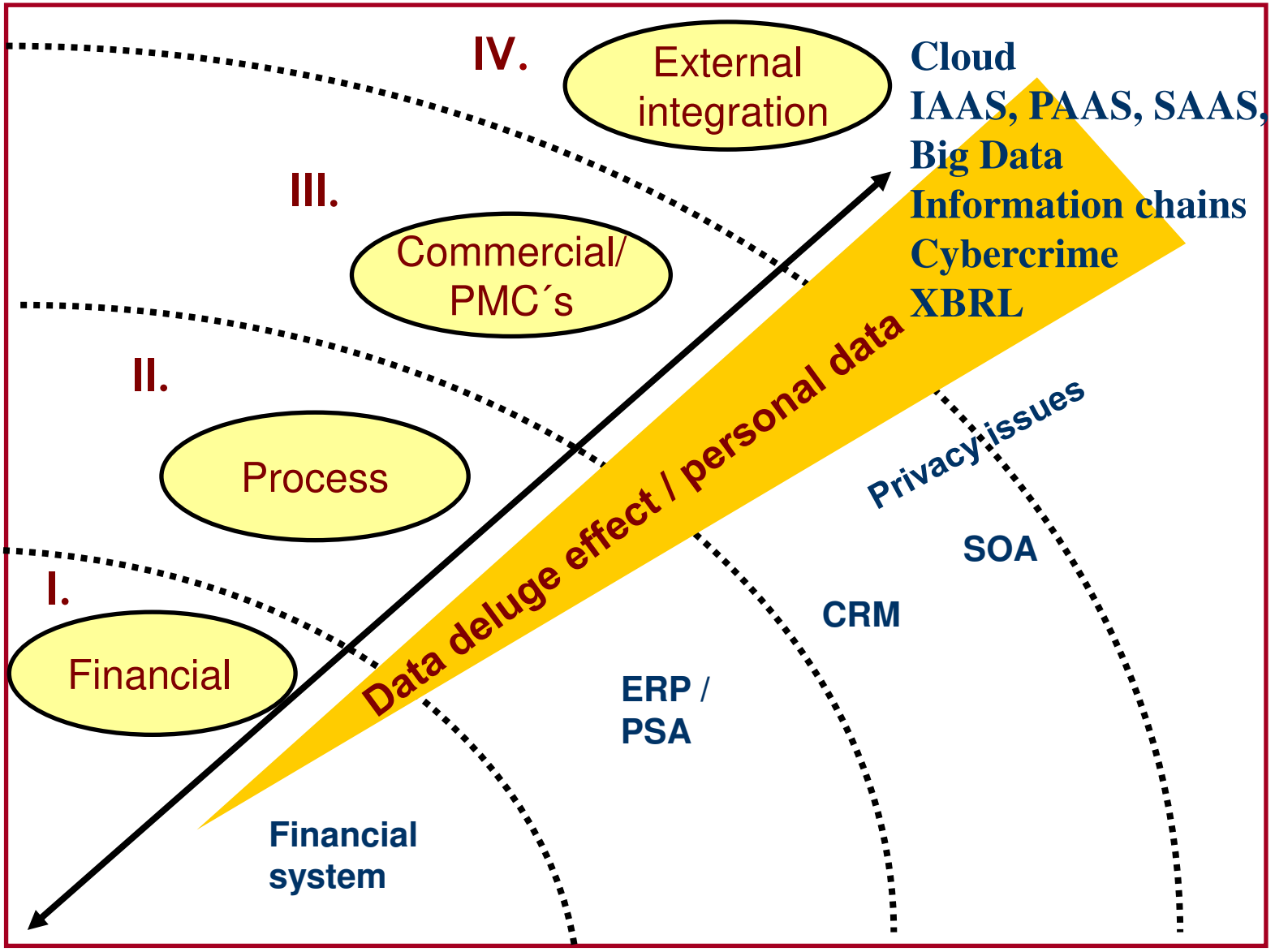
Systeem technische overgangen

Verschuivingen in Dominante macht

Verschillen in compliance

Meer frequente system changes

Toename risico's:
- Strategische rol IT
- Afhankelijkheid van beschikbaarheid IT
- Information chains
- Vitale infrastructuren
- Cyber security risks
- Ontstaan "hotspots"…..
- Surveillance en "the Man in the Middle"
- Aanscherping wet- en regelgeving
- ……



MAZARS

Digital Trust & Assurance:
het einde van IT Governance bubble

MAZARS

Kleine verdieping achtergrond IT-audit en Digital Assurance

Traditionele audit benaderingen (main stream)

➔Beheersdoelstellingen, risico's, beheersmaatregelen, stabiliteit
➔Rule based = "harde" normen en maatregelen
➔Principle based = formulering van beheersdoelstellingen

Noodzaak tot meer geavanceerd IT auditeren

➔Context based
- ➔De context zet de norm
- ➔Als de context verandert kloppen principles en rules niet meer
- ➔Een IT-systeem zou vooral:
  - A) een "afbeelding" moeten zijn van haar context
  - B) dus moeten kunnen anticiperen op haar context
  - C) IT-architectuur en -uitrusting moeten dat ondersteunen

➔Digital Assurance focust meer op de systeem context en IT-werkelijkheid

INHOUD

1) Introductie casusposities / “Setting the scene”

2) We doen de audit goed, maar doen we ook de goede audit?

3) Digital Trust en Digital Assurance

4) Drivers voor Digital Trust en Digital Assurance

5) Voorbeelden Digital Trust en Digital Assurance:
    a) Informatiebeveiliging
    b) Privacyvraagstukken

6) Rondvraag / discussie

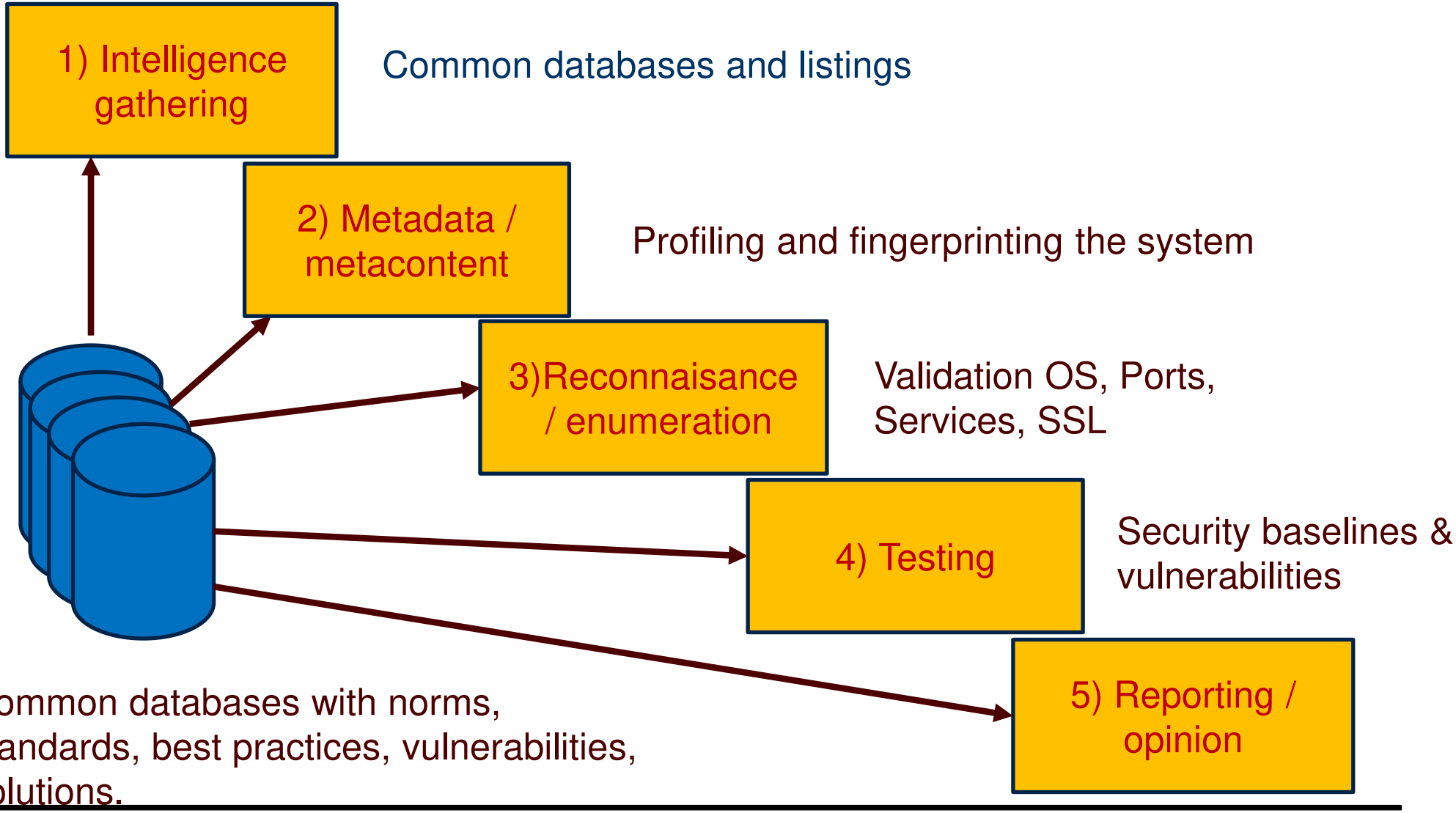
Voorbeeld Digital Assurance: logische toegangsbeveiling (1)

1) **Intern: netwerk en besturingssystemen / platform**:
Netwerk en architectuur zijn bekend en van binnenuit bereikbaar.

- Verkenning en scanning van netwerk en architectuur;
- Uitlezen van security instellingen gevonden objecten;
- Uitlezen van logfiles, sporen, violations, etc;
- Scannen van kwetsbaarheden en instellingen van binnen netwerk aanwezige objecten;
- Confrontatie met bevindingen ITGCs, procedures, informatiebeleid, contractuele afspraken etc;
- Rapportage van bevindingen (opinie over accountmanagement, logische toegangsbeveiliging, incident management, patch management, etc).

Voorbeeld Digital Assurance: logische toegangsbeveiling (2)

2) **Extern: Webapplicaties, URLs, IP-reeksen**

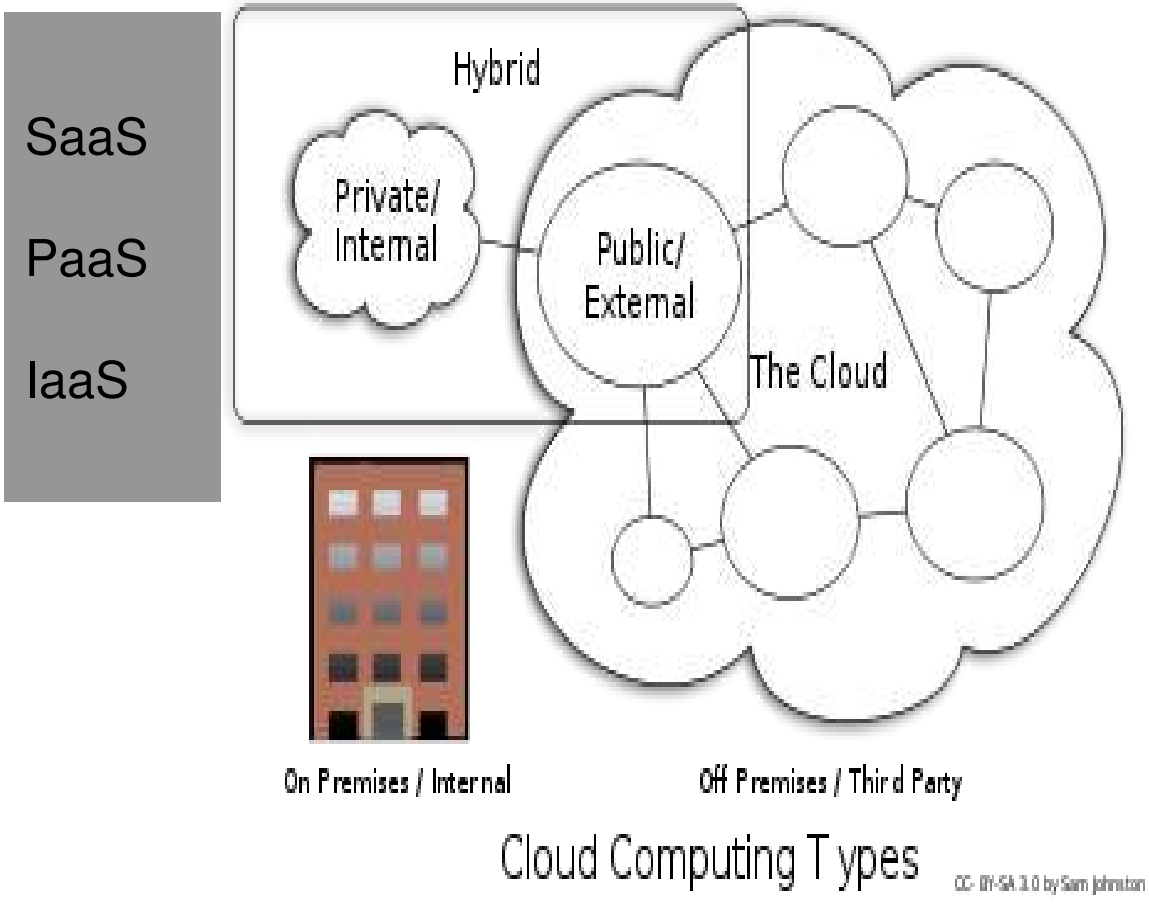


MAZARS

Voorbeeld Digital Assurance: privacy en architectuur (1)

Privacy Principes aantoonbaar ondersteund door IT-architectuur:

- Verantwoording
- Grondslag
- Transparantie
- Kwaliteit
- Doelbinding
- Gegevensminimalisatie
- PET / PbD
- Beveiliging
- Rechten individu:
  - user consent,
  - inzage, correctie
  - recht om vergeten te worden
- Derde landen buiten EER



Voorbeeld Digital Assurance: privacy en architectuur (2)

Privacy Risico's afgedekt door ICT-architectuur:

- 'Data deluge'-effect
- Ontstaan "hotspots"
- Waardestijging van persoonsgegevens
- 'Function creep'
- Inconsistente implementatie en naleving verantwoordingsbeginsel
- Geheime (niet transparante) verwerking van persoonsgegevens
- Niet toegestane verwerking van persoonsgegevens buiten de EU
- Datalekken
- Specifieke risico's ten aanzien van biometrische identificatie & authenticatie
- Onrechtmatig gebruik BSN-nummers
- Onrechtmatig gebruik van uniek identificerende gegevens

Digital Trust en Assurance aandachtsgebieden

- Transparantie van verwerkingen en systemen
- Actualiteit van security
- Eigendom van verwerkingen
- Hardening
- Segmentering op basis van (systeem)functiescheidingen / Hyper segmentering
- Pseudonimisering / Pseudo-identiteiten
- Privacy by Design
- Privacy Enhancing Technologies
- Revoked Attribuut Providing
- Security en encryptie technieken
- Intrusion detection
- Vulnerability scans / periodieke Penetratie testen
- Systeemontwikkelproces / Code reviews
- Invoervalidatie / Error Handling
- Change management / inbedding compliance risks (bijvoorbeeld PIA)

INHOUD

1) Introductie casusposities / “Setting the scene”

2) We doen de audit goed, maar doen we ook de goede audit?

3) Digital Trust en Digital Assurance

4) Drivers voor Digital Trust en Digital Assurance

5) Voorbeelden Digital Trust en Digital Assurance:
    a) Informatiebeveiliging
    b) Privacyvraagstukken

6) Rondvraag / discussie

Vragen en discussie

MAZARS

Digital Trust en Assurance

- Het werk van de IT-auditor wordt kritischer beoordeeld: Maatschappelijke relevantie en aandacht IT en dus IT-audit neemt toe. (wet- en regelgeving, politiek merkbaar falen, media aandacht).

- Wil de IT-auditor relevant blijven dan moet deze zich veel meer focussen op de “IT-werkelijkheid” en minder op governance, interne beheersing, aansprakelijkheid en compliance.

- Zonder tooling gaat het niet meer lukken.

- Het is ook de IT-architectuur en inrichting die compliant moet zijn.

- Transparantie van systemen en verwerkingen is de norm
  Het gaat om Trust door Transparency, desnoods zonder Assurance.

- Het einde van de governance bubble is onvermijdelijk. Wat moeten we straks nog met normen als normen als ISO/NEN, COBIT, etc?

Dank voor uw aandacht!

jan.matto@mazars.nl


06 535 78 232

@Jan_Matto