infomedics

Uw praktijk: een goudmijn voor internetcriminelen

Workshop Medisch Ondernemen Live
6/7 oktober 2017

Wat gaan we doen?

Uw verwachtingen

Uw gemoedstoestand

De digitale data-explosie

Nieuwe privacywetgeving (a giant leap for mankind)

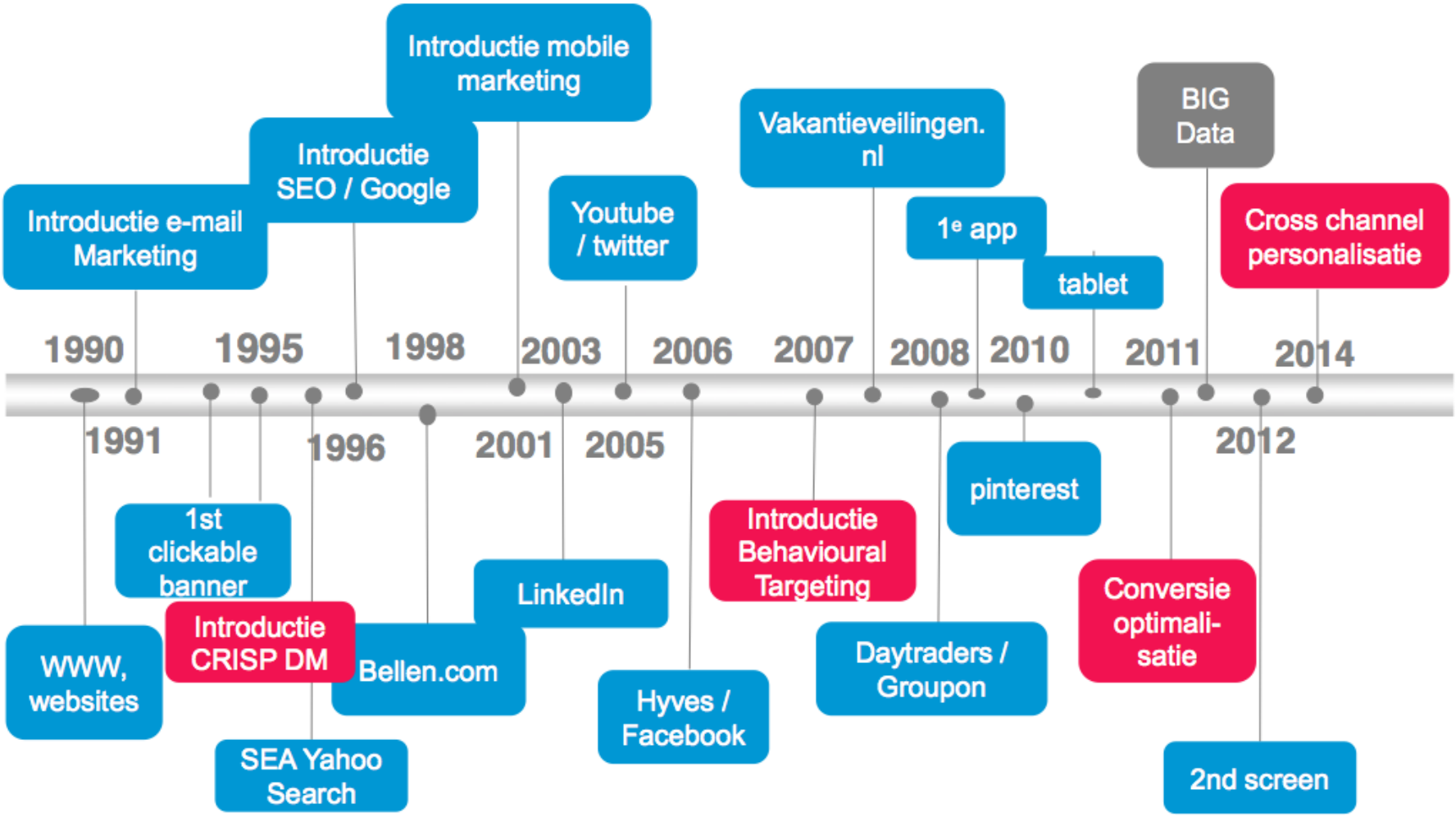
Wat wilt u onze hacker vragen?

Help! Uw praktijk ligt onder vuur!

Hoe heeft Infomedics uw informatieveiligheid georganiseerd?

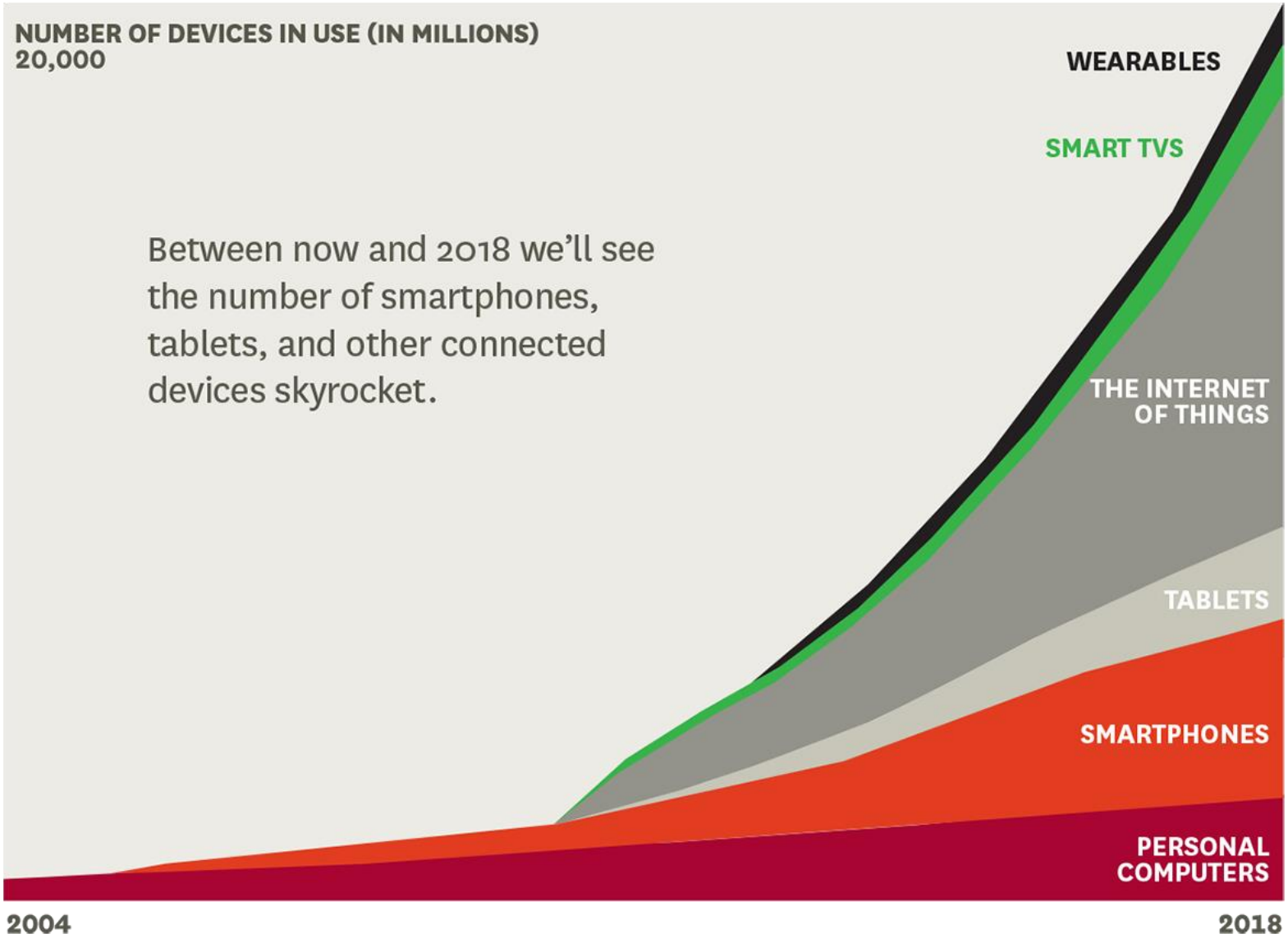
Wat kunt (moet?) u zelf doen?

What happened since www.....



infomedics

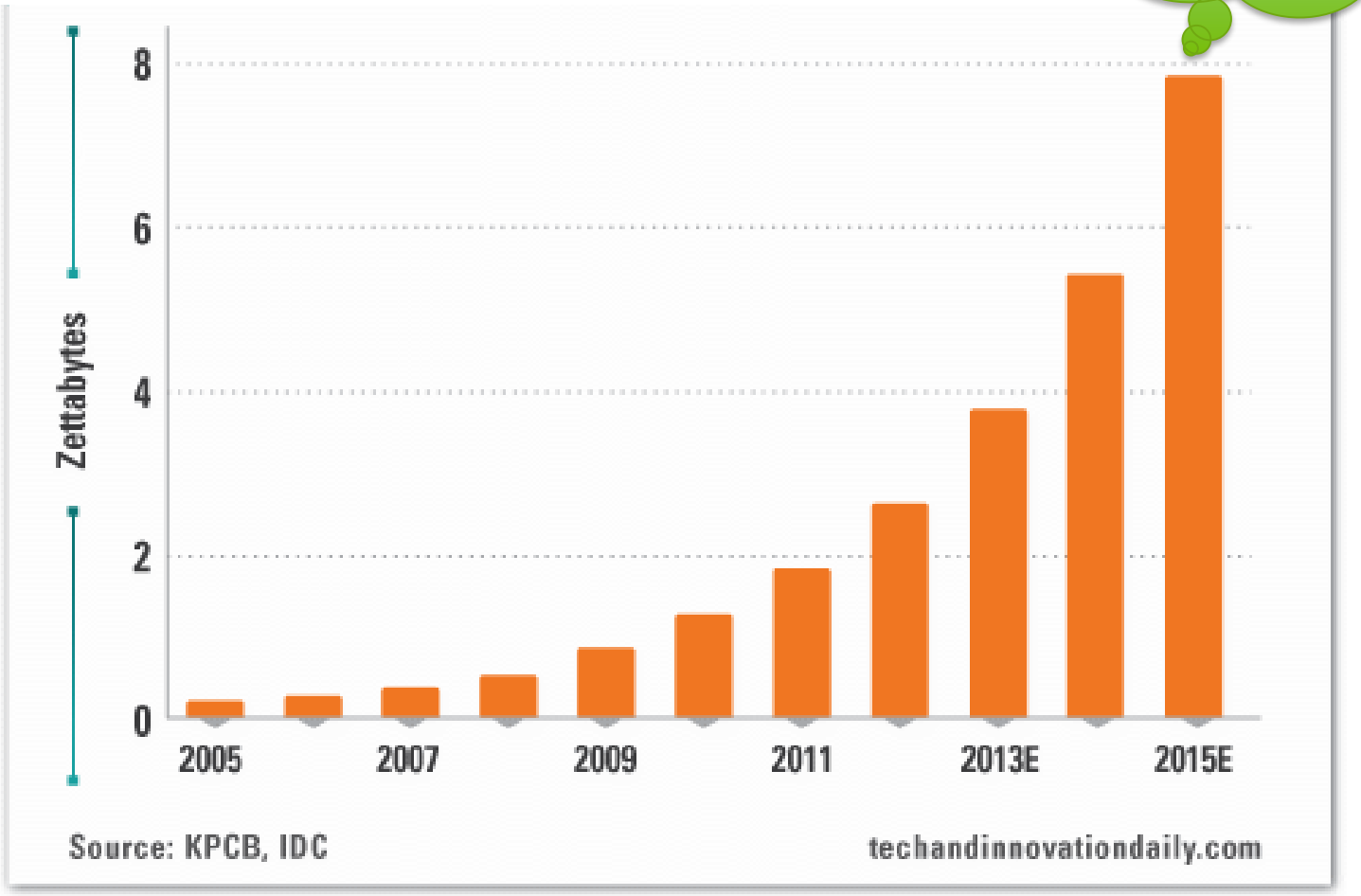
Ontwikkeling datagebruik



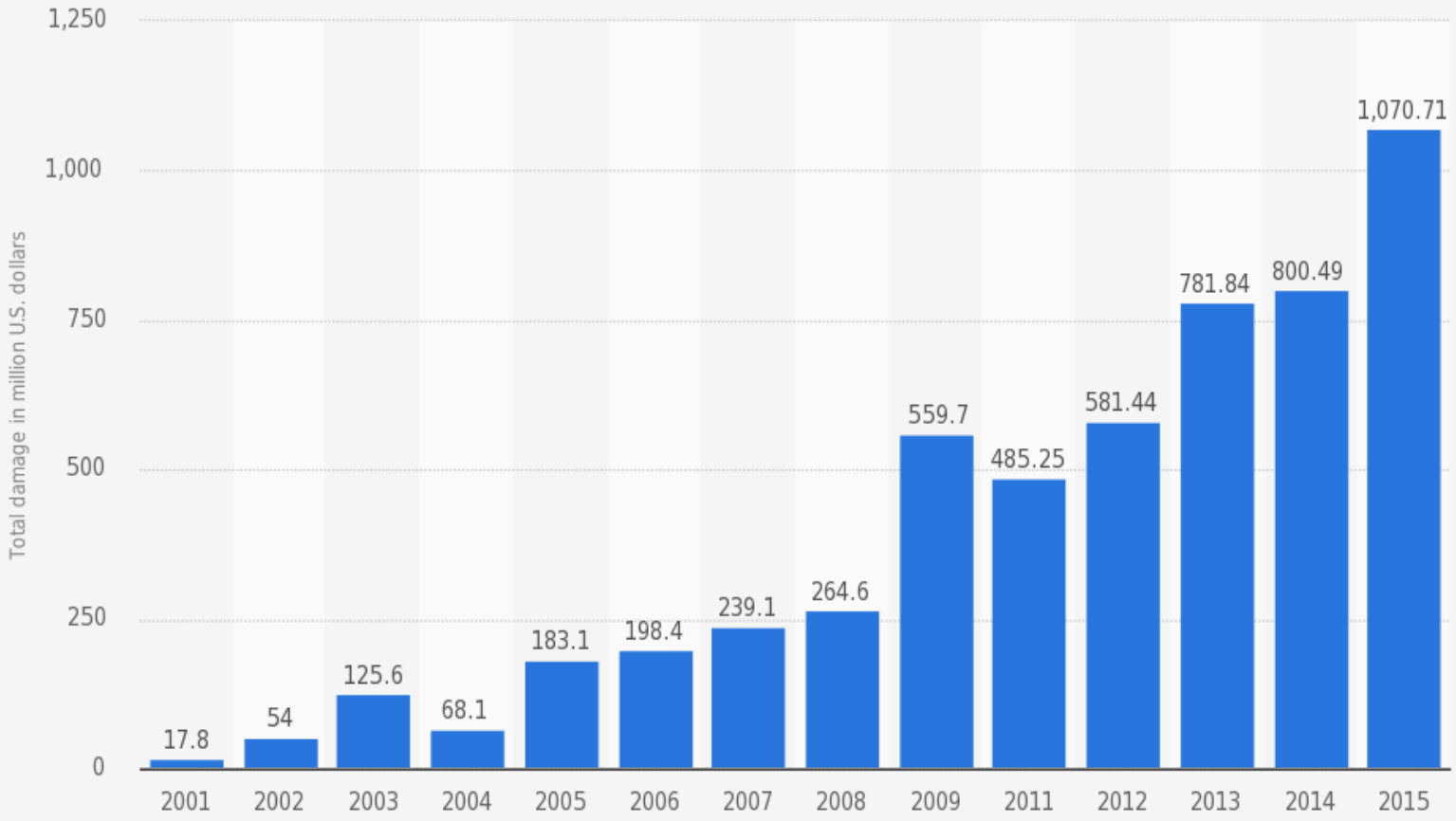
infomedics

De digitale data-explosie

16 miljard volle harde schijven van 500 GB



Ontwikkeling van datamisbruik



infomedics

Hacks in het nieuws…

Data is het nieuwe goud

- Data is overal
- De waarde van data is groot (vooral van complete datasets)
- Data is relatief eenvoudig te stelen, hackers zijn sluw, brutaal en vindingrijk
- De pakkans bij cyber crime is klein
- Transport van de buit is eenvoudig, smokkelen is niet nodig
- Data hotspots zijn kwetsbaar
- Voor een hacker is uw praktijk EEN PROJECT

Wetgeving in historisch perspectief

Wetgeving loopt altijd achter op dynamische werkelijkheid, maar met recente wetgeving is er flink gerepareerd.

Autoriteit Persoonsgegevens

Onze missie

Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.

AUTORITEIT
PERSOONSGEGEVENS

- Voorheen College Bescherming Persoonsgegevens (CPB)
- Belangrijke toezichthouder want privacy is een grondrecht
- Meer gewicht dan bijvoorbeeld de Nza
- Wet niet correct nageleefd > bindende aanwijzing
- Fout niet hersteld > boete van 4% van jaaromzet of max EUR 20 miljoen

Wat staat er in de AVG?

AVG gaat (nog steeds) over:

- Rechtmatigheid, eerlijkheid en transparantie
- Integriteit en vertrouwelijkheid
- Dataminimalisering
- Afbakening van het doel
- Afbakening van de opslag
- Nauwkeurigheid

Nieuwe zaken:

- Dataportabiliteit
- Recht om vergeten te worden
- Aantoonbaar maken dat regels structureel worden nageleefd

Identificeerbaarheid

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“betrokkene”).

Als informatie op wat voor manier dan ook iets zegt over of gekoppeld is aan een identificeerbare persoon, dan zijn het persoonsgegevens. De vorm doet niet ter zake.

Denk in uw praktijk aan:

- Een aantekening op een blocnote
- Een gesprek over de telefoon
- Een factuur
- Of alleen al de aanwezigheid van een patiënt in een wachtkamer

Verantwoordelijke en verwerker

De Verwerkingsverantwoordelijke is degene die het doel van en de middelen voor de verwerking vaststelt. Dat bent u dus.

De verwerker is degene die ten behoeve van de verwerkings-verantwoordelijke persoonsgegevens verwerkt. Dat zijn uw leveranciers die persoonsgegevens van uw patiënten van u ontvangen.

- Ga na welke leveranciers persoonsgegevens ontvangen
- Leg afspraken vast in een verwerkersovereenkomst
- Controleer regelmatig of deze partijen zich aan de afspraken houden

Privacy management

Artikel 24 lid 1 AVG

Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

Privacy management

Artikel 24 lid 1 AVG

Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

Privacy management

Artikel 24 lid 1 AVG

Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

Privacy management

Artikel 24 lid 1 AVG

Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

Privacy management

Artikel 24 lid 1 AVG

Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.

In 10 stappen voorbereid

1. Bewustwording
2. Rechten van betrokkenen
3. Overzicht verwerkingen
4. Data protection impact assessment (DPIA)
5. Privacy by design & privacy by default
6. Functionaris voor de gegevensbescherming
7. Meldplicht datalekken
8. Bewerkersovereenkomsten
9. Leidende toezichthouder
10. Toestemming

Bewustwording

- Alle relevante mensen in uw organisatie moeten op de hoogte zijn van de nieuwe privacy regels

- Organiseer regelmatig risico evaluaties:
  - wat zou er kunnen gebeuren als...?
  - wat is de kans en impact hierop?
  - Welke maatregelen kunnen en willen we nemen?

- Maak duidelijke keuzes die bij uw organisatie passen en documenteer uw keuzes in een informatiebeveiligingsbeleid

- Begin op tijd, het proces is belangrijk

Rechten van betrokkenen

Uw patiënten krijgen meer en verbeterde privacyrechten onder de AVG

- Recht op inzage
- Recht op correctie en verwijdering
- Recht op dataportabiliteit

Uw patiënten kunnen klachten indienen bij de Autoriteit Persoonsgegevens die ze vervolgens in behandeling moet nemen.

Is uw praktijksoftware klaar om deze rechten te verlenen?

Hoe gaat u om met backups en fysieke documentatie?

Heeft u een transparant klachtproces?

Overzicht verwerkingen

- Gegevensverwerkingen moeten in kaart worden gebracht
  - Welke persoonsgegevens ontvangt u van betrokkenen?
  - Voor welke doel gebruikt u deze persoonsgegevens?
  - Welke verwerkingen vinden binnen uw organisatie plaats?
  - Met wie deelt u deze persoonsgegevens?

- Dit verwerkingsregister dient de accountability (verantwoordingsplicht)

- U gebruikt het om te voldoen aan rechten van betrokkenen

- Vermeld ook obv welke wettelijke grondslag u de persoonsgegevens verwerkt
  - Gerechtvaardigd belang, of
  - Toestemming betrokkenen

Wanneer kan data lekken?

- Diefstal van een laptop
- Verlies USB stick
- Ex medewerker die nog steeds toegang heeft
- Onjuiste registratie van adresgegevens van patiënten
- Patiënten die meeluisteren of meekijken
- Geopende post op de balie
- Geen firewall of verouderde anti virus software
- Balie onbemand achterlaten
- Wifi voor patiënten op zakelijke netwerk
- Computers niet vergrendelen e/o ‘s nachts aan laten staan
- UZI pas in de houder laten zitten
- Slecht wachtwoord beleid
- Geen toezicht op leveranciers

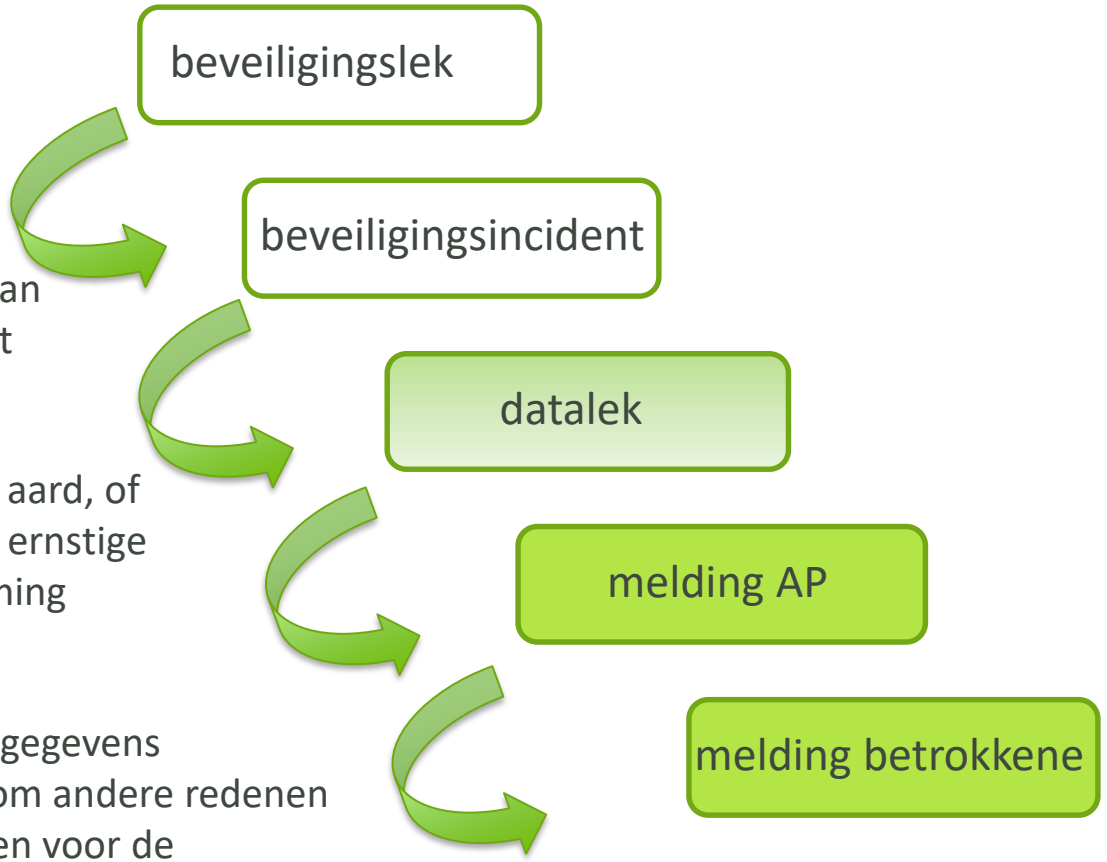
Meldplicht datalekken

Heeft zich een beveiligings-incident voorgedaan?

Persoonsgegevens verloren gegaan of onrechtmatige verwerking niet uitgesloten?

Persoonsgegevens van gevoelige aard, of sprake van (aanzienlijke kans op) ernstige nadelige gevolgen voor bescherming persoonsgegevens?

Waren niet alle gelekte persoonsgegevens versleuteld of heeft het datalek om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene?



Wat als .....

Boete

RODE KAART
€ 810.000
of 10% jaaromzet
Per overtreding

Niet melden van een datalek

- Ernstige verwijtbare nalatigheid
- Verwijtbaarheid van overtreder
- Houdt rekening met omstandigheden
- Boete verhoging (5jaar) of verlaging
- 50% Verhoging bij recidive

GELE KAART
€ 0
-
€ 810.000
Per overtreding

Wel melden van een datalek

- Eerst bindende aanwijzing van AP
- Afhankelijk van overtreding boete
- Hoor en wederhoor met AP
- Afhankelijk van uitkomst volgt boete
- Boete verhoging of verlaging

Wat wilt u onze hacker vragen?

A. Hoe hack je een praktijk?

B. Hoe gevaarlijk is een duckie?

C. Hoe vind je een potentieel slachtoffer?

D. Hoe ga je te werk als je een slachtoffer hebt?

E. Hoe groot is de kans dat je binnen komt?

F. Wat valt er te halen bij praktijken?

G. Hoe ziet het profiel van een hacker eruit?

Onderzoek Qfast tandartspraktijken

Onderzoeksopzet

- Forensische meting en verkeersanalyse 26 tandartspraktijken
- Scan op malafide IP-adressen, bekende exploits en digitaal gedrag systemen
- Onderzoeksperiode beslaat 5 maanden (2015/2016)

Conclusies

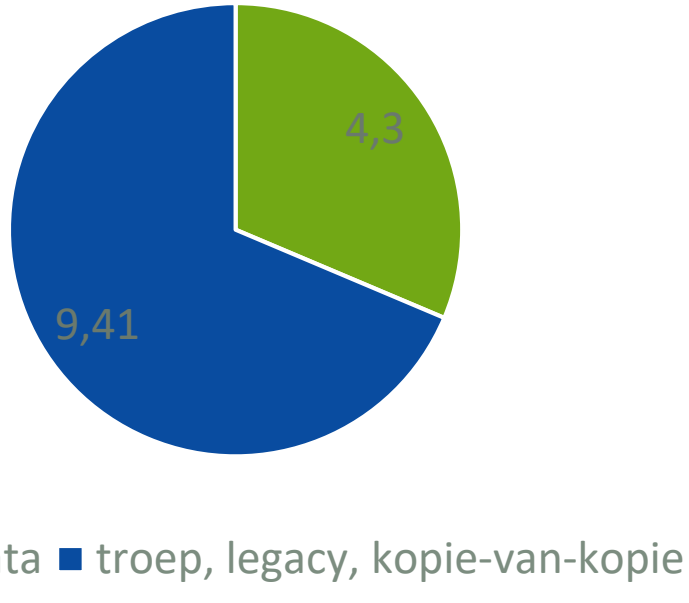
- Gemiddeld 6.000.000 aanvallen per maand (= 230.000 per praktijk)
- Technische beveiliging (firewall, antivirus) is vaak onder de maat
- Software is vaak niet up-to-date
- IT wordt niet of slecht beheerd, beheer vindt plaats op afroep en is reactief
- IT-beheer vindt niet plaats door echte professionals
- Veel menselijke fouten (onbeheerde werkstations, passwords op prikbord)

Vervolgonderzoek IT Checks

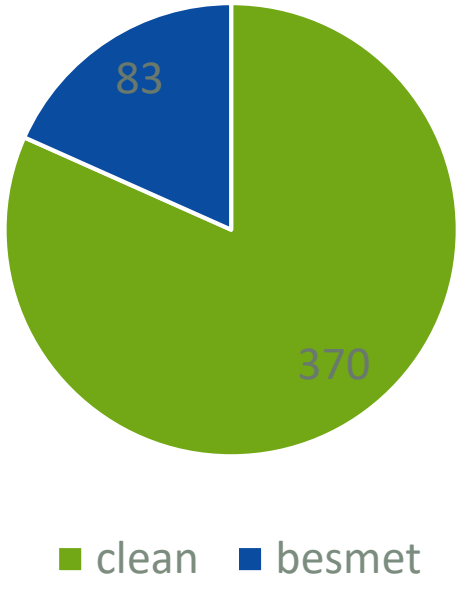
- Locatie, samenstelling, configuratie, IT systemen en netwerken
- In-dept analyse hardware & software
- 63 praktijken door heel Nederland (1 tot 6 stoelen)
- 453 computer systemen
- 13,71 TerraByte aan praktijk data

Resultaten IT Checks

Praktijkdata (in TerraBytes)



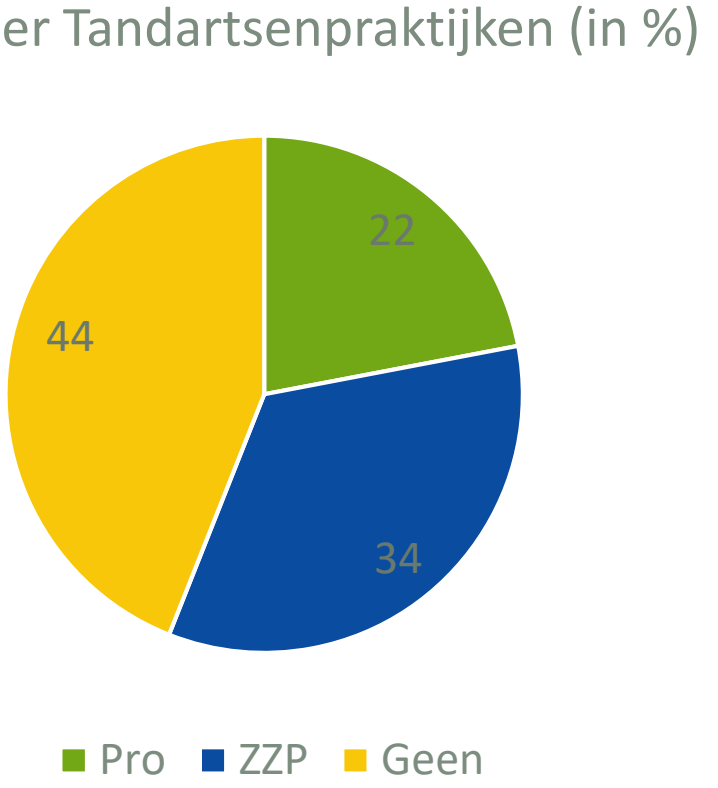
Virus/Malware besmetting (in #)



Resultaten IT Checks

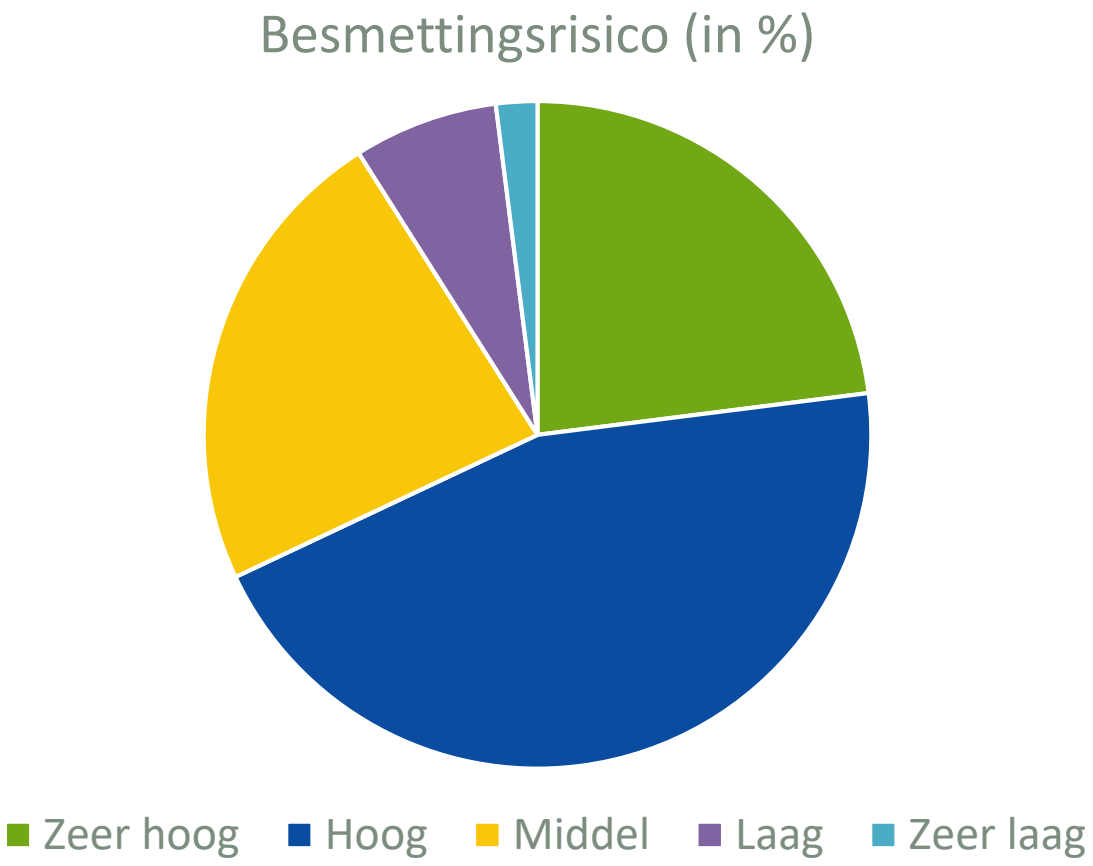
Hoe is de verdeling van praktijken ten opzichte van een IT beheerder?

Professioneel – 22%
Eenmanszaak – 34%
Zelf / Neef / Vriend – 44%



Resultaten IT Checks

Hoe staat het met de kansen op besmetting?



Resultaten IT Checks

Top 10 tekortkomingen

		% niet op orde
1.	Windows OS update	90%
2.	Antivirus	85%
3.	Remote / Thuiswerken	76%
4.	Back-up	71%
5.	WiFi	70%
6.	Verontreinigde disks	69%
7.	Verouderde applicatie software	63%
8.	Toegangscontrole	59%
9.	Niet gebruikte/relevante/onveilige software	58%
10.	Fysieke systemen	45%

Hoe gaat Infomedics hiermee om?

- Informatiebeveiliging in de genen > opgericht in jaar van introductie Wbp
- Nieuw systeem gebouwd vanaf 2010: ‘privacy by design’
- ISO 27001 certificering in 2015: internationaal erkende norm
- Geregistreerd bij Autoriteit Persoonsgegevens
- Lid van Centrum voor Informatiebeveiliging en Privacybescherming

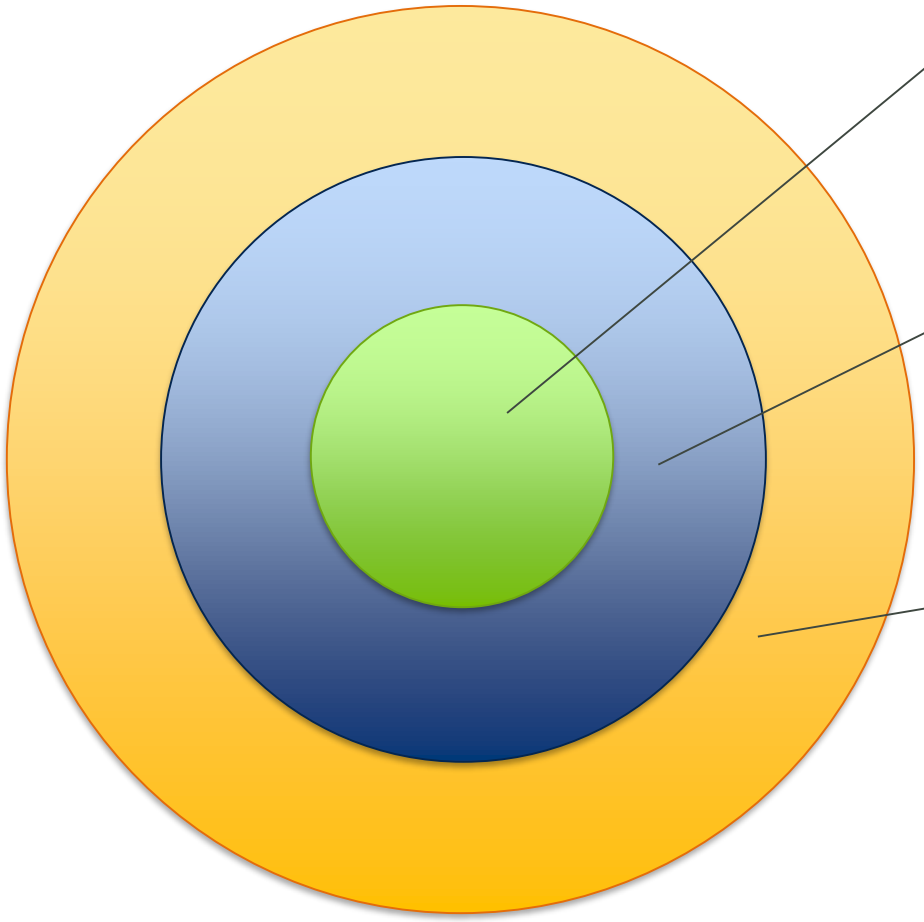
Onze privacy missie

Wij zijn het verlengstuk van zorgverleners en eren hun beroepsgeheim. Onze organisatie en medewerkers doen er alles aan om de persoonsgegevens van zorgverleners en patiënten maximaal te beschermen. Wij eisen hetzelfde niveau van informatiebeveiliging van onze partners en leveranciers.

Wat betekent dit concreet?

- Internal auditteam dat jaarlijks alle processen toetst
- Jaarlijkse hacktests op onze systemen door ethical hackers van Deloitte
- Elk jaar controle door ISO auditors van Lloyds Register
- Informatiebeveiligingsbeleid
- Control framework van 114 normen op informatiebeveiliging
- Bewustwording sessies en risico evaluaties op elke afdeling
- Systeem van incidentmeldingen intern (dagstarts)
- Melding van datalekken aan AP en betrokkenen
- PIT van 5 personen, inclusief Privacy Officer en IT Security Officer
- Uitwisseling bijzondere persoonsgegevens alleen via beveiligde verbinding
- Controle op de hele keten

Safety scope



<u>Uw praktijk</u>
- techniek
- fysieke inrichting
- gedrag van mensen

<u>Uw partners/leveranciers</u>
- bewerkersovereenkomst
- ISO27001 certificering
- controle op naleving

<u>Partners van uw partners</u>
- ketencertificering
- ISO 27001 en niets minder!
- controle op naleving

Uw praktijk: technische maatregelen

Vijf tips die u direct kunt opvolgen:

1. Schakel een IT expert in om uw infra structuur en beveiliging te checken en te upgraden
2. Lock computers en pas uw wachtwoordbeleid aan (langere wachtwoorden en regelmatig vervangen)
3. Breng scheiding aan tussen patiëntgegevens en bedrijf kritische informatie
4. Installeer firewall, antivirus programma's en laat software updates niet te lang liggen
5. Schakel computers uit als u 's avonds naar huis gaat en werk vanuit huis alleen via VPN

Uw praktijk: organisatorische maatregelen

Vijf tips die u direct kunt opvolgen:

1. Plan uw eerste risico evaluatie met het hele team en voer een structureel werkoverleg in met ‘informatieveiligheid’ als vaste item op de agenda
2. Werk uw informatiebeveiligingsbeleid uit en zorg voor een levend document
3. Voer clean desk policy in en laat geen wachtwoorden rondslingeren op prikborden of op notities achter de receptie/balie
4. Breng leveranciers in kaart, maak afspraken en leg deze vast in bewerkersovereenkomsten
5. Wees zeer terughoudend met het versturen van patientgegevens via e-mail

Uw praktijk: wettelijke verplichtingen

Vijf tips die u direct moet opvolgen:

1. Leg een verwerkingsregister vast
2. Registreer beveiligingsincidenten
3. Meldt datalekken aan AP en betrokkenen
4. Denk na over de rol van de FG
5. Geef concreet invulling aan de rechten van betrokkenen

Informatiebronnen

Vijf bronnen die u kunt raadplegen:

1. www.autoriteitpersoonsgegevens.nl
2. www.zbc.nu
3. www.medischondernemen.nl (Blogs Qfast)
4. *Grip op de AVG, de nieuwe privacywet voor niet-juristen*, Versmissen/Terstegge/Krijgsman, 2017, Wolters Kluwer
5. uw brancheverenigingen?

Afsluiting