MARSH

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

CYBERRISKS
VIRTUELE RISICO'S, ECHTE SCHADE
Adfiz 21 september 2016

Rogier Seinstra
Marsh Nederland

MARSH & McLENNAN COMPANIES

Cyberrisk

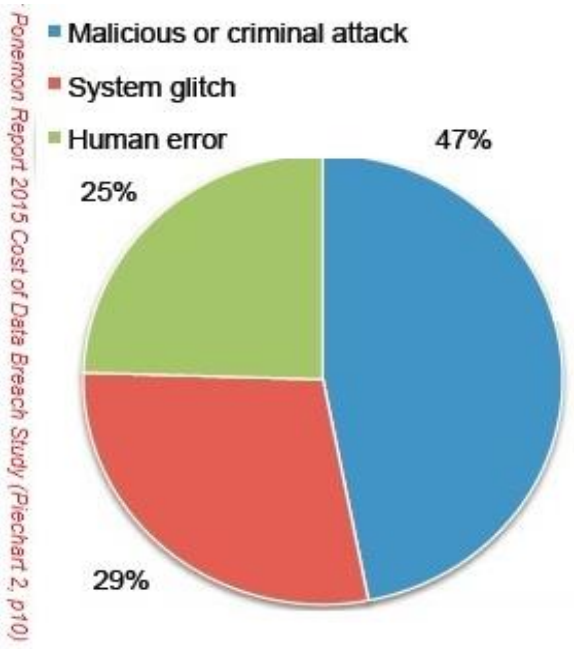
1 Wat is cyberrisk?

2 Risico-overdracht van cyberrisico's
- Verzekerbare schade en risico's
- Adviesrol makelaar of tussenpersoon
- Produkten

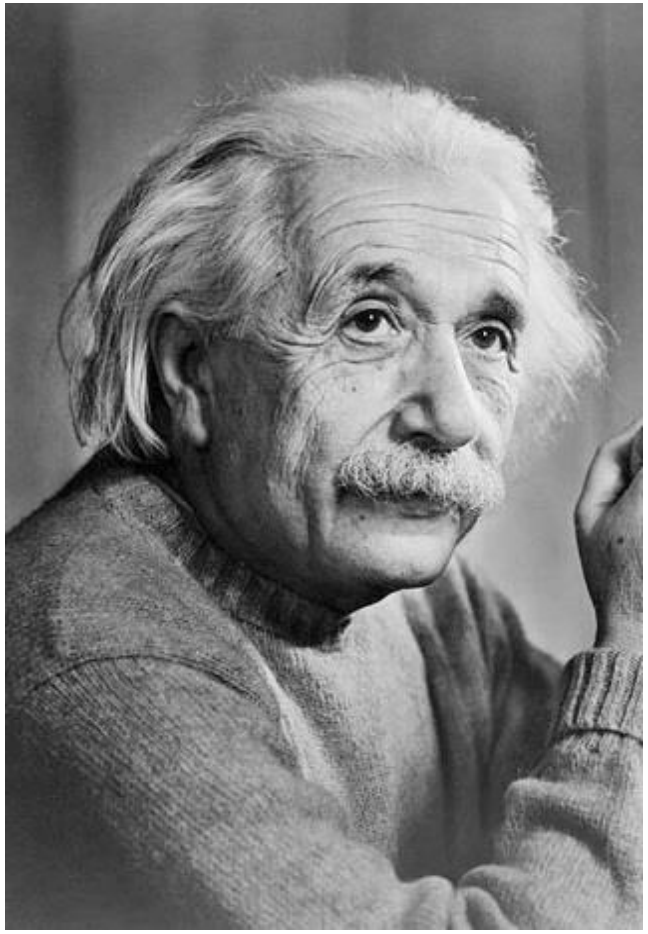
CYBERRISKS
BASIS

Cyberrisk
Basis

Cyberrisk	Financiële schade veroorzaakt door/met/via computers.
Niet alleen crimineel	Denk aan menselijke fouten, systeemstoring, etc.
Cyberschade	Dataverlies, datalek, aansprakelijkheid, bedrijfsschade.



Cyberrisk
100% beveiligen kan niet!



Logica brengt je van A naar B
Fantasie brengt je overal.
Albert Einstein

Menselijke factor

FENCEWORKS MARKETING DOWNLOADS CONTACT PARTNERS »

INFO SECURITY MAGAZINE

CeBIT 2016 14 - 18 March

HOME NIEUWS » BLOGS » WHITEPAPERS AGENDA MAGAZINE » ABONNEREN

Ontslagen systeembeheerder saboteert IT-systemen van fabriek

23 februari 2016 Nieuws

Regelmatig wordt gewaarschuwd voor het gevaar van 'Insider Threats', cyberaanvallen die vanuit het eigen bedrijf worden opgezet door bijvoorbeeld boze (ex-)werknemers. Dat deze dreigingen in de praktijk voor flinke schade kunnen zorgen blijkt uit een rechtszaak tegen een Amerikaanse systeembeheerder. De beheer heeft bekend IT-systemen van een fabriek waar hij is ontslagen doelbewust te hebben gesaboteerd.

Dit meldt het openbaar ministerie in het 'Middle District of Louisiana'. De 44-jarige systeembeheerder was werkzaam voor een fabriek in het Amerikaanse Port Hudson, Louisiana. De man geeft toe na zijn ontslag op afstand te hebben ingelogd op het netwerk van de fabriek en hier doelbewust het systeem dat de fabriek aanstuurt te hebben beschadigd. Hierdoor zou forse schade zijn ontstaan en de bedrijfsvoering van de fabriek zijn onderbroken.

Bron: http://infosecuritymagazine.nl/2016/02/23/ontslagen-systeembeheerder-saboteert-it-systemen-van-fabriek/

Technisch "falen" (zero-day)

Beveiligingslek Shellshock is groter dan Heartbleed

Gepubliceerd: donderdag 25 september 2014 in ict-beveiliging.

Experts hebben een beveiligingslek met de naam Shellshock ontdekt, dat mogelijk gevaarlijker is dan Heartbleed. Hackers kunnen het probleem in de beveiliging vrij eenvoudig misbruiken om de computer daarna allerlei opdrachten te laten uitvoeren.

Een beveilingsexpert op de BBC zegt dat zeker een half miljard computers en apparaten kwetsbaar zijn voor het lek dat al twintig jaar oud is. Het is heel moeilijk, zoniet onmogelijk alle systemen te updaten. Dat komt doordat het lek zit in een onderdeel van het besturingssysteem Unix, waar onder meer Linux en Apple's Mac OS X afgeleiden van zijn. Windows-computers hebben geen last van dit probleem.

Er is geen quick-fix voor Shellshock. Wachtwoorden veranderen, zoals het geval was bij Heartbleed, zal bij dit lek niets verhelpen. De bug zit in een stukje software met de naam Bash. Met Bash geef je commando's in het besturingssysteem Unix. De software wordt gebruikt voor routers en modems, maar bijvoorbeeld ook WiFi-hotspots en servers die internetpagina's aansturen. Met Shellshock kunnen virussen, afluisterprogramma's of andere kwaadaardige software worden geïnstalleerd. Vooralsnog is de enige mogelijkheid voor een oplossing om de laatste beveiligingsupdates te installeren, zodra die beschikbaar zijn.

Bron: http://www.beveiligingnieuws.nl/nieuws/19277/Beveiligingslek_Shellshock_is_groter_dan_Heartbleed.html

Fantasie

Cyberrisk
Voorbeelden van kosten & schade

Aansprakelijkstelling	Inbreuk copyright, datalek, verspreiding malware, ongewenst toegang verlenen.
Kosten n.a.v. datalek	Meldingskosten (toezichthouder, klanten, PCI), onderzoek, PR, klantenservice, reputatie, boetes.
Bedrijfsschade	Extrakosten om bedrijfsstagnatie te voorkomen a.g.v. uitval van (productie)systemen, website, etc.
Datareconstructie	Verwijderen malware, onderzoek, herinstallatie van software/systemen.
Cyberdiefstal	Geld, tegoeden, data/informatie
Cyberafpersing	Onderhandeling, losgeld, beloning.
Contractuele verplichting	In steeds meer B2B contracten vanwege beperkte dekking (beroeps)aansprakelijkheidsverzekering.
Cloud & Outsourcing	Werk kan geoutsourcet worden, niet het risico, de eigenaar van de data blijft verantwoordelijk!

Cyberrisk
Outsourcing & Cloud – algemeen risico

- Backoffice systemen / infra?
- Online portals / EDI / SaaS?
- Back-up en uitwijksysteem?
- Financieel/incasso systeem / ERP ?
- Domotica?

INFO SECURITY MAGAZINE

HOME NIEUWS » BLOGS WHITEPAPERS AGENDA MAGAZINE » ABONNEREN

Hacker verwijdert alle data en back-ups van Code Spaces-klanten

19 juni 2014 Nieuws

Code Spaces, een provider die beheerdiensten leverde voor softwareprojecten, staakt per direct zijn activiteiten. Een hacker heeft na een mislukte chantagepoging uit wraak nagenoeg alle data van Code Spaces-klanten verwijderd. De schade is dusdanig groot dat Code Spaces stelt zijn activiteiten per direct te moeten staken

Het bedrijf meldt op zijn eigen website afgelopen dinsdag het doelwit te zijn geworden van een gecoördineerde DDoS-aanval. De aanvaller liet zijn contactgegevens achter, waarna Code Spaces contact opnam met de cybercrimineel. Deze probeerde het bedrijf voor een grote geldsom af te persen om de cyberaanval te stoppen.

Mislukte tegenaanval van Code Spaces

Code Spaces besloot de zaak te onderzoeken en maatregelen te nemen om het Amazon EC-beheerderspaneel weer onder eigen controle te krijgen. De cybercrimineel was hier echter op bedacht en had vooraf maatregelen genomen om dit te voorkomen. Zo had hij meerdere inloggegevens aangemaakt om zeker te stellen dat hij de toegang tot het beheerderspaneel niet zou verliezen.

Zodra de hacker de pogingen van Code Spaces om het beheerderspaneel weer onder controle te krijgen ontdekte besloot de cybercrimineel wraak te nemen. De aanvaller verwijderde alle data van het beheerderspaneel om Code Spaces langer uit het systeem te houden, waarna hij ongehinderd zijn gang kon gaan. Het bedrijf slaagde er uiteindelijk in het beheerderspaneel weer onder controle te krijgen, maar niet voordat de cybercrimineel een gigantische schade had aangericht.

http://infosecuritymagazine.nl/2014/06/19/hacker-verwijdert-alle-data-en-back-ups-van-code-spaces-klanten/

Datalek
Algemeen schadevoorbeeld

Laatste update: 13 oktober 2013 08:06

Medewerker [redacted] verliest laptop met 40.000 klantgegevens

Een medewerker van [redacted] is een laptop verloren met persoonlijke gegevens van 40.143 klanten. Het gaat om klanten die recentelijk met de helpdesk van het bedrijf contact hebben gehad.

Foto: ANP

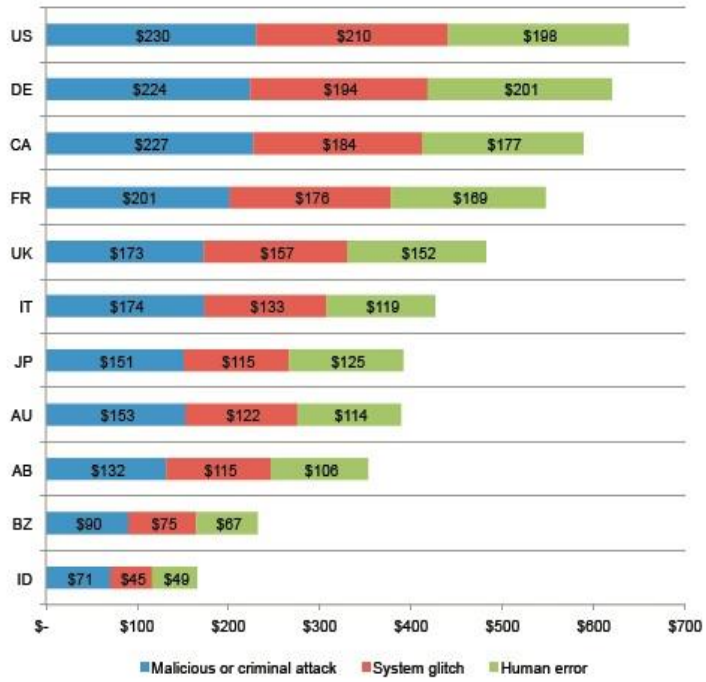
De gestolen laptop had een bestand met daarin het klantnummer, voorletters, achternaam, geslacht, e-mailadressen, postcode, de laatste vier cijfers van het bankrekeningnummer en het onderwerp van het gesprek.

De laptop was niet versleuteld, omdat het om een ouder apparaat gaat. Nieuwere bedrijfslaptops zijn standaard wel versleuteld. [redacted] heeft klanten inmiddels per brief op de hoogte gesteld over het verlies van de laptop.

Ponemon INSTITUTE

2015 Cost of Data Breach Study: Global Analysis

Figure 7. Per capita cost for three root causes of the data breach
Consolidated view (n=350), measured in US$



Kosten EUR 153 per record
gemiddelde DE, FR, UK voor menselijke fout

22.599 (units) x 153 = **EUR 3.457.647**
Zelfs 10% is nog **EUR 345.765** aan kosten

Kostencomponenten o.a.: incident response, externe experts, PR, meldkosten, IT-forensics, juridische bijstand, krediet-/ID-bescherming, juridische bijstand, extrakosten, bedrijfsschade

Datalek
Boetes toezichthouders

Voorbeelden van (komende) **boetes in Europe**

EUR 820.000

Per overtreding, of 10% van jaaromzet
1-1-2016 Meldplicht Datalekken van kracht (Wbp)

EUR 300.000

Tenzij ernstig lek
2009 Deutsche Bahn: EUR 1.123.503,50

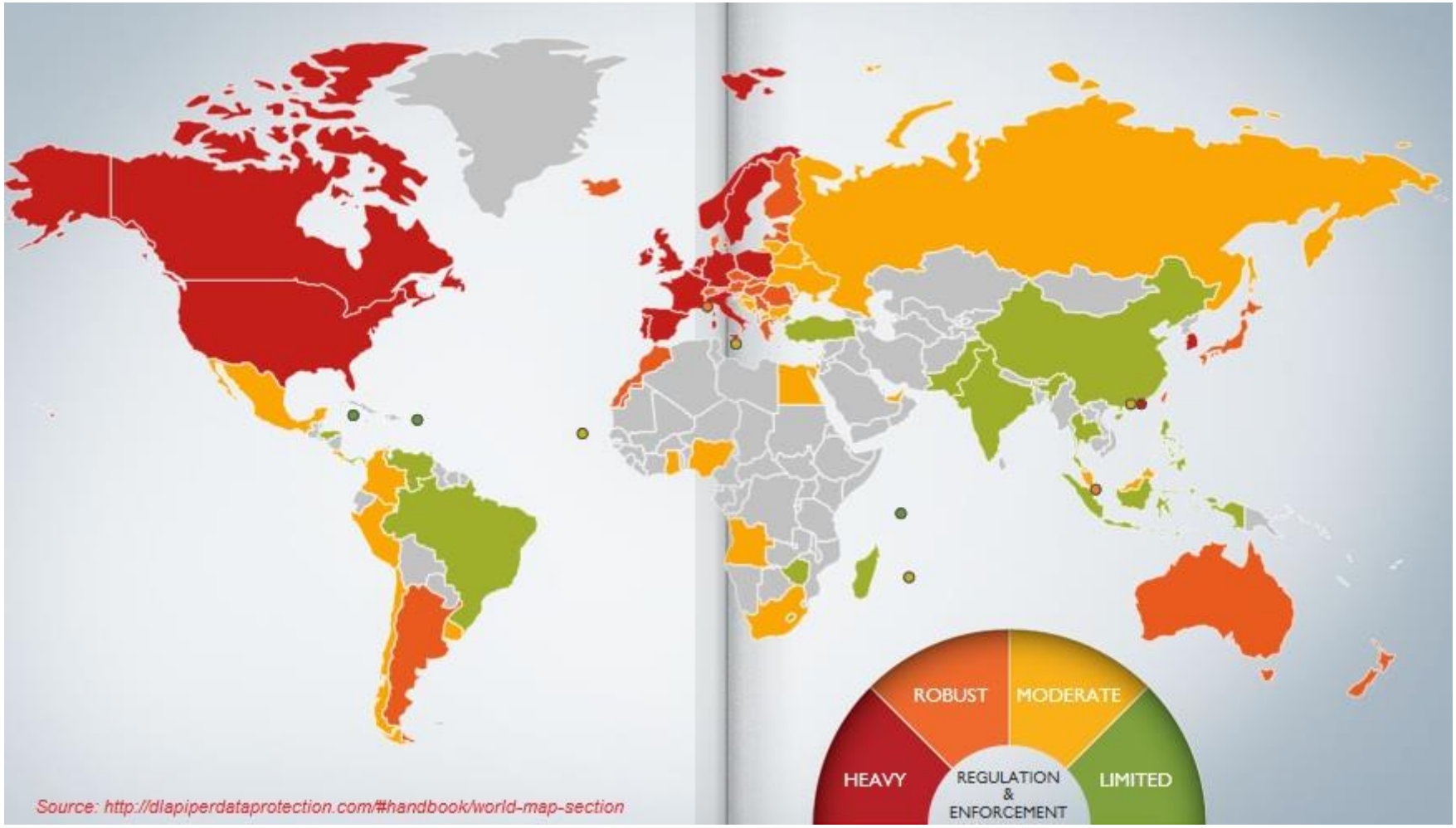
GBP 500.000

Tenzij ernstig lek
2010 verzekeraar Zurich GBP 2.275.000

EUR 20.000.000

Of 4% van wereldwijde jaaromzet
concept Data Protection Regulation (2018?)

Data Privacy Wetgeving
Overzicht wetgeving wereldwijd



CYBERRISK
RISICO-OVERDRACHT?

Cyberrisk
Moeilijke risico’s

Vraag:

Ongeveer 2 jaar geleden heb ik bij een assurantieclub een lezing bijgewoond over dit onderwerp. Wat toen naar voren kwam was dat alleen van origine buitenlandse verzekeraars verzekeringsoplossingen hadden voor het cyberrisico en dat er grote verschillen in dekking waren, maar dat de verzekeringen ook niet goed aansloten op de Nederlandse wetgeving. En wat kunnen de provinciale verzekeraars bieden?

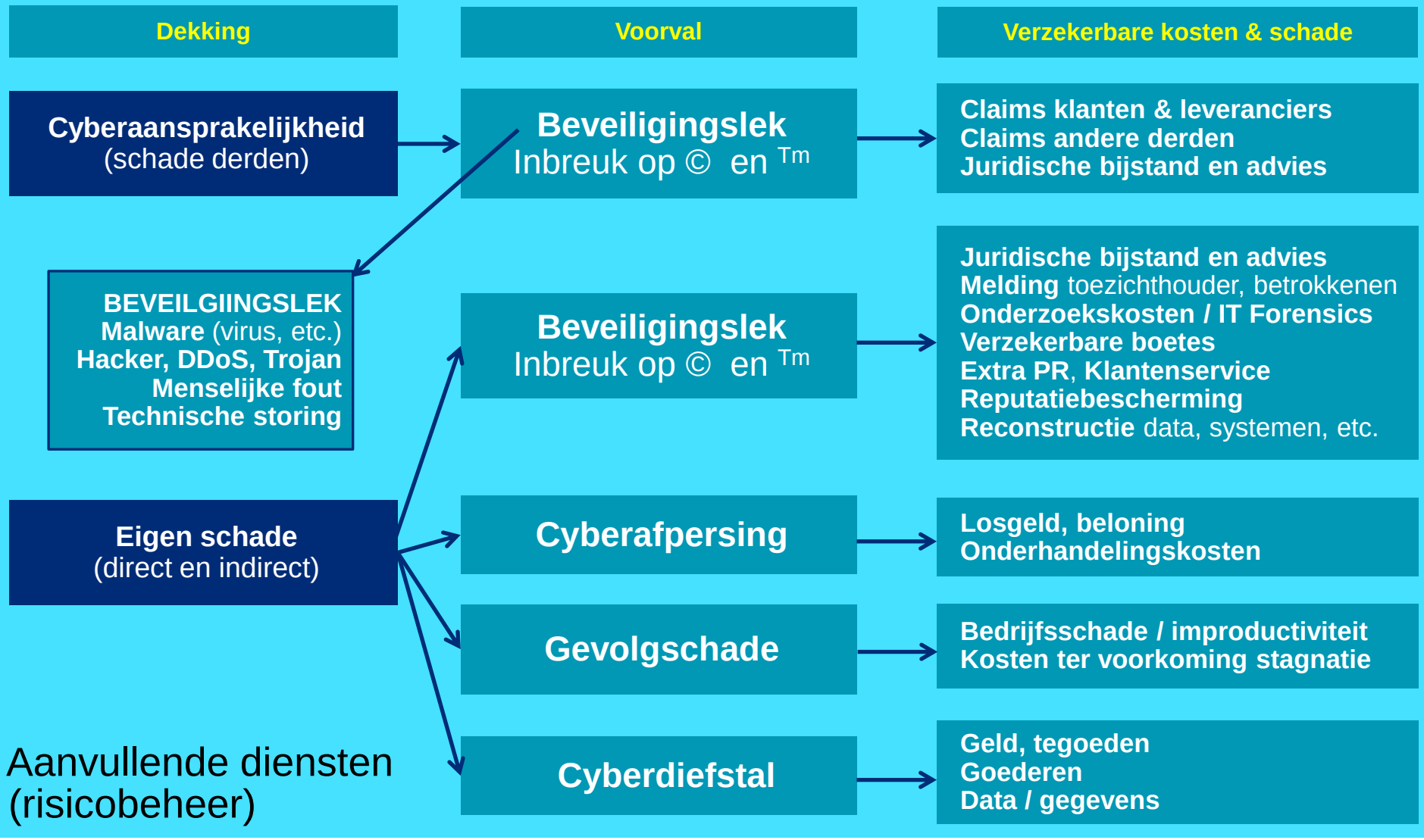
Cyberrisk
Moeilijke risico's

Vraag:

Zoals eerder besproken vinden wij de cybersecurity een belangrijk onderwerp en hebben wij onlangs getracht een verzekering voor ons kantoor af te sluiten. De eigen ervaring is het beste te gebruiken in de adviespraktijk naar onze klanten.

AIG heeft hiervoor een premiekaart. Echter na het opvragen van een offerte ontvingen wij een aanbod met een premie die 2x zo hoog was, omdat assurantiekantoren een verhoogd risico zijn. De premie werd hierdoor voor ons te hoog. Hoe komen wij er achter wat de gunstigste verzekeringsoplossing voor financieel advieskantoren is?

Cyberverzekering
Verzekerbare schade en risico's



Cyberrisk
Risico-overdracht via verzekering

Beperkte dekking traditionele verzekeringen

Cyberriskverzekering is calamiteitendekking

Verzekeringsmarkt cyberrisk is wisselvallig en individueel

Risico-informatie

- Certificering (ISO 9001, 27001/2)
- Data beveiligingsbeleid
- ICT preventie (binnendringen, malware)
- Detectie & opvolging voorval
- Systemen, toepassingen en data

Cyberrisk
Producten verzekeringsmarkt

Chubb (v/h Ace)	Dataguard
AIG	CyberEdge
Allianz	CyberProtect
Beazley	Global Breach Solution
Chubb (v/h Chubb)	CyberSecurity
CNA	NetProtect
Hiscox	Data Risks
Marsh	Cyberrisk rubrieken verzekering 2016

Cyberrisk
Moeilijke risico's

De volgend sectoren worden gezien als moeilijk verzekerbare risico's in de markt voor cyberrisk verzekeringen:

- **Verzamelen/beheren medische gegevens of creditcard informatie**
- **Financiële sector (Alles onder AFM of DNB toezicht)**
- **Medische- en zorginstellingen**
- **Call centers / telemarketing**
- **Publieke sector (overheden)**
- **Data processing bedrijven**
- **ISP / Telecom / Social networks**
- **Alles buiten de EU**

Cyberrisk
Perceptie van het risico

- Vaak verwijzing naar IT afdeling
- Cyberriskverzekering is aanvullend op beveiligingsbeleid
- Cyberrisk bij grote ondernemingen wel op de radar als reëel risico, maar koopbereidheid klein.
- Cyberrisk bij MKB ondernemingen wel op de radar, maar niet ervaren als risico met grote impact.
- Conversie offertes zeer laag: <10%

Cyberriskverzekering
Indicatiepremie grote ondernemingen

Polislimiet	EUR 2,5 Mio	EUR 5 Mio	EUR 10 mio
Incident management	EUR 2,5 Mio	EUR 5 Mio	EUR 10 Mio
Onderzoek/boete AP	EUR 2,5 Mio	EUR 5 Mio	EUR 10 Mio
Cyberaansprakelijkheid	EUR 2,5 Mio	EUR 5 Mio	EUR 10 Mio
Afpersing	EUR 2,5 Mio	EUR 5 Mio	EUR 10 Mio
Cyberbedrijfsschade	EUR 2,5 Mio	EUR 5 Mio	EUR 10 Mio
Algemeen eigen risico	EUR 250.000	EUR 250.000	EUR 250.000
Eigen risico boete toezichthouder (AP)	10% / Min. EUR 150.000	10% / Min. EUR 150.000	10% / Min. EUR 150.000
Wachttijd bedrijfsschade	12 uur	12 uur	12 uur
Indicatiepremie netto (excl. AB en fee)	EUR 20.875	EUR 29.125	EUR 37.375

Cyberriskverzekering
Indicatiepremie kleine ondernemingen (omzet < 1 mio)

Polislimiet	EUR 250.000	EUR 2,5 Mio
Incident management	EUR 250.000	EUR 2,5 Mio
Onderzoek/boete AP	EUR 250.000	EUR 2,5 Mio
Cyberaansprakelijkheid (3 jaar inloop)	EUR 250.000	EUR 2,5 Mio
Afpersing	EUR 250.000	EUR 2,5 Mio
Cyberbedrijfsschade	EUR 250.000	EUR 2,5 Mio
Algemeen eigen risico	EUR 1.000	EUR 1.000
Eigen risico boete toezichthouder (AP)	10% / Min. EUR 2.500	10% / Min. EUR 2.500
Wachttijd bedrijfsschade	12 uur	12 uur
Indicatiepremie bruto (af 17,5% commissie) (excl. AB)	EUR 700	EUR 2.750

Cyberrisk

“ Er zijn 2 soorten bedrijven: bedrijven die gehackt zijn en bedrijven die gehackt worden”

– Robert Mueller, FBI (2012)

De gemiddelde periode dat een hacker ongemerkt rondneust in uw systeem is 205 dagen!

– M-Trends Report FireEye (2015)

Einde, bedankt voor uw aandacht

Marsh Nederland Cyber Risk Practice

Erik van de Velde BSc Eng
Practice Leader Cyber Risk Marsh Nederland
TL: +31 (0) 6 538 33 961
E-mail: erik.vandevelde@marsh.com