ACADEMIE VOOR OVERHEIDSJURISTEN & ACADEMIE VOOR WETGEVING | 18 JUNI 2020

cybersecurity voor juristen

prof. mr. Gerrit-Jan Zwenne | mr. ir. Ard Jan Dunnik | Brenno de Winter

eLaw Leiden

De Winter Information Solutions
Openbaarheid van bestuur, journalistiek, training

COUPRY PELS RIJCKEN

Agenda

9:30	De juridische kaders. Een snelle uiteenzetting	Gerrit-Jan Zwenne & Ard Jan Dunnik
11:00	pauze	
11:20	Een casus	Brenno de Winter
12:30	Wrap up. Wat nu?	Gerrit-Jan Zwenne, & Brenno de Winter
13:00	Afsluiting	

Wie zijn wij…?

prof. mr. Gerrit-Jan Zwenne, hoogleraar te Universiteit Leiden en advocaat te Den Haag

mr. ir. Ard Jan Dunnik advocaat te Den Haag

Brenno de Winter openbaarheid van bestuur, journalistiek en training

cyber security is not an IT issue. It is a boardroom issue

maatschappelijk probleem

Volledige afhankelijkheid van digitalisering
Door de vrijwel volledige afhankelijkheid van digitalisering is de digitale veiligheid van processen en onderliggende (informatie)systemen essentieel geworden. Het belang van digitale

Analoge alternatieven en terugvalopties essentieel en vrijwel afwezig
Door het bijna volledig verdwijnen van analoge alternatieven en de afwezigheid van terugvalopties is de afhankelijkheid van gedigitaliseerde processen en systemen zo groot geworden dat aantasting hiervan kan leiden tot maatschappij-ontwrichtende schade. Hier hoeft geen opzet in het spel te zijn, ook storingen en

schade.[56,57,58] In de afgelopen rapportageperiode hebben DDoS-aanvallen ervoor gezorgd dat een aantal banken tijdelijk slecht bereikbaar was.[59] Maar ook diensten van de Rijksoverheid zijn regelmatig getroffen. Zo waren de Belastingdienst, de Douane en

digitale ontwrichting

ZOMAAR EEN CYBER SECURITY INCIDENT

Damsko Energie N.V.

- productie en levering
- beursgenoteerd (AEX)
- marktaandeel ca. 20-25 %

er is een probleem

het is vrijdag 16:45 als de telefoon gaat.....

IT Manager

Hoofd Juridische Zaken

- oud IT manager is in financiële en klantensysteem binnengedrongen
- onduidelijk wat hij heeft gedaan
- verder onderzoek volgt

acties

- wie erbij betrekken?
  - Directie, communicatie, juridische zaken, IT beveiliging, DPO
- schade beperken
  - lek dichten
  - betrokkenen
  - verzekering
- lek melden bij autoriteit(en)
  - Autoriteit Persoonsgegevens
  - ~~Autoriteit Telecom~~
  - ~~NCSC~~
- aangifte
- geheimhouding

het wordt erger

Een emailbericht waar iedereen zenuwachtig van wordt .....

IT Manager

Hoofd Juridische Zaken

From: Dhr. Ir. [redacted] IT-manager
Sent: Thursday 18 June 2020 (CEST) 9:14
To: Mw. Mr. [redacted] Head Legal
Cc: Legal-ALL; IT-ALL
Subject: Groot probleem!!

Hi [redacted]

Het probleem is veel groter. De vorige IT-manager had zelfs toegang tot de systemen waarmee productiecentrales kunnen worden afgeschakeld. Foute boel!

Er zijn grote fouten gemaakt. Ik houd je op de hoogte,

Cheerio,

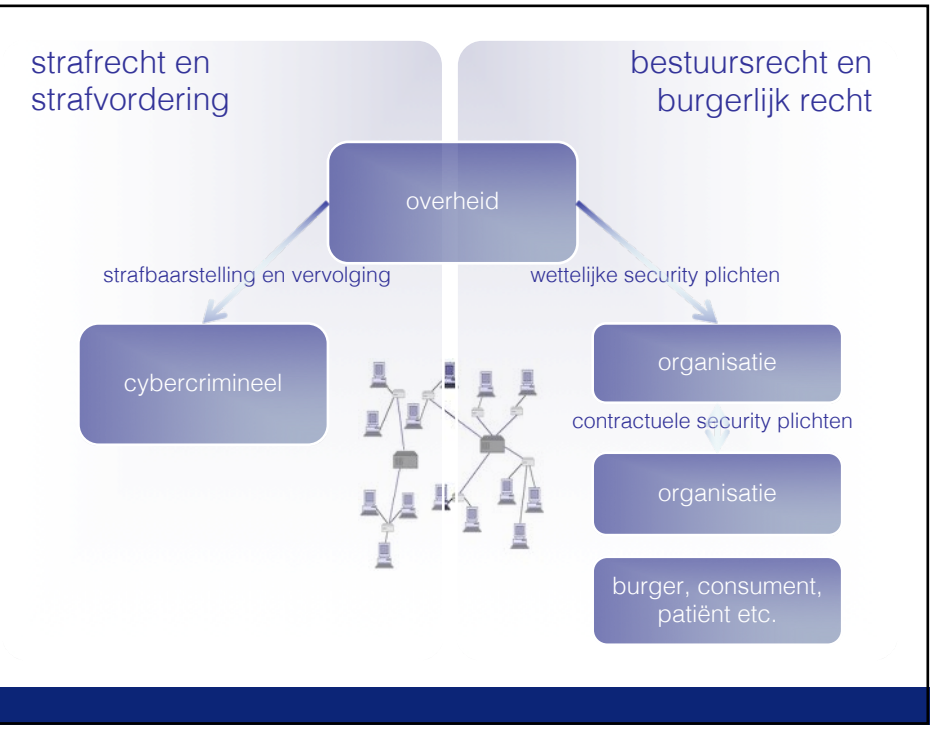
[redacted]

- aan de Hoofd Juridische Zaken, de IT afdeling en hoger management
- mogelijk heeft oud manager toegang tot systemen voor de elektriciteitscentrale
- “Er zijn grote fouten gemaakt” schrijft de IT manager

acties

- zakelijker communiceren
- need to know basis
- lek melden bij autoriteit(en)?

JURIDISCHE KADERS. EEN UITEENZETTING



vaak combinaties

cyber crime	cyber crime Sr	real life Sr
hacken	Art. 138ab lid 1 Sr. (computervredebreuk)	Art. 138 Sr. (huisvredebreuk)
gegevens vernielen	Art. 350a lid 1, 350b lid 1 Sr. (wissen, wijzigen (etc.) computer-gegevens)	Art. 350 Sr (vernielen)
gegevens stelen	Art. 138c 139g Sr. (“diefstal" en “heling” gegevens)	Art. 310 Sr (diefstal) wegnemen, niet kopiëren gegevens
gegevens aftappen	Art. 139c Sr. (d.m.v. geautomatiseerd werk)	Art. 139a/139b Sr (technisch hulpmiddel)
(d)dos aanval	Art. 138b Sr (belemmeren toegang)	
malware	Art. 350a lid 3, 350b lid 2 Sr (verspreiden schadelijke gegevens)	
phishing	Art. 326 Sr (“ter beschikbaar stellen gegevens")	Art. 326 Sr (bedrog)
ransomware	Art. 317 lid 2 Sr (afpersing door “gijzelen” gegevens)	Art. 317 lid 1 Sr (afpersing)

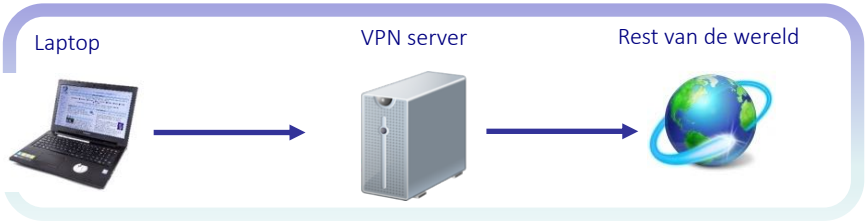
Wetboek van strafvordering (WvSv)

Wat kan het OM doen?

- inbeslagname computerapparatuur — Art. 94 Sv
- doorzoeking ter vastlegging gegevens — Art. 125i Sv
- verlengde netwerk doorzoeking — Art. 125j Sv
- decryptiebevel — Art. 125k Sv
- Op afstand computers doorzoeken — Art. 126nba Sv

OPENBAAR MINISTERIE
POLITIE

Internationaal



cyber crime vanuit het buitenland

- rechtsmacht
- Opsporing / uitvoerende rechtsmacht
  - wederzijdse assistentie
  - openbare bronnen
  - hacken?

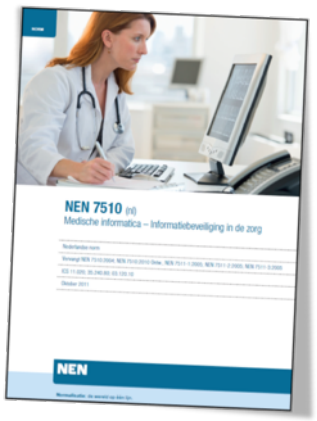
geheimhoudings- en beveiligingsplicht persoonsgegevens

Algemene Verordening Gegevensbescherming

- integriteit en vertrouwelijkheid — Art. 5(1)f AVG
- passende technische en organisatorische maatregelen — Art. 32 AVG
- bewerkersovereenkomst — Art. 28 AVG
- meldplicht — Art. 33 en 34 AVG

beveiligingsplicht gezondheidszorg

- Artikel 15j, eerste lid, Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg
- Beveiliging informatie-uitwisseling NEN 751x (Besluit elektronische gegevensuitwisseling zorgaanbieders)



beveiligingsplicht telecommunicatie

- passende organisatorische en technische maatregelen bescherming persoonsgegevens — art. 11.3 en 11.3a Tw
- passende organisatorische en technische maatregelen ter bescherming bescherming veiligheid en integriteit netwerken en diensten — art. 11a.1 en 11a.2 Tw


Boete KPN voor onvoldoende beveiliging klantgegevens

02-06-2015

De Autoriteit Consument & Markt (ACM) heeft KPN B.V. in december 2013 een boete opgelegd voor het onvoldoende beveiligen van systemen waarin de persoonsgegevens van klanten zijn opgeslagen. KPN heeft op grond van de Telecomwet de plicht om de persoonsgegevens en de persoonlijke levenssfeer van hun klanten voldoende te beschermen, zodat derden daarbij geen toegang hebben.

Tegen het sanctiebesluit heeft KPN beroep ingesteld bij de rechtbank Rotterdam. De

Autoriteit
Consument & Markt

beveiligingsplicht financiële ondernemingen

- DNB toetsingskader — art. 3:17 Wft jo. Art. 20 Bpr
- Meldplicht DNB/AFM — art. 3:10 lid 3 en 4:11 lid 4 Wft

geheimhouding en beveiliging door bestuursorganen

- geheimhoudingsplicht voor 'een ieder die is betrokken bij de uitvoering van de taak van een bestuursorgaan' — art. 2:5 lid 1 en 2 Awb:
- zenden elektronische bericht voldoende betrouwbare en vertrouwelijke manier.

art. 2:14 lid 3 Awb

beveiligingsplicht vertrouwensdienstverlener

- vertrouwensdienstverlener moet voldoen aan eisen

18.17a Tw

art. 19
Vo 910/2014 (eidas)

- Besluit vertrouwensdiensten: kennisgeving inbreuk
- Regeling vertrouwensdiensten: Agentschap Telecom - vertrouwenslijst

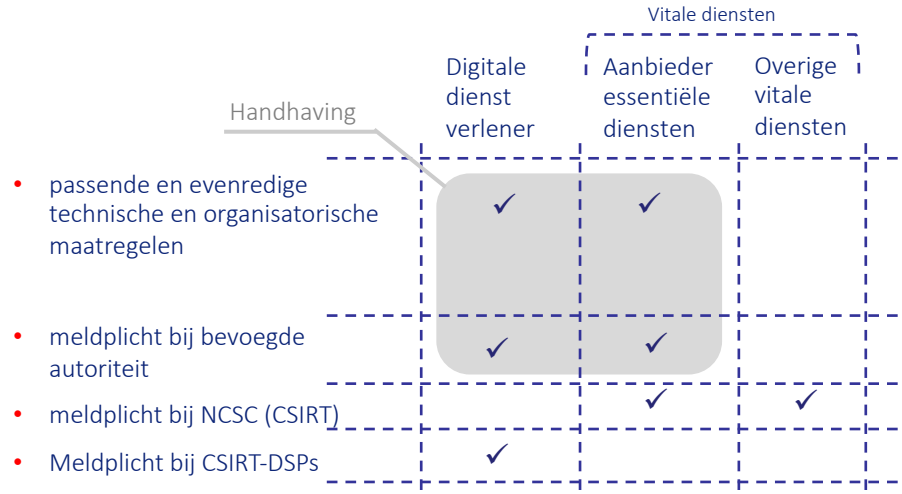
Autoriteit
Consument & Markt

Richtlijn NIB

europa.eu

- Beveiligingseisen aan netwerk en informatie beveiliging aan overheden en:
  - Internetdiensten: handelsplatform, betalingen, sociale netwerken, zoekmachines, cloud-computing, app-stores
  - Energie,
  - Vervoer,
  - Bankwezen,
  - Financiële infrastructuur,
  - Zorginstellingen.
- Meldplicht aan bevoegde autoriteit van inbreuken met aanzienlijke impact op beveiliging van kerndiensten.

Wet beveiliging netwerken informatiesystemen (Wbni)



Toezicht en handhaving:
Essentiële en digitale aanbieders

Agentschap Telecom
Ministerie van Economische Zaken en Klimaat
digitale infra
energie
+ digitale diensten

Inspectie Leefomgeving en Transport
Ministerie van Infrastructuur en Waterstaat
vervoer
drinkwater

DeNederlandscheBank
Infra financiële markt
bankwezen

Inspectie Gezondheidszorg en Jeugd
Ministerie van Volksgezondheid, Welzijn en Sport
gezondheidszorg

Advies en bijstand:
essentiële, digitale en andere vitale aanbieders

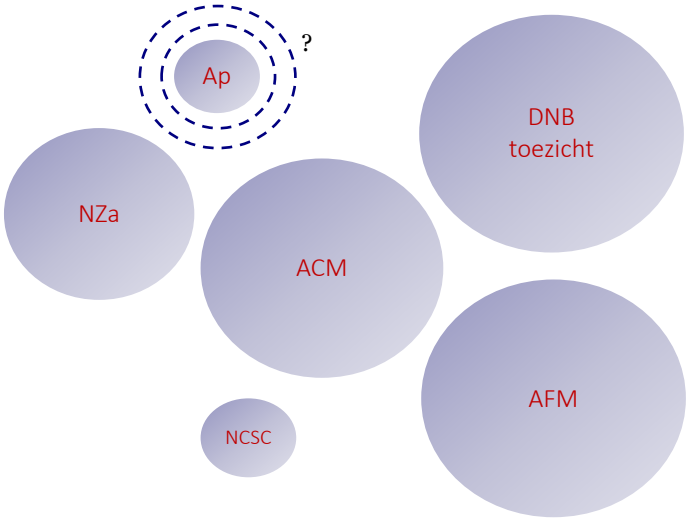
Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie
essentiële diensten
nucleair, waterkering
telefoon, sms, internet

CSIRT-DSP
Ministerie van Economische Zaken en Klimaat
digitale diensten

EU Cyber security act

- EU-breed raamwerk voor cybersecurity certificering
- Risk based approach
- ook voor NIB en artikel 32 AVG ?

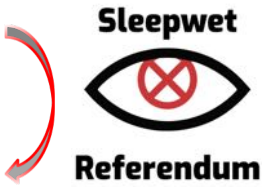
toezichthouders (en dergelijke)



Wet op de inlichtingen- en veiligheidsdiensten

Wat is er veranderd na het referendum over de Wiv?

De AIVD heeft met de nieuwe Wiv 2017 extra bevoegdheden gekregen om zijn werk te kunnen doen. Het gaat dan vooral om het verzamelen van gegevens van telefoon-, e-mail- en internetverkeer. De Wiv is per 1 mei 2018 van kracht.



- Inzet bevoegdheden zo gericht mogelijk
- Bewaartermijn verzamelde gegevens
- Samenwerking met buitenlandse diensten
- Gegevens van de kabel nauwelijks uit Nederland
- Medische gegevens
- Journalisten

Voldoende?

burgerlijk recht

In het onderhavige geval heeft Sjouerman […] door in de doorgang naar het toilet van een café een kelderluik te openen voor bezoekers die aan hun omgeving niet hun volledige aandacht zouden besteden, een ernstig gevaar geschapen, hetwelk hij met eenvoudige middelen had kunnen voorkomen.

Door aan S. te verwijten dat hij met de mogelijkheid van zodanige onoplettendheid geen rekening heeft gehouden en heeft nagelaten m.h.o. daarop zekere maatregelen te treffen heeft het Hof de maatstaven die voor de beoordeling van de schuld van S. aan het aan verweerder overkomen ongeval moeten worden aangelegd, niet miskend.

burgerlijk recht

beveiligingsplichten kunnen gevonden worden in....

- algemene overeenkomst (Boek 6 BW)
  - specifieke bepalingen met beveiligingseisen
  - redelijke en billijkheid (art. 6:248 BW)

→ rechtspraak: garantie

- bijzondere overeenkomsten (Boek 7 BW)
  - goed opdrachtnemerschap (art. 7:401 BW)
  - goed werkgeverschap (art. 7:611 BW)
  - .....

rechtspraak: ..... ?

- maatschappelijke betamelijkheid (onrechtmatige daad)

jurisprudentie

alleen contractuele aansprakelijkheid, en dan met expliciet garantie

- Rb. A'dam 30 juli 2014, ECLI:NL:RBAMS:2014:4888
  - Garantie

(...) the Seller represents and warrants to the Purchaser that:

(...)

(h) The Company has for its current business in place fully tested, current and otherwise appropriate disaster recovery plans and procedures for its IT Systems and Software in order to prevent the loss and facilitate the recovery of data lost through system failure, physical destruction or otherwise and has taken all reasonable steps and implemented all reasonable procedures to safeguard its IT Systems and Software and prevent unauthorised access thereto.",

- drie gebreken
  - verouderde software
  - credentials en wachtwoorden niet versleuteld opgeslagen
  - werkstation in zowel secure-net als office-net

- Rb. Rotterdam 22 augustus 2012 (ECLI:NL:RBROT:2012:BX7293)
  - Excessief telefoongebruik door Tri-Ennium door hack
  - Telespectrum de “beveiliging” van de lijnen gegarandeerd
  - ➢ Telespectrum in beginsel kosten dragen a.g.v. hack
- Rb. Rotterdam 10 april 2013 (ECLI:NL:RBROT:2013:CA2561)
  - Tri-Ennium usernames en passwords goed bewaard?
  - Telespectrum heeft in ieder geval verzuimd meteen maatregelen te nemen (continue bewaking)

- Gerechtshof Arnhem-Leeuwarden 4 september 2018 (ECLI:NL:GHARL:2018:7967)
  - Politie koopt systeem via wederverkoper Motiv met tokens van RSA
  - Tokens gecompromitteerd door hack en moesten worden vervangen. Politie dagvaardt Motiv voor schadevergoeding.
  - ➢ Hof: Fout ligt in risicosfeer RSA, dus niet bij Motiv
    Daar komt dan nog bij dat ieder computersysteem uiteindelijk kan worden gehackt, zodat de Politie ook geen volledig hackfree systeem mocht verwachten.

- Rechtbank Amsterdam 14 november 2018 (ECLI:NL:RBAMS:2018:10124)
  - IT leverancier levert IT infrastructuur aan O'Cliance, incl. beheer en onderhoud
  - Ransomeware aanval, O'Cliance betaalt voor ontsleutelen en meer er is meer bedrijfsschade die zij vordert op IT Leverancier
  - Geen schriftelijke overeenkomst

➢ Rachtbank: IT Leverancier schadeplichtig maar ook eigen schuld

[gedaagde] jegens O'Cliance aansprakelijk is voor de schade die kon ontstaan doordat [gedaagde] niet heeft voldaan aan de opdracht een adequate beveiliging aan te leggen, maar dat O'Cliance medeschuldig is aan het ontstaan van het lek in de beveiliging. De rechtbank zal de schade dan ook over beide partijen verdelen.

MAATREGELEN

maatregelen

- implementeren standaarden (normen en procedures)
- contracteren
- verzekeren

Baseline Informatiebeveiliging Rijksdienst

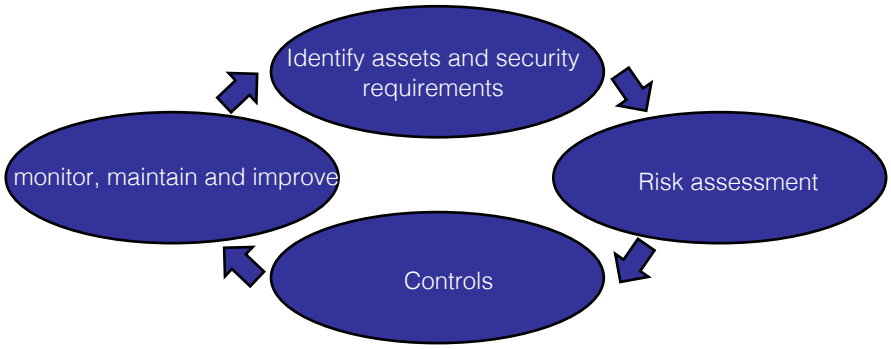
BIR2017
Baseline Informatiebeveiliging Rijksdienst

- Helpt met nemen van beslissingen over beveiliging
- Gebaseerd op ISO 27.001/27.002

ISO 27.001

de meest gebruikte generiek standaard voor information security

- Information security management system
- Confidentiality, Integrity, Availability



ISO 27.002: controls

13.1.3 Segregation in networks

DigiNotar Internet Trust Services

Control

Groups of information services, users and information systems should be segregated on networks.

Implementation guidance

One method of managing the security of large networks is to divide them into separate network domains. The domains can be chosen based on trust levels (e.g. public access domain, desktop domain, server

7.1.1 Screening

Control

Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:

a) terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;

b) log-off from applications or network services when no longer needed;

ISO 27.032

guidelines to cyber security

- aanvulling op ISO 27.001
- guidelines voor implementatie
- governance guidelines
- controls:
  - secure coding;
  - network monitoring;
  - server level controls
  - …

} focus op hacking, malware, spyware

standaarden

voordelen expliciet toepassen standaarden....

- helpt om over risico's en beveiligingsmaartregelen na te denken,
- is signaal naar andere partijen, soms verplicht (leveranciers, afnemers, toezichthouders),
- geeft houvast voor organisatie
- ....

maar oppassen dat ...

- een standaard geen doel op zich wordt
- het geen papieren tijger wordt
- ....

contracteren met ICT leverancier

helderheid creëren, met afdwingbare condities

- Gebruik normen/standaarden
- Meten/audit
- Risico analyse / kritische processen
- Welke schade is verhaalbaar, wanneer overmacht?
- Procedure afhandeling incidenten
- Continuïteit / uitwijk en back-upprocedures

naast afdwingbare condities, praktische afspraken

- Operationele afspraken
- Overlegstructuren
- Meldingsprocedures

Nederland NLDigital

Artikel 7 Beveiliging

Indien leverancier op grond van de overeenkomst gehouden is tot het voorzien in een vorm van informatiebeveiliging, zal die beveiliging beantwoorden aan de tussen partijen schriftelijk overeengekomen specificaties betreffende beveiliging. Leverancier staat er niet voor in dat de informatiebeveiliging onder alle omstandigheden doeltreffend is. Indien een uitdrukkelijk omschreven wijze van beveiliging in de overeenkomst ontbreekt, zal de beveiliging voldoen aan een niveau dat, gelet op de stand van de techniek, de uitvoeringskosten, de aan leverancier bekende aard, omvang en de context van de te beveiligen informatie, de doeleinden en het normale gebruik van zijn producten en diensten en de waarschijnlijkheid en ernst van voorzienbare risico's niet onredelijk is.

Schade (art. 16)

- beperkt: directe schade beperkt tot prijs overeenkomst (1 jaar)
- uitgesloten: o.m. indirecte schade, vervolgschade, gederfde winst, gemiste besparingen, bedrijfsstagnatie, aanspraken afnemers van klant, verminking, vernietiging of verlies van documenten.

Overmacht (art. 17)

- niet gehouden nakomen bij storing van internet, computernetwerk- of telecommunicatie-faciliteiten

ARBIT

1.9. Gebrek: iedere storing en/of ander mankement als gevolg waarvan de Prestatie niet geschikt is voor het Overeengekomen gebruik.

1.23. Overeengekomen gebruik: het door Opdrachtgever beoogde gebruik van de Prestatie zoals dat ten tijde van het sluiten van de Overeenkomst op grond van het Bestek en/ of op basis van de in artikel 4 bedoelde informatie, voor Wederpartij kenbaar is of redelijkerwijs moet zijn, een en ander voor zover dat gebruik in de Overeenkomst niet uitdrukkelijk is uitgesloten of beperkt.

26.2. De in artikel 26.1 bedoelde aansprakelijkheid voor persoons- en zaakschade en daaruit voortvloeiende schade, is beperkt tot een bedrag van EURO 1.250.000,- per gebeurtenis. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.

26.3. De in artikel 26.1 bedoelde aansprakelijkheid voor schade anders dan die bedoeld in artikel 26.2 is beperkt tot een bedrag van ten hoogste vier maal de hoogte van de Vergoeding per gebeurtenis. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.

Geen uitsluiting indirect schade, maar wel beperking andere schade dan persoons- en zaakschade tot vier maal vergoeding

contact / contract met gebruikers

afnemers: een helpende hand

- waarschuwen
- voorlichten
- verantwoordelijkheden (B2B)

werknemers: opleiding

- awareness
- training
- geheimhoudingsplicht

cyberverzekering nog in ontwikkeling

- cyberverzekering meer toegesneden op cyberschade
- nog weinig historische data, waardoor verscheidenheid aan verzekeringen (sommen en voorwaarden).
- toekomst: voorwaarden met juiste prikkels, klanten met de polissen die bij hen passen


Markt voor cyberverzekeringen heeft zetje nodig

Schade 2133 0

De cyberrisico's groeien, maar de verzekeringsmarkt kan vaak nog geen passende oplossingen bieden, constateert Swiss Re in een recente studie.

am: 1 maart 2017

Markt voor cyberverzekeringen verdubbeld

De markt voor cyberverzekeringen is in de afgelopen twee jaar meer dan verdubbeld. Het premie-inkomen is van maximaal tien miljoen euro in 2015 gegroeid naar minimaal twintig miljoen in 2017. Dat blijkt uit een enquête die het Centrum voor

Allianz AIG HISCOX AON

ter overdenking

- gebruik een standaard, maar verstandig
- gedreven door risico's
- beleggen verantwoordelijkheden
- oefenen en doordenken
- eenvoudige en begrijpelijke procedures
- ....

Dank u