



Cyber en Data Risks by Hiscox

Yasin Chalabi
28 November 2017, Vught

EVEN VOORSTELLEN

YASIN CHALABI

- Werkzaam bij Hiscox Benelux sinds 2006
- Manager zakelijke verzekeringen waaronder PI & Cyber
- Pionier in Cyber verzekeren
- Groot voorstander van innovatie en diensten aanbieden
- 16 jaar actief in verzekeringswereld



DOEL PRESENTATIE

WIJ WILLEN GRAAG...

- Kennis delen rondom Cyber en Data risico's en de actualiteiten
- Een toelichting geven op de verzekeringsmogelijkheden van Hiscox bij Surebusiness
- Vragen ?

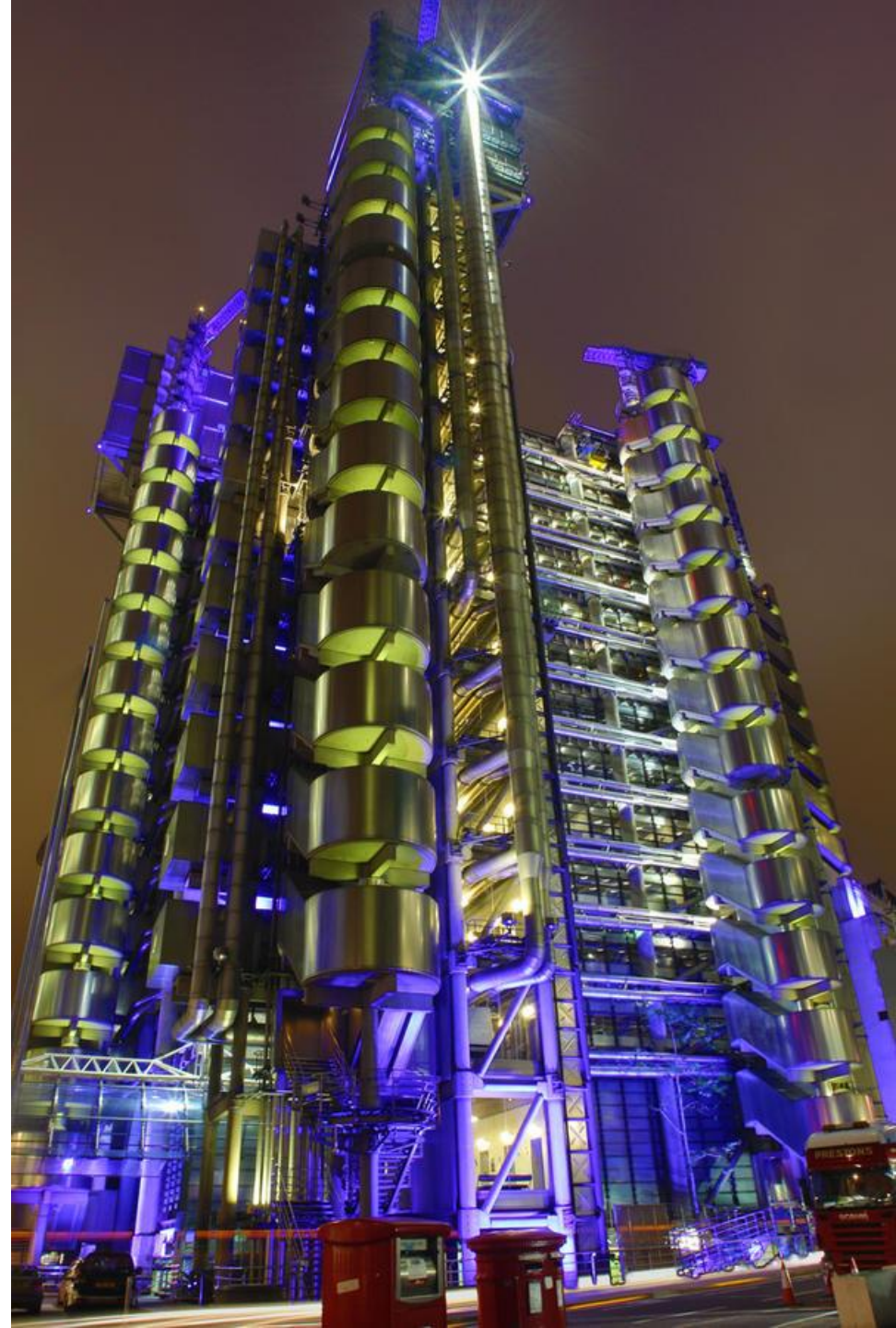


OVER HISCOX

VERZEKEREN

- Sinds 1901
- Internationale nicheverzekeraar, beursgenoteerd*
- **Professional Insurance**
gespecialiseerd in het verzekeren van beroepsaansprakelijkheid, Cyber & Data risico's / online risico's en Bestuurdersaansprakelijkheid
- **Art & Private Client**
gespecialiseerd in het verzekeren van kunst, kostbaarheden en vermogende particulieren
- Snelle en correcte claims afhandeling

* *London Stock Exchange*



PRODUCTEN VERZEKERINGEN

VERZEKERINGEN

CYBER & DATA
RISKS

BEROEPS-
AANSPRAKELIJKHEID

BEDRIJFS-
AANSPRAKELIJK-
HEID

BESTUURDERS &
COMMISSARISSEN
AANSPRAKELIJKHEID

PRE PRICED
PROPOSAL

CYBER EN DATA RISKS

WAT IS EEN INBREUK OP DATA?

Wanneer door een niet bevoegd persoon gevoelige, beschermde of vertrouwelijke gegevens, gekopieerd, overgedragen, gestolen of gebruikt worden.

Welke gegevens:

- financiële informatie (creditcard/bankgegevens)
- medische informatie
- toegangsgegevens (inlog/ wachtwoorden)
- handelsgeheimen of
- intellectuele eigendommen

Of gegevens:

- over raciale/etnische afkomst, politieke opvattingen, godsdienstige of levensbeschouwelijke overtuiging
- die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene (gokverslaving, werk of relatieproblemen);
- gegevens die kunnen worden misbruikt voor (identiteits)fraude (kopie paspoort/rijbewijs) (burgerservicenummer).



DE TRENDS VAN 2017

1. **Beroepscriminelen** voeren langdurige, hoogwaardige en geavanceerde operaties uit en vormen de grootste dreiging en richten de meeste schade aan.
2. **Spionage**; digitale economische spionage door buitenlandse inlichtingendiensten zet de concurrentiepositie van Nederland onder druk en worden gebruikt om democratische processen te beïnvloeden
3. **Internet of Things**; De kwetsbaarheid van het internet of things heeft tot versturende aanvallen geleid die de noodzaak tot het versterken van de digitale weerbaarheid onderschrijven
4. **Ransomware**; is dagelijkse kost en is nog geavanceerder geworden (WannaCry! / Petya)



CYBER EN DATA RISKS



NEDERLAND

**Aantal cyberpolissen stijgt hard
Vraag naar verzekering tegen
digitale gijzeling neemt na
aanval versneld toe**

Bron: AM , 16-5-2017



‘ANWB waarschuwt klanten webwinkel voor datalek’

Bron: Security.NL , 03-10-2017



**Werknemer is grootste veroorzaker datalek.
Bedrijfscultuur beste beveiliging tegen datalek.**

Bron: Onderzoek Willis Tower Watson, maart 2017



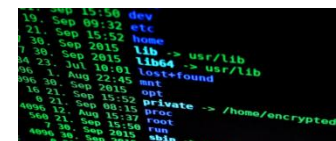
Datalekken doen aandelenkoers kelderen

Bij 65 onderzochte bedrijven verdampte ruim 52,4 mld aan beurswaarde door datalekken.

Bron: FD 20-09-2017



**Cyberaanvallen schadelijk voor omzet MKB'ers. Onnodig risico door verouderde
software, zwakker firewalls en DDoS-aanvallen** *Bron: Nationaal Ondernemers Onderzoek 2016*



INTERNET OF THINGS



*Vehicle, asset, person & pet
monitoring & controlling*



Agriculture automation



Energy consumption



*Security &
surveillance*



Building management



*Embedded
Mobile*

Internet of things

Everyday things get connected for smarter tomorrow



for smarter tomorrow



*M2M & wireless
sensor network*



Everyday things



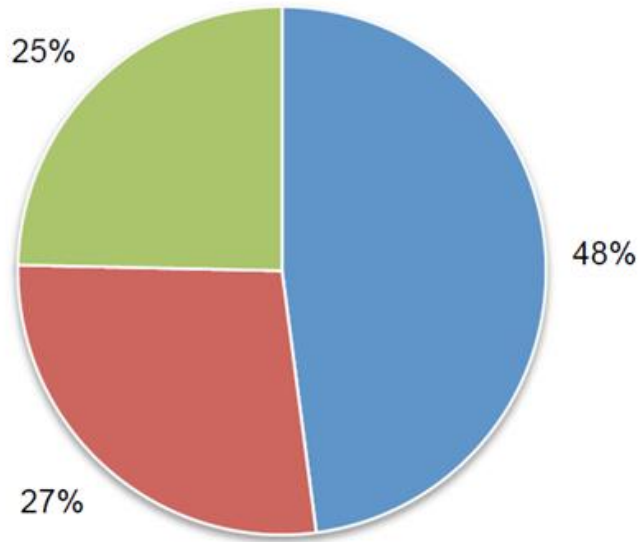
Smart homes & cities



Telemedicine & healthcare

CYBER EN DATA RISKS

3 factoren die zorgen voor een datalek (wereldwijd)



- Criminaliteit
- Systeemfout
- Menselijke fout



100% VEILIG BESTAAT NIET

BEROEPS CRIMINALITEIT



Triodos  **Bank**

Geachte klant,

We kregen veel mislukte inlogpogingen van uw online account.
Voor uw bescherming hebben we uw account geblokkeerd.

Om uw online toegang te herstellen, klikt u op: [Inloggen Internet Bankieren](#) en blijven het verificatieproces.

Gelieve niet direct antwoorden op deze e-mail bericht automatisch gegenereerd.

Met vriendelijke groet,
Team Online Banking

RANSOMWARE



Polite. ATTENTIE! Uw web...

POLITIE
Korps Landelijke Politiediensten
Openbaar Ministerie
CYBERCRIME POLITIE NEDERLAND

IP: Land: Netherlands
Regio: City:

ATTENTIE! Uw webbrowser wordt geblokkeerd om veiligheidsoverwegingen wegens de hieronder aangegeven redenen.
Alle activiteiten van deze computer zijn opgenomen.
Al uw bestanden worden versleuteld.

U wordt beschuldigd van het gebruik/opslaan en/of verspreiden van de pornografische productie wier inhoud wettelijk verboden is (kinderporno/zodifilie/verkrachting etc.). Hiervoor heeft u de voorwaarden van de internationale Declaratie over de bestrijding van kinderporno geschonden en daardoor wordt u beschuldigd van het plegen van een strafbaar feit waarvan artikel 161 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden van toepassing is.

De misdrijven van deze aard worden volgens artikel 161 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden gestraft met de vrijheidsontneming voor de duur van 5 tot 11 jaar.

Daarnaast wordt u ook verdacht van het schenden van de "Wet inzake het auteursrecht en naburige rechten" (het illegale downloaden van muziek, video, het gebruik van ongecertificeerde software) en van het gebruik maken van en/of verspreiden van de content waarop het auteursrecht rust. Daardoor wordt u verdacht van schenden van artikel 148 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden.

pincode: Paysafecard U kash

Waarde: 100

Waar kan ik een geldvoucher PaySafeCard aanschaffen?

PaySafeCards zijn vast en zeker dichtbij verkrijgbaar, in Nederland bijvoorbeeld bij veel tankstations (benzinestations), kiosken, supermarkten en sigarenwinkels. Overzicht verkoppertners: Trekpleister, HEMA, VIDCOLAND, T-Mobile, SuperCoop, TAMOIL, Postkantoor (www.Post.nl), RijkShop (www.RijkShop.nl), Gulf, Totaal Gemak, Primera, Coop Compact, Coop, Argos, AKO, Nanesen, Free Record Shop, Total, Texaco, Spar, Shell, Q8, Esso, BP, Axa.

NARVESEN

Cryptolocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount** in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/9/2013
4:25 PM

Time left
95 : 56 : 35

Next >>

CYBER EN DATA RISKS

Geen organisatie is immuun voor zowel interne als externe bedreigingen

Door de staat gesteund

Een groep in dienst van een staatsinstelling.

- Chinese staatshackers.
- Russische staatshackers.
- Elektronisch leger van Syrië.

Scriptkiddies

Personen of groepen meestal met beperkte kennis die op eigen initiatief handelen en niet vallen onder een andere dreigingscategorie.

- Een jongere die 'voor de grap' het netwerk van de school doet crashen.
- Personen die websites verminken om indruk op iemand te maken (niet vanuit politieke motieven).
- Groepen die met de botte bij geprefabriceerde malware of botnets inzetten voor malafide doeleinden.

Hacktivist

Een persoon of groep die aanvallen uitvoert om ergens de aandacht op te vestigen of om te verhinderen dat anderen zich inzetten voor zaken als bijvoorbeeld de vrijheid van meningsuiting.

- Anonymous.
- Lulzsec.
- WikiLeaks.

Georganiseerde misdaad

Criminele groepen die betrokken zijn bij illegale activiteiten om geld af te persen of worden ingehuurd om een aanval uit te voeren.

- Producenten van ransomware.
- Personen die gegevens stelen om ze op de zwarte markt te verkopen.

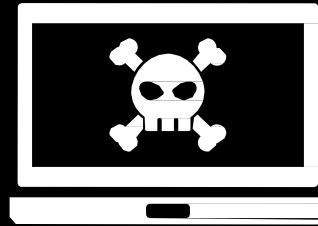
Insiders

Werknemers of andere bevoorrechte gebruikers aangesloten bij een organisatie.

- Werknemers.

Cyberterrorist

Iemand die aanvallen uitvoert om angst of paniek te zaaien. De persoon wordt gedreven door ideologische of politieke motieven of maakt deel uit van een bekende terreurgroep.



WETGEVING EN CYBER

CYBER EN DATA RISKS

MELDPLICHT DATALEKKEN

- Ingevoerd per 1-1-2016
- Voor commerciële instellingen en (semi-) overheid
- Binnen 72 uur melden bij falen van technische en organisatorische beveiliging met kans op verlies of onrechtmatige verwerking van persoonsgegevens
- Aard en vermoedelijke omvang van het datalek
- Inspanningen om de schade te herstellen
- Raadgevingen aan publiek en klanten
- Boete van bijvoorbeeld maximaal € 820.000,- of 10% van de jaaromzet



AUTORITEIT
PERSOONSgegevens

EU PRIVACY VERORDENING

KERNPUNTEN PER 25 MEI 2018

- Eén set regels binnen de EU
- Recht op vergetelheid
- Functionaris gegevensbescherming , overheid en publieke organisaties verplicht (ook zorg en Onderwijsinstellingen) maar ook als men op grote schaal bijzondere persoonsgegevens verwerkt
- Datalek, onverwijld binnen 72 uur melden
- Ook niet EU-ondernemingen
- One-stop shop
- Sancties oplopend tot EUR 20 mio of 4% (wereldwijde) jaaromzet.



GDPR

EU General Data Protection Regulation



AUTORITEIT
PERSOONSGEGEVENS

DE VERZEKERING = ONTZORGING

CYBER EN DATA RISKS



AANSPRAKELIJKHEID
(third party)

EIGEN SCHADE
(first party)

CYBER EN DATA RISKS

EIGEN SCHADE (first party)

- **Data inbreuk**
 - Forensisch ICT onderzoek
 - Kosten externe deskundigen melden inbreuk (juridisch, communicatie betrokkenen, meldplicht, callcenter etc.)
 - Kosten kredietbewaking betrokkenen
 - Kosten crisismangement en PR
- **Bedrijfsschade - business interruption**
Omzetsderving veroorzaakt door een hack
- **Hacker schade**
Kosten herstel website, intranet, netwerk, computersysteem, programma's of data
- **Cyber afpersing o.a. Ransomware**
Kosten en vergoedingen van onderzoek, assistentie en eventueel betaald losgeld
- **Verlies van geld op rekening**
- **Extra belkosten bij hacking van telefoonsysteem**



CYBER EN DATA RISKS

AANSPRAKELIJKHEID (third party)

➤ Privacy aansprakelijkheid

De gevolgen van gestolen privacygevoelige gegevens

- Kosten van onderzoek
- Claims van individuele personen
- Schending geheimhoudingsplicht
- Boetes opgelegd door toezichthouders

➤ Cyber aansprakelijkheid

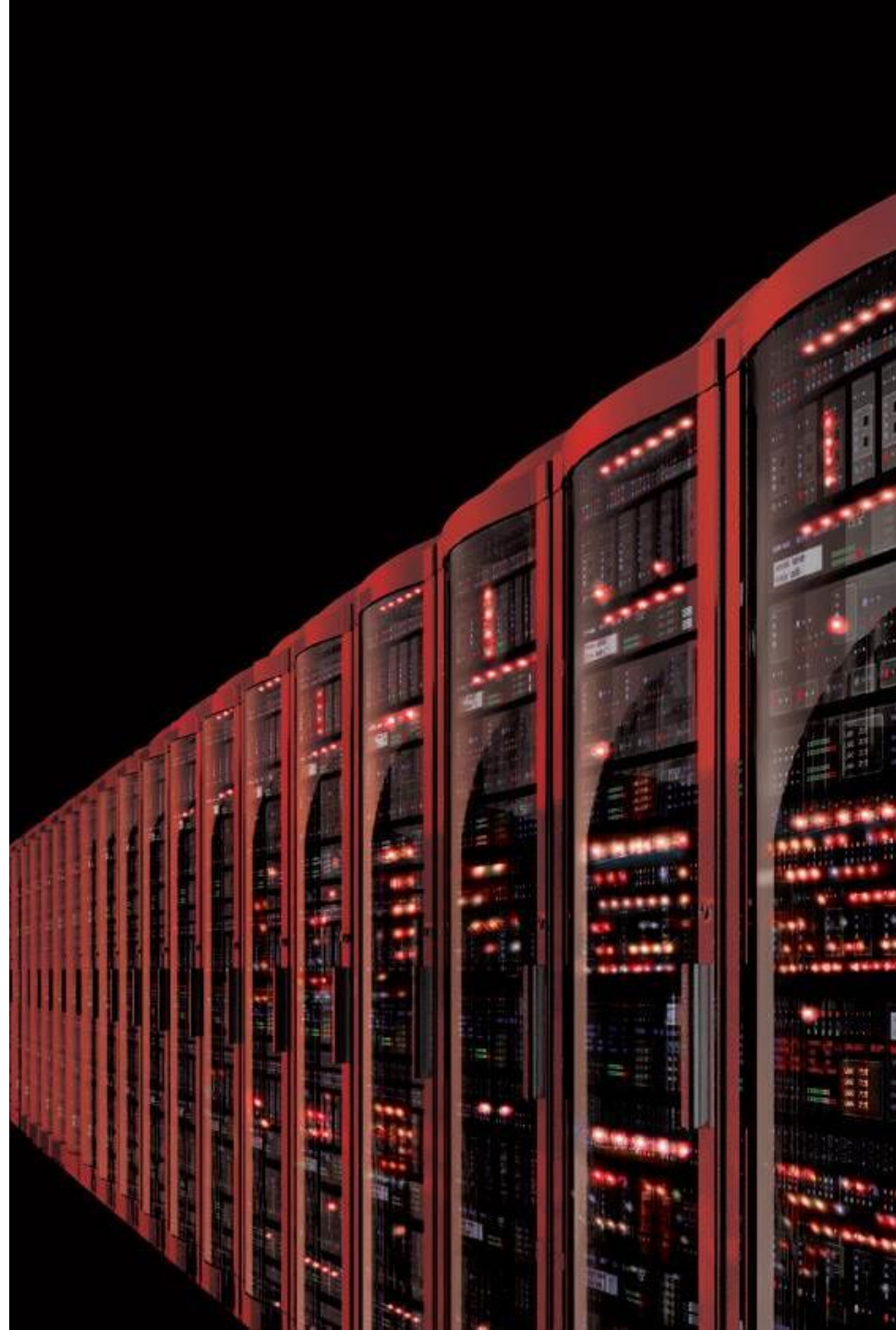
Schade die ontstaat als een website of e-mail onbedoeld een auteursrecht schendt, laster verspreidt of een virus bevat.



CYBER EN DATA RISKS

BEDRIJFSSCHADE

- Als de internet of bedrijfsactiviteiten van de onderneming stil is komen te liggen door een cyber incident.
- Deze schade wordt gecalculeerd naar het verlies van winst over een periode van maximaal 12 maanden.
- Voorraadbederf (***nieuwe dekking***) waarbij Hiscox de verzekerde schadeloos zal stellen voor verlies dat wordt veroorzaakt als gevolg van onbevoegde toegang, computervirus of een denial of service aanval (DoS) op het netwerk van verzekerde.
- Ook aan het internet gekoppelde MACHINES die stilvallen door een gedekt cyberevent valt onder de dekking.



CYBER EN DATA RISKS

IN DE PRAKTIJK (SCHADE NL)

- Groot **administratiekantoor** kreeg bij opstarten van de werkstations een foutmelding dat de bestanden op de server niet meer benaderbaar zouden zijn. Na inschakelen van het Hiscox Incident Response bleek ransomware het systeem en de back-up te hebben versleuteld. Deloitte Cyber heeft bij 50 uur nodig gehad voor forensisch onderzoek en herstel van data van systemen. Daarna melding AP en inschakelen advocaten ter begeleiding.
- **Brancheorganisatie** wordt door middel van een linkedin bericht op de hoogte gesteld van een datalek waarbij veel data is gecompriemeerd zoals bankgegevens, facturen , paspoorten. Klant heeft het Hiscox incident response team ingeschakeld en alle dienstverlening is ingeschakeld om de schade te begeleiden.
- **Transportbedrijf** – planning volledig afhankelijk van ICT , ICT ligt plat en men kan geen nieuwe opdrachten aannemen en men weet niet meer waar de vrachtauto's wat naar toe moet sturen.
- **Koelhuis**, voorraadbederf door hack klimaatsysteem

XOOSIH



PREVENTIE EN BEPERKING

TECHNISCH ADVIES

- Update altijd alle software;
- Neem een goede IT partner in de hand;
- Versleutel gevoelige data (encryptie);
- Maak back ups (los van het netwerk) en test deze;
- Breng in kaart van welke systemen de organisatie afhankelijk is;
- Laat de infrastructuur testen!



PREVENTIE EN BEPERKING



Programma	Vulnerability Assessment*	Security Scan*	Check Bewerkersovereenk omst	Disaster recovery maturity scan
Aangeboden door	ESET	RedSocks Security	ICTRecht	KPN
Doelgroep	Verzekerden tot een omzet van € 1 miljoen OF bedrijven met een eenvoudige IT infrastructuur (enkele devices)	Verzekerden met een omzet van € 1 miljoen OF bedrijven met een complexe IT infrastructuur	Alle verzekerden	Verzekerden vanaf een omzet van € 10 miljoen
Verplicht?	Nee	Nee	Nee	Nee
Vorm	Online scan	Online scan op afstand	Beoordeling op afstand	Op locatie
Rapportage Kenmerken	Online in een dashboard Een scan van de online verbindingen op kwetsbaarheden	In een persoonlijk gesprek Monitoring en beoordeling van al het uitgaande dataverkeer op bijzonderheden	Bespreking van de bevindingen bij ICT recht op kantoor Juridische beoordeling van de bewerkersovereenkomst.	Rapport Een scan van de disaster recovery maatregelen dmv een 3 fase aanpak.
Kosten	€ 50	Gratis	Gratis	Gratis
Meer informatie	Brochure	Brochure	N.V.T.	Brochure

* Indien in het verleden al eerder een scan is afgenomen geldt deze aanbieding niet.

GEHACKT EN WAT NU?!

DE 6 STAPPEN BIJ EEN HACK

- Schiet niet in de stress;
- Zet de computer NIET uit;
- Koppel de computer los van het netwerk;
- Blijf van de computer af;
- Schrijf op wat er gebeurd is;
- SCHAKEL HULP in door te bellen met het Incident Response team van Hiscox (24/7).



CYBER EN DATA RISKS

INCIDENT ROADMAP

ALS ONDERDEEL VAN DE HISCOX CYBER EN DATA RISK VERZEKERING, HEBBEN WE SAMEN MET ONZE PARTNERS EEN INCIDENT ROADMAP OPGESTELD.

HET INCIDENT ROADMAP PLAN IS ONTWIKKELD OM U TE ONDERSTEUNEN MET:

ONMIDDELIJK ACTIE ONDERNEMEN, IN HET GEVAL VAN SCHADE AAN UW DATABASE OF WEBSITE ALS GEVOLG VAN EEN HACK



CYBER EN DATA RISKS

INCIDENT RESPONSE PLAN

1

ACTIE VERZEKERDE:

Informeer direct uw adviseur en/of Hiscox .
24 uurs Hiscox Incident Response
alarmnummer: TEL: 0031 20 5170700



AANLEIDING:

Een incident zoals een hack of een datalek
heeft plaatsgevonden!

2

ONDERSTEUNING DOOR HISCOX:

Hiscox schakelt forensisch specialisten
in om binnen 72 uur te bepalen wat de
omvang en de oorzaak van het incident is.

Deloitte.



3

ACTIE VERZEKERDE:

De Autoriteit persoonsgegevens en/of
mogelijk de betrokkenen worden
geinformeerd. Hiscox incident response
team adviseert u.

Kennedy Van der Laan



6

ACTIE VERZEKERDE EN HISCOX:

Eventuele evaluatie en nabespreking tussen
Hiscox, adviseur en klant!

5

ACTIE VERZEKERDE MET ONDERSTEUNING VAN HISCOX:

Het herstellen van schade aan uw systemen en/of
netwerk door specialisten.

4

ONDERSTEUNING DOOR HISCOX

Aansprakelijkheden en eigen schade zijn een grote
zorg. Hiscox incident response team staat klaar,
om u bij te staan.

Tevens bijstand van een PR bureau voor advies bij
communicatie en hulp ter voorkoming van
reputatieschade indien nodig.

SMART & ABLE

CYBER EN DATA RISKS



DE VOORWAARDEN - CDRH 2017

- First response/dienst vergoeding voor (eigen) of zelf ingeschakelde IT specialisten;
- Vergoeding tot € 15.000,00 per aanspraak;
- Crisisconsulent, als zijn aanstelling door de eerste hulp consulent of de verzekeraar nodig wordt geacht in het kader van een daadwerkelijke of beweerde inbreuk op de bescherming van persoonsgegevens of bedrijfsgegevens, een beveiligingsfout of een systeem falen;
- Eerste hulp consulent voor het verlenen van juridische diensten;
- Op deze Eigen Service (dienst) dekking (48 uur) is geen eigen risico van toepassing.

Cyber en Data Risks by Hiscox
Polisvoorwaarden 2017



CYBER EN DATA RISKS

LOGISTIEK BIJ AANVRAGEN

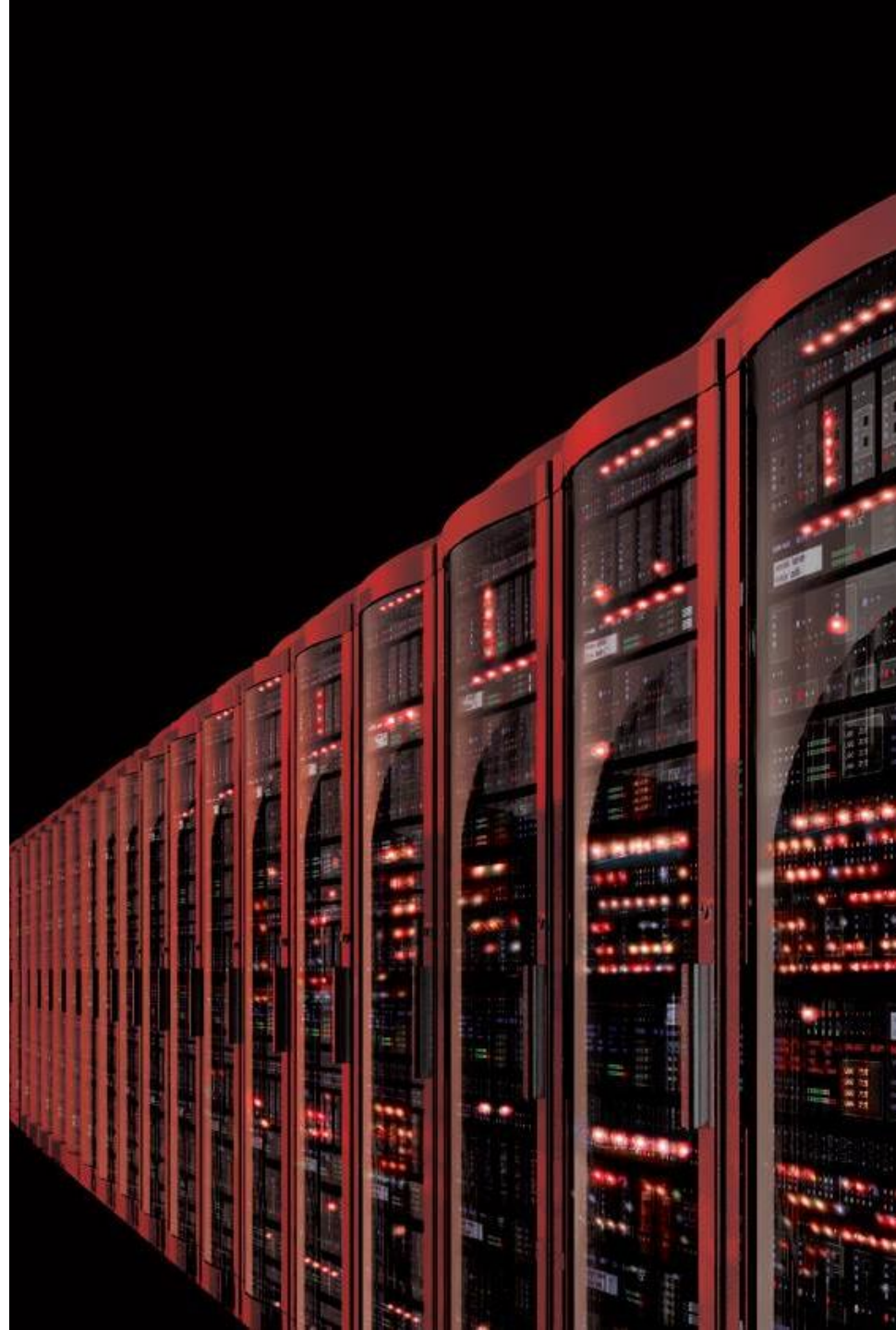
- Tot EUR 10.000.000 omzet / exploitatie en binnen de verklaringen heeft Sure Business een eigen volmacht.
- Daarbuiten behandelen wij graag uw maatwerkaanvragen via het maatwerkformulier Cyber en Data Risks by Hiscox.



ACCEPTATIE RICHTLIJN

TOT EUR 10.000.000 OMZET

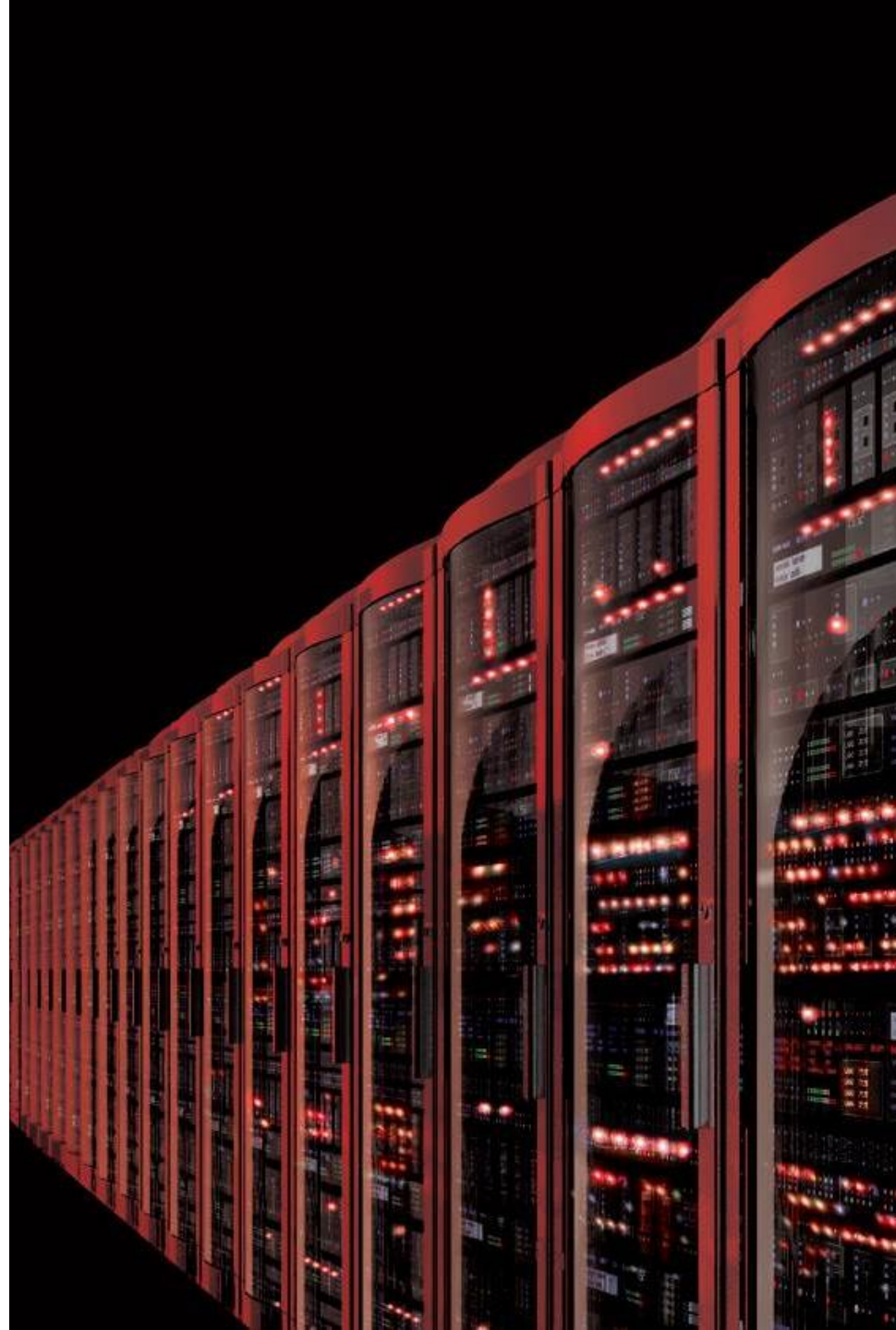
- Klant dient het volgende te kunnen verklaren :
- er geen omzet wordt gegenereerd direct of indirect in de Verenigde Staten en/of Canada;
- u niet bekend bent met enige (lopende) aanspraak of omstandigheid die leidt of kan leiden tot een vordering van een derde jegens verzekeringnemer/verzekerde tot vergoeding van schade en/of er geen feiten en/of omstandigheden te melden zijn ten aanzien van zowel het te verzekeren risico als ten aanzien van verzekeringnemer/verzekerde, die voor het beoordelen van deze verzekeringsaanvraag van belang zouden kunnen zijn;
- er nooit een officiële klacht tegen verzekeringnemer/verzekerde is ingediend, met betrekking tot de wijze waarmee verzekeringnemer/verzekerde met persoonsgegevens is omgegaan;



ACCEPTATIE RICHTLIJN

VERVOLG (10 MIO)

- tevens verklaart u dat verzekeringnemer/verzekerde nooit onderwerp is geweest van een onderzoek in verband met persoonsgegevens, inclusief maar niet beperkt tot betaalkaartgegevens, noch van uw activiteiten met betrekking tot privacy;
- verzekeringnemer/verzekerde van niet meer dan 100.000 betaalkaarten(creditcards) gegevens heeft en/of heeft opgeslagen in haar eigen netwerk en/of (computer)systemen of bij derden.
- verzekeringnemer/verzekerde een antivirus programma van een gerenommeerde leverancier (b.v. Eset, AVG, McAfee, Norton) heeft geïnstalleerd en geactiveerd op haar (computer)systemen, inclusief Apple computers.



ACCEPTATIE RICHTLIJN



PREMIE:

Eigen risico's :

Omzet categorie tot € 10.000.000,00:

Algemeen : € 2.000,-- per aanspraak/schade

Wachtermijn bedrijfsschade : 8 uur

Verzekerd bedrag en premie

Verzekerd bedrag per aanspraak en maximaal per verzekeringsjaar	Jaarlijkse omzet			
	T/M € 1 mln.	Tussen € 1 mln en € 2,5 mln	Tussen € 2,5 mln en € 5 mln.	Tussen € 5 mln en € 10 mln
€ 250.000	€ 690	€ 850	€ 1.125	€ 1.750
€ 500.000	€ 1.100	€ 1.175	€ 1.425	€ 2.050
€ 1.000.000	€ 1.450	€ 1.800	€ 2.100	€ 2.750
€ 2.000.000	€ 2.200	€ 2.550	€ 3.150	€ 3.750

VIDEOS

HACKERS WETEN VEEL OVER ONS!

[HTTPS://WWW.YOUTUBE.COM/WATCH?V=F7PYHN9IC9I](https://www.youtube.com/watch?v=F7PYHN9IC9I)

[HTTPS://WWW.YOUTUBE.COM/WATCH?V=1REVGXSBIRG](https://www.youtube.com/watch?v=1REVGXSBIRG)





BEDANKT VOOR DE AANDACHT!

