HISCOX

Cyberverzekering
Vragenlijst voor onderschrijving

Identificatie

Bedrijfsnaam en juridische vorm:

Adres:

Website(s):

KBO-nummer:

Uw activiteiten:

Omzet

Totaal gerealiseerde omzet:

Vorig boekjaar	Lopend boekjaar / schatting	Volgend boekjaar
€	€	€

Gemiddelde brutowinstmarge over de afgelopen 3 jaar: %

Hoeveel % van deze omzet werd via online transacties gerealiseerd? %

Aantal werknemers:

Uw gegevens

Aantal personen waarvan u waarschijnlijk gevoelige gegevens verzamelt en/of bewaart*:

*Gevoelige gegevens: 1. Identiteitskaartnummer, rijbewijs of paspoort. 2. Bankgegevens (creditcard, etc.) 3. Gegevens met betrekking tot ras, etniciteit, seksuele geaardheid, gezondheid, godsdienstige of levensbeschouwelijke overtuigingen, politieke denkbeelden of lidmaatschap van vakbonden.

Aantal / Type			
< 20.000	☐	**500.001 - 1.000.000**	☐
20.000 - 100.000	☐	**1.000.001 - 6.000.000**	☐
100.001 - 250.000	☐	**> 6.000.000**	☐
250.001 - 500.000	☐		

Vragen

Hoeveel % van uw jaaromzet wordt gegenereerd via export naar de VS en/of Canada?	%
Hebt u een vestiging buiten de Europese Unie? In geval van een of meer vestigingen buiten de EU, vermeld het (de) betreffende land(en) en hun aandeel in de totale jaaromzet in %: …… …… ……	Ja ☐ Nee ☐
Gebruiken alle vestigingen van de groep hetzelfde informatiesysteem? En hebben zij hetzelfde IT-beveiligingsniveau als de vestiging die de polis afsluit?	Ja ☐ Nee ☐ Ja ☐ Nee ☐
Indien er andere vestigingen zijn, zijn hun netwerken van elkaar afgeschermd? Zo ja, hoe? …….. ……..	Ja ☐ Nee ☐
Bevestigt u dat u geen besturingssystemen gebruikt die niet meer door de	Ja ☐ Nee ☐

producent worden geüpdatet (bijvoorbeeld Windows XP en Windows 7)? **Zo niet**, welk besturingssysteem gebruikt u? Licht toe hoe het is afgeschermd van de rest van uw netwerk en van het internet. ……	
Installeert u updates voor de software en systemen die u gebruikt (inclusief antivirussoftware en firewalls) binnen 30 dagen nadat ze door de ontwikkelaar worden uitgebracht?	Ja ☐ Nee ☐
Kent u beheerdersrechten alleen toe aan gebruikers die ze nodig hebben? **en** Hebben alle systeembeheerders twee accounts: één voor hun systeembeheertaken en één voor normaal gebruik?	Ja ☐ Nee ☐ Ja ☐ Nee ☐
Beperkt u de toegang van uw medewerkers tot uw informatiesysteem en tot gegevens op basis van wat zij nodig hebben om hun werk te doen? Wordt hun toegang systematisch opgeheven wanneer zij uw bedrijf verlaten?	Ja ☐ Nee ☐ Ja ☐ Nee ☐
Maakt u gebruik van tweestapsverificatie* (2FA) om toegang op afstand en/of toegang tot webapplicaties (bijvoorbeeld Gsuite of Office 365) te beheren? * Naast een gebruikersnaam en wachtwoord wordt een authenticatiecode aangemaakt die alleen de gebruiker op zijn telefoon, per e-mail of via een specifieke authenticatietoepassing kan ontvangen.	Ja ☐ Nee ☐
Zijn de gegevens die u bewaart versleuteld wanneer ze zich bevinden: - op uw netwerk? - op mobiele opslagapparaten of mobiele terminals? - op servers die door anderen in opdracht van u worden beheerd?	Ja ☐ Nee ☐
Als u onder Uw gegevens een aantal van meer dan 100.000 hebt aangevinkt Zijn gevoelige gegevens* (zie definitie op blz. 1) die op uw netwerk, opslagapparaten, mobiele apparaten (inclusief laptops en smartphones), servers en andere terminals staan versleuteld met een encryptie van minstens 256 bits?	Ja ☐ Nee ☐
Als u onder Uw gegevens een aantal van meer dan 100.000 hebt aangevinkt Krijgen alle medewerkers die toegang hebben tot gevoelige gegevens die u bewaart of bewerkt, een training en/of minstens eenmaal per jaar een opfriscursus over de vertrouwelijke behandeling van gegevens en cyberrisico's?	Ja ☐ Nee ☐
Als u kaartbetalingen ontvangt, voldoet u aan de norm PCI DSS 3.2 of gebruikt u een aanbieder van betalingsdiensten die hieraan voldoet? Als u het niet weet, vermeld dan de naam van de aanbieder: …… ……	Ja ☐ Nee ☐
Hanteert u een beleid voor het beheer van persoonsgegevens en IT-veiligheid dat voor alle diensten en vestigingen van de onderneming geldt? Als u gecertificeerd bent (bijvoorbeeld volgens ISO 27001), vermeld dan om welke certificering het gaat :…… ……	Ja ☐ Nee ☐
Als u hiertoe verplicht bent, hebt u een interne of externe functionaris voor gegevensbescherming aangewezen?	Ja ☐ Nee ☐
Worden van uw kritieke gegevens en systemen minstens wekelijkse back-ups gemaakt? Deze back-up bestaat uit: (a) ☐ minstens één fysieke back-up die op een bepaald moment van uw systemen wordt losgekoppeld en/of (b) ☐ een back-upoplossing die op een van de volgende clouddiensten is gebaseerd:	Ja ☐ Nee ☐

Microsoft OneDrive, Google Drive, iCloud of Azure Recovery Services Vault. *Gegevens en systemen worden als kritiek beschouwd wanneer u inkomsten kunt verliezen als deze gegevens en systemen meer dan 24 uur onbeschikbaar of offline zijn. **Zo niet:** Welke oplossing gebruikt u om back-ups te maken?..... En hoe vaak worden back-ups gemaakt? ……	
Bestaat er een plan voor herstel en voortzetting van activiteiten (Business Continuity Plan) in geval van een incident in uw informatiesystemen, dat regelmatig wordt getest? Zo ja, hoe vaak wordt dit plan getest? Zo ja, zijn scenario's van ransomewareaanvallen ook in dit plan opgenomen?	Ja ☐ Nee ☐ Ja ☐ Nee ☐

Aanvullende vragen

Onderbreking van uw activiteiten als gevolg van een cyberincident bij een van uw onderaannemers

Indien uw kritieke gegevens en systemen* door externe aanbieders worden gehost, gaat het om een of meer van de volgende aanbieders? AWS, Google, IBM, Alibaba, Salesforce, Microsoft, Oracle, of OVH. **Zo niet,** vermeld dan welke aanbieders uw kritieke gegevens en systemen hosten:……	Ja ☐ Nee ☐
Indien uw kritieke gegevens en systemen door externe aanbieders worden gehost, worden deze gehost in minstens twee datacenters die op minstens 350 km van elkaar liggen?	Ja ☐ Nee ☐
Maakt u gebruik van externe aanbieders van IT-diensten voor andere doelen dan hosting? Zo ja, welke en voor welke diensten/taken? ……	Ja ☐ Nee ☐
Voert u jaarlijks cyberveiligheidsaudits uit bij uw aanbieders van IT-diensten?	Ja ☐ Nee ☐
Hebt u, afgezien van IT-diensten, bepaalde diensten uitbesteed aan externe dienstverleners? Zo ja, aan welke dienstverleners en voor welke diensten/taken? …… Zo ja, voert u jaarlijks audits voor cyberveiligheid uit bij deze dienstverleners?	Ja ☐ Nee ☐ Ja ☐ Nee ☐
Geven uw onderaannemers, uw dienstverleners en hun verzekeraars zelf gevolg aan al uw vorderingen?	Ja ☐ Nee ☐
Zijn uw onderaannemers en dienstverleners tegen cyberrisico's verzekerd?	Ja ☐ Nee ☐

Specifieke vragen

Facultatieve vragen <u>behalve in de volgende gevallen</u>:

- **omzet hoger dan € 100 M en/of;**
- **activiteiten in de IT-sector en/of;**
- **u hebt onder Uw gegevens een aantal van meer dan 250.000 aangevinkt.**

Wie is verantwoordelijk voor het beleid betreffende het beheer en de beveiliging van persoonsgegevens: ☐ a. IT-manager ☐ b. veiligheidsmanager ☐ c. CEO of gelijkwaardig ☐ d. anders (specificeer) Wat is zijn/haar ervaring?	
Gelieve uw strategie voor de bescherming van back-ups toe te lichten: 1) Hoe beschermt u back-ups tegen versleuteling in geval van een ransomewareaanval? …… …… 2) Hoe beschermt u al uw back-ups tegen het risico van een situatie waarin hackers de informatiesystemen 45 dagen lang binnendringen? …… ……	
Hoe vaak worden de back-ups van uw systemen getest? …… Wanneer zijn de back-ups van uw systemen voor het laatst getest? ……	
Specificeer welke audits op uw netwerk worden uitgevoerd: a. kwetsbaarheidstest b. penetratietest c. anders (specificeer)	
Worden deze audits door een externe dienstverlener uitgevoerd? Zo ja, hoe vaak voert u deze audits uit? a. jaarlijks b. vaker, namelijk: c. nooit	Ja ☐ Nee ☐
Binnen welke termijn voert u correcties uit die bij een veiligheidsaudit noodzakelijk zijn gebleken? ……..	
Hebt u firewalls geïnstalleerd om het verkeer op het netwerk te reguleren? a) binnen het netwerk b) op alle IT-systemen en andere eindpunten c) WAF d) geen firewall geïnstalleerd	
Zijn verzonden gegevens versleuteld, ook bij gebruik van een VPN voor toegang op afstand?	Ja ☐ Nee ☐
Hebt u maatregelen ingevoerd om alle aanvallen, aanvalspogingen of incidenten op te sporen? Zo ja, gebruikt u een van de volgende waarschuwingssystemen? ☐ a. SIEM (Security Information and Event Management) ☐ b. interne SOC (Security Operations Center) ☐ c. beheerde SOC ☐ d. anders (specificeer)……	Ja ☐ Nee ☐
Bewaart u logbestanden en gegevens over mogelijke aanvallen? Zo ja, hoelang worden deze bewaard?	Ja ☐ Nee ☐
Worden correcties en nieuwe codes in een aparte testomgeving getest voordat ze in de echte omgeving worden geïnstalleerd?	Ja ☐ Nee ☐

Cyberfraude

Bestaat er een procedure met dubbele handtekening voor betalingen boven € 10.000? Nee ☐ een procedure met dubbele handtekening is vereist voor betalingen boven: …….. (specificeer het bedrag) Nee ☐ er is nooit een procedure met dubbele handtekening vereist	Ja ☐ Nee ☐
Zijn de functies voor betalingsmachtiging en betaling binnen uw organisatie gescheiden?	Ja ☐ Nee ☐
Welke controles worden in de boekhouding doorgevoerd om na te gaan of alle betalingen legaal zijn? ……	
Wanneer een nieuwe medewerker in dienst wordt genomen of een medewerker intern van functie verandert en deze persoon taken zal uitvoeren die verband houden met voorraadbeheer, boekhouding, beheer van leveringen en/of kasbeheer, inclusief betalingsmachtiging en betaling, worden diens eerdere taken en referenties dan gecontroleerd? Controleert u aan het eind van de procedure van interne of externe werving voor dit soort functies het strafblad van de betreffende persoon?	Ja ☐ Nee ☐ Ja ☐ Nee ☐

Hoeveel personen binnen de groep mogen toestemming geven voor overboekingen?	
Welke controles past u toe voor toevoeging, wijziging of verwijdering van een betalingsbegunstigde?	

Antecedenten

Hebt u de afgelopen 5 jaar een schadegeval gehad waarvan de totale kosten meer dan 1.500 euro bedroegen (ongeacht of het werd vergoed of niet)? Zo ja, vermeld het bedrag, de datum, de feiten en de maatregelen die zijn getroffen om herhaling te voorkomen …… ……	Ja ☐ Nee ☐
Bent u betrokken geweest bij een onderzoek dat door een nationale gegevensbeschermingsautoriteit is ingesteld? Zo ja, licht toe :…….. ……	Ja ☐ Nee ☐
Hebt u kennis van gebeurtenissen of omstandigheden die ertoe zouden kunnen leiden dat de verzekering moet worden ingeroepen? Zo ja, licht toe :…….. ……	Ja ☐ Nee ☐
Hebt u reeds eerder een cyberverzekering bij Hiscox afgesloten of hebt u in de afgelopen drie maanden een verzekeringsofferte aangevraagd?	Ja ☐ Nee ☐

HISCOX

Cyberverzekering
Vragenlijst voor onderschrijving

Verzekering

Gewenste ingangsdatum: ☐ Gewenste vervaldag: ☐

Slotverklaring

Ik verklaar dat de toelichtingen en gegevens in deze verklaring juist zijn en dat er geen materiële feiten zijn die fout zijn weergegeven.

Ik ga ermee akkoord dat deze verklaring samen met enige andere verschafte informatie de basis zal vormen van de verzekeringsovereenkomst.

Ik verbind mij ertoe de verzekeraars op de hoogte te stellen van enige materiële wijziging aan feiten die plaatsvindt voor de voltooiing of in de loop van het verzekeringscontract. Een materieel feit is een feit die het aanvaarden of beoordelen van het risico zou kunnen beïnvloeden.

Tevens verklaar ik kennis te hebben genomen van de toepasbare algemene voorwaarden en de omvang, uitsluitingen en beperkingen ervan te hebben begrepen.

Ondertekening

Ondergetekende verklaart verzekeringnemer bevoegd te vertegenwoordigen, zoals directeur, partner, of bevoegd manager.

☐

Gedaan te ☐ op ☐ / /

Handtekening ☐