Meijers
makelaars in assurantiën

Aanvraagformulier *Cyberverzekering*

A56.3

Dank voor uw interesse in een cyberverzekering. Wilt u voor de aanvraag hiervan de onderstaande vragenlijst invullen? Verzekeraars hanteren strikte voorwaarden om in aanmerking te komen hiervoor en de meest voorkomende uitgangspunten vindt u terug in de slotverklaring. Ook is er een begrippenlijst toegevoegd op de laatste pagina. Heeft u vragen? Neemt u dan vooral contact met ons op. Wij helpen u graag verder.

1. Uw gegevens

A. Naam van verzekeringnemer (moedermaatschappij) _____

B. Straat en nummer _____

C. Postcode en woonplaats _____

D. E-mailadres contactpersoon _____

E. Website _____

F. Aantal werknemers _____

G. Hoedanigheid/aard van de werkzaamheden en SBI-code(s) _____

H. Mee te verzekeren ondernemingen inclusief SBI-codes (meer dan 50% eigendom) _____

I. Jaarlijkse omzet inclusief de bij verzekerde(n) genoemde ondernemingen _____

J. Heeft u ondernemingen in het buitenland? ☐ Ja ☐ Nee

Zo ja, als bijlage organogram meesturen inclusief land en omzet per entiteit

K. Een van onze partners sluit de volgende sectoren uit:
Accreditatie bureau / Bedrijf o.h.g.v. adult content / Kredietbureau / Dienstverlener op het gebied van cryptovaluta / Cybersecurity products of services / Data processing bedrijf / Warehouse / Casino / Producent van medische invasieve apparatuur / Betalingsverwerker / Beveiligingsdienst (fysiek of digitaal) / Schadebehandelaar voor derden / Uitgever / Drukkerij / Telecombedrijf / Financiële instelling / IT-dienstverlener / Cloud service provider / Internetserviceprovider / Overheid / Mediabedrijf / Assurantietussenpersoon / Sociaal netwerk bedrijf / Callcenter.
Bent u werkzaam in een van deze sectoren? ☐ Ja ☐ Nee

L. Een van onze andere partners sluit de volgende sectoren uit:
Telecombedrijf / Financiële instelling / ICT onderneming / Overheidsinstelling / Gemeente / Mediabedrijf / Assurantietussenpersoon / Sociaal netwerkbedrijf / Callcenter / Telemarketing bureau / Transportonderneming / Advocatenkantoor / Onderwijsinstelling / Zorginstelling / Ziekenhuis.
Bent u werkzaam in een van deze sectoren? ☐ Ja ☐ Nee

2. IT-gegevens

A. Heeft u geavanceerde of volgende generatie antimalware en antivirus software met heuristische analyse permanent actief op alle verbonden apparaten en een proces voor opvolging van (dreigings)meldingen? ☐ Ja ☐ Nee

B. Maakt u minimaal maandelijks back-ups voor alle kritieke systemen en data? ☐ Ja ☐ Nee

C. Heeft u automatische updates geactiveerd voor minimaal het 'Operating System' (o.a. Windows of Apple OS) en de beveiligingssoftware (of EDR)? ☐ Ja ☐ Nee

D. Test u maandelijks het terugzetten van back-ups (restore)? ☐ Ja ☐ Nee

E. Vindt externe toegang tot uw systemen (bijvoorbeeld thuiswerken) altijd plaats via multifactor authenticatie (MFA)? ☐ Ja ☐ Nee

F. Heeft u een patchbeleid waarbij kritieke updates (conform publicatie door het Digital Trust Center van de rijksoverheid) binnen 7 dagen na publicatie worden uitgevoerd? ☐ Ja ☐ Nee

G. Heeft u beleid geïmplementeerd voor de toegang tot informatiesystemen, waarbij iedere gebruiker een eigen account en wachtwoord heeft conform de minimumvereisten van Microsoft.
Dit is een standaard instelling in Microsoft voor wachtwoorden, namelijk minimaal 8 karakters lang en met 3 van de volgende vereisten: 1 hoofdletter, 1 kleine letter, 1 getal en een bijzonder teken.
Zie ook learn.microsoft.com en zoek op “password complexity requirements”? ☐ Ja ☐ Nee

H. Voldoen verzekeringnemer en haar ondernemingen, voor zover bekend, aan alle relevante privacywet- en regelgeving in de rechtsgebieden waar men actief is? ☐ Ja ☐ Nee

I. Geef aan met welke maatregelen de back-ups voor bedrijfskritieke systemen van verzekeringnemer en haar ondernemingen worden beschermd (meerdere keuzes mogelijk).
- ☐ Immutable of Write Once Read Many (WORM) bescherming
- ☐ Volledig offline of air-gapped segmentatie die is losgekoppeld van de rest van het netwerk
- ☐ Toegang tot back-ups is alleen mogelijk via multi-factor authenticatie

J. Geef aan welke beveiligingsmaatregelen voor e-mail van kracht zijn voor verzekeringnemer en haar ondernemingen (meerdere keuzes mogelijk).
- ☐ Quarantaine service voor verdachte e-mails
- ☐ Mogelijkheid om bijlagen en links in een sandbox te plaatsen
- ☐ Sender Policy Framework (SPF) is ingesteld
- ☐ Microsoft Office macro’s zijn standaard uitgeschakeld voor documenten
- ☐ Minimaal eens per jaar phishing-simulaties of trainingen voor werknemers

K. Heeft de verzekeringnemer (IT) diensten/services uitbesteed aan derden? (zoals clouddiensten, Software as a Service, netwerk beheer, data-opslag etc.) ☐ Ja ☐ Nee

Zo ja, als bijlage tabel meesturen voor de belangrijkste dienstverleners met de kolommen ‘Dienstverlener’ en ‘Type IT Dienst / Service’

L. Versleutelt (encrypt) u alle bedrijfslaptops? ☐ Ja ☐ Nee

M. Verzekeringnemer bevestigt dat er een Endpoint Detection & Response (EDR) (ook wel next generation antivirus genoemd) aanwezig is op de werkstations/laptops (ook indien er in de cloud wordt gewerkt) en deze voldoet in ieder geval aan de volgende vereisten:
- detecteert ongebruikelijke gedragspatronen en neemt maatregelen tegen zogenoemde exploits (exploits protection);
- identificeert patronen die overeenkomen met bekende dreigingen/aanvallen;
- waarschuwt beveiligingspersoneel bij incidenten;
- biedt forensische- en analysemogelijkheden om analisten in staat te stellen op dreigingen/ aanvallen te reageren.

☐ Ja ☐ Nee

N. Selecteer het percentage van de inkomsten dat verzekeringnemer en haar deelnemingen genereren uit online verkopen: ☐ 0% - 25% ☐ >25% - 50% ☐ >50% - 100%

3. Polisgegevens

A. Gewenste limiet per jaar ☐ € 1.000.000 ☐ € 2.000.000 ☐ € 2.500.000

B. Gewenste ingangsdatum _____

C. Heeft u nog iets mee te delen dat voor de beoordeling van deze aanvraag van belang kan zijn? ☐ Ja ☐ Nee

Toelichting

_____

D. Zijn u schades of omstandigheden in de afgelopen 3 jaar bekend die onder deze polis verzekerd zouden zijn geweest? ☐ Ja ☐ Nee

Zo ja, wat is er gebeurd?

Wat was de impact?

Welke maatregelen heeft u genomen om herhaling te voorkomen?

4. Slotverklaring

(Kandidaat-)verzekeringnemer (verzekeringsnemer inclusief mee te verzekeren ondernemingen) verklaren middels ondertekening van deze akkoordverklaring:

i. dat u, of uw betalingsverwerker, geen creditcardgegevens verwerkt, verzamelt, beheert of bewerkt
ii. dat u geen dochteronderneming bent
iii. dat u direct of indirect niet meer dan 10% omzet in/uit de Verenigde Staten en/of Canada genereert
iv. dat het aantal personen dat geïnformeerd moet worden in geval van inbreuk met betrekking tot privacygegevens beheerd door verzekeringnemer en/of mee te verzekeren ondernemingen minder is dan 500.000
v. dat de verzekeringnemer geen vestiging, dochteronderneming, deelneming of joint venture of andere zaken (met partijen) heeft in Syrië, Cuba, Soedan, Iran, Myanmar, Venezuela, de Krim, Wit Rusland, Zimbabwe en/of Noord-Korea
vi. dat er geen vestiging buiten de EER (Europese Economische Ruimte) en/of Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland aanwezig is
vii. dat u niet bekend bent met een gebeurtenis, voorval of omstandigheid (zoals o.a. een security incident, datalek of ander privacy gerelateerd evenement), welke mogelijkerwijs aanleiding zou kunnen geven tot een claim onder deze polis dat u in de afgelopen 5 jaar geen:
    a verzekeringsovereenkomst is geweigerd, opgezegd of onder beperkte of bijzondere voorwaarden is voorgesteld
    b aanspraak op dekking geheel of gedeelte is afgewezen
    c schade is teruggevorderd door een verzekeraar in verband met onware opgave
viii. dat geen vestiging, dochteronderneming, deelneming en/of omzet wordt behaald in een land waarop de Verenigde Naties, de Verenigde Staten, de Europese Unie en/of Nederland een sanctieregeling van toepassing heeft verklaard

☐ Ja ☐ Nee

Artikel 7:928 BW bepaalt dat de verzekeringnemer verplicht is voor het sluiten van de overeenkomst alle feiten mee te delen die hij kent of behoort te kennen en waarvan, naar hij weet of behoort te begrijpen, de beslissing van de verzekeraar of, en zo ja, op welke voorwaarden, hij de verzekering zal willen sluiten afhangt of kan afhangen. Dit geldt ook voor de derden wiens belangen de verzekering dekt of mede dekt. Indien de mededelingsplicht niet of onvoldoende wordt nagekomen, kan de verzekeraar daar op grond van artikel 7:930 BW, afhankelijk van het verzuim, gevolgen aan verbinden waaronder het met dadelijke ingang opzeggen van de verzekering, het beperken van de dekking en het weigeren of beperken van een schadevergoeding op grond van de verzekering.

5. Ondertekening

Naam

Datum

Functie

Plaats

Handtekening

Begrippenlijst:

Wat betekent heuristische analyse?

- Een heuristische analyse gaat verder dan traditionele detectie op basis van bepaalde criteria door basis-antivirussoftware. Het zoekt naar verdachte eigenschappen in code en kan de gevoeligheid van een systeem bepalen voor een bedreiging met behulp van verschillende beslissingsregels of weegmethoden. Het doel hiervan is nieuwe computervirussen te detecteren.

Wat betekent Multifactor authenticatie (MFA)?

- MFA is een elektronische verificatiemethode bijvoorbeeld bij het inloggen met uw DIGID. Het wordt gebruikt om geautoriseerde personen toegang te geven tot specifieke systemen of gegevens.
- Een gebruiker moet twee of meer factoren presenteren – deze factoren zijn:
  - 1) iets wat je weet (e.g. wachtwoord),
  - 2) iets wat je hebt (e.g. je uniek te identificeren laptop),
  - 3) iets wat je bent (e.g. vingerafdruk).

Wat betekent Immutable of Write Once Read Many (WORM) bescherming?

- Immutable / WORM back-up is een gegevensopslagapparaat waarin informatie, eenmaal geschreven, niet kan worden gewijzigd.

Wat betekent volledig offline of air-gapped back-uppen?

- Een offline of air-gapped back-up van uw gegevens en configuraties die staat opgeslagen in een offline omgeving. Deze is gescheiden van de rest van uw netwerk. Fysieke tapeback-ups of niet-gekoppelde schijfback-ups die niet zijn verbonden met het internet of het LAN (local area network), worden als offline beschouwd.

Wat betekent 'Quarantaine service' voor verdachte e-mails?

- Het automatisch achterhouden van verdachte e-mails voor de geadresseerde(n). Deze e-mails worden tijdelijk en onzichtbaar 'in quarantaine' bewaard. De geadresseerde krijgt wel melding dat een e-mail is tegengehouden en kan, vaak met behulp van de IT-afdeling, de e-mail alsnog vrij laten geven als deze ten onrechte als verdacht is aangemerkt.

Wat betekent ''mogelijkheid om bijlagen en links in een sandbox te plaatsen''?

- In een aparte en veilige omgeving (i.e. de sandbox) wordt getest of een e-mail veilig is voordat ze naar uw netwerk- of e-mailservers gaan. Denk aan e-mails met onbekende en/of verdachte URL-koppelingen, bijlagen of andere bestanden.

Wat betekent 'Sender Policy Framework (SPF)'?

- SPF is een e-mailverificatiemethode dat wordt gebruikt om te voorkomen dat onbevoegden e-mailberichten worden verzonden vanuit uw domein. Het helpt e-mailgebruikers en -ontvangers te beschermen tegen spam en andere potentieel gevaarlijke e-mails.

Wat betekent ''Microsoft Office macro's zijn standaard uitgeschakeld voor documenten''?

- Macro's zijn kleine stukjes code die gebruikt worden in MS Word of MS Excel bestanden. Deze code kan automatisch geactiveerd worden bij het openen van een dergelijk bestand en kwaadaardige handelingen uitvoeren (als dat door een aanvaller zo is geprepareerd). Daarom dient het automatisch activeren van macro's standaard te zijn uitgeschakeld.