Inventarisatieformulier ICT Bedrijven - BAV/AVB en Cyber 28-7-2021

Algemene informatie

Naam verzekeringnemer	
Polisnummer	
Website	

Activiteiten

Zijn de activiteiten van de verzekerde(n) gewijzigd in het afgelopen jaar? ☐ Ja ☐ Nee

Indien ja, graag een toelichting.

Verkoop, overnames en deelnames

Heeft u de laatste 18 maanden bedrijven verkocht, nieuwe dochterondernemingen gecreëerd of deelgenomen aan fusies, overnames of joint ventures? ☐ Ja ☐ Nee

Indien ja, graag een toelichting.

Jaaromzet - Producten en diensten

Omschrijving van de activiteiten					
Hardware	Circa	**Software & diensten**	Circa	**Telecom & Netwerk diensten**	Circa
Servers	%	Pakket software - derden	%	Advies	%
PC's	%	Pakket software - zelf ontwikkeld	%	Installatie	%
Randapparatuur	%	Maatwerk software	%	Beheer	%
Mobiele telefoons	%	Saas	%	Overige:	
Overige:		Advies	%		%
	%	Implementatie	%		%
	%	Detachering	%		%
	%	Hosting	%		%
	%	Overige:			%
	%		%		%

1. Welk percentage van de omzet wordt verkregen van overheidsinstellingen?

_____%

2. Heeft u 3 of meer individuele contracten met overheidsinstellingen per jaar? ☐ Ja ☐ Nee

Jaaromzet - Landen

	Vorig boekjaar	Dit boekjaar (prognose)	Volgend boekjaar (prognose)
Nederland	€	€	€
USA/Canada (export*)	€	€	€
USA/Canada (lokaal**)	€	€	€
Overige landen	€	€	€
Totaal	€	€	€

* Onder "export" wordt verstaan de omzet die is gegenereerd door uw vestiging(en) buiten de USA of Canada, maar voortvloeiende uit overeenkomsten met opdrachtgevers die zich wel in de USA of Canada bevinden

** Onder "lokaal" wordt verstaan de omzet die is gegenereerd door uw lokale vestiging(en) binnen de USA of Canada en voortvloeiende uit overeenkomsten met opdrachtgevers die zich eveneens in de USA of Canada bevinden

1. Over welke boekjaren heeft u de laatste drie jaar een positief financieel resultaat behaald?

_____

Opdrachtgevers

1. Welke producten en diensten levert u op de volgende gebieden/aan de volgende sectoren:

Indien u geen enkel product of dienst op deze gebieden/aan deze sectoren levert, graag aangeven met "geen".

Gebied/sector	% omzet	Per product en dienst graag een toelichting geven op de activiteiten
Luchthavens/Luchtvaartmaatschappijen	%	
Gokken	%	
Militaire geleidingssystemen	%	
Massa vervoer	%	
Data aggregation	%	
Online beurzen / Handelsplatformen	%	
Satellieten	%	
Erotische content	%	
Sociale netwerken	%	
Nutsbedrijven	%	
Beveiliging / Cybersecurity	%	
Bankieren/Financiële transacties	%	
Gezondheidszorg	%	
ERP/CRM/ SCM/EAI	%	

Ruimte voor nadere toelichting (indien nodig):

2. Welke nieuwe producten of diensten bent u van plan de komende 12 maanden te gaan leveren?

   Indien er geen wijzigingen zullen plaatsvinden graag aangeven met "geen".

Contracten

1. Hoe vaak sluit u overeenkomsten met uw opdrachtgevers op basis van:

	Circa % van de jaaromzet
Uw eigen algemene leveringsvoorwaarden	%
Inkoopvoorwaarden van uw opdrachtgevers	%
Maatwerk voorwaarden	%
Anders, namelijk:	%

2. Gegevens van de drie grootste contracten in de laatste drie jaar:

	1.	2.	3.
Naam opdrachtgever			
Beschrijving product/dienst			
Totale contract waarde	€	€	€
Ingangsjaar contract			
Totale duur contract	mnd	mnd	mnd
*Ontwikkelingsperiode**	*mnd*	*mnd*	*mnd*
*Implementatieperiode**	*mnd*	*mnd*	*mnd*
*Onderhoudsperiode**	*mnd*	*mnd*	*mnd*
Ontwikkeling	%	%	%
Licentie inkomsten	%	%	%
Consultancy/implementatie	%	%	%
Onderhoud	%	%	%
Hardware	%	%	%
Algemene voorwaarden**			

* Indien van toepassing

** Bijvoorbeeld uw voorwaarden, inkoopvoorwaarden opdrachtgever, maatwerk, etc.

3. Accepteert u aansprakelijkheid voor gevolgschade, exclusief intellectueel eigendom en lichamelijk letsel ? ☐ Ja ☐ Nee

   Indien ja, tot welk bedrag beperkt u uw aansprakelijkheid voor gevolgschade, behalve in geval van intellectuele eigendomschade en personenschade;

   % van de contracten:

   a. Lager dan de contractwaarde _____%
   b. Gelijk aan contractwaarde _____%
   c. Hoger dan de contractwaarde _____%
   d. Geen beperking _____%
   e. Totaal 100 %

4. Omvang van de contracten:
   a. Gemiddelde contractwaarde € _____
   b. Looptijd gemiddeld contract _____ maanden
   c. Looptijd langste contract _____ maanden

5. Welke percentage van uw contracten bevatten acceptatiecriteria inclusief deliverables en installatie _____%

6. Heeft u een formele procedure voor het documenteren van wijzigingen in contracten gedurende de contractperiode?

   ☐ Ja ☐ Nee

Kwaliteitscontroles

1. Heeft u een schriftelijke en geformaliseerde procedure inzake kwaliteitscontrole? ☐ Ja ☐ Nee

Data Privacy

1. Voor hoeveel dossiers met persoonsgegevens bent u verantwoordelijk? _____
2. Voor hoeveel dossiers met gevoelige data bent u verantwoordelijk? _____
3. Verwerkt, bewerkt of beheert u gegevens voor of namens een derde? ☐ Ja ☐ Nee
   a. Indien ja, Gelieve toe te lichten:

Indien ja,

b. Voor hoeveel dossiers met persoonsgegevens die u voor of namens een derde verwerkt, bewerkt of beheert bent u verantwoordelijk? _____

c. Voor hoeveel dossiers met gevoelige data die u voor of namens een derde verwerkt, bewerkt of beheert bent u verantwoordelijk? _____

4. Wordt betaalkaartinformatie verwerkt, verzameld, beheerd of bewerkt ☐ Ja ☐ Nee
   a. Indien ja, worden deze activiteiten uitbesteed?

b. Beschrijf het niveau van uw (of uw outsourcer/uitbesteder) PCI DSS compliance, het aantal transacties, aantal betaalkaarten waarvan u informatie heeft, de naam van de betalingsverwerker en of de betalingsverwerker u schadeloos stelt in geval van schade:

☐ Niveau 1 (meer dan 6M) ☐ Niveau 2 (1M tot 6M)

☐ Niveau 3 (20.000 tot 1M) ☐ Niveau 4 (minder dan 20.000)

Data en informatiebeveiliging

Welke van de volgende maatregelen heeft u (of uw provider, indien uitbesteed) geïmplementeerd ter bescherming van informatie en systemen tegen een datalek of cyberincident?

Beleid		Bescherming en Technologie		Bedrijfscontinuatie	
Functionaris gegevensbescherming	☐	Firewalls & Antivirus	☐	Bedrijfscontinuiteitsplan	☐
				Testen bedrijfscontinuiteitsplan:	
				Regelmatig	☐
				Niet regelmatig	☐
Medewerker verantwoordelijk voor de IT beveiliging	☐	Kwetsbaarheidsscan	☐	Crisis herstelplan	☐
				Testen crisis herstelplan:	
				Regelmatig	☐
				Niet regelmatig	☐
Privacy beleid goedgekeurd en geïmplementeerd	☐	Endpoint protection	☐	Systeemback-up:	
				Dagelijks	☐
				Wekelijks	☐
				Maandelijks	☐
Regelmatig trainingen op het gebied van privacy en cyber	☐	Indringer detectie systeem	☐	Back-ups zijn in een offline omgeving opgeslagen en zijn niet verbonden met het netwerk	☐
Maatregelen genomen om te (blijven) voldoen aan toepasselijke privacywetgeving, waaronder de AVG	☐	Encryptie van gevoelige data:		Duplicatie en redundantie van systemen	☐
		Volledig	☐		
		Gedeeltelijk	☐	Duplicatie en redundantie van kritieke systemen in een offline omgeving	☐
		Niet	☐		
Incident respons plan:	☐	Multi-Factor Authentication 2FA is geïnstalleerd en ingeschakeld voor alle externe toegang (remote access) tot uw bedrijfs-systemen, Operational Technology systemen of software, zowel cloudgebaseerd als on-premises	☐		
Testen incident respons plan:					
Regelmatig	☐				
Niet regelmatig	☐				
Kritische updates en patches worden binnen één maand doorgevoerd	☐	Jaarlijks een externe pentest	☐		
Gebruik van Threat Intelligence	☐				
Authorisatiebeheer voor systemen	☐				
Testen van back-ups	☐				
Overige: (gelieve te omschrijven)					

Covid-19

1. Op welke wijze heeft COVID-19 uw activiteiten beïnvloed?

2. Voorziet u potentiële claims met betrekking tot COVID-19? ☐ Ja ☐ Nee

   (Bijvoorbeeld als gevolg van vertraging bij projecten) Zo ja, gaarne toelichten.

3. Wat zijn de implicaties van het niet kunnen werken op het terrein van de opdrachtgever (indien van toepassing)?

Schadeverloop

1. Bent u voor een schade aansprakelijk gesteld? ☐ Ja ☐ Nee

   Zo ja, graag een volledige omschrijving van de aanspraak zoals datum, aard en (potentiële)financiële omvang van de aanspraak en welke maatregelen u heeft getroffen om de schade te beperken of herhaling te voorkomen.

2. Heeft er zich bij u ooit een cyberincident voorgedaan zoals hacking, malware, Ddos aanval, afpersing, programmeer- of menselijke fout? ☐ Ja ☐ Nee

   Zo ja, graag een volledige omschrijving van het incident zoals datum, aard en omvang van het incident en welke maatregelen u heeft getroffen om de schade te beperken of herhaling te voorkomen.

3. Bent u zich bewust van enig handelen of nalaten of zijn er omstandigheden die mogelijk tot een aanspraak of een cyberincident zoals hacking, malware, Ddos aanval, afpersing, programmeer- of menselijke fout kunnen leiden? ☐ Ja ☐ Nee

   Zo ja, graag een volledige omschrijving.

Ondertekening

Ondergetekende, bevoegd om voor de onderneming te tekenen, verklaart de bovenstaande vragen volledig en naar waarheid te hebben beantwoord en geen voor deze verzekering belangrijke aspecten te hebben verzwegen en/of niet geheel juist te hebben voorgesteld.

Plaats _____ Datum _____

Naam _____ Functie _____

Handtekening

S.v.p. meezenden:
- Kopie van uw standaard contract(en), incl. algemene voorwaarden, en evt. SLA en/of verwerkersovereenkomst

Begrippenlijst

Autorisatiebeheer voor Systemen - Access Management Controls omvat het management van gebruiksnamen, wachtwoorden en toegang tot systemen en informatie.

Encryptie – Encryptie is een methode om data vanuit een leesbare format te converteren naar een gecodeerde format. Het kan alleen weer leesbaar worden (worden geopend) met behulp van een sleutel.

Endpoint Protection – Endpoint Protection zorgt voor de bescherming en bewaking van de eindpunten in uw netwerk. Eindpunten omvatten desktop-en laptopcomputers, tablets, mobiele telefoons, servers en elk ander apparaat dat verbonden is met uw netwerk.

Gevoelige data– Onder gevoelige data wordt o.a. verstaan gezondheids-of medische dossiers van werknemers of klanten, door de overheid uitgegeven identificatienummers, gebruikersnamen en wachtwoorden, e-mailadressen, creditcardnummers, intellectueel eigendom of andere persoonlijk identificeerbare informatie.

Indringer Detectie Systeem – Is een apparaat of software dat een network monitort op kwaadwillige activiteiten of beleidsschendingen.

Threat Intelligence– Bedreigingsinformatie is informatie over huidige beveiligingsbedreigingen, kwetsbaarheden, doelen, slechte actoren en implicaties die kunnen worden gebruikt om beveiligingsbeslissingen.