

Avéro Achmea
Sophialaan 50
8911 AE Leeuwarden
Nederland

Postbus 909
8901 BS Leeuwarden
Nederland
www.averoachmea.nl

Belangrijk: toelichting bij het invullen van dit formulier:

1. Als aanvrager van het Cyber Security-assessment moet u alle vragen in dit aanvraagformulier zo volledig mogelijk te beantwoorden.
2. Vul dit formulier in met uw IT-manager / IT-leverancier. Dit formulier vormt de basis voor het assessment.
3. Het eerste deel van deze vragenlijst zijn open vragen. In het tweede deel kunt u antwoorden met *Ja, Deels, Nee, Weet ik niet, Niet van toepassing*.
4. Stuur dit formulier na het invullen terug naar: accountbedrijvenschade.avero@achmea.nl

1 Uw onderneming

- a. Naam onderneming _____
- b. Aantal medewerkers _____
- c. Jaaromzet _____
- d. Aantal vestigingen _____
- e. Hoofdvestiging te _____
- f. Branche _____
- g. Wie beheert uw IT (zelf / (deels) uitbesteed aan) _____
- h. Wat zijn de voor uw organisatie belangrijkste kritieke bedrijfsactiviteiten? _____
- i. Welke kroonjuwelen/assets zijn bij uw organisatie van belang? Denkt u hierbij aan: het verwerken van geld, intellectueel eigendommen, persoonsgegevens, continuïteit van de website/webshop, continuïteit van industriële processen. _____
- j. Heeft u eerder te maken gehad met een ICT- of Cyberincident? Kunt u een toelichting geven op dit incident _____
- k. Hoe belangrijk vindt u cybersecurity voor uw organisatie? (Laag, Midden of Hoog). _____

2 Organisatie

- | | | | | | |
|---|----|-------|-----|--------------|---------------------|
| 1. Heeft uw directie beleid opgesteld voor cybersecurity en zijn de verantwoordelijkheden duidelijk verdeeld? | Ja | Deels | Nee | Weet ik niet | Niet van toepassing |
| 2. Heeft u beschikbaarheid, juistheid en vertrouwelijkheid van informatie besproken en vastgelegd in bijvoorbeeld een SLA met uw IT leverancier? | Ja | Deels | Nee | Weet ik niet | Niet van toepassing |
| 3. Schakelt u regelmatig een externe auditor in om de naleving van uw cybersecuritybeleid door te lichten? | Ja | Deels | Nee | Weet ik niet | Niet van toepassing |
| 4. Heeft uw IT-afdeling (of uw IT-leverancier) de technische maatregelen voor cybersecurity in zijn takenpakket? | Ja | Deels | Nee | Weet ik niet | Niet van toepassing |
| 5. Is uw onderneming voldoende op de hoogte van de specifieke wettelijke of andere juridische vereisten, waaraan verwerking van informatie moet voldoen? Denkt u hierbij aan de AVG (Algemene verordening gegevensbescherming) of voorschriften voor verwerking van credit cards (PCI). | Ja | Deels | Nee | Weet ik niet | Niet van toepassing |
| 6. Voldoet uw onderneming aan (contractuele) eisen die belangrijke toeleveranciers of afnemers stellen aan uw digitale veiligheid? | Ja | Deels | Nee | Weet ik niet | Niet van toepassing |
| 7. Voldoet uw organisatie aan wet- en regelgeving en contractuele verplichtingen voor gebruik van materiaal en producten waarop intellectueel eigendomsrecht van andere partijen berust? Denkt u hierbij bijvoorbeeld aan videomateriaal of betaalde rapporten. | Ja | Deels | Nee | Weet ik niet | Niet van toepassing |

8. Heeft u beleid opgesteld voor het ophalen, verwerken en opslaan van persoonsgegevens? Inclusief een privacyreglement?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
9. Is het gebruiksbeheer voor medewerkers en 'klanten' ingericht met 'Identity en Access Management'? Dit zijn afspraken en een technisch systeem waarin geregeld is wie waartoe toegang heeft op het netwerk.	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
10. Trekt u direct de toegangsrechten van medewerkers en contractanten die uit dienst gaan in. Wordt bedrijfsapparatuur direct ingeleverd en de data gewist?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
11. Heeft uw organisatie maatregelen genomen om de continuïteit van uw bedrijf en zeker de dienstverlening aan klanten te waarborgen? Voor het geval ICT uitvalt of ernstig verstoord raakt?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
12. Heeft uw organisatie maatregelen genomen om afscheid te kunnen nemen van een Cloud-leverancier en de eigen data weer terug te krijgen (exit-strategie)?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
13. Heeft u spelregels voor de indeling van informatie (b.v. documenten) naar mate van vertrouwelijkheid? Wordt de informatie ook daadwerkelijk geclassificeerd (bijvoorbeeld: openbaar, vertrouwelijk, bedrijfsgeheim)?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
14. Screent u nieuwe en huidige medewerkers die met vertrouwelijke (klant-) informatie werken?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
15. Heeft uw organisatie een geheimhoudings-overeenkomst opgesteld om gevoelige informatie te beschermen? Tekenend medewerkers (en indien relevant externe krachten) op gevoelige functies deze ook?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
16. Zijn er maatregelen getroffen om identiteitsfraude te voorkomen? (b.v. inloggen door crimineel onder andere naam, interne fraude en bestellingen naar andere adressen omzetten).	Ja	Deels	Nee	Weet ik niet	Niet van toepassing

3 Mens en middelen

17. Zijn belangrijke ICT-faciliteiten en informatiebronnen fysiek beschermd tegen ongeoorloofde toegang?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
18. Is ICT-apparatuur (m.n. serverruimte) beveiligd tegen brand en blikseminslag?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
19. Zijn kabels beschermd tegen beschadiging?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
20. Heeft u een werkwijze ingericht om afgedankte ICT-middelen veilig te verwijderen?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
21. Organiseert u activiteiten om medewerkers bewust te maken van het belang en de manier van (digitaal) veilig werken? Denkt u aan een training of communicatiemiddelen als posters, gesprekken, voorbeeldgedrag.	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
22. Heeft uw organisatie spelregels opgesteld rondom het zakelijk gebruik van social media. (zoals Twitter- en Facebookaccounts, webfora etc)?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
23. Is duidelijk welke apparatuur van het bedrijf is en welke regels er bij het gebruik hiervan horen?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
24. Hebben uw IT-beheerders voldoende kennis van cybersecurity bijvoorbeeld door het volgen van bijscholing of lezen van relevante vakbladen/websites?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing

4 Technologie

25. Maakt uw organisatie gebruik van firewalls op het netwerk en op werkstations?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
26. Zijn poorten die toegang bieden tot het netwerk en apparatuur, maar niet nodig zijn voor het dagelijkse werk, afgesloten?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
27. Zijn netwerkaansluiting(en) in openbare en/of voor klanten of leveranciers toegankelijke ruimten uitgeschakeld? Zij kunnen dus niet zonder meer het netwerk op.	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
28. Heeft u een WiFi-netwerk en is deze beschermd tegen oneigenlijke toegang?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
29. Heeft uw organisatie voorzieningen als VPN, SSL en andere beveiligingsprotocollen om thuiswerken mogelijk te maken?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing

30. Mogen uw medewerkers gebruik maken van eigen apparatuur op het bedrijfsnetwerk? Heeft u daar specifieke beveiligingsmaatregelen voor getroffen?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
31. Is uw remote beheer voor industriële controle-apparatuur (b.v. systemen voor klimaatbeheersing, pompen etc.) beveiligd? Bijvoorbeeld met VPN en een zelf instelbaar wachtwoord?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
32. Heeft u delen van het netwerk waar industriële controle-systemen draaien afgeschermd van de rest van het bedrijfsnetwerk (heeft u zogenaamde 'zonering' toegepast)?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
33. Heeft uw organisatie maatregelen genomen zodat medewerkers buiten kantoor (thuis of op klantlocatie) kunnen werken met vertrouwelijke bedrijfsinformatie?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
34. Zijn er over de beschikbaarheid van internet (vast en mobiel) afdoende afspraken gemaakt met de leverancier? Met 'afdoende' bedoelen we: er is een beschikbaarheid en bandbreedte gegarandeerd die past bij de behoeften van het bedrijf.	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
35. Is het CMS van de externe website veilig ingericht tegen aanvallen, om bijvoorbeeld kaping van accounts te voorkomen? Denkt u hierbij aan het direct doorvoeren van beschikbare patches (het dichten van een lek)?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
36. Is de financiële afhandeling van diensten die via de website worden verkocht, veilig ingeregeld?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
37. Zijn alle persoonsgegevens die klanten op de website invullen, veilig opgeslagen?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
38. Houdt u precies bij (monitoren) wat er op het bedrijfs-netwerk gebeurt door ge-autoriseerde en ongeautoriseerde gebruikers (incl. machines)?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
39. Maakt u regelmatig updates en voert u (auto)patches uit op ALLE gebruikte systemen?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
40. Maakt u regelmatig backups en bewaart u deze op een externe locatie?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
41. Past u automatische systeemvergrendeling toe bij langere inactiviteit bij een werkstation?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
42. Verplicht u het regelmatig wijzigen van wachtwoorden?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
43. Beschikt uw organisatie over up-to-date antivirus-programmatuur op servers en werkstations?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
44. Test u nieuwe ICT-voorzieningen ook zelf uitgebreid op securityaspecten voordat u ze implementeert?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
45. Past u voor inloggen op kritieke of gevoelige systemen een 2-factorauthenticatie toe? Hiermee bedoelen we bijvoorbeeld dat u moet inloggen met een wachtwoord en een code via sms.	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
46. Gebruikt u altijd encryptie (versleutelen) binnen uw bedrijf voor het digitaal versturen en opslaan van vertrouwelijke informatie?	Ja	Deels	Nee	Weet ik niet	Niet van toepassing
47. Worden ook niet-kantoorautomatiseringssystemen regelmatig gepatcht? Hiermee bedoelen we met name industriële controlesystemen.	Ja	Deels	Nee	Weet ik niet	Niet van toepassing

Goed om te weten

Wat doen wij en wie zijn wij?

Wij bieden verzekeringen, financiële diensten en producten aan.
We verkopen onze producten en oplossingen niet zelf aan onze klanten.
Daarvoor werken we samen met adviseurs. Zij geven u onafhankelijk advies.

Wij horen bij Achmea

Avéro Achmea is een merk van Achmea Schadeverzekeringen N.V. in Apeldoorn. Achmea is de grootste verzekeraar van Nederland. Achmea Schadeverzekeringen N.V. is ingeschreven bij de Kamer van Koophandel onder nummer 08053410 en de AFM onder nummer 12000606.

Uw gegevens in vertrouwde handen

Sluit u een verzekering, financiële dienst of product af? Dan hebben wij uw gegevens nodig. Denk aan uw naam, adres en woonplaats, e-mailadres, telefoonnummer en bankrekeningnummer. Soms hebben wij ook meer gegevens van u nodig. Achmea B.V. is verantwoordelijk voor een goede verwerking van uw persoonsgegevens.

Wilt u weten welke gegevens wij verwerken en waarvoor?

Kijk dan in ons Privacy Statement op averoachmea.nl/privacy. Daar leest u ook wat uw rechten zijn. En wanneer u bezwaar kunt maken tegen verwerking van uw gegevens.

Staan er fouten in dit formulier?

Ons doel is dat al onze informatie klopt en volledig is. En dat u alles zo goed mogelijk begrijpt. Maar er kan altijd ergens een fout staan. Wij zijn niet aansprakelijk voor eventuele gevolgen van die fout.

Staat er iets anders in de productvoorwaarden?

Uw en onze rechten en plichten staan in de productvoorwaarden. Staat in dit formulier wat anders dan in de productvoorwaarden? Dan gelden de productvoorwaarden.

Bent u niet tevreden? Laat het ons weten

Bent u het niet met ons eens of heeft u een klacht? Dan horen wij dit graag. We willen u namelijk zo goed mogelijk helpen. Kijk voor meer informatie en ons klachtenformulier op averoachmea.nl/klachtdoorgeven. U kunt ook een brief sturen naar:

Avéro Achmea
Klantsignaalmanagement
Postbus 101
7300 AC Apeldoorn

Meer informatie over Avéro Achmea

Kijk voor meer informatie over ons en ons beleid, onze producten en onze gegevens op averoachmea.nl.

De adressen van Avéro Achmea zijn:

Laan van Malkenschoten 20
7333 NP Apeldoorn

Sophialaan 50
8911 AE Leeuwarden