Cyberverzekering
Voorwaarden

ACYB24

Startpagina

Klik op het **hoofdstuk** om er naar toe te gaan

* Deze voorwaarden gelden alleen wanneer u deze Rubriek verzekerd heeft. Dit staat op het polisblad.

Voorwaarden zijn rechten en plichten voor u en voor ons.

7313G-23-08

1. Algemeen

Inhoud

Klik op de **vraag** om het antwoord te lezen

Verzekerd

1. Algemeen

Verzekerd

1. Wie zijn de verzekerden?

Verzekeringnemer = u.

- (Rechts)persoon die de cyberverzekering heeft afgesloten.
  - U gaat over het contract.
  - U betaalt de premie.
  - U kunt de verzekering stoppen.
  - U kunt vragen de verzekering te veranderen.

Bestuurders van uw bedrijf.

2. Welke begrippen gebruiken we in deze voorwaarden?

Gebeurtenis = voorval dat verzekerd is volgens deze verzekering.

Aanspraak = een verzekerde wordt schriftelijk aansprakelijk gesteld.

- Een ander eist schadevergoeding van de verzekerde.
  - Een eis om iets te doen of na te laten is geen aanspraak.

Melding = het moment dat een verzekerde de gebeurtenis of aanspraak bij ons meldt.

- Dit moment bepaalt of deze verzekering geldt voor deze gebeurtenis of aanspraak.

Omstandigheid = een voorval waarvan u verwacht dat er een aanspraak volgt.

- Maar er ligt op dit moment nog geen aanspraak bij u.
- Meld een omstandigheid uiterlijk 30 dagen na het stoppen van de verzekering.

Schade = uw financiële schade die het gevolg is van een gebeurtenis.

- Of de financiële schade van een ander die het gevolg is van een gebeurtenis.
  - Alleen als u daarvoor aansprakelijk bent.
- Ook kosten die wij maken om u te helpen.
  - Ook kosten die u zelf maakt.
    - Alleen als deze kosten redelijk zijn.
  - Alleen als wij daarvoor schriftelijk toestemming hebben verleend.

3. Wanneer geldt deze verzekering?

Als een gebeurtenis plaatsvindt binnen 30 dagen voor ingangsdatum van deze verzekering.

- En de verzekerde was van deze gebeurtenis niet op de hoogte en kon dit ook niet zijn.
- En u meldt de gebeurtenis tijdens de looptijd van deze verzekering.
- En u ontvangt de aanspraak tijdens de looptijd van de verzekering.

Als een gebeurtenis plaatsvindt tijdens de looptijd van deze verzekering.

- En u de gebeurtenis uiterlijk 30 dagen na het stoppen van deze verzekering bij ons meldt.

Als u een aanspraak ontvangt tijdens de looptijd van deze verzekering.

- En u de aanspraak uiterlijk 30 dagen na het stoppen van deze verzekering bij ons meldt.

Als u een aanspraak ontvangt na het stoppen van deze verzekering.

- En u de omstandigheid, die leidde tot deze aanspraak, tijdens de looptijd van deze verzekering bij ons meldde.
  - Of uiterlijk uiterlijk 30 dagen na het stoppen van deze verzekering.

1. Algemeen

4. Waar geldt deze verzekering?

In de hele wereld, behalve in de Verenigde Staten van Amerika of Canada.

- Niet verzekerd is de aansprakelijkheid voor schade volgens het recht van de Verenigde Staten van Amerika of Canada.
- Niet verzekerd is de aansprakelijkheid voor in de Verenigde Staten van Amerika of Canada veroorzaakte schade.
- Niet verzekerd is de aansprakelijkheid voor in de Verenigde Staten van Amerika of Canada geleden schade.

Let op: met de Verenigde Staten van Amerika bedoelen we ook:

- Puerto Rico, Amerikaans-Samoa, De Noordelijke Marianen, Guam en de Amerikaanse Maagdeneilanden.

5. Welke veranderingen meldt u zo snel mogelijk aan ons?

- Informatie op het polisblad klopt niet meer.
- U krijgt bedrijven of rechtspersonen in uw bezit die niet op uw polisblad staan.
- U richt een buitenlandse vestiging op.
- Een fusie of overname van uw bedrijf.
- Of van onderdelen van uw bedrijf.

Let op: deze veranderingen zijn niet automatisch verzekerd.

- Pas als wij het polisblad of de voorwaarden hebben aangepast.

6. Wat als u deze veranderingen niet zo snel mogelijk meldt?

Of u bent niet verzekerd.

- Als wij de verzekering zouden stoppen door de verandering.

Of u bent niet helemaal verzekerd.

- Als wij de voorwaarden zouden aanpassen door de verandering.
- Dit geldt ook als u geen informatie geeft als wij dat vragen.

7. Wat doet u om schade te voorkomen?

- U heeft een wachtwoordbeleid
  - Iedere gebruiker heeft een eigen account.
  - Alleen IT-administrators hebben toegang tot administrator accounts of privileged accounts.
  - Alle standaardwachtwoorden of standaardtoegangscodes worden bij het eerste gebruik direct gewijzigd en veilig bewaard.
  - Wachtwoorden bestaan uit 8 of meer tekens.
    - En bestaan uit een combinatie van minimaal drie van de volgende elementen: hoofdletters, kleine letters, speciale symbolen, cijfers.
  - U gebruikt dus geen:
    - Woordenboekwoorden (bijvoorbeeld: “wachtwoord”).
    - Opeenvolgende of herhalende tekens (bijvoorbeeld “1234”, “1111”, “abcde”).
    - Toetsenbordpatronen (bijvoorbeeld “asdfgh”).
    - Persoonlijke informatie van de gebruiker (bijvoorbeeld een geboortedatum of een naam).
- U gebruikt een firewall om uw netwerk en computersystemen te beveiligen.
- U gebruikt anti-virus-, anti-spyware- en firewallsoftware die automatisch worden geüpdatet.
  - Of vergelijkbare malware-beveiligingssoftware.
  - Als het nodig is wordt deze software wekelijks handmatig geüpdatet.

1. Algemeen

vervolg

7. Wat doet u om schade te voorkomen?

- U past updates op uw computersystemen en computernetwerken automatisch toe.
  - Of u past deze handmatig toe als dat nodig is.
  - Als die updates zijn uitgegeven om uw computersystemen of computernetwerken te beschermen.
  - Voor computersystemen of computernetwerken die met internet zijn verbonden past u de update toe binnen 30 dagen nadat de update is gepubliceerd.
  - Voor Operationele technologie (OT) en Embedded systems past u de update toe binnen 90 dagen nadat de update is gepubliceerd.
    - Of binnen de periode die de betreffende fabrikant aanbeveelt.
  - Voor andere computersystemen past u de update toe binnen 60 dagen nadat de update is gepubliceerd.
- U maakt wekelijks backups van digitale data op uw computersystemen.
  - U test regelmatig herstelprocedures van uw computersystemen.
  - U bewaart de back-up apart van uw computersystemen waarop de originele digitale data staat.
    - Bijvoorbeeld op een andere server op een andere locatie of bij een andere clouddienst.
- U vervangt software en hardware uiterlijk 3 maanden nadat de fabrikant stopte met de ondersteuning.
  - Of u zorgt voor een upgrade.
- Als u één of meerdere van bovengenoemde maatregelen aan een ander bedrijf uitbesteedt:
  - Dan staat in de overeenkomst met het andere bedrijf dat het verplicht is om de bovengenoemde maatregelen uit te voeren.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Operationele technologie (OT) = een verzameling hardware en software die de werking van een industrieel proces kan beïnvloeden.
  - OT houdt meestal toezicht op fysieke processen zoals productie, energie, geneeskunde, gebouwenbeheer en ecosystemen.
- Embedded systems = een computersysteem met een specifieke taak en ingebed in een groter systeem.
  - Bijvoorbeeld een computersysteem in medische apparatuur.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
  - Voor stroomvoorziening;
  - Voor telecommunicatie;
  - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
  - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Neemt verzekerde deze maatregelen niet? Dan is schade niet verzekerd.

1. Algemeen

8. Wie regelt de schade bij een schade die valt onder Rubriek 2 Gegevensinbreuk, Rubriek 6 Privacy aansprakelijkheid, Rubriek 7 Netwerkaansprakelijkheid en Rubriek 9 Media-aansprakelijkheid?

Wij regelen de schade en hebben hierbij de leiding.

- Wij mogen een ander rechtstreeks betalen.
- Wij mogen zelf afspraken maken met een ander.
- Alleen als u deze rubrieken afgesloten hebt.
  - Dit staat op het polisblad.

2. Gegevensinbreuk

Inhoud

Klik op de **vraag** om het antwoord te lezen

2. Gegevensinbreuk

Verzekerd

9. Wat is verzekerd?

Hulp en kosten bij een gegevensinbreuk of een vermoedelijke gegevensinbreuk.

- Gegevensinbreuk = het verliezen van vertrouwelijke informatie of persoonsgegevens uit uw computersysteem.
  - Zonder toestemming van de verantwoordelijke.
  - Daardoor zijn vertrouwelijke informatie of persoonsgegevens weg, beschadigd, toegankelijk of openbaar.
    - Ook vertrouwelijke informatie of persoonsgegevens uit uw computersysteem en geprint op papier.
  - Vertrouwelijke informatie = commercieel gevoelige bedrijfsinformatie.
    - Ook bedrijfsgeheimen.
    - Ook als niet is aangegeven dat die vertrouwelijk zijn.
  - Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
    - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
    - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
    - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Ook verzekerd bij een gegevensinbreuk op het computersysteem van een IT dienstverlener van u.
  - En dat computersysteem werd gebruikt bij aan u verleende diensten.
  - Alleen voor het deel van de schade dat met u te maken heeft.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken.
      - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

10. Welke hulp en kosten zijn verzekerd?

Een expert die de gegevensinbreuk of een vermoedelijke gegevensinbreuk voor u onderzoekt.

- De expert deelt de resultaten van het onderzoek met u.
- Wij kiezen de expert.

Een expert die de gegevensinbreuk beperkt.

- Bijvoorbeeld door getroffen gebruikersaccounts uit te schakelen of door malware te verwijderen.
- Wij kiezen de expert.

Kosten voor het documenteren van de gegevensinbreuk door de expert die de gegevensinbreuk voor u onderzoekt.

- Ook voor het opstellen van advies voor het beter beveiligen van uw computersysteem.
  - Tegen vergelijkbare gegevensinbreuken.

Een expert die uw reputatie beschermt.

- Maximaal tot het eind van de reputatiebeschermingsperiode.
  - De reputatiebeschermingsperiode staat op het polisblad.
- Alleen de kosten voor advies.
- Wij kiezen de expert.

2. Gegevensinbreuk

vervolg

10. Welke hulp en kosten zijn verzekerd?

Kosten voor het inrichten en bemannen van een crisis management centrum door experts bij een gegevensinbreuk.

- Ook kosten voor het inrichten en bemannen van een call centre.
- Alleen verzekerd als wij toestemming geven voor inschakeling.
- Wij kiezen de expert.
- Wij vergoeden de kosten tot 30 dagen nadat u de gebeurtenis bij ons meldde.

Een expert die helpt bij detectie van identiteitsdiefstal of betaalkaartfraude.

- Alleen een expert die de persoon helpt van wie de privacy is geschonden.
- Alleen verzekerd als wij schriftelijk toestemming hebben gegeven.

Hulp en kosten voor het nakomen van verplichtingen vanuit privacywetten.

- Bijvoorbeeld voor het informeren van de toezichthouder.
  - Of personen van wie de privacy is geschonden.

Vergoeding van een wettelijk verzekerbare bestuurlijke boete.

- Aan u opgelegd door de Autoriteit Persoonsgegevens in Nederland.
- Als direct gevolg van een gegevensinbreuk op uw computersysteem of het computersysteem van een IT dienstverlener.
- Niet verzekerd: een dwangsom opgelegd door een toezichthouder.

Verweer als de toezichthouder maatregelen tegen u neemt.

- Alleen bij een verzekerde gegevensinbreuk.
- En wij voor de verzekerde rechtshulp inschakelen.
  - Of vooraf toestemming geven voor inschakeling.
- En wij het verweer bepalen.
- Wij betalen dan ook de proceskosten.
  - Bijvoorbeeld kosten van experts, onderzoeken, zittingen, taxaties, inspecties en procedures.
- Niet uw eigen algemene kosten.
  - Bijvoorbeeld salarissen en overheadkosten.

11. Welk bedrag voor hulp en kosten samen is verzekerd?

Wij betalen maximaal het verzekerd bedrag per gebeurtenis.

- Het verzekerd bedrag staat op het polisblad.
- Dit geldt voor alle verzekerden samen.
- Dit geldt voor alle rubrieken samen.
- Houden meerdere gebeurtenissen verband met 1 oorzaak? Dan tellen we die gebeurtenissen als 1 gebeurtenis.

Per verzekeringsjaar betalen wij een maximaal bedrag.

- Dit bedrag staat op het polisblad.
- Dit geldt voor alle verzekerden samen.
  - Het moment van de 1e melding bepaalt bij welk verzekeringsjaar de gebeurtenis hoort.
- Dit geldt voor alle rubrieken samen.

Let op: u betaalt eerst een eigen risico.

- Het eigen risico per verzekerde gebeurtenis staat op het polisblad.
- U betaalt geen eigen risico voor hulp door een expert tijdens de eerste 48 uur nadat u de gebeurtenis aan ons meldde.

2. Gegevensinbreuk

12. Welke kosten zijn boven het verzekerd bedrag verzekerd?

Kosten van experts.

- Alleen voor het bepalen van de hoogte van de schade.
- De kosten van onze expert.
- De kosten van de expert van verzekerde tot en met de kosten van onze expert.
  - Rekent de expert van verzekerde meer? Dan blijven die extra kosten voor rekening van verzekerde.
- De kosten van de 3e expert.
- Alle experts zijn ingeschreven in het register van het Nederlands Instituut Van Register Experts (NIVRE).
  - Of bij een vergelijkbare beroepsorganisatie.
    - En in de statuten en reglementen van deze organisatie:
      - Staat een duidelijke klacht- en tuchtprocedure.
      - Zijn de eisen beschreven voor permanente opleiding van experts.
  - Alle experts houden zich aan de Gedragscode schade-expertiseorganisaties van het Verbond van Verzekeraars.

Voldoet een expert niet aan deze eisen? Dan zijn de kosten van die expert niet verzekerd.

Let op: we betalen alleen als deze kosten noodzakelijk zijn door een schade die verzekerd is.

2. Gegevensinbreuk

Niet verzekerd

Kijk ook in de algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Sanctiewet 1977.
- Ernstige conflicten (molest).
- Atoomkernreacties.
- Fraude.
- Terrorisme.
- Niet nakomen voorwaarden.

Per situatie staat in de algemene voorwaarden precies wat nooit verzekerd is.

Hieronder staat wat verder niet verzekerd is bij uw cyberverzekering.

13. Wanneer bent u niet verzekerd?

Als wij volgens wet- of regelgeving u niet mogen verzekeren voor de hulp, schade of de kosten.

Als de gebeurtenis voor het begin van de verzekering plaatsvond.

- En de verzekerde de gebeurtenis had kunnen of moeten ontdekken.

14. Welke schade is niet verzekerd?

Schade door een cyberoperatie.

Cyberoperatie =

- Het gebruik van een computersysteem door een soevereine staat.
  - Ook: het gebruik van een computersysteem op aanwijzing van een soevereine staat.
  - Ook: het gebruik van een computersysteem onder controle van een soevereine staat.
    - Met als doel om een ander computersysteem te verstoren.
    - En/of de toegang tot dat computersysteem te blokkeren.
    - En/of de functionaliteit ervan te verminderen.
    - En/of data in een computersysteem te kopiëren, verwijderen, vernietigen, wijzigen of te blokkeren.
- Alleen als wij bewijzen dat het een cyberoperatie is.
  - Wij kijken naar elk beschikbaar, redelijk en objectief bewijs.
    - Bijvoorbeeld: de regering van de staat, waarin de getroffen computersystemen zich fysiek bevinden, geeft een verklaring uit waarin de cyberoperatie aan een andere soevereine staat wordt toegeschreven.
      - Of wordt toegeschreven aan personen die op aanwijzing of onder controle van een andere soevereine staat handelden.

Soevereine staat = een land dat binnen het grondgebied het hoogste gezag voert.

- En dat niet afhankelijk is van een andere staat.

Schade door terrorisme.

- Kijk ook in onze algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Wel verzekerd schade door cyberterrorisme.
  - Cyberterrorisme = Toegang krijgen tot of beschadigen, vernietigen, verstoren van uw computersystemen of computernetwerken door een of meerdere personen die dat doen met een politiek, religieus, ideologisch of politiek doel.

2. Gegevensinbreuk

vervolg

14. Welke schade is niet verzekerd?

Schade doordat apparatuur of een installatie van een ander niet of niet goed werkt.

- Apparaten en installaties die ervoor zorgen dat de energievoorziening blijft werken.
  - De energievoorziening van computersystemen en gegevensopslag.
  - Bijvoorbeeld, noodstroomvoorzieningen en stand-alone-generatoren.
- Airconditioning.
- Wel verzekerd als apparatuur of installatie van een IT dienstverlener niet goed werkt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade door gevaarlijke, verontreinigende of vervuilende stoffen.

Schade doordat uw computersysteem in beslag wordt genomen.

- Door een instantie die dat mag doen volgens de wet.
  - Bijvoorbeeld de overheid, een toezichthouder of een rechtbank.

Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.

- Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
- Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
- Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Verlies van zaken.

- En de directe gevolgen daarvan.
- Ook als zaken kapot, weg of verontreinigd zijn.
- Zaken=losse spullen, onroerend goed of dieren.

Schade aan personen.

- Verwonding, ziekte (lichamelijk of geestelijk) of overlijden.
- En de directe gevolgen daarvan.

Diefstal, schending of openbaarmaking van intellectueel eigendom.

- Bijvoorbeeld patenten, handelsmerken of auteursrechten.

Beleggingsverliezen of handelsverliezen.

- Bijvoorbeeld als het niet meer lukt om effecten te verkopen.

Schade door geplande stilstand van uw computersystemen.

- Of van onderdelen van uw computersystemen.

Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.

- Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
- Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
- Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Betalingen die u doet om goede wil te tonen.

- Bijvoorbeeld kortingen, vouchers of coulancebetalingen.

2. Gegevensinbreuk

vervolg

14. Welke schade is niet verzekerd?

Schade aan branded currency of cryptogeld.

Branded currency = combinatie van digitale betaalmiddelen of loyaliteitspunten uitgevoerd via een digitale mobiele portemonnee. En uniek voor een bepaalde winkelketen of webshop.

- Bijvoorbeeld een digitale cadeaukaart, digitale coupons of digitale promotiecodes.

Cryptogeld = digitaal geld dat niet wordt uitgegeven door een bank. Cryptogeld zit in een digitale portemonnee.

- Bijvoorbeeld: bitcoins

Ook niet verzekerd: verlies van branded currency of cryptogeld.

15. Bij welk gedrag bent u niet verzekerd?

Bij opzet van verzekerde of uw IT dienstverlener.

Verzekerde heeft geen dekking als verzekerde of de IT dienstverlener in strijd met het recht met opzet iets doet of niet doet waardoor schade ontstaat. De in feite toegebrachte schade is hierbij een te verwachten of normaal gevolg van wat een verzekerde of de IT dienstverlener doet of niet doet. Heeft verzekerde geen dekking? Dan heeft verzekerde dat ook niet voor de schade die mogelijk later nog ontstaat.

In welke gevallen geldt de opzetuitsluiting?

De uitsluiting geldt als verzekerde of de IT dienstverlener zich maatschappelijk ongewenst of crimineel gedraagt. Dat is in ieder geval zo bij gedragingen die een gevaar voor personen of zaken kunnen opleveren, zoals:

- Brandstichting, vernieling en beschadiging.
- Afpersing, bedrog, oplichting, bedreiging, beroving, verduistering, diefstal en inbraak. Ook als verzekerde of de IT dienstverlener dat met een computer of ander (technisch) hulpmiddel doet.
- Geweldpleging, mishandeling, doodslag en moord.

Er is sprake van opzet als verzekerde of de IT dienstverlener iets doet of niet doet waarbij verzekerde:

- De bedoeling heeft schade te veroorzaken (opzet als oogmerk).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener zeker weet dat er schade ontstaat (opzet met zekerheidsbewustzijn).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener de aanmerkelijke kans dat er schade ontstaat voor lief neemt. En toch handelt verzekerde (niet) zo (voorwaardelijk opzet).

Opzet wordt objectief uit de feiten, omstandigheden en/of gedragingen van verzekerde of de IT dienstverlener afgeleid.

Deze opzetuitsluiting geldt ook bij:

- Groepsaansprakelijkheid.
  - Als verzekerde niet zelf maar wel iemand in een groep waarvan verzekerde deel uitmaakt iets doet of niet doet.
- Alcohol en drugs.
  - Als verzekerde zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat verzekerde zijn eigen wil niet meer kon bepalen. Of als iemand in een groep waarvan verzekerde deel uitmaakt zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat hij of zij de eigen wil niet meer kon bepalen.

2. Gegevensinbreuk

vervolg

15. Bij welk gedrag bent u niet verzekerd?

IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.

- Maar niet een dienstverlener:
  - Voor stroomvoorziening;
  - Voor telecommunicatie;
  - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade doordat de verzekerde seksueel of seksueel getint gedrag vertoont.

- Geldt alleen voor de verzekerde die het gedrag vertoont.
- Alleen of in een groep.
  - Ook niet verzekerd: als verzekerde zelf niets doet.
  - Maar wel deel uitmaakt van een groep die dit gedrag vertoont.

Als u niet goed samenwerkt met de toezichthouder.

- Om te voorkomen dat een cyberincident of gegevensinbreuk plaatsvindt.
- Om te voorkomen dat aanspraak tegen u wordt ingediend.
- Om te voorkomen dat de toezichthouder u een straf of maatregel oplegt.
  - Als gevolg van een cyberincident, gegevensinbreuk of aanspraak.

Als u niet betaalt voor diensten of producten.

- En daardoor ontstaat schade of ontstaan kosten voor u of een ander.
- Bijvoorbeeld als u een leaseovereenkomst of licentie niet verlengt.
- Ook niet verzekerd als een IT dienstverlener van u niet betaalt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
      - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

2. Gegevensinbreuk

vervolg

15. Bij welk gedrag bent u niet verzekerd?

Als u zich niet houdt aan de preventieafspraken.

En de schade is hierdoor veroorzaakt of verergerd.

Preventieafspraken =

- U heeft een wachtwoordbeleid
  - Iedere gebruiker heeft een eigen account.
  - Alleen IT-administrators hebben toegang tot administrator accounts of privileged accounts.
  - Alle standaardwachtwoorden of standaardtoegangscodes worden bij het eerste gebruik direct gewijzigd en veilig bewaard.
  - Wachtwoorden bestaan uit 8 of meer tekens.
    - En bestaan uit een combinatie van minimaal drie van de volgende elementen: hoofdletters, kleine letters, speciale symbolen, cijfers.
  - U vermijdt gebruik van:
    - Woordenboekwoorden (bijvoorbeeld: “wachtwoord”).
    - Opeenvolgende of herhalende tekens (bijvoorbeeld “1234”, “1111”, “abcde”).
    - Toetsenbordpatronen (bijvoorbeeld “asdfgh”).
    - Persoonlijke informatie van de gebruiker (bijvoorbeeld een geboortedatum of een naam).
- U gebruikt een firewall om uw netwerk en computersystemen te beveiligen.
- U gebruikt anti-virus-, anti-spyware- en firewallsoftware die automatisch worden geüpdatet.
  - Of vergelijkbare malware-beveiligingssoftware.
  - Als het nodig is wordt deze software wekelijks handmatig geüpdatet.
- U past updates op uw computersystemen en computernetwerken automatisch toe.
  - Of u past deze handmatig toe als dat nodig is.
  - Als die updates zijn uitgegeven om uw computersystemen of computernetwerken te beschermen.
  - Voor computersystemen of computernetwerken die met internet zijn verbonden past u de update toe binnen 30 dagen nadat de update is gepubliceerd.
  - Voor Operationele technologie (OT) en Embedded systems past u de update toe binnen 90 dagen nadat de update is gepubliceerd.
  - Of binnen de periode die de betreffende fabrikant aanbeveelt.
- Voor andere computersystemen past u de update toe binnen 60 dagen nadat de update is gepubliceerd.
- U maakt wekelijks backups van digitale data op uw computersystemen.
- U test regelmatig herstelprocedures van uw computersystemen.
- U bewaart de back-up apart van uw computersystemen waarop de originele digitale data staat.
  - Bijvoorbeeld op een andere server op een andere locatie of bij een andere clouddienst.
- U vervangt software en hardware uiterlijk 3 maanden nadat de fabrikant stopte met de ondersteuning.
  - Of u zorgt voor een upgrade.

2. Gegevensinbreuk

vervolg

15. Bij welk gedrag bent u niet verzekerd?

- Als u één of meerdere van bovengenoemde maatregelen aan een ander bedrijf uitbesteedt:
  - Dan staat in de overeenkomst met het andere bedrijf dat het verplicht is om de bovengenoemde maatregelen uit te voeren.
    - Wel verzekerd als u bewijst dat u zich per ongeluk niet hield aan de preventieafspraken.
      - Bijvoorbeeld als de schade wordt veroorzaakt of verergerd omdat u in de week van de gebeurtenis geen back-up maakte.
      - En u bewijst dat u in de periode voor de gebeurtenis wel altijd een back-up maakte.
      - En u bewijst dat de back-up tijdens de gebeurtenis niet gemaakt is door een technische storing waar u niets aan kon doen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Operationele technologie (OT) = een verzameling hardware en software die de werking van een industrieel proces kan beïnvloeden.
  - OT houdt meestal toezicht op fysieke processen zoals productie, energie, geneeskunde, gebouwenbeheer en ecosystemen.
- Embedded systems = een computersysteem met een specifieke taak en ingebed in een groter systeem.
  - Bijvoorbeeld een computersysteem in medische apparatuur.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

2. Gegevensinbreuk

Bij schade

16. Wanneer meldt een verzekerde een gebeurtenis?

Zo snel mogelijk.

- Meld een gebeurtenis bij ons.
  - Een verzekerde meldt het ook als hij een gebeurtenis vermoedt.

17. Wat doet een verzekerde bij schade?

- De verzekerde meldt de schade zo snel mogelijk.
- De verzekerde werkt mee aan de afhandeling van de schade.
- De verzekerde doet alles om de schade zo veel mogelijk te beperken.
- De verzekerde geeft ons alle informatie die nodig is om de omvang en de oorzaak van de schade vast te stellen.
- De verzekerde bewaart alle hardware, software en gegevens.
  - En geeft die voor onderzoek aan ons of een expert als dat nodig is.
- De verzekerde doet aangifte bij de politie bij een strafbaar feit.
  - Bijvoorbeeld bij cyberafpersing.
- De verzekerde helpt ons de betaalde schadevergoeding bij een ander terug te halen.
- De verzekerde geeft alle verzekeringen op die deze schade verzekeren.
- De verzekerde tekent een geheimhoudingsverklaring als de incident response provider daarom vraagt.
  - Tekent u niet? Dan kunnen wij uw schade mogelijk niet of niet volledig afhandelen.

18. Wie bepaalt de hoogte van het schadebedrag?

Of: wij.

Of: onze expert.

Of: onze expert met een expert van de verzekerde.

- Voor zij starten, kiezen zij een 3e expert.
  - Die bepaalt de schade als zij het oneens zijn.
  - Hij bepaalt de schade tussen het laagste en hoogste bedrag.
- Alle experts zijn ingeschreven in het register van het Nederlands Instituut Van Register Experts (NIVRE).
  - Of bij een vergelijkbare beroepsorganisatie.
    - En in de statuten en reglementen van deze organisatie:
      - Staat een duidelijke klacht- en tuchtprocedure.
      - Zijn de eisen beschreven voor permanente opleiding van experts.
  - Alle experts houden zich aan de Gedragscode schade-expertiseorganisaties van het Verbond van Verzekeraars.

Let op: dat wij het schadebedrag bepalen, betekent niet dat we de schade betalen.

19. Wat als een verzekerde ook op een andere verzekering is verzekerd?

De andere verzekering gaat voor.

- Als de verzekerde daarop verzekerd is of verzekerd zou zijn als onze verzekering niet zou bestaan.
- Wij betalen de schade boven het maximale bedrag van de andere verzekering.
  - Wij betalen niet uw eigen risico bij de andere verzekering.

20. Wat als bij schade blijkt dat deze verzekering in strijd is met wet- en regelgeving?

Wij houden ons altijd aan de wet- en regelgeving die van toepassing is.

- We zoeken dan naar een oplossing die in lijn is met deze verzekering.

3. Herstel

Inhoud

Klik op de **vraag** om het antwoord te lezen

3. Herstel

Verzekerd

21. Wat is verzekerd?

Kosten voor een expert die het cyberincident of een vermoeden van een cyberincident voor u onderzoekt.

- De expert deelt de resultaten van het onderzoek met u.
- Wij kiezen de expert.

Kosten voor een expert die het cyberincident beperkt.

- Bijvoorbeeld door getroffen gebruikersaccounts uit te schakelen of door malware te verwijderen.
- Wij kiezen de expert.

Kosten voor het documenteren van het cyberincident door de expert die het cyberincident voor u onderzoekt.

- Ook voor het opstellen van advies voor het beter beveiligen van uw computersysteem.
  - Tegen vergelijkbare cyberincidenten.

Kosten voor het inrichten en bemannen van een crisis management centrum door experts bij een cyberincident.

- Ook kosten voor het inrichten en bemannen van een call centre.
- Alleen verzekerd als wij toestemming geven voor inschakeling.
- Wij kiezen de expert.
- Wij vergoeden de kosten tot 30 dagen nadat u de gebeurtenis bij ons meldde.

Herstelkosten bij een cyberincident.

- Cyberincident =
  - Malware op uw computersystemen of computernetwerk.
    - Software of code die is ontworpen om:
      - Schade te veroorzaken aan uw computersysteem of computernetwerk.
      - De werking van uw computersysteem of computernetwerk te verstoren.
      - Toegang te krijgen tot uw computersysteem of computernetwerk.
    - Bijvoorbeeld spyware, ransomware, virussen of Trojaanse paarden.
  - Iemand anders breekt in in uw computersysteem of computernetwerk.
    - Met als doel om schade te maken aan uw computersysteem of computernetwerk.
      - U gaf hiervoor geen toestemming.
    - Of als doel om toegang te krijgen tot uw computersysteem of computernetwerk.
      - U gaf hiervoor geen toestemming.
    - Of om gegevens op uw computersysteem of computernetwerk te openbaren.
      - U gaf hiervoor geen toestemming.
  - DoS-aanval.
    - Iemand overbelast bewust uw computersysteem of computernetwerk.
      - Waardoor uw computersysteem of computernetwerk niet of niet meer goed werkt.
    - Ook DDoS-aanvallen.
  - Diefstal van digitale data.
  - Menselijke fout van uw medewerker of een medewerker van een IT dienstverlener.
    - Bij het bedienen van uw computersysteem of het computersysteem van de IT dienstverlener.
    - Bijvoorbeeld de keuze voor verkeerde software, een programmeerfout, of een installatiefout.

3. Herstel

vervolg

21. Wat is verzekerd?

- Ook verzekerd als het cyberincident plaatsvond op het computersysteem van een IT dienstverlener van u.
  - En dat computersysteem werd gebruikt bij aan u verleende diensten.
  - Alleen voor het deel van de schade dat met u te maken heeft.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
      - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.

- Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
- Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
- Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

22. Welke kosten zijn verzekerd bij een cyberincident?

Uw kosten om uw software en computersysteem te configureren.

Uw kosten om uw digitale data, software en computersysteem te herstellen.

- Zodat uw computersysteem of computernetwerk weer zo goed mogelijk werkt.
  - Zo dichtbij mogelijk de situatie zoals die was vlak voordat het cyberincident plaatsvond.

  Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Niet verzekerd zijn de kosten voor verbeteringen van uw computersysteem of van data.

Uw kosten om uw hardware te vervangen.

- Om uw activiteiten weer op te kunnen starten.
- Alleen als het vervangen goedkoper en efficiënter is dan het herstellen of opnieuw configureren van uw computersysteem.
  - Alleen als een expert dat vaststelt.
    - Wij kiezen de expert.
- En alleen als de vervangende hardware van gelijke standaard en functionaliteit is als uw hardware vóór het cyberincident.

Niet verzekerd: de kosten voor vervangen van hardware in operationele technologie (OT) en embedded systems.

- Operationele technologie (OT) = een verzameling hardware en software die de werking van een industrieel proces kan beïnvloeden.
  - OT houdt meestal toezicht op fysieke processen zoals productie, energie, geneeskunde, gebouwenbeheer en ecosystemen.
- Embedded systems = een computersysteem met een specifieke taak en ingebed in een groter systeem.
  - Bijvoorbeeld een computersysteem in medische apparatuur.

3. Herstel

23. Welk bedrag voor hulp en kosten samen is verzekerd?

Wij betalen maximaal het verzekerd bedrag per gebeurtenis.

- Het verzekerd bedrag staat op het polisblad.
- Dit geldt voor alle verzekerden samen.
- Dit geldt voor alle rubrieken samen.
- Houden meerdere gebeurtenissen verband met 1 oorzaak? Dan tellen we die gebeurtenissen als 1 gebeurtenis.

Per verzekeringsjaar betalen wij een maximaal bedrag.

- Dit bedrag staat op het polisblad.
- Dit geldt voor alle verzekerden samen.
  - Het moment van de 1e melding bepaalt bij welk verzekeringsjaar de gebeurtenis hoort.
- Dit geldt voor alle rubrieken samen.

Let op: u betaalt eerst een eigen risico.

- Het eigen risico per verzekerde gebeurtenis staat op het polisblad.

24. Welke kosten zijn boven het verzekerd bedrag verzekerd?

Kosten van experts.

- Alleen voor het bepalen van de hoogte van de schade.
- De kosten van onze expert.
- De kosten van de expert van verzekerde tot en met de kosten van onze expert.
  - Rekent de expert van verzekerde meer? Dan blijven die extra kosten voor rekening van verzekerde.
- De kosten van de 3e expert.
- Alle experts zijn ingeschreven in het register van het Nederlands Instituut Van Register Experts (NIVRE).
  - Of bij een vergelijkbare beroepsorganisatie.
    - En in de statuten en reglementen van deze organisatie:
      - Staat een duidelijke klacht- en tuchtprocedure.
      - Zijn de eisen beschreven voor permanente opleiding van experts.
  - Alle experts houden zich aan de Gedragscode schade-expertiseorganisaties van het Verbond van Verzekeraars.

  Voldoet een expert niet aan deze eisen? Dan zijn de kosten van die expert niet verzekerd.

Let op: we betalen alleen als deze kosten noodzakelijk zijn door een schade die verzekerd is.

3. Herstel

Niet verzekerd

Kijk ook in de algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Sanctiewet 1977.
- Ernstige conflicten (molest).
- Atoomkernreacties.
- Fraude.
- Terrorisme.
- Niet nakomen voorwaarden.

Per situatie staat in de algemene voorwaarden precies wat nooit verzekerd is.

Hieronder staat wat verder niet verzekerd is bij uw cyberverzekering.

25. Wanneer bent u niet verzekerd?

Als wij volgens wet- of regelgeving u niet mogen verzekeren voor de hulp, schade of de kosten. Als de gebeurtenis voor het begin van de verzekering plaatsvond.

- En de verzekerde de gebeurtenis had kunnen of moeten ontdekken.

26. Welke schade is niet verzekerd?

Schade door een cyberoperatie.

Cyberoperatie =

- Het gebruik van een computersysteem door een soevereine staat.
  - Ook: het gebruik van een computersysteem op aanwijzing van een soevereine staat.
  - Ook: het gebruik van een computersysteem onder controle van een soevereine staat.
    - Met als doel om een ander computersysteem te verstoren.
    - En/of de toegang tot dat computersysteem te blokkeren.
    - En/of de functionaliteit ervan te verminderen.
    - En/of data in een computersysteem te kopiëren, verwijderen, vernietigen, wijzigen of te blokkeren.
- Alleen als wij bewijzen dat het een cyberoperatie is.
  - Wij kijken naar elk beschikbaar, redelijk en objectief bewijs.
    - Bijvoorbeeld: de regering van de staat, waarin de getroffen computersystemen zich fysiek bevinden, geeft een verklaring uit waarin de cyberoperatie aan een andere soevereine staat wordt toegeschreven.
      - Of wordt toegeschreven aan personen die op aanwijzing of onder controle van een andere soevereine staat handelden.

Soevereine staat = een land dat binnen het grondgebied het hoogste gezag voert.

- En dat niet afhankelijk is van een andere staat.

Schade door terrorisme.

- Kijk ook in onze algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Wel verzekerd schade door cyberterrorisme.
  - Cyberterrorisme = Toegang krijgen tot of beschadigen, vernietigen, verstoren van uw computersystemen of computernetwerken door een of meerdere personen die dat doen met een politiek, religieus, ideologisch of politiek doel.

3. Herstel

vervolg

26. Welke schade is niet verzekerd?

Schade doordat apparatuur of een installatie van een ander niet of niet goed werkt.

- Apparaten en installaties die ervoor zorgen dat de energievoorziening blijft werken.
  - De energievoorziening van computersystemen en gegevensopslag.
  - Bijvoorbeeld, noodstroomvoorzieningen en stand-alone-generatoren.
- Airconditioning.
- Wel verzekerd als apparatuur of installatie van een IT dienstverlener niet goed werkt.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
      - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade door gevaarlijke, verontreinigende of vervuilende stoffen.

Schade doordat uw computersysteem in beslag wordt genomen.

- Door een instantie die dat mag doen volgens de wet.
  - Bijvoorbeeld de overheid, een toezichthouder of een rechtbank.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Verlies van zaken.

- En de directe gevolgen daarvan.
- Ook als zaken kapot, weg of verontreinigd zijn.
- Zaken = losse spullen, onroerend goed of dieren.

Schade aan personen.

- Verwonding, ziekte (lichamelijk of geestelijk) of overlijden.
  - En de directe gevolgen daarvan.

Diefstal, schending of openbaarmaking van intellectueel eigendom.

- Bijvoorbeeld patenten, handelsmerken of auteursrechten.

Boetes en schadevergoedingen opgelegd door overheid of toezichthouder.

Beleggingsverliezen of handelsverliezen.

- Bijvoorbeeld als het niet meer lukt om effecten te verkopen.

Schade door geplande stilstand van uw computersystemen.

- Of van onderdelen van uw computersystemen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Betalingen die u doet om goede wil te tonen.

- Bijvoorbeeld kortingen, vouchers of coulancebetalingen.

3. Herstel

vervolg

26. Welke schade is niet verzekerd?

Schade aan branded currency of cryptogeld.

Branded currency = combinatie van digitale betaalmiddelen of loyaliteitspunten uitgevoerd via een digitale mobiele portemonnee. En uniek voor een bepaalde winkelketen of webshop.

- Bijvoorbeeld een digitale cadeaukaart, digitale coupons of digitale promotiecodes.

Cryptogeld = digitaal geld dat niet wordt uitgegeven door een bank. Cryptogeld zit in een digitale portemonnee.

- Bijvoorbeeld: bitcoins

Ook niet verzekerd: verlies van branded currency of cryptogeld.

27. Bij welk gedrag bent u niet verzekerd?

Bij opzet van verzekerde of uw IT dienstverlener.

Verzekerde heeft geen dekking als verzekerde of de IT dienstverlener in strijd met het recht met opzet iets doet of niet doet waardoor schade ontstaat. De in feite toegebrachte schade is hierbij een te verwachten of normaal gevolg van wat een verzekerde of de IT dienstverlener doet of niet doet. Heeft verzekerde geen dekking? Dan heeft verzekerde dat ook niet voor de schade die mogelijk later nog ontstaat.

In welke gevallen geldt de opzetuitsluiting?

De uitsluiting geldt als verzekerde of de IT dienstverlener zich maatschappelijk ongewenst of crimineel gedraagt. Dat is in ieder geval zo bij gedragingen die een gevaar voor personen of zaken kunnen opleveren, zoals:

- Brandstichting, vernieling en beschadiging.
- Afpersing, bedrog, oplichting, bedreiging, beroving, verduistering, diefstal en inbraak. Ook als verzekerde of de IT dienstverlener dat met een computer of ander (technisch) hulpmiddel doet.
- Geweldpleging, mishandeling, doodslag en moord.

Er is sprake van opzet als verzekerde of de IT dienstverlener iets doet of niet doet waarbij verzekerde:

- De bedoeling heeft schade te veroorzaken (opzet als oogmerk).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener zeker weet dat er schade ontstaat (opzet met zekerheidsbewustzijn).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener de aanmerkelijke kans dat er schade ontstaat voor lief neemt. En toch handelt verzekerde (niet) zo (voorwaardelijk opzet).

Opzet wordt objectief uit de feiten, omstandigheden en/of gedragingen van verzekerde of de IT dienstverlener afgeleid.

Deze opzetuitsluiting geldt ook bij:

- Groepsaansprakelijkheid.
  - Als verzekerde niet zelf maar wel iemand in een groep waarvan verzekerde deel uitmaakt iets doet of niet doet.
- Alcohol en drugs.
  - Als verzekerde zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat verzekerde zijn eigen wil niet meer kon bepalen. Of als iemand in een groep waarvan verzekerde deel uitmaakt zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat hij of zij de eigen wil niet meer kon bepalen.

3. Herstel

vervolg

27. Bij welk gedrag bent u niet verzekerd?

IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.

- Maar niet een dienstverlener:
  - Voor stroomvoorziening;
  - Voor telecommunicatie;
  - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade doordat de verzekerde seksueel of seksueel getint gedrag vertoont.

- Geldt alleen voor de verzekerde die het gedrag vertoont.
- Alleen of in een groep.
  - Ook niet verzekerd: als verzekerde zelf niets doet.
  - Maar wel deel uitmaakt van een groep die dit gedrag vertoont.

Als u niet goed samenwerkt met de toezichthouder.

- Om te voorkomen dat een cyberincident of gegevensinbreuk plaatsvindt.
- Om te voorkomen dat aanspraak tegen u wordt ingediend.
- Om te voorkomen dat de toezichthouder u een straf of maatregel oplegt.
  - Als gevolg van een cyberincident, gegevensinbreuk of aanspraak.

Als u niet betaalt voor diensten of producten.

- En daardoor ontstaat schade of ontstaan kosten voor u of een ander.
- Bijvoorbeeld als u een leaseovereenkomst of licentie niet verlengt.
- Ook niet verzekerd als een IT dienstverlener van u niet betaalt.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
      - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

3. Herstel

vervolg

27. Bij welk gedrag bent u niet verzekerd?

Als u zich niet houdt aan de preventieafspraken.

En de schade is hierdoor veroorzaakt of verergerd.

Preventieafspraken =

- U heeft een wachtwoordbeleid
  - Iedere gebruiker heeft een eigen account.
  - Alleen IT-administrators hebben toegang tot administrator accounts of privileged accounts.
  - Alle standaardwachtwoorden of standaardtoegangscodes worden bij het eerste gebruik direct gewijzigd en veilig bewaard.
  - Wachtwoorden bestaan uit 8 of meer tekens.
    - En bestaan uit een combinatie van minimaal drie van de volgende elementen: hoofdletters, kleine letters, speciale symbolen, cijfers.
  - U vermijdt gebruik van:
    - Woordenboekwoorden (bijvoorbeeld: “wachtwoord”).
    - Opeenvolgende of herhalende tekens (bijvoorbeeld “1234”, “1111”, “abcde”).
    - Toetsenbordpatronen (bijvoorbeeld “asdfgh”).
    - Persoonlijke informatie van de gebruiker (bijvoorbeeld een geboortedatum of een naam).
- U gebruikt een firewall om uw netwerk en computersystemen te beveiligen.
- U gebruikt anti-virus-, anti-spyware- en firewallsoftware die automatisch worden geüpdatet.
  - Of vergelijkbare malware-beveiligingssoftware.
  - Als het nodig is wordt deze software wekelijks handmatig geüpdatet.
- U past updates op uw computersystemen en computernetwerken automatisch toe.
  - Of u past deze handmatig toe als dat nodig is.
  - Als die updates zijn uitgegeven om uw computersystemen of computernetwerken te beschermen.
  - Voor computersystemen of computernetwerken die met internet zijn verbonden past u de update toe binnen 30 dagen nadat de update is gepubliceerd.
  - Voor Operationele technologie (OT) en Embedded systems past u de update toe binnen 90 dagen nadat de update is gepubliceerd.
  - Of binnen de periode die de betreffende fabrikant aanbeveelt.
  - Voor andere computersystemen past u de update toe binnen 60 dagen nadat de update is gepubliceerd.
- U maakt wekelijks backups van digitale data op uw computersystemen.
- U test regelmatig herstelprocedures van uw computersystemen.
- U bewaart de back-up apart van uw computersystemen waarop de originele digitale data staat.
  - Bijvoorbeeld op een andere server op een andere locatie of bij een andere clouddienst.
- U vervangt software en hardware uiterlijk 3 maanden nadat de fabrikant stopte met de ondersteuning.
  - Of u zorgt voor een upgrade.

3. Herstel

vervolg

27. Bij welk gedrag bent u niet verzekerd?

Als u één of meerdere van bovengenoemde maatregelen aan een ander bedrijf uitbesteedt:

- Dan staat in de overeenkomst met het andere bedrijf dat het verplicht is om de bovengenoemde maatregelen uit te voeren.
  - Wel verzekerd als u bewijst dat u zich per ongeluk niet hield aan de preventieafspraken.
    - Bijvoorbeeld als de schade wordt veroorzaakt of verergerd omdat u in de week van de gebeurtenis geen back-up maakte.
    - En u bewijst dat u in de periode voor de gebeurtenis wel altijd een back-up maakte.
    - En u bewijst dat de back-up tijdens de gebeurtenis niet gemaakt is door een technische storing waar u niets aan kon doen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Operationele technologie (OT) = een verzameling hardware en software die de werking van een industrieel proces kan beïnvloeden.
  - OT houdt meestal toezicht op fysieke processen zoals productie, energie, geneeskunde, gebouwenbeheer en ecosystemen.
- Embedded systems = een computersysteem met een specifieke taak en ingebed in een groter systeem.
  - Bijvoorbeeld een computersysteem in medische apparatuur.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

3. Herstel

Bij schade

28. Wanneer meldt een verzekerde een gebeurtenis?

Zo snel mogelijk.

- Meld een gebeurtenis bij ons.
  - Een verzekerde meldt het ook als hij een gebeurtenis vermoedt .

29. Wat doet een verzekerde bij schade?

- De verzekerde meldt de schade zo snel mogelijk.
- De verzekerde werkt mee aan de afhandeling van de schade.
- De verzekerde doet alles om de schade zo veel mogelijk te beperken.
- De verzekerde geeft ons alle informatie die nodig is om de omvang en de oorzaak van de schade vast te stellen.
- De verzekerde bewaart alle hardware, software en gegevens.
  - En geeft die voor onderzoek aan ons of een expert als dat nodig is.
- De verzekerde doet aangifte bij de politie bij een strafbaar feit.
  - Bijvoorbeeld bij cyberafpersing.
- De verzekerde helpt ons de betaalde schadevergoeding bij een ander terug te halen.
- De verzekerde geeft alle verzekeringen op die deze schade verzekeren.
- De verzekerde tekent een geheimhoudingsverklaring als de incident response provider daarom vraagt.
  - Tekent u niet? Dan kunnen wij de schade mogelijk niet of niet volledig afhandelen.

30. Wie bepaalt de hoogte van het schadebedrag?

Of: wij.

Of: onze expert.

Of: onze expert met een expert van de verzekerde.

- Voor zij starten, kiezen zij een 3e expert.
  - Die bepaalt de schade als zij het oneens zijn.
  - Hij bepaalt de schade tussen het laagste en hoogste bedrag.
- Alle experts zijn ingeschreven in het register van het Nederlands Instituut Van Register Experts (NIVRE).
  - Of bij een vergelijkbare beroepsorganisatie.
    - En in de statuten en reglementen van deze organisatie:
      - Staat een duidelijke klacht- en tuchtprocedure.
      - Zijn de eisen beschreven voor permanente opleiding van experts.
  - Alle experts houden zich aan de Gedragscode schade-expertiseorganisaties van het Verbond van Verzekeraars.

Let op: dat wij het schadebedrag bepalen, betekent niet dat we de schade betalen.

31. Wat als een verzekerde ook op een andere verzekering is verzekerd?

De andere verzekering gaat voor.

- Als de verzekerde daarop verzekerd is of verzekerd zou zijn als onze verzekering niet zou bestaan.
- Wij betalen de schade boven het maximale bedrag van de andere verzekering.
  - Wij betalen niet uw eigen risico bij de andere verzekering.

32. Wat als bij schade blijkt dat deze verzekering in strijd is met wet- en regelgeving?

- Wij houden ons altijd aan de wet- en regelgeving die van toepassing is.
- We zoeken dan naar een oplossing die in lijn is met deze verzekering.

4. Bedrijfsschade

Inhoud

Klik op de **vraag** om het antwoord te lezen

4. Bedrijfsschade

Verzekerd

33. Wat is verzekerd?

Kosten voor een expert die het cyberincident of een vermoeden van een cyberincident voor u onderzoekt.

- De expert deelt de resultaten van het onderzoek met u.
- Wij kiezen de expert.

Kosten voor een expert die het cyberincident beperkt.

- Bijvoorbeeld door getroffen gebruikersaccounts uit te schakelen of door malware te verwijderen.
- Wij kiezen de expert.

Kosten voor het documenteren van het cyberincident door de expert die het cyberincident voor u onderzoekt.

- Ook voor het opstellen van advies voor het beter beveiligen van uw computersysteem.
  - Tegen vergelijkbare cyberincidenten.

Kosten voor het inrichten en bemannen van een crisis management centrum door experts bij een cyberincident.

- Ook kosten voor het inrichten en bemannen van een call centre.
- Alleen verzekerd als wij toestemming geven voor inschakeling.
- Wij kiezen de expert.
- Wij vergoeden de kosten tot 30 dagen nadat u de gebeurtenis bij ons meldde.

Bedrijfsschade door een cyberincident.

- Bedrijfsschade = brutowinst die u misloopt door omzet- of productverlies.
  - Doordat uw computersysteem of uw digitale data door het cyberincident volledig of gedeeltelijk onbeschikbaar zijn.
    - Of doordat uw computersysteem of uw digitale data door het cyberincident minder goed werken dan direct voor het cyberincident.
  - Brutowinst = het verschil tussen de omzet en de variabele kosten.
    - Of vaste kosten vermeerderd met de nettowinst.
- Cyberincident =
  - Malware op uw computersystemen of computernetwerk.
    - Software of code die is ontworpen om:
      - Schade te maken aan uw computersysteem of computernetwerk.
      - De werking van uw computersysteem of computernetwerk te verstoren.
      - Toegang te krijgen tot uw computersysteem of computernetwerk.
    - Bijvoorbeeld spyware, ransomware, virussen of Trojaanse paarden.
  - Iemand anders breekt in in uw computersysteem of computernetwerk.
    - Met als doel om schade te maken aan uw computersysteem of computernetwerk.
      - U gaf hiervoor geen toestemming.
    - Of als doel om toegang te krijgen tot uw computersysteem of computernetwerk.
      - U gaf hiervoor geen toestemming.
    - Of om gegevens op uw computersysteem of computernetwerk te openbaren.
      - U gaf hiervoor geen toestemming.
  - DoS-aanval.
    - Iemand overbelast bewust uw computersysteem of computernetwerk.
      - Waardoor uw computersysteem of computernetwerk niet of niet meer goed werkt.
    - Ook DDoS-aanvallen.
  - Diefstal van digitale data.

4. Bedrijfsschade

vervolg

33. Wat is verzekerd?

- Menselijke fout van uw medewerker of een medewerker van een IT dienstverlener.
  - Bij het bedienen van uw computersysteem of het computersysteem van de IT dienstverlener.
    - Bijvoorbeeld de keuze voor verkeerde software, een programmeerfout, of een installatiefout.
- Ook verzekerd als het cyberincident plaatsvindt op het computersysteem van een IT dienstverlener van u.
  - En dat computersysteem werd gebruikt bij aan u verleende diensten.
  - Alleen voor het deel van de schade dat met u te maken heeft.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
      - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.
  - We betalen alleen de herstelkosten om uw bedrijf weer te laten lopen.
    - Dus niet voor uw dienstverlener.

Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.

- Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
- Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
- Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Extra kosten om uw bedrijfsschade te voorkomen of te beperken

- Alleen als deze redelijk en noodzakelijk zijn om uw bedrijfsschade te voorkomen of te beperken.
- Alleen verzekerd als wij vooraf schriftelijk toestemming hebben gegeven.
- Niet verzekerd als de extra kosten al verzekerd zijn onder een andere Rubriek dan bedrijfsschade.

34. Welke kosten zijn boven het verzekerd bedrag verzekerd?

Kosten van experts.

- Alleen voor het bepalen van de hoogte van de schade.
- De kosten van onze expert.
- De kosten van de expert van verzekerde tot en met de kosten van onze expert.
  - Rekent de expert van verzekerde meer? Dan blijven die extra kosten voor rekening van verzekerde.
- De kosten van de 3e expert.
- Alle experts zijn ingeschreven in het register van het Nederlands Instituut Van Register Experts (NIVRE).
  - Of bij een vergelijkbare beroepsorganisatie.
    - En in de statuten en reglementen van deze organisatie:
      - Staat een duidelijke klacht- en tuchtprocedure.
      - Zijn de eisen beschreven voor permanente opleiding van experts.
  - Alle experts houden zich aan de Gedragscode schade-expertiseorganisaties van het Verbond van Verzekeraars.

Voldoet een expert niet aan deze eisen? Dan zijn de kosten van die expert niet verzekerd.

Let op: we betalen alleen als deze kosten noodzakelijk zijn door een schade die verzekerd is.

4. Bedrijfsschade

Niet verzekerd

Kijk ook in de algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Sanctiewet 1977.
- Ernstige conflicten (molest).
- Atoomkernreacties.
- Fraude.
- Terrorisme.
- Niet nakomen voorwaarden.

Per situatie staat in de algemene voorwaarden precies wat nooit verzekerd is.

Hieronder staat wat verder niet verzekerd is bij uw cyberverzekering.

35. Wanneer bent u niet verzekerd?

Als wij volgens wet- of regelgeving u niet mogen verzekeren voor de hulp, schade of de kosten.

Als de gebeurtenis voor het begin van de verzekering plaatsvond.

- En de verzekerde de gebeurtenis had kunnen of moeten ontdekken.

36. Welke schade is niet verzekerd?

Schade door een cyberoperatie.

Cyberoperatie =

- Het gebruik van een computersysteem door een soevereine staat.
  - Ook: het gebruik van een computersysteem op aanwijzing van een soevereine staat.
  - Ook: het gebruik van een computersysteem onder controle van een soevereine staat.
    - Met als doel om een ander computersysteem te verstoren.
    - En/of de toegang tot dat computersysteem te blokkeren.
    - En/of de functionaliteit ervan te verminderen.
    - En/of data in een computersysteem te kopiëren, verwijderen, vernietigen, wijzigen of te blokkeren.
- Alleen als wij bewijzen dat het een cyberoperatie is.
  - Wij kijken naar elk beschikbaar, redelijk en objectief bewijs.
    - Bijvoorbeeld: de regering van de staat, waarin de getroffen computersystemen zich fysiek bevinden, geeft een verklaring uit waarin de cyberoperatie aan een andere soevereine staat wordt toegeschreven.
      - Of wordt toegeschreven aan personen die op aanwijzing of onder controle van een andere soevereine staat handelden.

Soevereine staat = een land dat binnen het grondgebied het hoogste gezag voert.

- En dat niet afhankelijk is van een andere staat.

Schade door terrorisme.

- Kijk ook in onze algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Wel verzekerd schade door cyberterrorisme.
  - Cyberterrorisme = Toegang krijgen tot of beschadigen, vernietigen, verstoren van uw computersystemen of computernetwerken door een of meerdere personen die dat doen met een politiek, religieus, ideologisch of politiek doel.

4. Bedrijfsschade

vervolg

36. Welke schade is niet verzekerd?

Schade doordat apparatuur of een installatie van een ander niet of niet goed werkt.

- Apparaten en installaties die ervoor zorgen dat de energievoorziening blijft werken.
  - De energievoorziening van computersystemen en gegevensopslag.
  - Bijvoorbeeld, noodstroomvoorzieningen en stand-alone-generatoren.
- Airconditioning.
- Wel verzekerd als apparatuur of installatie van een IT dienstverlener niet goed werkt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade door gevaarlijke, verontreinigende of vervuilende stoffen.

Schade doordat uw computersysteem in beslag wordt genomen.

- Door een instantie die dat mag doen volgens de wet.
  - Bijvoorbeeld de overheid, een toezichthouder of een rechtbank.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Verlies van zaken.

- En de directe gevolgen daarvan.
- Ook als zaken kapot, weg of verontreinigd zijn.
- Zaken = losse spullen, onroerend goed of dieren.

Schade aan personen.

- Verwonding, ziekte (lichamelijk of geestelijk) of overlijden.
  - En de directe gevolgen daarvan.

Diefstal, schending of openbaarmaking van intellectueel eigendom.

- Bijvoorbeeld patenten, handelsmerken of auteursrechten.

Boetes en schadevergoedingen opgelegd door overheid of toezichthouder.

Beleggingsverliezen of handelsverliezen.

- Bijvoorbeeld als het niet meer lukt om effecten te verkopen.

Schade door geplande stilstand van uw computersystemen.

- Of van onderdelen van uw computersystemen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Betalingen die u doet om goede wil te tonen.

- Bijvoorbeeld kortingen, vouchers of coulancebetalingen.

4. Bedrijfsschade

vervolg

36. Welke schade is niet verzekerd?

Schade aan branded currency of cryptogeld.

Branded currency = combinatie van digitale betaalmiddelen of loyaliteitspunten uitgevoerd via een digitale mobiele portemonnee. En uniek voor een bepaalde winkelketen of webshop.

- Bijvoorbeeld een digitale cadeaukaart, digitale coupons of digitale promotiecodes.

Cryptogeld = digitaal geld dat niet wordt uitgegeven door een bank. Cryptogeld zit in een digitale portemonnee.

- Bijvoorbeeld: bitcoins

Ook niet verzekerd: verlies van branded currency of cryptogeld.

37. Bij welk gedrag bent u niet verzekerd?

Bij opzet van verzekerde of uw IT dienstverlener.

Verzekerde heeft geen dekking als verzekerde of de IT dienstverlener in strijd met het recht met opzet iets doet of niet doet waardoor schade ontstaat. De in feite toegebrachte schade is hierbij een te verwachten of normaal gevolg van wat een verzekerde of de IT dienstverlener doet of niet doet. Heeft verzekerde geen dekking? Dan heeft verzekerde dat ook niet voor de schade die mogelijk later nog ontstaat.

In welke gevallen geldt de opzetuitsluiting?

De uitsluiting geldt als verzekerde of de IT dienstverlener zich maatschappelijk ongewenst of crimineel gedraagt. Dat is in ieder geval zo bij gedragingen die een gevaar voor personen of zaken kunnen opleveren, zoals:

- Brandstichting, vernieling en beschadiging.
- Afpersing, bedrog, oplichting, bedreiging, beroving, verduistering, diefstal en inbraak. Ook als verzekerde of de IT dienstverlener dat met een computer of ander (technisch) hulpmiddel doet.
- Geweldpleging, mishandeling, doodslag en moord.

Er is sprake van opzet als verzekerde of de IT dienstverlener iets doet of niet doet waarbij verzekerde:

- De bedoeling heeft schade te veroorzaken (opzet als oogmerk).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener zeker weet dat er schade ontstaat (opzet met zekerheidsbewustzijn).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener de aanmerkelijke kans dat er schade ontstaat voor lief neemt. En toch handelt verzekerde (niet) zo (voorwaardelijk opzet).

Opzet wordt objectief uit de feiten, omstandigheden en/of gedragingen van verzekerde of de IT dienstverlener afgeleid.

Deze opzetuitsluiting geldt ook bij:

- Groepsaansprakelijkheid.
  - Als verzekerde niet zelf maar wel iemand in een groep waarvan verzekerde deel uitmaakt iets doet of niet doet.
- Alcohol en drugs.
  - Als verzekerde zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat verzekerde zijn eigen wil niet meer kon bepalen. Of als iemand in een groep waarvan verzekerde deel uitmaakt zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat hij of zij de eigen wil niet meer kon bepalen.

4. Bedrijfsschade

vervolg

37. Bij welk gedrag bent u niet verzekerd?

IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.

- Maar niet een dienstverlener:
  - Voor stroomvoorziening;
  - Voor telecommunicatie;
  - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade doordat de verzekerde seksueel of seksueel getint gedrag vertoont.

- Geldt alleen voor de verzekerde die het gedrag vertoont.
- Alleen of in een groep.
  - Ook niet verzekerd: als verzekerde zelf niets doet.
  - Maar wel deel uitmaakt van een groep die dit gedrag vertoont.

Als u niet goed samenwerkt met de toezichthouder.

- Om te voorkomen dat een cyberincident of gegevensinbreuk plaatsvindt.
- Om te voorkomen dat aanspraak tegen u wordt ingediend.
- Om te voorkomen dat de toezichthouder u een straf of maatregel oplegt.
  - Als gevolg van een cyberincident, gegevensinbreuk of aanspraak.

Als u niet betaalt voor diensten of producten.

- En daardoor ontstaat schade of ontstaan kosten voor u of een ander.
- Bijvoorbeeld als u een leaseovereenkomst of licentie niet verlengt.
- Ook niet verzekerd als een IT dienstverlener van u niet betaalt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

4. Bedrijfsschade

vervolg

37. Bij welk gedrag bent u niet verzekerd?

Als u zich niet houdt aan de preventieafspraken.

En de schade is hierdoor veroorzaakt of verergerd.

Preventieafspraken =

- U heeft een wachtwoordbeleid
  - Iedere gebruiker heeft een eigen account.
  - Alleen IT-administrators hebben toegang tot administrator accounts of privileged accounts.
  - Alle standaardwachtwoorden of standaardtoegangscodes worden bij het eerste gebruik direct gewijzigd en veilig bewaard.
  - Wachtwoorden bestaan uit 8 of meer tekens.
    - En bestaan uit een combinatie van minimaal drie van de volgende elementen: hoofdletters, kleine letters, speciale symbolen, cijfers.
  - U vermijdt gebruik van:
    - Woordenboekwoorden (bijvoorbeeld: “wachtwoord”).
    - Opeenvolgende of herhalende tekens (bijvoorbeeld “1234”, “1111”, “abcde”).
    - Toetsenbordpatronen (bijvoorbeeld “asdfgh”).
    - Persoonlijke informatie van de gebruiker (bijvoorbeeld een geboortedatum of een naam).
- U gebruikt een firewall om uw netwerk en computersystemen te beveiligen.
- U gebruikt anti-virus-, anti-spyware- en firewallsoftware die automatisch worden geüpdatet.
  - Of vergelijkbare malware-beveiligingssoftware.
  - Als het nodig is wordt deze software wekelijks handmatig geüpdatet.
- U past updates op uw computersystemen en computernetwerken automatisch toe.
  - Of u past deze handmatig toe als dat nodig is.
  - Als die updates zijn uitgegeven om uw computersystemen of computernetwerken te beschermen.
  - Voor computersystemen of computernetwerken die met internet zijn verbonden past u de update toe binnen 30 dagen nadat de update is gepubliceerd.
  - Voor Operationele technologie (OT) en Embedded systems past u de update toe binnen 90 dagen nadat de update is gepubliceerd.
  - Of binnen de periode die de betreffende fabrikant aanbeveelt.
- Voor andere computersystemen past u de update toe binnen 60 dagen nadat de update is gepubliceerd.
- U maakt wekelijks backups van digitale data op uw computersystemen.
- U test regelmatig herstelprocedures van uw computersystemen.
- U bewaart de back-up apart van uw computersystemen waarop de originele digitale data staat.
  - Bijvoorbeeld op een andere server op een andere locatie of bij een andere clouddienst.
- U vervangt software en hardware uiterlijk 3 maanden nadat de fabrikant stopte met de ondersteuning.
  - Of u zorgt voor een upgrade.

4. Bedrijfsschade

vervolg

37. Bij welk gedrag bent u niet verzekerd?

- Als u één of meerdere van bovengenoemde maatregelen aan een ander bedrijf uitbesteedt:
  - Dan staat in de overeenkomst met het andere bedrijf dat het verplicht is om de bovengenoemde maatregelen uit te voeren.
    - Wel verzekerd als u bewijst dat u zich per ongeluk niet hield aan de preventieafspraken.
      - Bijvoorbeeld als de schade wordt veroorzaakt of verergerd omdat u in de week van de gebeurtenis geen back-up maakte.
      - En u bewijst dat u in de periode voor de gebeurtenis wel altijd een back-up maakte.
      - En u bewijst dat de back-up tijdens de gebeurtenis niet gemaakt is door een technische storing waar u niets aan kon doen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Operationele technologie (OT) = een verzameling hardware en software die de werking van een industrieel proces kan beïnvloeden.
  - OT houdt meestal toezicht op fysieke processen zoals productie, energie, geneeskunde, gebouwenbeheer en ecosystemen.
- Embedded systems = een computersysteem met een specifieke taak en ingebed in een groter systeem.
  - Bijvoorbeeld een computersysteem in medische apparatuur.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

4. Bedrijfsschade

Bij schade

38. Wanneer meldt een verzekerde een gebeurtenis?

Zo snel mogelijk.

- Meld een gebeurtenis bij ons.
  - Een verzekerde meldt het ook als hij een gebeurtenis vermoedt.

39. Wat doet een verzekerde bij schade?

- De verzekerde meldt de schade zo snel mogelijk.
- De verzekerde werkt mee aan de afhandeling van de schade.
- De verzekerde doet alles om de schade zo veel mogelijk te beperken.
- De verzekerde geeft ons alle informatie die nodig is om de omvang en de oorzaak van de schade vast te stellen.
- De verzekerde bewaart alle hardware, software en gegevens.
  - En geeft die voor onderzoek aan ons of een expert als dat nodig is.
- De verzekerde doet aangifte bij de politie bij een strafbaar feit.
  - Bijvoorbeeld bij cyberafpersing.
- De verzekerde helpt ons de betaalde schadevergoeding bij een ander terug te halen.
- De verzekerde geeft alle verzekeringen op die deze schade verzekeren.
- De verzekerde tekent een geheimhoudingsverklaring als de incident response provider daarom vraagt.
  - Tekent u niet? Dan kunnen wij uw schade mogelijk niet of niet volledig afhandelen.

40. Wat is het verzekerd bedrag?

Het verzekerd bedrag staat op het polisblad.

- Dit is het totale verzekerd bedrag per gebeurtenis of aanspraak voor deze verzekering.
- Dit is ook het maximale bedrag dat we per verzekeringsjaar uitkeren.
  - Voor alle schades en kosten bij elkaar.
  - Hieronder vallen ook betalingen van ons aan een expert.
- Dit geldt voor alle rubrieken samen.

41. Wie bepaalt de hoogte van het schadebedrag?

Of: wij.

Of: onze expert.

Of: onze expert met een expert van de verzekerde.

- Voor zij starten, kiezen zij een 3e expert.
  - Die bepaalt de schade als zij het oneens zijn.
  - Hij bepaalt de schade tussen het laagste en hoogste bedrag.
- Alle experts zijn ingeschreven in het register van het Nederlands Instituut Van Register Experts (NIVRE).
  - Of bij een vergelijkbare beroepsorganisatie.
    - En in de statuten en reglementen van deze organisatie:
      - Staat een duidelijke klacht- en tuchtprocedure.
      - Zijn de eisen beschreven voor permanente opleiding van experts.
  - Alle experts houden zich aan de Gedragscode schade-expertiseorganisaties van het Verbond van Verzekeraars.

Let op: dat wij het schadebedrag bepalen, betekent niet dat we de schade betalen.

4. Bedrijfsschade

42. Hoe berekent onze expert uw bedrijfsschade?

Onze expert bepaalt hoeveel uw brutowinst door het cyberincident is verslechterd.

- Hij bekijkt wat uw brutowinst was in de 12 maanden voorafgaand aan het cyberincident.
- Hij houdt rekening met de ontwikkeling van uw brutowinst.
  - Als er geen bedrijfsschade had plaatsgevonden.
- Hij houdt rekening met factoren die uw brutowinst beïnvloeden.
  - Bijvoorbeeld seizoensinvloeden of orders in uw portefeuille.
- Hij houdt rekening met uw extra kosten en besparingen.
  - Alleen als deze gemaakt zijn om uw bedrijfsschade te voorkomen of verminderen.
  - Alleen verzekerd als wij vooraf schriftelijk toestemming hebben gegeven om deze kosten te maken.
- Hij houdt rekening met de wachttermijn die geldt.
  - De wachttermijn is het aantal uren waarbij de bedrijfsschade voor rekening van uzelf komt.
  - De wachttermijn begint zodra de gebeurtenis is ontdekt.
  - De wachttermijn staat op uw polisblad.
- Hij kijkt naar de uitkeringsperiode.
  - Dit is de periode dat uw computersysteem niet of niet helemaal beschikbaar is.
  - Deze periode begint na de wachttermijn.
  - Deze periode eindigt nadat uw computersysteem en digitale data weer helemaal beschikbaar zijn.
    - En uw brutowinst weer op het niveau is van direct voorafgaand aan het cyberincident.
  - De uitkeringsperiode duurt nooit langer dan 90 dagen nadat u de gebeurtenis ontdekte.
  - Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
    - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
    - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
    - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Brutowinst = het verschil tussen de omzet en de variabele kosten.
  - Of vaste kosten vermeerderd met de nettowinst

43. Wat als een verzekerde ook op een andere verzekering is verzekerd?

De andere verzekering gaat voor.

- Als de verzekerde daarop verzekerd is of verzekerd zou zijn als onze verzekering niet zou bestaan.
- Wij betalen de schade boven het maximale bedrag van de andere verzekering.
  - Wij betalen niet uw eigen risico bij de andere verzekering.

44. Wat als bij schade blijkt dat deze verzekering in strijd is met wet- en regelgeving?

Wij houden ons altijd aan de wet- en regelgeving die van toepassing is.

- We zoeken dan naar een oplossing die in lijn is met deze verzekering.

5. Cyberafpersing

Inhoud

Klik op de **vraag** om het antwoord te lezen

5. Cyberafpersing

Verzekerd

45. Wat is verzekerd?

Hulp bij cyberafpersing of een vermoeden van cyberafpersing.

- Cyberafpersing = een ander dreigt een verzekerde schade te veroorzaken op uw computersysteem, tenzij u geld betaalt.
  - Of een ander veroorzaakt een verzekerde schade en vraagt geld om het probleem op te lossen.
    - Ook verzekerd als hij cryptogeld vraagt.
  - Alleen verzekerd als het een geloofwaardige dreiging is.
  - Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
    - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
    - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
    - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Niet verzekerd als u bekend maakte dat u deze verzekering heeft afgesloten.

46. Welke hulp is verzekerd bij cyberafpersing?

Een expert die de cyberafpersing of een vermoedelijke cyberafpersing voor u onderzoekt.

- De expert deelt de resultaten van het onderzoek met u.
- Wij kiezen de expert.

Een expert die de cyberafpersing beperkt.

- Bijvoorbeeld door getroffen gebruikersaccounts uit te schakelen of door malware te verwijderen.
- Wij kiezen de expert.

Kosten voor het documenteren van de cyberafpersing door de expert die de cyberafpersing voor u onderzoekt.

- Ook voor het opstellen van advies voor het beter beveiligen van uw computersysteem.
  - Tegen vergelijkbare cyberafpersingen.

Kosten voor het inrichten en bemannen van een crisis management centrum door experts bij een cyberafpersing.

- Ook kosten voor het inrichten en bemannen van een call centre.
- Alleen verzekerd als wij toestemming geven voor inschakeling.
- Wij kiezen de expert.
- Wij vergoeden de kosten tot 30 dagen nadat u de gebeurtenis bij ons meldde.

Wij vergoeden losgeld dat u moet betalen.

- Alleen als er geen andere opties meer zijn om de cyberafpersing op te lossen.
- Alleen als u hebt overlegd met een expert cyber afpersing voordat u besluit losgeld te betalen.
- Alleen als dat mag volgens de wet.
  - Vergoeding van losgeld is volgens de wet meestal niet toegestaan.
- Ook cryptogeld.
  - Bijvoorbeeld bitcoins.

We vergoeden redelijke kosten die nodig zijn om de cyberafpersing op te lossen.

- Alleen met onze toestemming.

5. Cyberafpersing

47. Welk bedrag voor hulp en kosten samen is verzekerd?

Wij betalen maximaal het verzekerd bedrag per gebeurtenis.

- Het verzekerd bedrag staat op het polisblad.
- Dit geldt voor alle verzekerden samen.
- Dit geldt voor alle rubrieken samen.
- Houden meerdere gebeurtenissen verband met 1 oorzaak? Dan tellen we die gebeurtenissen als 1 gebeurtenis.

Per verzekeringsjaar betalen wij een maximaal bedrag.

- Dit bedrag staat op het polisblad.
- Dit geldt voor alle verzekerden samen.
  - Het moment van de 1e melding bepaalt bij welk verzekeringsjaar de gebeurtenis hoort.
- Dit geldt voor alle rubrieken samen.

Let op: u betaalt eerst een eigen risico.

- Het eigen risico per verzekerde gebeurtenis staat op het polisblad.

48. Welke kosten zijn boven het verzekerd bedrag verzekerd?

Kosten van experts.

- Alleen voor het bepalen van de hoogte van de schade.
- De kosten van onze expert.
- De kosten van de expert van verzekerde tot en met de kosten van onze expert.
  - Rekent de expert van verzekerde meer? Dan blijven die extra kosten voor rekening van verzekerde.
- De kosten van de 3e expert.
- Alle experts zijn ingeschreven in het register van het Nederlands Instituut Van Register Experts (NIVRE).
  - Of bij een vergelijkbare beroepsorganisatie.
    - En in de statuten en reglementen van deze organisatie:
      - Staat een duidelijke klacht- en tuchtprocedure.
      - Zijn de eisen beschreven voor permanente opleiding van experts.
  - Alle experts houden zich aan de Gedragscode schade-expertiseorganisaties van het Verbond van Verzekeraars.

  Voldoet een expert niet aan deze eisen? Dan zijn de kosten van die expert niet verzekerd.

Let op: we betalen alleen als deze kosten noodzakelijk zijn door een schade die verzekerd is.

5. Cyberafpersing

Niet verzekerd

Kijk ook in de algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Sanctiewet 1977.
- Ernstige conflicten (molest).
- Atoomkernreacties.
- Fraude.
- Terrorisme.
- Niet nakomen voorwaarden.

Per situatie staat in de algemene voorwaarden precies wat nooit verzekerd is.

Hieronder staat wat verder niet verzekerd is bij uw cyberverzekering.

49. Wanneer bent u niet verzekerd?

Als wij volgens wet- of regelgeving u niet mogen verzekeren voor de hulp, schade of de kosten.

Als de gebeurtenis voor het begin van de verzekering plaatsvond.

- En de verzekerde de gebeurtenis had kunnen of moeten ontdekken.

50. Welke schade is niet verzekerd?

Schade door een cyberoperatie.

Cyberoperatie =

- Het gebruik van een computersysteem door een soevereine staat.
  - Ook: het gebruik van een computersysteem op aanwijzing van een soevereine staat.
  - Ook: het gebruik van een computersysteem onder controle van een soevereine staat.
    - Met als doel om een ander computersysteem te verstoren.
    - En/of de toegang tot dat computersysteem te blokkeren.
    - En/of de functionaliteit ervan te verminderen.
    - En/of data in een computersysteem te kopiëren, verwijderen, vernietigen, wijzigen of te blokkeren.
- Alleen als wij bewijzen dat het een cyberoperatie is.
  - Wij kijken naar elk beschikbaar, redelijk en objectief bewijs.
    - Bijvoorbeeld: de regering van de staat, waarin de getroffen computersystemen zich fysiek bevinden, geeft een verklaring uit waarin de cyberoperatie aan een andere soevereine staat wordt toegeschreven.
      - Of wordt toegeschreven aan personen die op aanwijzing of onder controle van een andere soevereine staat handelden.

Soevereine staat = een land dat binnen het grondgebied het hoogste gezag voert.

- En dat niet afhankelijk is van een andere staat.

Schade door terrorisme.

- Kijk ook in onze algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Wel verzekerd schade door cyberterrorisme
  - Cyberterrorisme = Toegang krijgen tot of beschadigen, vernietigen, verstoren van uw computersystemen of computernetwerken door een of meerdere personen die dat doen met een politiek, religieus, ideologisch of politiek doel.

5. Cyberafpersing

vervolg

50. Welke schade is niet verzekerd?

Schade doordat apparatuur of een installatie van een ander niet of niet goed werkt.

- Apparaten en installaties die ervoor zorgen dat de energievoorziening blijft werken.
  - De energievoorziening van computersystemen en gegevensopslag.
  - Bijvoorbeeld, noodstroomvoorzieningen en stand-alone-generatoren.
- Airconditioning.
- Wel verzekerd als apparatuur of installatie van een IT dienstverlener niet goed werkt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade door gevaarlijke, verontreinigende of vervuilende stoffen.

Schade doordat uw computersysteem in beslag wordt genomen.

- Door een instantie die dat mag doen volgens de wet.
  - Bijvoorbeeld de overheid, een toezichthouder of een rechtbank.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Verlies van zaken.

- En de directe gevolgen daarvan.
- Ook als zaken kapot, weg of verontreinigd zijn.
- Zaken = losse spullen, onroerend goed of dieren.

Schade aan personen.

- Verwonding, ziekte (lichamelijk of geestelijk) of overlijden.
  - En de directe gevolgen daarvan.

Diefstal, schending of openbaarmaking van intellectueel eigendom.

- Bijvoorbeeld patenten, handelsmerken of auteursrechten.

Boetes en schadevergoedingen opgelegd door overheid of toezichthouder.

Beleggingsverliezen of handelsverliezen.

- Bijvoorbeeld als het niet meer lukt om effecten te verkopen.

Schade door geplande stilstand van uw computersystemen.

- Of van onderdelen van uw computersystemen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Betalingen die u doet om goede wil te tonen.

- Bijvoorbeeld kortingen, vouchers of coulancebetalingen.

5. Cyberafpersing

vervolg

50. Welke schade is niet verzekerd?

Schade aan branded currency of cryptogeld.

Branded currency = combinatie van digitale betaalmiddelen of loyaliteitspunten uitgevoerd via een digitale mobiele portemonnee. En uniek voor een bepaalde winkelketen of webshop.

- Bijvoorbeeld een digitale cadeaukaart, digitale coupons of digitale promotiecodes.

Cryptogeld = digitaal geld dat niet wordt uitgegeven door een bank. Cryptogeld zit in een digitale portemonnee.

- Bijvoorbeeld: bitcoins

Ook niet verzekerd: verlies van branded currency of cryptogeld.

51. Bij welk gedrag bent u niet verzekerd?

Bij opzet van verzekerde of uw IT dienstverlener.

Verzekerde heeft geen dekking als verzekerde of de IT dienstverlener in strijd met het recht met opzet iets doet of niet doet waardoor schade ontstaat. De in feite toegebrachte schade is hierbij een te verwachten of normaal gevolg van wat een verzekerde of de IT dienstverlener doet of niet doet. Heeft verzekerde geen dekking? Dan heeft verzekerde dat ook niet voor de schade die mogelijk later nog ontstaat.

In welke gevallen geldt de opzetuitsluiting?

De uitsluiting geldt als verzekerde of de IT dienstverlener zich maatschappelijk ongewenst of crimineel gedraagt. Dat is in ieder geval zo bij gedragingen die een gevaar voor personen of zaken kunnen opleveren, zoals:

- Brandstichting, vernieling en beschadiging.
- Afpersing, bedrog, oplichting, bedreiging, beroving, verduistering, diefstal en inbraak. Ook als verzekerde of de IT dienstverlener dat met een computer of ander (technisch) hulpmiddel doet.
- Geweldpleging, mishandeling, doodslag en moord.

Er is sprake van opzet als verzekerde of de IT dienstverlener iets doet of niet doet waarbij verzekerde:

- De bedoeling heeft schade te veroorzaken (opzet als oogmerk).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener zeker weet dat er schade ontstaat (opzet met zekerheidsbewustzijn).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener de aanmerkelijke kans dat er schade ontstaat voor lief neemt. En toch handelt verzekerde (niet) zo (voorwaardelijk opzet).

Opzet wordt objectief uit de feiten, omstandigheden en/of gedragingen van verzekerde of de IT dienstverlener afgeleid.

Deze opzetuitsluiting geldt ook bij:

- Groepsaansprakelijkheid.
  - Als verzekerde niet zelf maar wel iemand in een groep waarvan verzekerde deel uitmaakt iets doet of niet doet.
- Alcohol en drugs.
  - Als verzekerde zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat verzekerde zijn eigen wil niet meer kon bepalen. Of als iemand in een groep waarvan verzekerde deel uitmaakt zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat hij of zij de eigen wil niet meer kon bepalen.

5. Cyberafpersing

vervolg

51. Bij welk gedrag bent u niet verzekerd?

IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.

- Maar niet een dienstverlener:
  - Voor stroomvoorziening;
  - Voor telecommunicatie;
  - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade doordat de verzekerde seksueel of seksueel getint gedrag vertoont.

- Geldt alleen voor de verzekerde die het gedrag vertoont.
- Alleen of in een groep.
  - Ook niet verzekerd: als verzekerde zelf niets doet.
  - Maar wel deel uitmaakt van een groep die dit gedrag vertoont.

Als u niet goed samenwerkt met de toezichthouder.

- Om te voorkomen dat een cyberincident of gegevensinbreuk plaatsvindt.
- Om te voorkomen dat aanspraak tegen u wordt ingediend.
- Om te voorkomen dat de toezichthouder u een straf of maatregel oplegt.
  - Als gevolg van een cyberincident, gegevensinbreuk of aanspraak.

Als u niet betaalt voor diensten of producten.

- En daardoor ontstaat schade of ontstaan kosten voor u of een ander.
- Bijvoorbeeld als u een leaseovereenkomst of licentie niet verlengt.
- Ook niet verzekerd als een IT dienstverlener van u niet betaalt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

5. Cyberafpersing

vervolg

51. Bij welk gedrag bent u niet verzekerd?

Als u zich niet houdt aan de preventieafspraken.

En de schade is hierdoor veroorzaakt of verergerd.

Preventieafspraken =

- U heeft een wachtwoordbeleid
  - Iedere gebruiker heeft een eigen account.
  - Alleen IT-administrators hebben toegang tot administrator accounts of privileged accounts.
  - Alle standaardwachtwoorden of standaardtoegangscodes worden bij het eerste gebruik direct gewijzigd en veilig bewaard.
  - Wachtwoorden bestaan uit 8 of meer tekens.
    - En bestaan uit een combinatie van minimaal drie van de volgende elementen: hoofdletters, kleine letters, speciale symbolen, cijfers.
  - U vermijdt gebruik van:
    - Woordenboekwoorden (bijvoorbeeld: “wachtwoord”).
    - Opeenvolgende of herhalende tekens (bijvoorbeeld “1234”, “1111”, “abcde”).
    - Toetsenbordpatronen (bijvoorbeeld “asdfgh”).
    - Persoonlijke informatie van de gebruiker (bijvoorbeeld een geboortedatum of een naam).
- U gebruikt een firewall om uw netwerk en computersystemen te beveiligen.
- U gebruikt anti-virus-, anti-spyware- en firewallsoftware die automatisch worden geüpdatet.
  - Of vergelijkbare malware-beveiligingssoftware.
  - Als het nodig is wordt deze software wekelijks handmatig geüpdatet.
- U past updates op uw computersystemen en computernetwerken automatisch toe.
  - Of u past deze handmatig toe als dat nodig is.
  - Als die updates zijn uitgegeven om uw computersystemen of computernetwerken te beschermen.
  - Voor computersystemen of computernetwerken die met internet zijn verbonden past u de update toe binnen 30 dagen nadat de update is gepubliceerd.
  - Voor Operationele technologie (OT) en Embedded systems past u de update toe binnen 90 dagen nadat de update is gepubliceerd.
  - Of binnen de periode die de betreffende fabrikant aanbeveelt.
- Voor andere computersystemen past u de update toe binnen 60 dagen nadat de update is gepubliceerd.
- U maakt wekelijks backups van digitale data op uw computersystemen.
- U test regelmatig herstelprocedures van uw computersystemen.
- U bewaart de back-up apart van uw computersystemen waarop de originele digitale data staat.
  - Bijvoorbeeld op een andere server op een andere locatie of bij een andere clouddienst.
- U vervangt software en hardware uiterlijk 3 maanden nadat de fabrikant stopte met de ondersteuning.
  - Of u zorgt voor een upgrade.

Als u één of meerdere van bovengenoemde maatregelen aan een ander bedrijf uitbesteedt:

- Dan staat in de overeenkomst met het andere bedrijf dat het verplicht is om de bovengenoemde maatregelen uit te voeren.
  - Wel verzekerd als u bewijst dat u zich per ongeluk niet hield aan de preventieafspraken.
    - Bijvoorbeeld als de schade wordt veroorzaakt of verergerd omdat u in de week van de gebeurtenis geen back-up maakte.
    - En u bewijst dat u in de periode voor de gebeurtenis wel altijd een back-up maakte.
    - En u bewijst dat de back-up tijdens de gebeurtenis niet gemaakt is door een technische storing waar u niets aan kon doen.

5. Cyberafpersing

vervolg

51. Bij welk gedrag bent u niet verzekerd?

- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Operationele technologie (OT) = een verzameling hardware en software die de werking van een industrieel proces kan beïnvloeden.
  - OT houdt meestal toezicht op fysieke processen zoals productie, energie, geneeskunde, gebouwenbeheer en ecosystemen.
- Embedded systems = een computersysteem met een specifieke taak en ingebed in een groter systeem.
  - Bijvoorbeeld een computersysteem in medische apparatuur.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

52. Aan wie mag de verzekerde bekend maken dat u Rubriek 4: Cyberafpersing heeft afgesloten?

Aan uw senior managers en professionele adviseurs.
Aan personen die het moeten weten volgens de wet.
Aan anderen als de verzekerde daarvoor onze toestemming heeft.

53. Wat als de verzekerde aan anderen bekend maakt dat u Rubriek 4: Cyberafpersing heeft afgesloten?

Dan bent u niet verzekerd voor schade door cyberafpersing.

- En wij mogen deze verzekering stoppen.
- Wel verzekerd als de verzekerde onze toestemming had om dit bekend te maken aan anderen.

5. Cyberafpersing

Bij schade

54. Wanneer meldt een verzekerde een gebeurtenis?

Zo snel mogelijk.

- Meld een gebeurtenis bij ons.
  - Meld het ook als u een gebeurtenis vermoedt.

55. Wat doet een verzekerde bij schade?

- De verzekerde meldt de schade zo snel mogelijk.
- De verzekerde werkt mee aan de afhandeling van de schade.
- De verzekerde doet alles om de schade zo veel mogelijk te beperken.
- De verzekerde geeft ons alle informatie die nodig is om de omvang en de oorzaak van de schade vast te stellen.
- De verzekerde bewaart alle hardware, software en gegevens.
  - En geeft die voor onderzoek aan ons of een expert als dat nodig is.
- De verzekerde doet aangifte bij de politie bij een strafbaar feit.
  - Bijvoorbeeld bij cyberafpersing.
- De verzekerde helpt ons de betaalde schadevergoeding bij een ander terug te halen.
- De verzekerde geeft alle verzekeringen op die deze schade verzekeren.
- De verzekerde tekent een geheimhoudingsverklaring als de incident response provider daarom vraagt.
  - Tekent u niet? Dan kunnen wij uw schade mogelijk niet of niet volledig afhandelen.

56. Wie bepaalt de hoogte van het schadebedrag?

Of: wij.

Of: onze expert.

Of: onze expert met een expert van de verzekerde.

- Voor zij starten, kiezen zij een 3e expert.
  - Die bepaalt de schade als zij het oneens zijn.
  - Hij bepaalt de schade tussen het laagste en hoogste bedrag.
- Alle experts zijn ingeschreven in het register van het Nederlands Instituut Van Register Experts (NIVRE).
  - Of bij een vergelijkbare beroepsorganisatie.
    - En in de statuten en reglementen van deze organisatie:
      - Staat een duidelijke klacht- en tuchtprocedure.
      - Zijn de eisen beschreven voor permanente opleiding van experts.
  - Alle experts houden zich aan de Gedragscode schade-expertiseorganisaties van het Verbond van Verzekeraars.

Let op: dat wij het schadebedrag bepalen, betekent niet dat we de schade betalen.

57. Wat als een verzekerde ook op een andere verzekering is verzekerd?

De andere verzekering gaat voor.

- Als de verzekerde daarop verzekerd is of verzekerd zou zijn als onze verzekering niet zou bestaan.
- Wij betalen de schade boven het maximale bedrag van de andere verzekering.
  - Wij betalen niet uw eigen risico bij de andere verzekering.

58. Wat als bij schade blijkt dat deze verzekering in strijd is met wet- en regelgeving?

Wij houden ons altijd aan de wet- en regelgeving die van toepassing is.

- We zoeken dan naar een oplossing die in lijn is met deze verzekering.

6. Privacy aansprakelijkheid

Inhoud

Klik op de **vraag** om het antwoord te lezen

6. Privacy aansprakelijkheid

Verzekerd

59. Wat is verzekerd?

De schade van een ander of een medewerker als u aansprakelijk gesteld wordt.

- En u bent hiervoor aansprakelijk.
- Voor de gevolgen van een gegevensinbreuk.
  - Ook als u door een gegevensinbreuk de privacyregels die voor u gelden, heeft overtreden.
  - Gegevensinbreuk = het verliezen van vertrouwelijke informatie of persoonsgegevens uit uw computersysteem.
    - Zonder toestemming van de verantwoordelijke.
    - Daardoor zijn vertrouwelijke informatie of persoonsgegevens weg, beschadigd, toegankelijk of openbaar.
      - Ook vertrouwelijke informatie of persoonsgegevens uit uw computersysteem en geprint op papier.
    - Vertrouwelijk informatie = commercieel gevoelige bedrijfsinformatie.
      - Ook bedrijfsgeheimen.
      - Ook als niet is aangegeven dat de informatie vertrouwelijk is.
    - Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
      - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
      - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
      - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Ook verzekerd bij een gegevensinbreuk op het computersysteem van een IT dienstverlener van u
  - En dat computersysteem werd gebruikt bij aan u verleende diensten.
    - Alleen voor het deel van de schade dat met u te maken heeft.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

60. Welke kosten zijn verzekerd als u aansprakelijk gesteld wordt?

Kosten voor verweer.

- Alleen als de schade verzekerd is.
- En wij voor u rechtshulp inschakelen.
  - Of vooraf toestemming geven voor inschakeling.
- En wij het verweer bepalen.
- Wij betalen dan ook de proceskosten.
- Bijvoorbeeld experts, onderzoeken, zittingen, taxaties, inspecties en procedures.
- Niet uw eigen algemene kosten.
  - Bijvoorbeeld salarissen en overheadkosten.

6. Privacy aansprakelijkheid

vervolg

60. Welke kosten zijn verzekerd als u aansprakelijk gesteld wordt?

Kosten om direct dreigende schade te voorkomen of te beperken.

- Alleen als u voor de schade aansprakelijk bent.
- En de schade verzekerd is.
- En u deze kosten maakt of laat maken.
- Ook schade aan iets wat een verzekerde hiervoor gebruikt.
- En wij belang hebben bij de maatregelen.
- Ook als het niet lukt.

6. Privacy aansprakelijkheid

Niet verzekerd

Kijk ook in de algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Sanctiewet 1977.
- Ernstige conflicten (molest).
- Atoomkernreacties.
- Fraude.
- Terrorisme.
- Niet nakomen voorwaarden.

Per situatie staat in de algemene voorwaarden precies wat nooit verzekerd is.

Hieronder staat wat verder niet verzekerd is bij uw cyberverzekering.

61. Wanneer bent u niet verzekerd?

Als wij volgens wet- of regelgeving u niet mogen verzekeren voor de hulp, schade of de kosten.

Als de gebeurtenis voor het begin van de verzekering plaatsvond.

- En de verzekerde de gebeurtenis had kunnen of moeten ontdekken.

62. Welke schade is niet verzekerd?

Schade door een cyberoperatie.

Cyberoperatie =

- Het gebruik van een computersysteem door een soevereine staat.
  - Ook: het gebruik van een computersysteem op aanwijzing van een soevereine staat.
  - Ook: het gebruik van een computersysteem onder controle van een soevereine staat.
    - Met als doel om een ander computersysteem te verstoren.
    - En/of de toegang tot dat computersysteem te blokkeren.
    - En/of de functionaliteit ervan te verminderen.
    - En/of data in een computersysteem te kopiëren, verwijderen, vernietigen, wijzigen of te blokkeren.
- Alleen als wij bewijzen dat het een cyberoperatie is.
  - Wij kijken naar elk beschikbaar, redelijk en objectief bewijs.
    - Bijvoorbeeld: de regering van de staat, waarin de getroffen computersystemen zich fysiek bevinden, geeft een verklaring uit waarin de cyberoperatie aan een andere soevereine staat wordt toegeschreven.
      - Of wordt toegeschreven aan personen die op aanwijzing of onder controle van een andere soevereine staat handelden.

Soevereine staat = een land dat binnen het grondgebied het hoogste gezag voert.

- En dat niet afhankelijk is van een andere staat.

Schade door terrorisme.

- Kijk ook in onze algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Wel verzekerd schade door cyberterrorisme.
  - Cyberterrorisme = Toegang krijgen tot of beschadigen, vernietigen, verstoren van uw computersystemen of computernetwerken door een of meerdere personen die dat doen met een politiek, religieus, ideologisch of politiek doel.

Schade waarvoor een bestuurder persoonlijk aansprakelijk wordt gesteld.

6. Privacy aansprakelijkheid

vervolg

62. Welke schade is niet verzekerd?

Schade doordat apparatuur of een installatie van een ander niet of niet goed werkt.

- Apparaten en installaties die ervoor zorgen dat de energievoorziening blijft werken.
  - De energievoorziening van computersystemen en gegevensopslag.
  - Bijvoorbeeld noodstroomvoorzieningen en stand alone generatoren.
- Airconditioning.
- Wel verzekerd als apparatuur of installatie van een IT dienstverlener niet goed werkt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade door gevaarlijke, verontreinigende of vervuilende stoffen.

Schade doordat uw computersysteem in beslag wordt genomen.

- Door een instantie die dat mag doen volgens de wet.
  - Bijvoorbeeld de overheid, een toezichthouder of een rechtbank.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.

Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Verlies van zaken.

- En de directe gevolgen daarvan.
- Ook als zaken kapot, weg of verontreinigd zijn.
- Zaken = losse spullen, onroerend goed of dieren.

Schade aan personen.

- Verwonding, ziekte (lichamelijk of geestelijk) of overlijden.
  - En de directe gevolgen daarvan.
- Wel verzekerd is schade door aantasting van het gevoel voor eigenwaarde en de waardering die verzekerde bij anderen geniet.
  - De wet noemt dit aantasting van eer of goede naam.
- Wel verzekerd is schade door ernstige schendingen van de persoonlijke levenssfeer.
  - Let op: niet geestelijk letsel!
    - De wet noemt dit een persoonsaantasting.

Diefstal, schending of openbaarmaking van patenten.

Boetes en schadevergoedingen opgelegd door overheid of toezichthouder.

Beleggingsverliezen of handelsverliezen.

- Bijvoorbeeld als het niet meer lukt om effecten te verkopen.

6. Privacy aansprakelijkheid

vervolg

62. Welke schade is niet verzekerd?

Schade door geplande stilstand van uw computersystemen.

- Of van onderdelen van uw computersystemen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Betalingen die u doet om goede wil te tonen.

- Bijvoorbeeld kortingen, vouchers of coulancebetalingen.

Schade aan branded currency of cryptogeld.

Branded currency = combinatie van digitale betaalmiddelen of loyaliteitspunten uitgevoerd via een digitale mobiele portemonnee. En uniek voor een bepaalde winkelketen of webshop.

- Bijvoorbeeld een digitale cadeaukaart, digitale coupons of digitale promotiecodes.

Cryptogeld = digitaal geld dat niet wordt uitgegeven door een bank. Cryptogeld zit in een digitale portemonnee.

- Bijvoorbeeld: bitcoins

Ook niet verzekerd: verlies van branded currency of cryptogeld.

63. Wanneer is aansprakelijkheid niet verzekerd?

Bij opzet van verzekerde of uw IT dienstverlener.

Verzekerde heeft geen dekking als verzekerde of de IT dienstverlener in strijd met het recht met opzet iets doet of niet doet waardoor schade ontstaat. De in feite toegebrachte schade is hierbij een te verwachten of normaal gevolg van wat een verzekerde of de IT dienstverlener doet of niet doet. Heeft verzekerde geen dekking? Dan heeft verzekerde dat ook niet voor de schade die mogelijk later nog ontstaat.

In welke gevallen geldt de opzetuitsluiting?

De uitsluiting geldt als verzekerde of de IT dienstverlener zich maatschappelijk ongewenst of crimineel gedraagt. Dat is in ieder geval zo bij gedragingen die een gevaar voor personen of zaken kunnen opleveren, zoals:

- Brandstichting, vernieling en beschadiging.
- Afpersing, bedrog, oplichting, bedreiging, beroving, verduistering, diefstal en inbraak. Ook als verzekerde of de IT dienstverlener dat met een computer of ander (technisch) hulpmiddel doet.
- Geweldpleging, mishandeling, doodslag en moord.

Er is sprake van opzet als verzekerde of de IT dienstverlener iets doet of niet doet waarbij verzekerde:

- De bedoeling heeft schade te veroorzaken (opzet als oogmerk).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener zeker weet dat er schade ontstaat (opzet met zekerheidsbewustzijn).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener de aanmerkelijke kans dat er schade ontstaat voor lief neemt. En toch handelt verzekerde (niet) zo (voorwaardelijk opzet).

Opzet wordt objectief uit de feiten, omstandigheden en/of gedragingen van verzekerde of de IT dienstverlener afgeleid.

6. Privacy aansprakelijkheid

vervolg

63. Wanneer is aansprakelijkheid niet verzekerd?

Deze opzetuitsluiting geldt ook bij:

- Groepsaansprakelijkheid.
  - Als verzekerde niet zelf maar wel iemand in een groep waarvan verzekerde deel uitmaakt iets doet of niet doet.
- Alcohol en drugs.
  - Als verzekerde zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat verzekerde zijn eigen wil niet meer kon bepalen. Of als iemand in een groep waarvan verzekerde deel uitmaakt zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat hij of zij de eigen wil niet meer kon bepalen.

IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.

- Maar niet een dienstverlener:
  - Voor stroomvoorziening;
  - Voor telecommunicatie;
  - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade doordat de verzekerde seksueel of seksueel getint gedrag vertoont.

- Geldt alleen voor de verzekerde die het gedrag vertoont.
- Alleen of in een groep.
  - Ook niet verzekerd: als verzekerde zelf niets doet.
  - Maar wel deel uitmaakt van een groep die dit gedrag vertoont.

Als u aansprakelijk gesteld wordt door:

- Een (rechts)persoon met zeggenschap over u.
- Een rechtspersoon waar u zeggenschap over heeft.
  - Bijvoorbeeld een dochteronderneming.
  - Of waar uw dochteronderneming zeggenschap over heeft.
- Een rechtspersoon waarin u een financieel belang heeft.
- Een samenwerking of joint venture waar u onderdeel van bent.

Als u ook aansprakelijk bent volgens een contract.

- En deze contractuele aansprakelijkheid gaat voor op de wettelijke aansprakelijkheid.

Aansprakelijkheid door een beroepsfout.

- Bijvoorbeeld een verkeerd advies of ontwerp.

64. Bij welk gedrag bent u niet verzekerd?

Als u niet goed samenwerkt met de toezichthouder.

- Om te voorkomen dat een cyberincident of gegevensinbreuk plaatsvindt.
- Om te voorkomen dat aanspraak tegen u wordt ingediend.
- Om te voorkomen dat de toezichthouder u een straf of maatregel oplegt.
  - Als gevolg van een cyberincident, gegevensinbreuk of aanspraak.

6. Privacy aansprakelijkheid

vervolg

64. Bij welk gedrag bent u niet verzekerd?

Als u niet betaalt voor diensten of producten.

- En daardoor ontstaat schade of ontstaan kosten voor u of een ander.
- Bijvoorbeeld als u een leaseovereenkomst of licentie niet verlengt.
- Ook niet verzekerd als een IT dienstverlener van u niet betaalt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Als u zich niet houdt aan de preventieafspraken.

En de schade is hierdoor veroorzaakt of verergerd.

Preventieafspraken =

- U heeft een wachtwoordbeleid
  - Iedere gebruiker heeft een eigen account.
  - Alleen IT-administrators hebben toegang tot administrator accounts of privileged accounts.
  - Alle standaardwachtwoorden of standaardtoegangscodes worden bij het eerste gebruik direct gewijzigd en veilig bewaard.
  - Wachtwoorden bestaan uit 8 of meer tekens.
    - En bestaan uit een combinatie van minimaal drie van de volgende elementen: hoofdletters, kleine letters, speciale symbolen, cijfers.
  - U vermijdt gebruik van:
    - Woordenboekwoorden (bijvoorbeeld: “wachtwoord”).
    - Opeenvolgende of herhalende tekens (bijvoorbeeld “1234”, “1111”, “abcde”).
    - Toetsenbordpatronen (bijvoorbeeld “asdfgh”).
    - Persoonlijke informatie van de gebruiker (bijvoorbeeld een geboortedatum of een naam).
- U gebruikt een firewall om uw netwerk en computersystemen te beveiligen.
- U gebruikt anti-virus-, anti-spyware- en firewallsoftware die automatisch worden geüpdatet.
  - Of vergelijkbare malware-beveiligingssoftware.
  - Als het nodig is wordt deze software wekelijks handmatig geüpdatet.
- U past updates op uw computersystemen en computernetwerken automatisch toe.
  - Of u past deze handmatig toe als dat nodig is.
  - Als die updates zijn uitgegeven om uw computersystemen of computernetwerken te beschermen.
  - Voor computersystemen of computernetwerken die met internet zijn verbonden past u de update toe binnen 30 dagen nadat de update is gepubliceerd.
  - Voor Operationele technologie (OT) en Embedded systems past u de update toe binnen 90 dagen nadat de update is gepubliceerd.
  - Of binnen de periode die de betreffende fabrikant aanbeveelt.
- Voor andere computersystemen past u de update toe binnen 60 dagen nadat de update is gepubliceerd.
- U maakt wekelijks backups van digitale data op uw computersystemen.
- U test regelmatig herstelprocedures van uw computersystemen.

6. Privacy aansprakelijkheid

vervolg

64. Bij welk gedrag bent u niet verzekerd?

- U bewaart de back-up apart van uw computersystemen waarop de originele digitale data staat.
  - Bijvoorbeeld op een andere server op een andere locatie of bij een andere clouddienst.
- U vervangt software en hardware uiterlijk 3 maanden nadat de fabrikant stopte met de ondersteuning.
  - Of u zorgt voor een upgrade.

Als u één of meerdere van bovengenoemde maatregelen aan een ander bedrijf uitbesteedt:

- Dan staat in de overeenkomst met het andere bedrijf dat het verplicht is om de bovengenoemde maatregelen uit te voeren.
  - Wel verzekerd als u bewijst dat u zich per ongeluk niet hield aan de preventieafspraken.
    - Bijvoorbeeld als de schade wordt veroorzaakt of verergerd omdat u in de week van de gebeurtenis geen back-up maakte.
    - En u bewijst dat u in de periode voor de gebeurtenis wel altijd een back-up maakte.
    - En u bewijst dat de back-up tijdens de gebeurtenis niet gemaakt is door een technische storing waar u niets aan kon doen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Operationele technologie (OT) = een verzameling hardware en software die de werking van een industrieel proces kan beïnvloeden.
  - OT houdt meestal toezicht op fysieke processen zoals productie, energie, geneeskunde, gebouwenbeheer en ecosystemen.
- Embedded systems = een computersysteem met een specifieke taak en ingebed in een groter systeem.
  - Bijvoorbeeld een computersysteem in medische apparatuur.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

6. Privacy aansprakelijkheid

Bij schade

65. Wanneer meldt een verzekerde een aanspraak?

Zo snel mogelijk.

- Meld het bij ons als u aansprakelijk gesteld bent.
- Of het waarschijnlijk is dat u later aansprakelijk gesteld wordt.
- Meld een aanspraak bij ons.
  - Een verzekerde meldt het ook als hij een gebeurtenis vermoedt.

66. Wanneer meldt een verzekerde een omstandigheid?

Zodra een verzekerde vermoedt dat een voorval leidt tot een aanspraak.

En het waarschijnlijk is dat hij de aanspraak ontvangt.

- Verzekerde meldt een omstandigheid altijd schriftelijk.
- Verzekerde geeft in de melding informatie over de gebeurtenis die tot schade heeft geleid.
- Verzekerde vermeldt wie de vermoedelijke eisers zijn.
- Verzekerde geeft alle informatie die hij heeft over de hoogte van het schadebedrag.

67. Welke omstandigheden meldt een verzekerde?

Omstandigheden waarvan u denkt dat die kunnen leiden tot een aanspraak.

- Komt de echte aanspraak binnen 30 dagen na stoppen van de verzekering? Dan bent u toch verzekerd.

68. Wanneer geldt een omstandigheid als gemeld?

Zodra wij schriftelijk bevestigen dat wij de melding als omstandighedenmelding accepteren.

69. Wat doet een verzekerde bij een aanspraak?

- De verzekerde meldt de aanspraak zo snel mogelijk.
- De verzekerde werkt mee aan de afhandeling van de aanspraak.
- De verzekerde doet alles om de schade zo veel mogelijk te beperken.
- De verzekerde geeft ons alle informatie die nodig is om de omvang en de oorzaak van de schade vast te stellen.
- De verzekerde bewaart alle hardware, software en gegevens.
  - En geeft die voor onderzoek aan ons of een expert als dat nodig is.
- De verzekerde doet aangifte bij de politie bij een strafbaar feit.
  - Bijvoorbeeld bij cyberafpersing.
- De verzekerde helpt ons de betaalde schadevergoeding bij een ander terug te halen.
- De verzekerde geeft alle verzekeringen op die deze schade verzekeren.

70. Wat doet een verzekerde niet bij een aanspraak?

- Zeggen dat hij wel of niet schuldig is.
- Zeggen dat hij wel of niet aansprakelijk is.
- Betalen voor de schade.
- Iets zeggen of doen wat nadelig is voor ons.
- Post over de schade beantwoorden.
  - Bijvoorbeeld: een dagvaarding.
  - Bijvoorbeeld: een brief waarin iemand de verzekerde aansprakelijk stelt.

6. Privacy aansprakelijkheid

71. Wat als de verzekerde zich niet houdt aan de verplichtingen bij schade?

Dan verliest verzekerde het recht op vergoeding van schade en kosten.

- Alleen als wij hierdoor in een redelijk belang zijn geschaad.
- Erkenning van feiten heeft geen gevolgen voor de vergoeding van schade en kosten.
- Terechte erkenning van schuld of aansprakelijkheid heeft geen gevolgen voor de vergoeding van schade en kosten.

72. Wat als de verzekerde zich bewust niet houdt aan de verplichtingen bij schade?

- En verzekerde doet dit om ons te misleiden?
- Dan verliest verzekerde het recht op vergoeding van schade en kosten.

73. Welk bedrag voor schade en kosten samen is verzekerd?

Per aanspraak betalen wij maximaal het bedrag op het polisblad.

- Dit geldt voor alle verzekerden samen.
- Houden meerdere aanspraken verband met 1 oorzaak? Dan tellen we die aanspraken als 1 aanspraak.
- Leidt 1 gebeurtenis tot aanspraken op meerdere verzekerden? Dan tellen we die aanspraken als 1 aanspraak.
  - Het moment van de 1e melding, bepaalt of deze verzekering geldt voor de aanspraak.

Per verzekeringsjaar betalen wij voor schade en kosten samen een maximaal bedrag.

- Dit bedrag staat op het polisblad.
- Dit geldt voor alle verzekerden samen.
  - Het moment van de 1e melding bepaalt bij welk verzekeringsjaar de aanspraak hoort.
- Dit geldt voor alle rubrieken samen.

Let op: u betaalt eerst een eigen risico.

- Het eigen risico per verzekerde gebeurtenis staat op het polisblad.
- Voor kosten van verweer geldt geen eigen risico.

74. Wie bepaalt de hoogte van de schadevergoeding?

Wij.

- Is de schade hoger dan het verzekerd bedrag? Dan overleggen wij met u.

75. Wat als wij een ander de schadevergoeding hebben betaald?

U betaalt ons het eigen risico zo snel mogelijk terug.

- Het eigen risico per verzekerde gebeurtenis staat op het polisblad.
  - Is bij 1 aanspraak of gebeurtenis meer dan 1 regeling voor een eigen risico?
    - Dan geldt het hoogste eigen risico.

76. Wat als wij uitbetalen en een ander moet de schade aan u terugbetalen?

Wij worden in uw plaats de schuldeiser van die ander.

- De ander betaalt ons eerst alle kosten en vergoedingen terug.
- Daarna betaalt de ander u terug voor de betalingen die u nog heeft gedaan.
- U zorgt ervoor dat u en wij het recht hierop houden.

6. Privacy aansprakelijkheid

77. Wat als een verzekerde ook op een andere verzekering is verzekerd?

De andere verzekering gaat voor.

- Als de verzekerde daarop verzekerd is of verzekerd zou zijn als onze verzekering niet zou bestaan.
- Wij betalen de schade boven het maximale bedrag van de andere verzekering.
  - Wij betalen niet uw eigen risico bij de andere verzekering.

78. Wat als bij schade blijkt dat deze verzekering in strijd is met wet- en regelgeving?

Wij houden ons altijd aan de wet- en regelgeving die van toepassing is.

- We zoeken dan naar een oplossing die in lijn is met deze verzekering.

7. Netwerk aansprakelijkheid

Inhoud

Klik op de **vraag** om het antwoord te lezen

7. Netwerk aansprakelijkheid

Verzekerd

79. Wat is verzekerd?

De schade van een ander als u aansprakelijk bent.

- Voor gegevensinbreuk, diefstal of vernietigen van digitale data, wijzigen van digitale data en onbeschikbaarheid van het computersysteem bij een ander.
  - Door een cyberincident op uw computersysteem.
  - Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
    - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
    - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
    - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
  - Digitale data = elektronisch verwerkbare gegevens zoals tekst, cijfers, afbeeldingen, video en software.
  - Gegevensinbreuk = het verliezen van vertrouwelijke informatie of persoonsgegevens uit een computersysteem zonder toestemming van de verantwoordelijke.
    - Daardoor zijn vertrouwelijke informatie of persoonsgegevens weg, beschadigd, toegankelijk of openbaar.
    - Ook vertrouwelijke informatie of persoonsgegevens uit een computersysteem en geprint op papier.
    - Vertrouwelijke informatie = commercieel gevoelige bedrijfsinformatie.
      - Ook als niet is aangegeven dat de informatie vertrouwelijk is.

80. Welke kosten zijn verzekerd als u aansprakelijk gesteld wordt?

Kosten voor verweer.

- Alleen als de schade verzekerd is.
- En wij voor de u rechtshulp inschakelen.
  - Of vooraf toestemming geven voor inschakeling.
- En wij het verweer bepalen.
- Wij betalen dan ook de proceskosten.
- Bijvoorbeeld experts, onderzoeken, zittingen, taxaties, inspecties en procedures.
- Niet uw eigen algemene kosten.
  - Bijvoorbeeld salarissen en overheadkosten.

Kosten om direct dreigende schade te voorkomen of te beperken.

- Alleen als u voor de schade aansprakelijk bent.
- En de schade verzekerd is.
- En u deze kosten maakt of laat maken.
- Ook schade aan iets wat een verzekerde hiervoor gebruikt.
- En wij belang hebben bij de maatregelen.
- Ook als het niet lukt.

7. Netwerk aansprakelijkheid

Niet verzekerd

Kijk ook in de algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Sanctiewet 1977.
- Ernstige conflicten (molest).
- Atoomkernreacties.
- Fraude.
- Terrorisme.
- Niet nakomen voorwaarden.

Per situatie staat in de algemene voorwaarden precies wat nooit verzekerd is.

Hieronder staat wat verder niet verzekerd is bij uw cyberverzekering.

81. Wanneer bent u niet verzekerd?

Als wij volgens wet- of regelgeving u niet mogen verzekeren voor de hulp, schade of de kosten.

Als de gebeurtenis voor het begin van de verzekering plaatsvond.

- En de verzekerde de gebeurtenis had kunnen of moeten ontdekken.

82. Welke schade is niet verzekerd?

Schade door een cyberoperatie.

Cyberoperatie =

- Het gebruik van een computersysteem door een soevereine staat.
  - Ook: het gebruik van een computersysteem op aanwijzing van een soevereine staat.
  - Ook: het gebruik van een computersysteem onder controle van een soevereine staat.
    - Met als doel om een ander computersysteem te verstoren.
    - En/of de toegang tot dat computersysteem te blokkeren.
    - En/of de functionaliteit ervan te verminderen.
    - En/of data in een computersysteem te kopiëren, verwijderen, vernietigen, wijzigen of te blokkeren.
- Alleen als wij bewijzen dat het een cyberoperatie is.
  - Wij kijken naar elk beschikbaar, redelijk en objectief bewijs.
    - Bijvoorbeeld: de regering van de staat, waarin de getroffen computersystemen zich fysiek bevinden, geeft een verklaring uit waarin de cyberoperatie aan een andere soevereine staat wordt toegeschreven.
      - Of wordt toegeschreven aan personen die op aanwijzing of onder controle van een andere soevereine staat handelden.

Soevereine staat = een land dat binnen het grondgebied het hoogste gezag voert.

- En dat niet afhankelijk is van een andere staat.

Schade door terrorisme.

- Kijk ook in onze algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Wel verzekerd schade door cyberterrorisme.
  - Cyberterrorisme = Toegang krijgen tot of beschadigen, vernietigen, verstoren van uw computersystemen of computernetwerken door een of meerdere personen die dat doen met een politiek, religieus, ideologisch of politiek doel.

Schade waarvoor een bestuurder persoonlijk aansprakelijk wordt gesteld.

7. Netwerk aansprakelijkheid

vervolg

82. Welke schade is niet verzekerd?

Schade doordat apparatuur of een installatie van een ander niet of niet goed werkt.

- Apparaten en installaties die ervoor zorgen dat de energievoorziening blijft werken.
  - De energievoorziening van computersystemen en gegevensopslag.
  - Bijvoorbeeld, noodstroomvoorzieningen en stand-alone-generatoren.
- Airconditioning.
- Wel verzekerd als apparatuur of installatie van een IT dienstverlener niet goed werkt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade door gevaarlijke, verontreinigende of vervuilende stoffen.

Schade doordat uw computersysteem in beslag wordt genomen.

- Door een instantie die dat mag doen volgens de wet.
  - Bijvoorbeeld de overheid, een toezichthouder of een rechtbank.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Verlies van zaken.

- En de directe gevolgen daarvan.
- Ook als zaken kapot, weg of verontreinigd zijn.
- Zaken = losse spullen, onroerend goed of dieren.

Schade aan personen.

- Verwonding, ziekte (lichamelijk of geestelijk) of overlijden.
  - En de directe gevolgen daarvan.

Diefstal, schending of openbaarmaking van intellectueel eigendom.

- Bijvoorbeeld patenten, handelsmerken of auteursrechten.

Boetes en schadevergoedingen opgelegd door overheid of toezichthouder.

Beleggingsverliezen of handelsverliezen.

- Bijvoorbeeld als het niet meer lukt om effecten te verkopen.

Schade door geplande stilstand van uw computersystemen.

- Of van onderdelen van uw computersystemen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Betalingen die u doet om goede wil te tonen.

- Bijvoorbeeld kortingen, vouchers of coulancebetalingen.

7. Netwerk aansprakelijkheid

vervolg

82. Welke schade is niet verzekerd?

Schade aan branded currency of cryptogeld.

Branded currency = combinatie van digitale betaalmiddelen of loyaliteitspunten uitgevoerd via een digitale mobiele portemonnee. En uniek voor een bepaalde winkelketen of webshop.

- Bijvoorbeeld een digitale cadeaukaart, digitale coupons of digitale promotiecodes.

Cryptogeld = digitaal geld dat niet wordt uitgegeven door een bank. Cryptogeld zit in een digitale portemonnee.

- Bijvoorbeeld: bitcoins

Ook niet verzekerd: verlies van branded currency of cryptogeld.

83. Wanneer is aansprakelijkheid niet verzekerd?

Bij opzet van verzekerde of uw IT dienstverlener.

Verzekerde heeft geen dekking als verzekerde of de IT dienstverlener in strijd met het recht met opzet iets doet of niet doet waardoor schade ontstaat. De in feite toegebrachte schade is hierbij een te verwachten of normaal gevolg van wat een verzekerde of de IT dienstverlener doet of niet doet. Heeft verzekerde geen dekking? Dan heeft verzekerde dat ook niet voor de schade die mogelijk later nog ontstaat.

In welke gevallen geldt de opzetuitsluiting?

De uitsluiting geldt als verzekerde of de IT dienstverlener zich maatschappelijk ongewenst of crimineel gedraagt. Dat is in ieder geval zo bij gedragingen die een gevaar voor personen of zaken kunnen opleveren, zoals:

- Brandstichting, vernieling en beschadiging.
- Afpersing, bedrog, oplichting, bedreiging, beroving, verduistering, diefstal en inbraak. Ook als verzekerde of de IT dienstverlener dat met een computer of ander (technisch) hulpmiddel doet.
- Geweldpleging, mishandeling, doodslag en moord.

Er is sprake van opzet als verzekerde of de IT dienstverlener iets doet of niet doet waarbij verzekerde:

- De bedoeling heeft schade te veroorzaken (opzet als oogmerk).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener zeker weet dat er schade ontstaat (opzet met zekerheidsbewustzijn).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener de aanmerkelijke kans dat er schade ontstaat voor lief neemt. En toch handelt verzekerde (niet) zo (voorwaardelijk opzet).

Opzet wordt objectief uit de feiten, omstandigheden en/of gedragingen van verzekerde of de IT dienstverlener afgeleid.

Deze opzetuitsluiting geldt ook bij:

- Groepsaansprakelijkheid.
  - Als verzekerde niet zelf maar wel iemand in een groep waarvan verzekerde deel uitmaakt iets doet of niet doet.
- Alcohol en drugs.
  - Als verzekerde zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat verzekerde zijn eigen wil niet meer kon bepalen. Of als iemand in een groep waarvan verzekerde deel uitmaakt zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat hij of zij de eigen wil niet meer kon bepalen.

7. Netwerk aansprakelijkheid

vervolg

83. Wanneer is aansprakelijkheid niet verzekerd?

IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.

- Maar niet een dienstverlener:
  - Voor stroomvoorziening;
  - Voor telecommunicatie;
  - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade doordat de verzekerde seksueel of seksueel getint gedrag vertoont.

- Geldt alleen voor de verzekerde die het gedrag vertoont.
- Alleen of in een groep.
  - Ook niet verzekerd: als verzekerde zelf niets doet.
  - Maar wel deel uitmaakt van een groep die dit gedrag vertoont.

Als u aansprakelijk gesteld wordt door:

- Een (rechts)persoon met zeggenschap over u.
- Een rechtspersoon waar u zeggenschap over heeft.
  - Bijvoorbeeld een dochteronderneming.
  - Of waar uw dochteronderneming zeggenschap over heeft.
- Een rechtspersoon waarin u een financieel belang heeft.
- Een samenwerking of joint venture waar u onderdeel van bent.

Als u ook aansprakelijk bent volgens een contract.

- En deze contractuele aansprakelijkheid gaat voor op de wettelijke aansprakelijkheid.

Aansprakelijkheid door een beroepsfout.

- Bijvoorbeeld een verkeerd advies of ontwerp.

84. Bij welk gedrag bent u niet verzekerd?

Als u niet goed samenwerkt met de toezichthouder.

- Om te voorkomen dat een cyberincident of gegevensinbreuk plaatsvindt.
- Om te voorkomen dat aanspraak tegen u wordt ingediend.
- Om te voorkomen dat de toezichthouder u een straf of maatregel oplegt.
  - Als gevolg van een cyberincident, gegevensinbreuk of aanspraak.

Als u niet betaalt voor diensten of producten.

- En daardoor ontstaat schade of ontstaan kosten voor u of een ander.
- Bijvoorbeeld als u een leaseovereenkomst of licentie niet verlengt.
- Ook niet verzekerd als een IT dienstverlener van u niet betaalt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

7. Netwerk aansprakelijkheid

vervolg

84. Bij welk gedrag bent u niet verzekerd?

Als u zich niet houdt aan de preventieafspraken.

En de schade is hierdoor veroorzaakt of verergerd.

Preventieafspraken =

- U heeft een wachtwoordbeleid
  - Iedere gebruiker heeft een eigen account.
  - Alleen IT-administrators hebben toegang tot administrator accounts of privileged accounts.
  - Alle standaardwachtwoorden of standaardtoegangscodes worden bij het eerste gebruik direct gewijzigd en veilig bewaard.
  - Wachtwoorden bestaan uit 8 of meer tekens.
    - En bestaan uit een combinatie van minimaal drie van de volgende elementen: hoofdletters, kleine letters, speciale symbolen, cijfers.
  - U vermijdt gebruik van:
    - Woordenboekwoorden (bijvoorbeeld: “wachtwoord”).
    - Opeenvolgende of herhalende tekens (bijvoorbeeld “1234”, “1111”, “abcde”).
    - Toetsenbordpatronen (bijvoorbeeld “asdfgh”).
    - Persoonlijke informatie van de gebruiker (bijvoorbeeld een geboortedatum of een naam).
- U gebruikt een firewall om uw netwerk en computersystemen te beveiligen.
- U gebruikt anti-virus-, anti-spyware- en firewallsoftware die automatisch worden geüpdatet.
  - Of vergelijkbare malware-beveiligingssoftware.
  - Als het nodig is wordt deze software wekelijks handmatig geüpdatet.
- U past updates op uw computersystemen en computernetwerken automatisch toe.
  - Of u past deze handmatig toe als dat nodig is.
  - Als die updates zijn uitgegeven om uw computersystemen of computernetwerken te beschermen.
  - Voor computersystemen of computernetwerken die met internet zijn verbonden past u de update toe binnen 30 dagen nadat de update is gepubliceerd.
  - Voor Operationele technologie (OT) en Embedded systems past u de update toe binnen 90 dagen nadat de update is gepubliceerd.
  - Of binnen de periode die de betreffende fabrikant aanbeveelt.
- Voor andere computersystemen past u de update toe binnen 60 dagen nadat de update is gepubliceerd.
- U maakt wekelijks backups van digitale data op uw computersystemen.
- U test regelmatig herstelprocedures van uw computersystemen.
- U bewaart de back-up apart van uw computersystemen waarop de originele digitale data staat.
  - Bijvoorbeeld op een andere server op een andere locatie of bij een andere clouddienst.
- U vervangt software en hardware uiterlijk 3 maanden nadat de fabrikant stopte met de ondersteuning.
  - Of u zorgt voor een upgrade.

7. Netwerk aansprakelijkheid

vervolg

84. Bij welk gedrag bent u niet verzekerd?

Als u één of meerdere van bovengenoemde maatregelen aan een ander bedrijf uitbesteedt:

- Dan staat in de overeenkomst met het andere bedrijf dat het verplicht is om de bovengenoemde maatregelen uit te voeren.
  - Wel verzekerd als u bewijst dat u zich per ongeluk niet hield aan de preventieafspraken.
  - Bijvoorbeeld als de schade wordt veroorzaakt of verergerd omdat u in de week van de gebeurtenis geen back-up maakte.
  - En u bewijst dat u in de periode voor de gebeurtenis wel altijd een back-up maakte.
  - En u bewijst dat de back-up tijdens de gebeurtenis niet gemaakt is door een technische storing waar u niets aan kon doen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Operationele technologie (OT) = een verzameling hardware en software die de werking van een industrieel proces kan beïnvloeden.
  - OT houdt meestal toezicht op fysieke processen zoals productie, energie, geneeskunde, gebouwenbeheer en ecosystemen.
- Embedded systems = een computersysteem met een specifieke taak en ingebed in een groter systeem.
  - Bijvoorbeeld een computersysteem in medische apparatuur.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

7. Netwerk aansprakelijkheid

Bij schade

85. Wanneer meldt een verzekerde een aanspraak?

Zo snel mogelijk.

- Meld het bij ons als u aansprakelijk gesteld bent.
- Of het waarschijnlijk is dat u later aansprakelijk gesteld wordt.
- Meld een aanspraak bij ons.
  - Een verzekerde meldt het ook als hij een gebeurtenis vermoedt.

86. Wanneer meldt een verzekerde een omstandigheid?

Zodra een verzekerde vermoedt dat een voorval leidt tot een aanspraak.

En het waarschijnlijk is dat hij de aanspraak ontvangt.

- Verzekerde meldt een omstandigheid altijd schriftelijk.
- Verzekerde geeft in de melding informatie over de gebeurtenis die tot schade heeft geleid.
- Verzekerde vermeldt wie de vermoedelijke eisers zijn.
- Verzekerde geeft alle informatie die hij heeft over de hoogte van het schadebedrag.

87. Welke omstandigheden meldt een verzekerde?

Omstandigheden waarvan u denkt dat die kunnen leiden tot een aanspraak.

- Komt de echte aanspraak binnen 30 dagen na stoppen van de verzekering? Dan bent u toch verzekerd.

88. Wanneer geldt een omstandigheid als gemeld?

Zodra wij schriftelijk bevestigen dat wij de melding als omstandighedenmelding accepteren.

89. Wat doet een verzekerde bij een aanspraak?

- De verzekerde meldt de aanspraak zo snel mogelijk.
- De verzekerde werkt mee aan de afhandeling van de aanspraak.
- De verzekerde doet alles om de schade zo veel mogelijk te beperken.
- De verzekerde geeft ons alle informatie die nodig is om de omvang en de oorzaak van de schade vast te stellen.
- De verzekerde bewaart alle hardware, software en gegevens.
  - En geeft die voor onderzoek aan ons of een expert als dat nodig is.
- De verzekerde doet aangifte bij de politie bij een strafbaar feit.
  - Bijvoorbeeld bij cyberafpersing.
- De verzekerde helpt ons de betaalde schadevergoeding bij een ander terug te halen.
- De verzekerde geeft alle verzekeringen op die deze schade verzekeren.

90. Wat doet een verzekerde niet bij een aanspraak?

- Zeggen dat hij wel of niet schuldig is.
- Zeggen dat hij wel of niet aansprakelijk is.
- Betalen voor de schade.
- Iets zeggen of doen wat nadelig is voor ons.
- Post over de schade beantwoorden.
  - Bijvoorbeeld: een dagvaarding.
  - Bijvoorbeeld: een brief waarin iemand de verzekerde aansprakelijk stelt.

7. Netwerk aansprakelijkheid

91. Wat als de verzekerde zich niet houdt aan de verplichtingen bij schade?

Dan verliest verzekerde het recht op vergoeding van schade en kosten.

- Alleen als wij hierdoor in een redelijk belang zijn geschaad.
- Erkenning van feiten heeft geen gevolgen voor de vergoeding van schade en kosten.
- Terechte erkenning van schuld of aansprakelijkheid heeft geen gevolgen voor de vergoeding van schade en kosten.

92. Wat als de verzekerde zich bewust niet houdt aan de verplichtingen bij schade?

- En verzekerde doet dit om ons te misleiden?
- Dan verliest verzekerde het recht op vergoeding van schade en kosten.

93. Welk bedrag voor schade en kosten samen is verzekerd?

Per aanspraak betalen wij maximaal het bedrag op het polisblad.

- Dit geldt voor alle verzekerden samen.
- Houden meerdere aanspraken verband met 1 oorzaak? Dan tellen we die aanspraken als 1 aanspraak.
- Leidt 1 gebeurtenis tot aanspraken op meerdere verzekerden? Dan tellen we die aanspraken als 1 aanspraak.
  - Het moment van de 1e melding, bepaalt of deze verzekering geldt voor de aanspraak.

Per verzekeringsjaar betalen wij voor schade en kosten samen een maximaal bedrag.

- Dit bedrag staat op het polisblad.
- Dit geldt voor alle verzekerden samen.
  - Het moment van de 1e melding bepaalt bij welk verzekeringsjaar de aanspraak hoort.
- Dit geldt voor alle rubrieken samen.

Let op: u betaalt eerst een eigen risico.

- Het eigen risico per verzekerde gebeurtenis staat op het polisblad.
- Voor kosten van verweer geldt geen eigen risico.

94. Wie bepaalt de hoogte van de schadevergoeding?

Wij.

- Is de schade hoger dan het verzekerd bedrag? Dan overleggen wij met u.

95. Wat als wij een ander de schadevergoeding hebben betaald?

U betaalt ons het eigen risico zo snel mogelijk terug.

- Het eigen risico per verzekerde gebeurtenis staat op het polisblad.
  - Is bij 1 aanspraak of gebeurtenis meer dan 1 regeling voor een eigen risico?
    - Dan geldt het hoogste eigen risico.

96. Wat als wij uitbetalen en een ander moet de schade aan u terugbetalen?

Wij worden in uw plaats de schuldeiser van die ander.

- De ander betaalt ons eerst alle kosten en vergoedingen terug.
- Daarna betaalt de ander u terug voor de betalingen die u nog heeft gedaan.
- U zorgt ervoor dat u en wij het recht hierop houden.

7. Netwerk aansprakelijkheid

97. Wat als een verzekerde ook op een andere verzekering is verzekerd?

De andere verzekering gaat voor.

- Als de verzekerde daarop verzekerd is of verzekerd zou zijn als onze verzekering niet zou bestaan.
- Wij betalen de schade boven het maximale bedrag van de andere verzekering.
  - Wij betalen niet uw eigen risico bij de andere verzekering.

98. Wat als bij schade blijkt dat deze verzekering in strijd is met wet- en regelgeving?

Wij houden ons altijd aan de wet- en regelgeving die van toepassing is.

- We zoeken dan naar een oplossing die in lijn is met deze verzekering.

8. Cyberdiefstal

Inhoud

Klik op de **vraag** om het antwoord te lezen

8. Cyberdiefstal

Verzekerd

99. Wat is verzekerd?

Kosten voor een expert die de diefstal of een vermoeden daarvan voor u onderzoekt.

- De expert deelt de resultaten van het onderzoek met u.
- Wij kiezen de expert.

Kosten voor een expert die de diefstal beperkt.

- Bijvoorbeeld door getroffen gebruikersaccounts uit te schakelen of door malware te verwijderen.
- Wij kiezen de expert.

Kosten voor het documenteren van het cyberincident door de expert die de cyberdiefstal voor u onderzoekt.

- Ook voor het opstellen van advies voor het beter beveiligen van uw computersysteem.
  - Tegen vergelijkbare cyberdiefstallen.

Kosten voor het inrichten en bemannen van een crisis management centrum door experts bij een cyberdiefstal.

- Ook kosten voor het inrichten en bemannen van een call centre.
  - Alleen verzekerd als wij toestemming geven voor inschakeling.
  - Wij kiezen de expert.
  - Wij vergoeden de kosten tot 30 dagen nadat u de gebeurtenis bij ons meldde.

Diefstal van uw geld.

- Doordat een ander een bedrag elektronisch overmaakt vanaf uw rekening.
  - Zonder uw toestemming.
- Doordat een ander gegevens in uw computersysteem wijzigt.
  - Zonder uw toestemming.
  - Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
    - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
    - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
    - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Alleen verzekerd als u de gestolen bedragen niet terug kunt krijgen.
- Niet verzekerd: diefstal van cryptogeld.

100. Welk bedrag voor kosten is verzekerd?

Wij betalen maximaal het verzekerd bedrag per gebeurtenis.

- Het verzekerd bedrag staat op het polisblad.
- Dit geldt voor alle verzekerden samen.
- Dit geldt voor alle rubrieken samen.
- Houden meerdere gebeurtenissen verband met 1 oorzaak? Dan tellen we die gebeurtenissen als 1 gebeurtenis.

Per verzekeringsjaar betalen wij een maximaal bedrag.

- Dit bedrag staat op het polisblad.
- Dit geldt voor alle verzekerden samen.
  - Het moment van de 1e melding bepaalt bij welk verzekeringsjaar de gebeurtenis hoort.
- Dit geldt voor alle rubrieken samen.

Let op: u betaalt eerst een eigen risico.

- Het eigen risico per verzekerde gebeurtenis staat op het polisblad.

8. Cyberdiefstal

101. Welke kosten zijn boven het verzekerd bedrag verzekerd?

Kosten van experts.

- Alleen voor het bepalen van de hoogte van de schade.
- De kosten van onze expert.
- De kosten van de expert van verzekerde tot en met de kosten van onze expert.
  - Rekent de expert van verzekerde meer? Dan blijven die extra kosten voor rekening van verzekerde.
- De kosten van de 3e expert.
- Alle experts zijn ingeschreven in het register van het Nederlands Instituut Van Register Experts (NIVRE).
  - Of bij een vergelijkbare beroepsorganisatie.
    - En in de statuten en reglementen van deze organisatie:
      - Staat een duidelijke klacht- en tuchtprocedure.
      - Zijn de eisen beschreven voor permanente opleiding van experts.
  - Alle experts houden zich aan de Gedragscode schade-expertiseorganisaties van het Verbond van Verzekeraars.

Voldoet een expert niet aan deze eisen? Dan zijn de kosten van die expert niet verzekerd.

Let op: we betalen alleen als deze kosten noodzakelijk zijn door een schade die verzekerd is.

8. Cyberdiefstal

Niet verzekerd

Kijk ook in de algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Sanctiewet 1977.
- Ernstige conflicten (molest).
- Atoomkernreacties.
- Fraude.
- Terrorisme.
- Niet nakomen voorwaarden.

Per situatie staat in de algemene voorwaarden precies wat nooit verzekerd is.

Hieronder staat wat verder niet verzekerd is bij uw cyberverzekering.

102. Wanneer bent u niet verzekerd?

Als wij volgens wet- of regelgeving u niet mogen verzekeren voor de hulp, schade of de kosten.

Als de gebeurtenis voor het begin van de verzekering plaatsvond.

- En de verzekerde de gebeurtenis had kunnen of moeten ontdekken.

103. Welke schade is niet verzekerd?

Schade door een cyberoperatie.

Cyberoperatie =

- Het gebruik van een computersysteem door een soevereine staat.
  - Ook: het gebruik van een computersysteem op aanwijzing van een soevereine staat.
  - Ook: het gebruik van een computersysteem onder controle van een soevereine staat.
    - Met als doel om een ander computersysteem te verstoren.
    - En/of de toegang tot dat computersysteem te blokkeren.
    - En/of de functionaliteit ervan te verminderen.
    - En/of data in een computersysteem te kopiëren, verwijderen, vernietigen, wijzigen of te blokkeren.
- Alleen als wij bewijzen dat het een cyberoperatie is.
  - Wij kijken naar elk beschikbaar, redelijk en objectief bewijs.
    - Bijvoorbeeld: de regering van de staat, waarin de getroffen computersystemen zich fysiek bevinden, geeft een verklaring uit waarin de cyberoperatie aan een andere soevereine staat wordt toegeschreven.
      - Of wordt toegeschreven aan personen die op aanwijzing of onder controle van een andere soevereine staat handelden.

Soevereine staat = een land dat binnen het grondgebied het hoogste gezag voert.

- En dat niet afhankelijk is van een andere staat.

Schade door terrorisme.

- Kijk ook in onze algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Wel verzekerd schade door cyberterrorisme.
  - Cyberterrorisme = Toegang krijgen tot of beschadigen, vernietigen, verstoren van uw computersystemen of computernetwerken door een of meerdere personen die dat doen met een politiek, religieus, ideologisch of politiek doel.

8. Cyberdiefstal

vervolg

103. Welke schade is niet verzekerd?

Schade doordat apparatuur of een installatie van een ander niet of niet goed werkt.

- Apparaten en installaties die ervoor zorgen dat de energievoorziening blijft werken.
  - De energievoorziening van computersystemen en gegevensopslag.
  - Bijvoorbeeld, noodstroomvoorzieningen en stand-alone-generatoren.
- Airconditioning.
- Wel verzekerd als apparatuur of installatie van een IT dienstverlener niet goed werkt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade door gevaarlijke, verontreinigende of vervuilende stoffen.

Schade doordat uw computersysteem in beslag wordt genomen.

- Door een instantie die dat mag doen volgens de wet.
  - Bijvoorbeeld de overheid, een toezichthouder of een rechtbank.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Verlies van zaken.

- En de directe gevolgen daarvan.
- Ook als zaken kapot, weg of verontreinigd zijn.
- Zaken = losse spullen, onroerend goed of dieren.

Schade aan personen.

- Verwonding, ziekte (lichamelijk of geestelijk) of overlijden.
  - En de directe gevolgen daarvan.

Diefstal, schending of openbaarmaking van intellectueel eigendom.

- Bijvoorbeeld patenten, handelsmerken of auteursrechten.

Boetes en schadevergoedingen opgelegd door overheid of toezichthouder.

Beleggingsverliezen of handelsverliezen.

- Bijvoorbeeld als het niet meer lukt om effecten te verkopen.

Schade door geplande stilstand van uw computersystemen.

- Of van onderdelen van uw computersystemen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Betalingen die u doet om goede wil te tonen.

- Bijvoorbeeld kortingen, vouchers of coulancebetalingen.

8. Cyberdiefstal

vervolg

103. Welke schade is niet verzekerd?

Schade aan branded currency of cryptogeld.

Branded currency = combinatie van digitale betaalmiddelen of loyaliteitspunten uitgevoerd via een digitale mobiele portemonnee. En uniek voor een bepaalde winkelketen of webshop.

- Bijvoorbeeld een digitale cadeaukaart, digitale coupons of digitale promotiecodes.

Cryptogeld = digitaal geld dat niet wordt uitgegeven door een bank. Cryptogeld zit in een digitale portemonnee.

- Bijvoorbeeld: bitcoins

Ook niet verzekerd: verlies van branded currency of cryptogeld.

104. Bij welk gedrag bent u niet verzekerd?

Bij opzet van verzekerde of uw IT dienstverlener.

Verzekerde heeft geen dekking als verzekerde of de IT dienstverlener in strijd met het recht met opzet iets doet of niet doet waardoor schade ontstaat. De in feite toegebrachte schade is hierbij een te verwachten of normaal gevolg van wat een verzekerde of de IT dienstverlener doet of niet doet. Heeft verzekerde geen dekking? Dan heeft verzekerde dat ook niet voor de schade die mogelijk later nog ontstaat.

In welke gevallen geldt de opzetuitsluiting?

De uitsluiting geldt als verzekerde of de IT dienstverlener zich maatschappelijk ongewenst of crimineel gedraagt. Dat is in ieder geval zo bij gedragingen die een gevaar voor personen of zaken kunnen opleveren, zoals:

- Brandstichting, vernieling en beschadiging.
- Afpersing, bedrog, oplichting, bedreiging, beroving, verduistering, diefstal en inbraak. Ook als verzekerde of de IT dienstverlener dat met een computer of ander (technisch) hulpmiddel doet.
- Geweldpleging, mishandeling, doodslag en moord.

Er is sprake van opzet als verzekerde of de IT dienstverlener iets doet of niet doet waarbij verzekerde:

- De bedoeling heeft schade te veroorzaken (opzet als oogmerk).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener zeker weet dat er schade ontstaat (opzet met zekerheidsbewustzijn).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener de aanmerkelijke kans dat er schade ontstaat voor lief neemt. En toch handelt verzekerde (niet) zo (voorwaardelijk opzet).

Opzet wordt objectief uit de feiten, omstandigheden en/of gedragingen van verzekerde of de IT dienstverlener afgeleid.

Deze opzetuitsluiting geldt ook bij:

- Groepsaansprakelijkheid.
  - Als verzekerde niet zelf maar wel iemand in een groep waarvan verzekerde deel uitmaakt iets doet of niet doet.
- Alcohol en drugs.
  - Als verzekerde zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat verzekerde zijn eigen wil niet meer kon bepalen. Of als iemand in een groep waarvan verzekerde deel uitmaakt zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat hij of zij de eigen wil niet meer kon bepalen.

8. Cyberdiefstal

vervolg

104. Bij welk gedrag bent u niet verzekerd?

IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.

- Maar niet een dienstverlener:
  - Voor stroomvoorziening;
  - Voor telecommunicatie;
  - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade doordat de verzekerde seksueel of seksueel getint gedrag vertoont.

- Geldt alleen voor de verzekerde die het gedrag vertoont.
- Alleen of in een groep.
  - Ook niet verzekerd: als verzekerde zelf niets doet.
  - Maar wel deel uitmaakt van een groep die dit gedrag vertoont.

Als u niet goed samenwerkt met de toezichthouder.

- Om te voorkomen dat een cyberincident of gegevensinbreuk plaatsvindt.
- Om te voorkomen dat aanspraak tegen u wordt ingediend.
- Om te voorkomen dat de toezichthouder u een straf of maatregel oplegt.
  - Als gevolg van een cyberincident, gegevensinbreuk of aanspraak.

Als u niet betaalt voor diensten of producten.

- En daardoor ontstaat schade of ontstaan kosten voor u of een ander.
- Bijvoorbeeld als u een leaseovereenkomst of licentie niet verlengt.
- Ook niet verzekerd als een IT dienstverlener van u niet betaalt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

8. Cyberdiefstal

vervolg

104. Bij welk gedrag bent u niet verzekerd?

Als u zich niet houdt aan de preventieafspraken.

En de schade is hierdoor veroorzaakt of verergerd.

Preventieafspraken =

- U heeft een wachtwoordbeleid
  - Iedere gebruiker heeft een eigen account.
  - Alleen IT-administrators hebben toegang tot administrator accounts of privileged accounts.
  - Alle standaardwachtwoorden of standaardtoegangscodes worden bij het eerste gebruik direct gewijzigd en veilig bewaard.
  - Wachtwoorden bestaan uit 8 of meer tekens.
    - En bestaan uit een combinatie van minimaal drie van de volgende elementen: hoofdletters, kleine letters, speciale symbolen, cijfers.
  - U vermijdt gebruik van:
    - Woordenboekwoorden (bijvoorbeeld: “wachtwoord”).
    - Opeenvolgende of herhalende tekens (bijvoorbeeld “1234”, “1111”, “abcde”).
    - Toetsenbordpatronen (bijvoorbeeld “asdfgh”).
    - Persoonlijke informatie van de gebruiker (bijvoorbeeld een geboortedatum of een naam).
- U gebruikt een firewall om uw netwerk en computersystemen te beveiligen.
- U gebruikt anti-virus-, anti-spyware- en firewallsoftware die automatisch worden geüpdatet.
  - Of vergelijkbare malware-beveiligingssoftware.
  - Als het nodig is wordt deze software wekelijks handmatig geüpdatet.
- U past updates op uw computersystemen en computernetwerken automatisch toe.
  - Of u past deze handmatig toe als dat nodig is.
  - Als die updates zijn uitgegeven om uw computersystemen of computernetwerken te beschermen.
  - Voor computersystemen of computernetwerken die met internet zijn verbonden past u de update toe binnen 30 dagen nadat de update is gepubliceerd.
  - Voor Operationele technologie (OT) en Embedded systems past u de update toe binnen 90 dagen nadat de update is gepubliceerd.
  - Of binnen de periode die de betreffende fabrikant aanbeveelt.
- Voor andere computersystemen past u de update toe binnen 60 dagen nadat de update is gepubliceerd.
- U maakt wekelijks backups van digitale data op uw computersystemen.
- U test regelmatig herstelprocedures van uw computersystemen.
- U bewaart de back-up apart van uw computersystemen waarop de originele digitale data staat.
  - Bijvoorbeeld op een andere server op een andere locatie of bij een andere clouddienst.
- U vervangt software en hardware uiterlijk 3 maanden nadat de fabrikant stopte met de ondersteuning.
  - Of u zorgt voor een upgrade.

Als u één of meerdere van bovengenoemde maatregelen aan een ander bedrijf uitbesteedt:

- Dan staat in de overeenkomst met het andere bedrijf dat het verplicht is om de bovengenoemde maatregelen uit te voeren.
  - Wel verzekerd als u bewijst dat u zich per ongeluk niet hield aan de preventieafspraken.
    - Bijvoorbeeld als de schade wordt veroorzaakt of verergerd omdat u in de week van de gebeurtenis geen back-up maakte.
    - En u bewijst dat u in de periode voor de gebeurtenis wel altijd een back-up maakte.
    - En u bewijst dat de back-up tijdens de gebeurtenis niet gemaakt is door een technische storing waar u niets aan kon doen.

8. Cyberdiefstal

vervolg

104. Bij welk gedrag bent u niet verzekerd?

- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Operationele technologie (OT) = een verzameling hardware en software die de werking van een industrieel proces kan beïnvloeden.
  - OT houdt meestal toezicht op fysieke processen zoals productie, energie, geneeskunde, gebouwenbeheer en ecosystemen.
- Embedded systems = een computersysteem met een specifieke taak en ingebed in een groter systeem.
  - Bijvoorbeeld een computersysteem in medische apparatuur.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

8. Cyberdiefstal

Bij schade

105. Wanneer meldt een verzekerde een gebeurtenis?

Zo snel mogelijk.

- Meld een gebeurtenis bij ons.
  - Een verzekerde meldt het ook als hij een gebeurtenis vermoedt.

106. Wat doet een verzekerde bij schade?

- De verzekerde meldt de schade zo snel mogelijk.
- De verzekerde werkt mee aan de afhandeling van de schade.
- De verzekerde doet alles om de schade zo veel mogelijk te beperken.
- De verzekerde geeft ons alle informatie die nodig is om de omvang en de oorzaak van de schade vast te stellen.
- De verzekerde bewaart alle hardware, software en gegevens.
  - En geeft die voor onderzoek aan ons of een expert als dat nodig is.
- De verzekerde doet aangifte bij de politie bij een strafbaar feit.
  - Bijvoorbeeld bij cyberafpersing.
- De verzekerde helpt ons de betaalde schadevergoeding bij een ander terug te halen.
- De verzekerde geeft alle verzekeringen op die deze schade verzekeren.
- De verzekerde tekent een geheimhoudingsverklaring als de incident response provider daarom vraagt.
  - Tekent u niet? Dan kunnen wij uw schade mogelijk niet of niet volledig afhandelen.

107. Wie bepaalt de hoogte van het schadebedrag?

Of: wij.

Of: onze expert.

Of: onze expert met een expert van de verzekerde.

- Voor zij starten, kiezen zij een 3e expert.
  - Die bepaalt de schade als zij het oneens zijn.
  - Hij bepaalt de schade tussen het laagste en hoogste bedrag.
- Alle experts zijn ingeschreven in het register van het Nederlands Instituut Van Register Experts (NIVRE).
  - Of bij een vergelijkbare beroepsorganisatie.
    - En in de statuten en reglementen van deze organisatie:
      - Staat een duidelijke klacht- en tuchtprocedure.
      - Zijn de eisen beschreven voor permanente opleiding van experts.
  - Alle experts houden zich aan de Gedragscode schade-expertiseorganisaties van het Verbond van Verzekeraars.

Let op: dat wij het schadebedrag bepalen, betekent niet dat we de schade betalen.

108. Wat als een verzekerde ook op een andere verzekering is verzekerd?

De andere verzekering gaat voor.

- Als de verzekerde daarop verzekerd is of verzekerd zou zijn als onze verzekering niet zou bestaan.
- Wij betalen de schade boven het maximale bedrag van de andere verzekering.
  - Wij betalen niet uw eigen risico bij de andere verzekering.

109. Wat als bij schade blijkt dat deze verzekering in strijd is met wet- en regelgeving?

Wij houden ons altijd aan de wet- en regelgeving die van toepassing is.

- We zoeken dan naar een oplossing die in lijn is met deze verzekering.

9. Media-aansprakelijkheid

Inhoud

Klik op de **vraag** om het antwoord te lezen

9. Media-aansprakelijkheid

Verzekerd

110. Wat is verzekerd?

De schade van een ander door uw online media-activiteiten als u aansprakelijk bent.

- Als u aansprakelijk bent voor de gevolgen van:
  - Smaad.
  - Schending van privacy.
  - Inbreuk op auteursrecht, eigendomsrecht, slogans, handelsmerken, handelsnamen, dienstmerken, dienstnamen of domeinnamen.
- Online media-activiteiten =
  - Verspreiden van tekst, beeld, video of geluid.
    - Via uw website of uw social media.
    - Via e-mail met nieuws, promotie, reclame of vergelijkbare inhoud.
      - Naar personen buiten uw bedrijf of naar andere bedrijven.

111. Welke kosten zijn verzekerd als u aansprakelijk gesteld wordt?

Kosten voor verweer.

- Alleen als de schade verzekerd is.
- En wij voor u rechtshulp inschakelen.
  - Of vooraf toestemming geven voor inschakeling.
- En wij het verweer bepalen.
- Wij betalen dan ook de proceskosten.
- Bijvoorbeeld experts, onderzoeken, zittingen, taxaties, inspecties en procedures.
- Niet uw eigen algemene kosten.
  - Bijvoorbeeld salarissen en overheadkosten.

Kosten om direct dreigende schade te voorkomen of te beperken.

- Alleen als u aansprakelijk bent voor de schade.
- En de schade verzekerd is.
- En u deze kosten maakt of laat maken.
- Ook schade aan iets wat een verzekerde hiervoor gebruikt.
- En wij belang hebben bij de maatregelen.
- Ook als het niet lukt.

9. Media-aansprakelijkheid

Niet verzekerd

Kijk ook in de algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Sanctiewet 1977.
- Ernstige conflicten (molest).
- Atoomkernreacties.
- Fraude.
- Terrorisme.
- Niet nakomen voorwaarden.

Per situatie staat in de algemene voorwaarden precies wat nooit verzekerd is.

Hieronder staat wat verder niet verzekerd is bij uw cyberverzekering.

112. Wanneer bent u niet verzekerd?

Als wij volgens wet- of regelgeving u niet mogen verzekeren voor de hulp, schade of de kosten.

Als de gebeurtenis voor het begin van de verzekering plaatsvond.

- En de verzekerde de gebeurtenis had kunnen of moeten ontdekken.

113. Welke schade is niet verzekerd?

Schade door een cyberoperatie.

Cyberoperatie =

- Het gebruik van een computersysteem door een soevereine staat.
  - Ook: het gebruik van een computersysteem op aanwijzing van een soevereine staat.
  - Ook: het gebruik van een computersysteem onder controle van een soevereine staat.
    - Met als doel om een ander computersysteem te verstoren.
    - En/of de toegang tot dat computersysteem te blokkeren.
    - En/of de functionaliteit ervan te verminderen.
    - En/of data in een computersysteem te kopiëren, verwijderen, vernietigen, wijzigen of te blokkeren.
- Alleen als wij bewijzen dat het een cyberoperatie is.
  - Wij kijken naar elk beschikbaar, redelijk en objectief bewijs.
    - Bijvoorbeeld: de regering van de staat, waarin de getroffen computersystemen zich fysiek bevinden, geeft een verklaring uit waarin de cyberoperatie aan een andere soevereine staat wordt toegeschreven.
      - Of wordt toegeschreven aan personen die op aanwijzing of onder controle van een andere soevereine staat handelden.

Soevereine staat = een land dat binnen het grondgebied het hoogste gezag voert.

- En dat niet afhankelijk is van een andere staat.

Schade door terrorisme.

- Kijk ook in onze algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Wel verzekerd schade door cyberterrorisme.
  - Cyberterrorisme = Toegang krijgen tot of beschadigen, vernietigen, verstoren van uw computersystemen of computernetwerken door een of meerdere personen die dat doen met een politiek, religieus, ideologisch of politiek doel.

Schade doordat u de verkeerde beschrijving of prijs geeft van goederen of diensten.

Schade waarvoor een bestuurder persoonlijk aansprakelijk wordt gesteld

9. Media-aansprakelijkheid

vervolg

113. Welke schade is niet verzekerd?

Schade doordat apparatuur of een installatie van een ander niet of niet goed werkt.

- Apparaten en installaties die ervoor zorgen dat de energievoorziening blijft werken.
  - De energievoorziening van computersystemen en gegevensopslag.
  - Bijvoorbeeld, noodstroomvoorzieningen en stand-alone-generatoren.
- Airconditioning.
- Wel verzekerd als apparatuur of installatie van een IT dienstverlener niet goed werkt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade door gevaarlijke, verontreinigende of vervuilende stoffen.

Schade doordat uw computersysteem in beslag wordt genomen.

- Door een instantie die dat mag doen volgens de wet.
  - Bijvoorbeeld de overheid, een toezichthouder of een rechtbank.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Verlies van zaken.

- En de directe gevolgen daarvan.
- Ook als zaken kapot, weg of verontreinigd zijn.
- Zaken = losse spullen, onroerend goed of dieren.

Schade aan personen.

- Verwonding, ziekte (lichamelijk of geestelijk) of overlijden.
  - En de directe gevolgen daarvan.
- Wel verzekerd is schade door aantasting van het gevoel voor eigenwaarde en de waardering die verzekerde bij anderen geniet.
  - De wet noemt dit aantasting van eer of goede naam.
- Wel verzekerd is schade door ernstige schendingen van de persoonlijke levenssfeer.
  - **Let op:** niet geestelijk letsel!
    - De wet noemt dit een persoonsaantasting.

Diefstal, schending of openbaarmaking van patenten.

Boetes en schadevergoedingen opgelegd door overheid of toezichthouder.

Beleggingsverliezen of handelsverliezen.

- Bijvoorbeeld als het niet meer lukt om effecten te verkopen.

9. Media-aansprakelijkheid

vervolg

113. Welke schade is niet verzekerd?

Schade door geplande stilstand van uw computersystemen.

- Of van onderdelen van uw computersystemen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Betalingen die u doet om goede wil te tonen.

- Bijvoorbeeld kortingen, vouchers of coulancebetalingen.

Schade doordat de verzekerde seksueel of seksueel getint gedrag vertoont.

- Geldt alleen voor de verzekerde die het gedrag vertoont.
- Alleen of in een groep.
  - Ook niet verzekerd: als verzekerde zelf niets doet.
  - Maar wel deel uitmaakt van een groep die dit gedrag vertoont.

Schade aan branded currency of cryptogeld.

Branded currency = combinatie van digitale betaalmiddelen of loyaliteitspunten uitgevoerd via een digitale mobiele portemonnee. En uniek voor een bepaalde winkelketen of webshop.

- Bijvoorbeeld een digitale cadeaukaart, digitale coupons of digitale promotiecodes.

Cryptogeld = digitaal geld dat niet wordt uitgegeven door een bank. Cryptogeld zit in een digitale portemonnee.

- Bijvoorbeeld: bitcoins

Ook niet verzekerd: verlies van branded currency of cryptogeld.

114. Wanneer is aansprakelijkheid niet verzekerd?

Als u aansprakelijk gesteld wordt door:

- Een (rechts)persoon met zeggenschap over u.
- Een rechtspersoon waar u zeggenschap over heeft.
  - Bijvoorbeeld een dochteronderneming.
  - Of waar uw dochteronderneming zeggenschap over heeft.
- Een rechtspersoon waarin u een financieel belang heeft.

Een samenwerking of joint venture waar u onderdeel van bent.

Als u ook aansprakelijk bent volgens een contract.

- En deze contractuele aansprakelijkheid gaat voor op de wettelijke aansprakelijkheid.

Aansprakelijkheid door een beroepsfout.

- Bijvoorbeeld een verkeerd advies of ontwerp.

9. Media-aansprakelijkheid

115. Bij welk gedrag bent u niet verzekerd?

Bij opzet van verzekerde of uw IT dienstverlener.

Verzekerde heeft geen dekking als verzekerde of de IT dienstverlener in strijd met het recht met opzet iets doet of niet doet waardoor schade ontstaat. De in feite toegebrachte schade is hierbij een te verwachten of normaal gevolg van wat een verzekerde of de IT dienstverlener doet of niet doet. Heeft verzekerde geen dekking? Dan heeft verzekerde dat ook niet voor de schade die mogelijk later nog ontstaat.

In welke gevallen geldt de opzetuitsluiting?

De uitsluiting geldt als verzekerde of de IT dienstverlener zich maatschappelijk ongewenst of crimineel gedraagt. Dat is in ieder geval zo bij gedragingen die een gevaar voor personen of zaken kunnen opleveren, zoals:

- Brandstichting, vernieling en beschadiging.
- Afpersing, bedrog, oplichting, bedreiging, beroving, verduistering, diefstal en inbraak. Ook als verzekerde of de IT dienstverlener dat met een computer of ander (technisch) hulpmiddel doet.
- Geweldpleging, mishandeling, doodslag en moord.

Er is sprake van opzet als verzekerde of de IT dienstverlener iets doet of niet doet waarbij verzekerde:

- De bedoeling heeft schade te veroorzaken (opzet als oogmerk).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener zeker weet dat er schade ontstaat (opzet met zekerheidsbewustzijn).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener de aanmerkelijke kans dat er schade ontstaat voor lief neemt. En toch handelt verzekerde (niet) zo (voorwaardelijk opzet).

Opzet wordt objectief uit de feiten, omstandigheden en/of gedragingen van verzekerde of de IT dienstverlener afgeleid.

Deze opzetuitsluiting geldt ook bij:

- Groepsaansprakelijkheid.
  - Als verzekerde niet zelf maar wel iemand in een groep waarvan verzekerde deel uitmaakt iets doet of niet doet.
- Alcohol en drugs.
  - Als verzekerde zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat verzekerde zijn eigen wil niet meer kon bepalen. Of als iemand in een groep waarvan verzekerde deel uitmaakt zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat hij of zij de eigen wil niet meer kon bepalen.

IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.

- Maar niet een dienstverlener:
  - Voor stroomvoorziening;
  - Voor telecommunicatie;
  - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Als u niet goed samenwerkt met de toezichthouder.

- Om te voorkomen dat een cyberincident of gegevensinbreuk plaatsvindt.
- Om te voorkomen dat aanspraak tegen u wordt ingediend.
- Om te voorkomen dat de toezichthouder u een straf of maatregel oplegt.
  - Als gevolg van een cyberincident, gegevensinbreuk of aanspraak.

9. Media-aansprakelijkheid

vervolg

115. Bij welk gedrag bent u niet verzekerd?

Als u niet betaalt voor diensten of producten.

- En daardoor ontstaat schade of ontstaan kosten voor u of een ander.
- Bijvoorbeeld als u een leaseovereenkomst of licentie niet verlengt.
- Ook niet verzekerd als een IT dienstverlener van u niet betaalt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Als u zich niet houdt aan de preventieafspraken.

En de schade is hierdoor veroorzaakt of verergerd.

Preventieafspraken =

- U heeft een wachtwoordbeleid
  - Iedere gebruiker heeft een eigen account.
  - Alleen IT-administrators hebben toegang tot administrator accounts of privileged accounts.
  - Alle standaardwachtwoorden of standaardtoegangscodes worden bij het eerste gebruik direct gewijzigd en veilig bewaard.
  - Wachtwoorden bestaan uit 8 of meer tekens.
    - En bestaan uit een combinatie van minimaal drie van de volgende elementen: hoofdletters, kleine letters, speciale symbolen, cijfers.
  - U vermijdt gebruik van:
    - Woordenboekwoorden (bijvoorbeeld: “wachtwoord”).
    - Opeenvolgende of herhalende tekens (bijvoorbeeld “1234”, “1111”, “abcde”).
    - Toetsenbordpatronen (bijvoorbeeld “asdfgh”).
    - Persoonlijke informatie van de gebruiker (bijvoorbeeld een geboortedatum of een naam).
- U gebruikt een firewall om uw netwerk en computersystemen te beveiligen.
- U gebruikt anti-virus-, anti-spyware- en firewallsoftware die automatisch worden geüpdatet.
  - Of vergelijkbare malware-beveiligingssoftware.
  - Als het nodig is wordt deze software wekelijks handmatig geüpdatet.
- U past updates op uw computersystemen en computernetwerken automatisch toe.
  - Of u past deze handmatig toe als dat nodig is.
  - Als die updates zijn uitgegeven om uw computersystemen of computernetwerken te beschermen.
  - Voor computersystemen of computernetwerken die met internet zijn verbonden past u de update toe binnen 30 dagen nadat de update is gepubliceerd.
  - Voor Operationele technologie (OT) en Embedded systems past u de update toe binnen 90 dagen nadat de update is gepubliceerd.
  - Of binnen de periode die de betreffende fabrikant aanbeveelt.
- Voor andere computersystemen past u de update toe binnen 60 dagen nadat de update is gepubliceerd.
- U maakt wekelijks backups van digitale data op uw computersystemen.
- U test regelmatig herstelprocedures van uw computersystemen.

9. Media-aansprakelijkheid

vervolg

115. Bij welk gedrag bent u niet verzekerd?

- U bewaart de back-up apart van uw computersystemen waarop de originele digitale data staat.
  - Bijvoorbeeld op een andere server op een andere locatie of bij een andere clouddienst.
- U vervangt software en hardware uiterlijk 3 maanden nadat de fabrikant stopte met de ondersteuning.
  - Of u zorgt voor een upgrade.

Als u één of meerdere van bovengenoemde maatregelen aan een ander bedrijf uitbesteedt:

- Dan staat in de overeenkomst met het andere bedrijf dat het verplicht is om de bovengenoemde maatregelen uit te voeren.
  - Wel verzekerd als u bewijst dat u zich per ongeluk niet hield aan de preventieafspraken.
- Bijvoorbeeld als de schade wordt veroorzaakt of verergerd omdat u in de week van de gebeurtenis geen back-up maakte.
- En u bewijst dat u in de periode voor de gebeurtenis wel altijd een back-up maakte.
- En u bewijst dat de back-up tijdens de gebeurtenis niet gemaakt is door een technische storing waar u niets aan kon doen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Operationele technologie (OT) = een verzameling hardware en software die de werking van een industrieel proces kan beïnvloeden.
  - OT houdt meestal toezicht op fysieke processen zoals productie, energie, geneeskunde, gebouwenbeheer en ecosystemen.
- Embedded systems = een computersysteem met een specifieke taak en ingebed in een groter systeem.
  - Bijvoorbeeld een computersysteem in medische apparatuur.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

9. Media-aansprakelijkheid

Bij schade

116. Wanneer meldt een verzekerde een aanspraak?

Zo snel mogelijk.

- Meld het bij ons als u aansprakelijk gesteld bent.
- Of het waarschijnlijk is dat u later aansprakelijk gesteld wordt.
- Meld een aanspraak bij ons.
  - Een verzekerde meldt het ook als hij een gebeurtenis vermoedt.

117. Wanneer meldt een verzekerde een omstandigheid?

Zodra een verzekerde vermoedt dat een voorval leidt tot een aanspraak.

En het waarschijnlijk is dat hij de aanspraak ontvangt.

- Verzekerde meldt een omstandigheid altijd schriftelijk.
- Verzekerde geeft in de melding informatie over de gebeurtenis die tot schade heeft geleid.
- Verzekerde vermeldt wie de vermoedelijke eisers zijn.
- Verzekerde geeft alle informatie die hij heeft over de hoogte van het schadebedrag.

118. Welke omstandigheden meldt een verzekerde?

Omstandigheden waarvan u denkt dat die kunnen leiden tot een aanspraak.

- Komt de echte aanspraak binnen 30 dagen na stoppen van de verzekering? Dan bent u toch verzekerd.

119. Wanneer geldt een omstandigheid als gemeld?

Zodra wij schriftelijk bevestigen dat wij de melding als omstandighedenmelding accepteren.

120. Wat doet een verzekerde bij een aanspraak?

- De verzekerde meldt de aanspraak zo snel mogelijk.
- De verzekerde werkt mee aan de afhandeling van de aanspraak.
- De verzekerde doet alles om de schade zo veel mogelijk te beperken.
- De verzekerde geeft ons alle informatie die nodig is om de omvang en de oorzaak van de schade vast te stellen.
- De verzekerde bewaart alle hardware, software en gegevens.
  - En geeft die voor onderzoek aan ons of een expert als dat nodig is.
- De verzekerde doet aangifte bij de politie bij een strafbaar feit.
  - Bijvoorbeeld bij cyberafpersing.
- De verzekerde helpt ons de betaalde schadevergoeding bij een ander terug te halen.
- De verzekerde geeft alle verzekeringen op die deze schade verzekeren.

121. Wat doet een verzekerde niet bij een aanspraak?

- Zeggen dat hij wel of niet schuldig is.
- Zeggen dat hij wel of niet aansprakelijk is.
- Betalen voor de schade.
- Iets zeggen of doen wat nadelig is voor ons.
- Post over de schade beantwoorden.
  - Bijvoorbeeld: een dagvaarding.
  - Bijvoorbeeld: een brief waarin iemand de verzekerde aansprakelijk stelt.

9. Media-aansprakelijkheid

122. Wat als de verzekerde zich niet houdt aan de verplichtingen bij schade?

Dan verliest verzekerde het recht op vergoeding van schade en kosten.

- Alleen als wij hierdoor in een redelijk belang zijn geschaad.
- Erkenning van feiten heeft geen gevolgen voor de vergoeding van schade en kosten.
- Terechte erkenning van schuld of aansprakelijkheid heeft geen gevolgen voor de vergoeding van schade en kosten.

123. Welk bedrag voor schade en kosten samen is verzekerd?

Per aanspraak betalen wij maximaal het bedrag op het polisblad.

- Dit geldt voor alle verzekerden samen.
- Houden meerdere aanspraken verband met 1 oorzaak? Dan tellen we die aanspraken als 1 aanspraak.
- Leidt 1 gebeurtenis tot aanspraken op meerdere verzekerden? Dan tellen we die aanspraken als 1 aanspraak.
  - Het moment van de 1e melding, bepaalt of deze verzekering geldt voor de aanspraak.

Per verzekeringsjaar betalen wij voor schade en kosten samen een maximaal bedrag.

- Dit bedrag staat op het polisblad.
- Dit geldt voor alle verzekerden samen.
  - Het moment van de 1e melding bepaalt bij welk verzekeringsjaar de aanspraak hoort.
- Dit geldt voor alle rubrieken samen.

Let op: u betaalt eerst een eigen risico.

- Het eigen risico per verzekerde gebeurtenis staat op het polisblad.
- Voor kosten van verweer geldt geen eigen risico.

124. Wie bepaalt de hoogte van de schadevergoeding?

Wij.

- Is de schade hoger dan het verzekerd bedrag? Dan overleggen wij met u.

125. Wat als wij een ander de schadevergoeding hebben betaald?

U betaalt ons het eigen risico zo snel mogelijk terug.

- Het eigen risico per verzekerde gebeurtenis staat op het polisblad.
  - Is bij 1 aanspraak of gebeurtenis meer dan 1 regeling voor een eigen risico?
    - Dan geldt het hoogste eigen risico.

126. Wat als wij uitbetalen en een ander moet de schade aan u terugbetalen?

Wij worden in uw plaats de schuldeiser van die ander.

- De ander betaalt ons eerst alle kosten en vergoedingen terug.
- Daarna betaalt de ander u terug voor de betalingen die u nog heeft gedaan.
- U zorgt ervoor dat u en wij het recht hierop houden.

127. Wat als een verzekerde ook op een andere verzekering is verzekerd?

De andere verzekering gaat voor.

- Als de verzekerde daarop verzekerd is of verzekerd zou zijn als onze verzekering niet zou bestaan.
- Wij betalen de schade boven het maximale bedrag van de andere verzekering.
  - Wij betalen niet uw eigen risico bij de andere verzekering.

9. Media-aansprakelijkheid

128. Wat als bij schade blijkt dat deze verzekering in strijd is met wet- en regelgeving?

Wij houden ons altijd aan de wet- en regelgeving die van toepassing is.

- We zoeken dan naar een oplossing die in lijn is met deze verzekering.

10. PCI-DSS

Inhoud

Klik op de **vraag** om het antwoord te lezen

10. PCI-DSS

Verzekerd

129. Wat is verzekerd?

Overtreden van de PCI-DSS door een cyberincident.

- PCI-DSS = Payment Card Industry Data Security Standards.
- Cyberincident =
  - Malware op uw computersystemen of computernetwerk.
    - Software of code die is ontworpen om:
      - Schade te maken aan uw computersysteem.
      - De werking van uw computersysteem te verstoren.
      - Toegang te krijgen tot uw computersysteem.
    - Bijvoorbeeld spyware, ransomware, virussen of Trojaanse paarden.
  - Iemand anders breekt in in uw computersysteem of computernetwerk.
    - Met als doel om schade te maken aan uw computersysteem of computernetwerk.
      - U gaf hiervoor geen toestemming.
    - Of als doel om toegang te krijgen tot uw computersysteem of computernetwerk.
      - U gaf hiervoor geen toestemming.
    - Of om gegevens op uw computersysteem of computernetwerk te openbaren.
      - U gaf hiervoor geen toestemming.
  - DoS-aanval.
    - Iemand overbelast bewust uw computersysteem of computernetwerk.
      - Waardoor uw computersysteem of computernetwerk niet of niet meer goed werkt.
    - Ook DDoS-aanvallen.
  - Diefstal van digitale data.
  - Menselijke fout van uw medewerker of een medewerker van een IT dienstverlener.
    - Bij het bedienen van uw computersysteem of het computersysteem van de IT dienstverlener.
    - Bijvoorbeeld de keuze voor verkeerde software, een programmeerfout, of een installatiefout.
  - Ook verzekerd als het cyberincident plaatsvond op het computersysteem van een IT dienstverlener van u.
    - En dat computersysteem werd gebruikt bij aan u verleende diensten.
    - Alleen voor het deel van de schade dat met u te maken heeft.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

  Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

10. PCI-DSS

130. Welke schade en kosten zijn verzekerd?

Boetes die een betaalkaartmerk u oplegt.

- Alleen als het betaalkaartmerk verplicht is om te controleren op PCI-DSS.
  - Bijvoorbeeld American Express, Discover, JCB, Mastercard en Visa.

Kosten voor een expert om de overtreding te onderzoeken.

- Alleen experts die goedgekeurd zijn door de PCI Security Standards Council.
- Alleen als het betaalkaartmerk om een onderzoek naar de overtreding vraagt.

Kosten voor het documenteren van het cyberincident door de expert die het cyberincident voor u onderzoekt.

- Ook voor het opstellen van advies voor het beter beveiligen van uw computersysteem.
  - Tegen vergelijkbare cyberincidenten.

Kosten voor een expert die het cyberincident beperkt.

- Bijvoorbeeld door getroffen gebruikersaccounts uit te schakelen of door malware te verwijderen.
- Wij kiezen de expert.

Kosten voor het inrichten en bemannen van een crisis management centrum door experts bij een cyberincident.

- Ook kosten voor het inrichten en bemannen van een call centre.
- Alleen verzekerd als wij toestemming geven voor inschakeling.
- Wij kiezen de expert.
- Wij vergoeden de kosten tot 30 dagen nadat u de gebeurtenis bij ons meldde.

Kosten om opnieuw gecertificeerd te worden voor PCI-DSS.

- Alleen als het betaalkaartmerk hierom vraagt.

Kosten om creditcards, betaalkaarten of prepaidkaarten opnieuw uit te geven.

131. Welk bedrag voor kosten is verzekerd?

Wij betalen maximaal het verzekerd bedrag per gebeurtenis.

- Het verzekerd bedrag staat op het polisblad.
- Dit geldt voor alle verzekerden samen.
- Dit geldt voor alle rubrieken samen.
- Houden meerdere gebeurtenissen verband met 1 oorzaak? Dan tellen we die gebeurtenissen als 1 gebeurtenis.

Per verzekeringsjaar betalen wij een maximaal bedrag.

- Dit bedrag staat op het polisblad.
- Dit geldt voor alle verzekerden samen.
  - Het moment van de 1e melding bepaalt bij welk verzekeringsjaar de gebeurtenis hoort.
- Dit geldt voor alle rubrieken samen.

Let op: u betaalt eerst een eigen risico.

- Het eigen risico per verzekerde gebeurtenis staat op het polisblad.

10. PCI-DSS

132. Welke kosten zijn boven het verzekerd bedrag verzekerd?

Kosten van experts.

- Alleen voor het bepalen van de hoogte van de schade.
- De kosten van onze expert.
- De kosten van de expert van verzekerde tot en met de kosten van onze expert.
  - Rekent de expert van verzekerde meer? Dan blijven die extra kosten voor rekening van verzekerde.
- De kosten van de 3e expert.
- Alle experts zijn ingeschreven in het register van het Nederlands Instituut Van Register Experts (NIVRE).
  - Of bij een vergelijkbare beroepsorganisatie.
    - En in de statuten en reglementen van deze organisatie:
      - Staat een duidelijke klacht- en tuchtprocedure.
      - Zijn de eisen beschreven voor permanente opleiding van experts.
  - Alle experts houden zich aan de Gedragscode schade-expertiseorganisaties van het Verbond van Verzekeraars.

Voldoet een expert niet aan deze eisen? Dan zijn de kosten van die expert niet verzekerd.

Let op: we betalen alleen als deze kosten noodzakelijk zijn door een schade die verzekerd is.

10. PCI-DSS

Niet verzekerd

Kijk ook in de algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Sanctiewet 1977.
- Ernstige conflicten (molest).
- Atoomkernreacties.
- Fraude.
- Terrorisme.
- Niet nakomen voorwaarden.

Per situatie staat in de algemene voorwaarden precies wat nooit verzekerd is.

Hieronder staat wat verder niet verzekerd is bij uw cyberverzekering.

133. Wanneer bent u niet verzekerd?

Als wij volgens wet- of regelgeving u niet mogen verzekeren voor de hulp, schade of de kosten.

Als de gebeurtenis voor het begin van de verzekering plaatsvond.

- En de verzekerde de gebeurtenis had kunnen of moeten ontdekken.

134. Welke schade is niet verzekerd?

Schade door een cyberoperatie.

Cyberoperatie =

- Het gebruik van een computersysteem door een soevereine staat.
  - Ook: het gebruik van een computersysteem op aanwijzing van een soevereine staat.
  - Ook: het gebruik van een computersysteem onder controle van een soevereine staat.
    - Met als doel om een ander computersysteem te verstoren.
    - En/of de toegang tot dat computersysteem te blokkeren.
    - En/of de functionaliteit ervan te verminderen.
    - En/of data in een computersysteem te kopiëren, verwijderen, vernietigen, wijzigen of te blokkeren.
- Alleen als wij bewijzen dat het een cyberoperatie is.
  - Wij kijken naar elk beschikbaar, redelijk en objectief bewijs.
    - Bijvoorbeeld: de regering van de staat, waarin de getroffen computersystemen zich fysiek bevinden, geeft een verklaring uit waarin de cyberoperatie aan een andere soevereine staat wordt toegeschreven.
      - Of wordt toegeschreven aan personen die op aanwijzing of onder controle van een andere soevereine staat handelden.

Soevereine staat = een land dat binnen het grondgebied het hoogste gezag voert.

- En dat niet afhankelijk is van een andere staat.

Schade door terrorisme.

- Kijk ook in onze algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Wel verzekerd schade door cyberterrorisme.
  - Cyberterrorisme = Toegang krijgen tot of beschadigen, vernietigen, verstoren van uw computersystemen of computernetwerken door een of meerdere personen die dat doen met een politiek, religieus, ideologisch of politiek doel.

10. PCI-DSS

vervolg

134. Welke schade is niet verzekerd?

Schade doordat apparatuur of een installatie van een ander niet of niet goed werkt.

- Apparaten en installaties die ervoor zorgen dat de energievoorziening blijft werken.
  - De energievoorziening van computersystemen en gegevensopslag.
  - Bijvoorbeeld, noodstroomvoorzieningen en stand-alone-generatoren.
- Airconditioning.
- Wel verzekerd als apparatuur of installatie van een IT dienstverlener niet goed werkt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade door gevaarlijke, verontreinigende of vervuilende stoffen.

Schade doordat uw computersysteem in beslag wordt genomen.

- Door een instantie die dat mag doen volgens de wet.
  - Bijvoorbeeld de overheid, een toezichthouder of een rechtbank.
  - Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
    - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
    - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
    - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Verlies van zaken.

- En de directe gevolgen daarvan.
- Ook als zaken kapot, weg of verontreinigd zijn.
- Zaken = losse spullen, onroerend goed of dieren.

Schade aan personen.

- Verwonding, ziekte (lichamelijk of geestelijk) of overlijden.
  - En de directe gevolgen daarvan.

Diefstal, schending of openbaarmaking van intellectueel eigendom.

- Bijvoorbeeld patenten, handelsmerken of auteursrechten.

Boetes en schadevergoedingen opgelegd door overheid of toezichthouder.

Beleggingsverliezen of handelsverliezen.

- Bijvoorbeeld als het niet meer lukt om effecten te verkopen.

Schade door geplande stilstand van uw computersystemen.

- Of van onderdelen van uw computersystemen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Betalingen die u doet om goede wil te tonen.

- Bijvoorbeeld kortingen, vouchers of coulancebetalingen.

10. PCI-DSS

vervolg

134. Welke schade is niet verzekerd?

Schade aan branded currency of cryptogeld.

Branded currency = combinatie van digitale betaalmiddelen of loyaliteitspunten uitgevoerd via een digitale mobiele portemonnee. En uniek voor een bepaalde winkelketen of webshop.

- Bijvoorbeeld een digitale cadeaukaart, digitale coupons of digitale promotiecodes.

Cryptogeld = digitaal geld dat niet wordt uitgegeven door een bank. Cryptogeld zit in een digitale portemonnee.

- Bijvoorbeeld: bitcoins

Ook niet verzekerd: verlies van branded currency of cryptogeld.

135. Bij welk gedrag bent u niet verzekerd?

Bij opzet van verzekerde of uw IT dienstverlener.

Verzekerde heeft geen dekking als verzekerde of de IT dienstverlener in strijd met het recht met opzet iets doet of niet doet waardoor schade ontstaat. De in feite toegebrachte schade is hierbij een te verwachten of normaal gevolg van wat een verzekerde of de IT dienstverlener doet of niet doet. Heeft verzekerde geen dekking? Dan heeft verzekerde dat ook niet voor de schade die mogelijk later nog ontstaat.

In welke gevallen geldt de opzetuitsluiting?

De uitsluiting geldt als verzekerde of de IT dienstverlener zich maatschappelijk ongewenst of crimineel gedraagt. Dat is in ieder geval zo bij gedragingen die een gevaar voor personen of zaken kunnen opleveren, zoals:

- Brandstichting, vernieling en beschadiging.
- Afpersing, bedrog, oplichting, bedreiging, beroving, verduistering, diefstal en inbraak. Ook als verzekerde of de IT dienstverlener dat met een computer of ander (technisch) hulpmiddel doet.
- Geweldpleging, mishandeling, doodslag en moord.

Er is sprake van opzet als verzekerde of de IT dienstverlener iets doet of niet doet waarbij verzekerde:

- De bedoeling heeft schade te veroorzaken (opzet als oogmerk).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener zeker weet dat er schade ontstaat (opzet met zekerheidsbewustzijn).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener de aanmerkelijke kans dat er schade ontstaat voor lief neemt. En toch handelt verzekerde (niet) zo (voorwaardelijk opzet).

Opzet wordt objectief uit de feiten, omstandigheden en/of gedragingen van verzekerde of de IT dienstverlener afgeleid.

Deze opzetuitsluiting geldt ook bij:

- Groepsaansprakelijkheid.
  - Als verzekerde niet zelf maar wel iemand in een groep waarvan verzekerde deel uitmaakt iets doet of niet doet.
- Alcohol en drugs.
  - Als verzekerde zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat verzekerde zijn eigen wil niet meer kon bepalen. Of als iemand in een groep waarvan verzekerde deel uitmaakt zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat hij of zij de eigen wil niet meer kon bepalen.

IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.

- Maar niet een dienstverlener:
  - Voor stroomvoorziening;
  - Voor telecommunicatie;
  - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

10. PCI-DSS

vervolg

135. Bij welk gedrag bent u niet verzekerd?

Schade doordat de verzekerde seksueel of seksueel getint gedrag vertoont.

- Geldt alleen voor de verzekerde die het gedrag vertoont.
- Alleen of in een groep.
  - Ook niet verzekerd: als verzekerde zelf niets doet.
  - Maar wel deel uitmaakt van een groep die dit gedrag vertoont.

Als u niet goed samenwerkt met de toezichthouder.

- Om te voorkomen dat een cyberincident of gegevensinbreuk plaatsvindt.
- Om te voorkomen dat aanspraak tegen u wordt ingediend.
- Om te voorkomen dat de toezichthouder u een straf of maatregel oplegt.
  - Als gevolg van een cyberincident, gegevensinbreuk of aanspraak.

Als u niet betaalt voor diensten of producten.

- En daardoor ontstaat schade of ontstaan kosten voor u of een ander.
- Bijvoorbeeld als u een leaseovereenkomst of licentie niet verlengt.
- Ook niet verzekerd als een IT dienstverlener van u niet betaalt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Als u zich niet houdt aan de preventieafspraken.

En de schade is hierdoor veroorzaakt of verergerd.

Preventieafspraken =

- U heeft een wachtwoordbeleid
  - Iedere gebruiker heeft een eigen account.
  - Alleen IT-administrators hebben toegang tot administrator accounts of privileged accounts.
  - Alle standaardwachtwoorden of standaardtoegangscodes worden bij het eerste gebruik direct gewijzigd en veilig bewaard.
  - Wachtwoorden bestaan uit 8 of meer tekens.
    - En bestaan uit een combinatie van minimaal drie van de volgende elementen: hoofdletters, kleine letters, speciale symbolen, cijfers.
  - U vermijdt gebruik van:
    - Woordenboekwoorden (bijvoorbeeld: “wachtwoord”).
    - Opeenvolgende of herhalende tekens (bijvoorbeeld “1234”, “1111”, “abcde”).
    - Toetsenbordpatronen (bijvoorbeeld “asdfgh”).
    - Persoonlijke informatie van de gebruiker (bijvoorbeeld een geboortedatum of een naam).
- U gebruikt een firewall om uw netwerk en computersystemen te beveiligen.
- U gebruikt anti-virus-, anti-spyware- en firewallsoftware die automatisch worden geüpdatet.
  - Of vergelijkbare malware-beveiligingssoftware.
  - Als het nodig is wordt deze software wekelijks handmatig geüpdatet.

10. PCI-DSS

vervolg

135. Bij welk gedrag bent u niet verzekerd?

- U past updates op uw computersystemen en computernetwerken automatisch toe.
  - Of u past deze handmatig toe als dat nodig is.
  - Als die updates zijn uitgegeven om uw computersystemen of computernetwerken te beschermen.
  - Voor computersystemen of computernetwerken die met internet zijn verbonden past u de update toe binnen 30 dagen nadat de update is gepubliceerd.
  - Voor Operationele technologie (OT) en Embedded systems past u de update toe binnen 90 dagen nadat de update is gepubliceerd.
  - Of binnen de periode die de betreffende fabrikant aanbeveelt.
- Voor andere computersystemen past u de update toe binnen 60 dagen nadat de update is gepubliceerd.
- U maakt wekelijks backups van digitale data op uw computersystemen.
- U test regelmatig herstelprocedures van uw computersystemen.
- U bewaart de back-up apart van uw computersystemen waarop de originele digitale data staat.
  - Bijvoorbeeld op een andere server op een andere locatie of bij een andere clouddienst.
- U vervangt software en hardware uiterlijk 3 maanden nadat de fabrikant stopte met de ondersteuning.
  - Of u zorgt voor een upgrade.

Als u één of meerdere van bovengenoemde maatregelen aan een ander bedrijf uitbesteedt:

- Dan staat in de overeenkomst met het andere bedrijf dat het verplicht is om de bovengenoemde maatregelen uit te voeren.
  - Wel verzekerd als u bewijst dat u zich per ongeluk niet hield aan de preventieafspraken.
    - Bijvoorbeeld als de schade wordt veroorzaakt of verergerd omdat u in de week van de gebeurtenis geen back-up maakte.
    - En u bewijst dat u in de periode voor de gebeurtenis wel altijd een back-up maakte.
    - En u bewijst dat de back-up tijdens de gebeurtenis niet gemaakt is door een technische storing waar u niets aan kon doen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Operationele technologie (OT) = een verzameling hardware en software die de werking van een industrieel proces kan beïnvloeden.
  - OT houdt meestal toezicht op fysieke processen zoals productie, energie, geneeskunde, gebouwenbeheer en ecosystemen.
- Embedded systems = een computersysteem met een specifieke taak en ingebed in een groter systeem.
  - Bijvoorbeeld een computersysteem in medische apparatuur.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

10. PCI-DSS

Bij schade

136. Wanneer meldt een verzekerde een gebeurtenis?

Zo snel mogelijk.

- Meld een gebeurtenis bij ons.
  - Een verzekerde meldt het ook als hij een gebeurtenis vermoedt.

137. Wat doet een verzekerde bij schade?

- De verzekerde meldt de schade zo snel mogelijk.
- De verzekerde werkt mee aan de afhandeling van de schade.
- De verzekerde doet alles om de schade zo veel mogelijk te beperken.
- De verzekerde geeft ons alle informatie die nodig is om de omvang en de oorzaak van de schade vast te stellen.
- De verzekerde bewaart alle hardware, software en gegevens.
  - En geeft die voor onderzoek aan ons of een expert als dat nodig is.
- De verzekerde doet aangifte bij de politie bij een strafbaar feit.
  - Bijvoorbeeld bij cyberafpersing.
- De verzekerde helpt ons de betaalde schadevergoeding bij een ander terug te halen.
- De verzekerde geeft alle verzekeringen op die deze schade verzekeren.
- De verzekerde tekent een geheimhoudingsverklaring als de incident response provider daarom vraagt.
  - Tekent u niet? Dan kunnen wij uw schade mogelijk niet of niet volledig afhandelen.

138. Welk bedrag voor schade en kosten samen is verzekerd?

Per gebeurtenis betalen wij maximaal het bedrag op het polisblad.

- Dit geldt voor alle verzekerden samen.
- Houden meerdere gebeurtenissen verband met 1 oorzaak? Dan tellen we die aanspraken als 1 gebeurtenis.

Per verzekeringsjaar betalen wij samen een maximaal bedrag.

- Dit bedrag staat op het polisblad.
- Dit geldt voor alle verzekerden samen.
- Het moment van de 1e melding bepaalt bij welk verzekeringsjaar de gebeurtenis hoort.
- Dit geldt voor alle rubrieken samen.

Let op: u betaalt eerst een eigen risico.

- Het eigen risico per verzekerde gebeurtenis staat op het polisblad.

10. PCI-DSS

139. Wie bepaalt de hoogte van het schadebedrag?

Of: wij.

Of: onze expert.

Of: onze expert met een expert van de verzekerde.

- Voor zij starten, kiezen zij een 3e expert.
  - Die bepaalt de schade als zij het oneens zijn.
  - Hij bepaalt de schade tussen het laagste en hoogste bedrag.
- Alle experts zijn ingeschreven in het register van het Nederlands Instituut Van Register Experts (NIVRE).
  - Of bij een vergelijkbare beroepsorganisatie.
    - En in de statuten en reglementen van deze organisatie:
      - Staat een duidelijke klacht- en tuchtprocedure.
      - Zijn de eisen beschreven voor permanente opleiding van experts.
  - Alle experts houden zich aan de Gedragscode schade-expertiseorganisaties van het Verbond van Verzekeraars.

Let op: dat wij het schadebedrag bepalen, betekent niet dat we de schade betalen.

140. Wat als een verzekerde ook op een andere verzekering is verzekerd?

De andere verzekering gaat voor.

- Als de verzekerde daarop verzekerd is of verzekerd zou zijn als onze verzekering niet zou bestaan.
- Wij betalen de schade boven het maximale bedrag van de andere verzekering.
  - Wij betalen niet uw eigen risico bij de andere verzekering.

141. Wat als bij schade blijkt dat deze verzekering in strijd is met wet- en regelgeving?

Wij houden ons altijd aan de wet- en regelgeving die van toepassing is.

- We zoeken dan naar een oplossing die in lijn is met deze verzekering.

11. Telefoonhacking

Inhoud

Klik op de **vraag** om het antwoord te lezen

11. Telefoonhacking

Verzekerd

142. Wat is verzekerd?

Kosten voor een expert die het cyberincident of een vermoeden van een cyberincident voor u onderzoekt.

- De expert deelt de resultaten van het onderzoek met u.
- Wij kiezen de expert.

Kosten voor een expert die het cyberincident beperkt.

- Bijvoorbeeld door getroffen gebruikersaccounts uit te schakelen of door malware te verwijderen.
- Wij kiezen de expert.

Kosten voor het documenteren van het cyberincident door de expert die het cyberincident voor u onderzoekt.

- Ook voor het opstellen van advies voor het beter beveiligen van uw computersysteem.
  - Tegen vergelijkbare cyberincidenten.

Kosten voor het inrichten en bemannen van een crisis management centrum door experts bij een cyberincident.

- Ook kosten voor het inrichten en bemannen van een call centre.
- Alleen verzekerd als wij toestemming geven voor inschakeling.
- Wij kiezen de expert.
- Wij vergoeden de kosten tot 30 dagen nadat u de gebeurtenis bij ons meldde.

Kosten die het gevolg zijn van een cyberincident op uw telefoonsysteem.

- Als door het cyberincident zonder uw toestemming belkosten zijn gemaakt.
  - Of gebruik is gemaakt van uw bandbreedte.
- Cyberincident =
  - Malware op uw computersystemen of computernetwerk.
    - Software of code die is ontworpen om:
      - Schade te maken aan uw computersysteem.
      - De werking van uw computersysteem te verstoren.
      - Toegang te krijgen tot uw computersysteem.
    - Bijvoorbeeld spyware, ransomware, virussen of Trojaanse paarden.
  - Iemand anders breekt in in uw computersysteem of computernetwerk.
    - Met als doel om schade te maken aan uw computersysteem of computernetwerk.
      - U gaf hiervoor geen toestemming.
    - Of als doel om toegang te krijgen tot uw computersysteem of computernetwerk.
      - U gaf hiervoor geen toestemming.
    - Of om gegevens op uw computersysteem of computernetwerk te openbaren
      - U gaf hiervoor geen toestemming.
  - DoS-aanval.
    - Iemand overbelast bewust uw computersysteem of computernetwerk.
      - Waardoor uw computersysteem of computernetwerk niet of niet meer goed werkt.
    - Ook DDoS-aanvallen.
  - Diefstal van digitale data.
  - Menselijke fout van uw medewerker of een medewerker van een IT dienstverlener.
    - Bij het bedienen van uw computersysteem of het computersysteem van de IT dienstverlener.
      - Bijvoorbeeld de keuze voor verkeerde software, een programmeerfout, of een installatiefout.

11. Telefoonhacking

vervolg

142. Wat is verzekerd?

- Ook verzekerd als het cyberincident plaatsvindt op het computersysteem van een IT dienstverlener van u.
  - En dat computersysteem werd gebruikt bij aan u verleende diensten.
  - Alleen voor het deel van de schade dat met u te maken heeft.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
      - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

• Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

143. Welk bedrag voor kosten is verzekerd?

Wij betalen maximaal het verzekerd bedrag per gebeurtenis.

• Het verzekerd bedrag staat op het polisblad.
• Dit geldt voor alle verzekerden samen.
• Dit geldt voor alle rubrieken samen.
• Houden meerdere gebeurtenissen verband met 1 oorzaak? Dan tellen we die gebeurtenissen als 1 gebeurtenis.

Per verzekeringsjaar betalen wij een maximaal bedrag.

• Dit bedrag staat op het polisblad.
• Dit geldt voor alle verzekerden samen.
  - Het moment van de 1e melding bepaalt bij welk verzekeringsjaar de gebeurtenis hoort.
• Dit geldt voor alle rubrieken samen.

Let op: u betaalt eerst een eigen risico.

• Het eigen risico per verzekerde gebeurtenis staat op het polisblad.

11. Telefoonhacking

144. Welke kosten zijn boven het verzekerd bedrag verzekerd?

Kosten van experts.

- Alleen voor het bepalen van de hoogte van de schade.
- De kosten van onze expert.
- De kosten van de expert van verzekerde tot en met de kosten van onze expert.
  - Rekent de expert van verzekerde meer? Dan blijven die extra kosten voor rekening van verzekerde.
- De kosten van de 3e expert.
- Alle experts zijn ingeschreven in het register van het Nederlands Instituut Van Register Experts (NIVRE).
  - Of bij een vergelijkbare beroepsorganisatie.
    - En in de statuten en reglementen van deze organisatie:
      - Staat een duidelijke klacht- en tuchtprocedure.
      - Zijn de eisen beschreven voor permanente opleiding van experts.
  - Alle experts houden zich aan de Gedragscode schade-expertiseorganisaties van het Verbond van Verzekeraars.

Voldoet een expert niet aan deze eisen? Dan zijn de kosten van die expert niet verzekerd.

Let op: we betalen alleen als deze kosten noodzakelijk zijn door een schade die verzekerd is.

11. Telefoonhacking

Niet verzekerd

Kijk ook in de algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Sanctiewet 1977.
- Ernstige conflicten (molest).
- Atoomkernreacties.
- Fraude.
- Terrorisme.
- Niet nakomen voorwaarden.

Per situatie staat in de algemene voorwaarden precies wat nooit verzekerd is.

Hieronder staat wat verder niet verzekerd is bij uw cyberverzekering.

145. Wanneer bent u niet verzekerd?

Als wij volgens wet- of regelgeving u niet mogen verzekeren voor de hulp, schade of de kosten.

Als de gebeurtenis voor het begin van de verzekering plaatsvond.

- En de verzekerde de gebeurtenis had kunnen of moeten ontdekken.

146. Welke schade is niet verzekerd?

Schade door een cyberoperatie.

Cyberoperatie =

- Het gebruik van een computersysteem door een soevereine staat.
  - Ook: het gebruik van een computersysteem op aanwijzing van een soevereine staat.
  - Ook: het gebruik van een computersysteem onder controle van een soevereine staat.
    - Met als doel om een ander computersysteem te verstoren.
    - En/of de toegang tot dat computersysteem te blokkeren.
    - En/of de functionaliteit ervan te verminderen.
    - En/of data in een computersysteem te kopiëren, verwijderen, vernietigen, wijzigen of te blokkeren.
- Alleen als wij bewijzen dat het een cyberoperatie is.
  - Wij kijken naar elk beschikbaar, redelijk en objectief bewijs.
    - Bijvoorbeeld: de regering van de staat, waarin de getroffen computersystemen zich fysiek bevinden, geeft een verklaring uit waarin de cyberoperatie aan een andere soevereine staat wordt toegeschreven.
      - Of wordt toegeschreven aan personen die op aanwijzing of onder controle van een andere soevereine staat handelden.

Soevereine staat = een land dat binnen het grondgebied het hoogste gezag voert.

- En dat niet afhankelijk is van een andere staat.

Schade door terrorisme.

- Kijk ook in onze algemene voorwaarden.

In onze algemene voorwaarden staan situaties die nooit verzekerd zijn.

- Wel verzekerd schade door cyberterrorisme.
  - Cyberterrorisme = Toegang krijgen tot of beschadigen, vernietigen, verstoren van uw computersystemen of computernetwerken door een of meerdere personen die dat doen met een politiek, religieus, ideologisch of politiek doel. Schade doordat apparatuur of een installatie van een ander niet of niet goed werkt.

11. Telefoonhacking

vervolg

146. Welke schade is niet verzekerd?

Schade doordat apparatuur of een installatie van een ander niet of niet goed werkt.

- Apparaten en installaties die ervoor zorgen dat de energievoorziening blijft werken.
  - De energievoorziening van computersystemen en gegevensopslag.
  - Bijvoorbeeld, noodstroomvoorzieningen en stand-alone-generatoren.
- Airconditioning.
- Wel verzekerd als apparatuur of installatie van een IT dienstverlener niet goed werkt.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
  - Voor stroomvoorziening;
  - Voor telecommunicatie;
  - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
  - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade doordat apparatuur of een installatie van een ander niet of niet goed werkt.

- Apparaten en installaties die ervoor zorgen dat de energievoorziening blijft werken.
  - De energievoorziening van computersystemen en gegevensopslag.
  - Bijvoorbeeld, noodstroomvoorzieningen en stand-alone-generatoren.
- Airconditioning.
- Wel verzekerd als apparatuur of installatie van een IT dienstverlener niet goed werkt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade door gevaarlijke, verontreinigende of vervuilende stoffen.

Schade doordat uw computersysteem in beslag wordt genomen.

- Door een instantie die dat mag doen volgens de wet.
  - Bijvoorbeeld de overheid, een toezichthouder of een rechtbank.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Verlies van zaken.

- En de directe gevolgen daarvan.
- Ook als zaken kapot, weg of verontreinigd zijn.
- Zaken = losse spullen, onroerend goed of dieren.

Schade aan personen.

- Verwonding, ziekte (lichamelijk of geestelijk) of overlijden.
  - En de directe gevolgen daarvan.

Diefstal, schending of openbaarmaking van intellectueel eigendom.

- Bijvoorbeeld patenten, handelsmerken of auteursrechten.

11. Telefoonhacking

vervolg

146. Welke schade is niet verzekerd?

Boetes en schadevergoedingen opgelegd door overheid of toezichthouder.

Beleggingsverliezen of handelsverliezen.

- Bijvoorbeeld als het niet meer lukt om effecten te verkopen.

Schade door geplande stilstand van uw computersystemen.

- Of van onderdelen van uw computersystemen.
- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.

Schade waarvoor een bestuurder persoonlijk aansprakelijk wordt gesteld.

Betalingen die u doet om goede wil te tonen.

Bijvoorbeeld kortingen, vouchers of coulancebetalingen.

Schade aan branded currency of cryptogeld.

Branded currency = combinatie van digitale betaalmiddelen of loyaliteitspunten uitgevoerd via een digitale mobiele portemonnee. En uniek voor een bepaalde winkelketen of webshop.

- Bijvoorbeeld een digitale cadeaukaart, digitale coupons of digitale promotiecodes.

Cryptogeld = digitaal geld dat niet wordt uitgegeven door een bank. Cryptogeld zit in een digitale portemonnee.

- Bijvoorbeeld: bitcoins

Ook niet verzekerd: verlies van branded currency of cryptogeld.

147. Bij welk gedrag bent u niet verzekerd?

Bij opzet van verzekerde of uw IT dienstverlener.

Verzekerde heeft geen dekking als verzekerde of de IT dienstverlener in strijd met het recht met opzet iets doet of niet doet waardoor schade ontstaat. De in feite toegebrachte schade is hierbij een te verwachten of normaal gevolg van wat een verzekerde of de IT dienstverlener doet of niet doet. Heeft verzekerde geen dekking? Dan heeft verzekerde dat ook niet voor de schade die mogelijk later nog ontstaat.

In welke gevallen geldt de opzetuitsluiting?

De uitsluiting geldt als verzekerde of de IT dienstverlener zich maatschappelijk ongewenst of crimineel gedraagt. Dat is in ieder geval zo bij gedragingen die een gevaar voor personen of zaken kunnen opleveren, zoals:

- Brandstichting, vernieling en beschadiging.
- Afpersing, bedrog, oplichting, bedreiging, beroving, verduistering, diefstal en inbraak. Ook als verzekerde of de IT dienstverlener dat met een computer of ander (technisch) hulpmiddel doet.
- Geweldpleging, mishandeling, doodslag en moord.

Er is sprake van opzet als verzekerde of de IT dienstverlener iets doet of niet doet waarbij verzekerde:

- De bedoeling heeft schade te veroorzaken (opzet als oogmerk).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener zeker weet dat er schade ontstaat (opzet met zekerheidsbewustzijn).
- Niet de bedoeling heeft schade te veroorzaken, maar verzekerde of de IT dienstverlener de aanmerkelijke kans dat er schade ontstaat voor lief neemt. En toch handelt verzekerde (niet) zo (voorwaardelijk opzet).

Opzet wordt objectief uit de feiten, omstandigheden en/of gedragingen van verzekerde of de IT dienstverlener afgeleid.

11. Telefoonhacking

vervolg

147. Bij welk gedrag bent u niet verzekerd?

Deze opzetuitsluiting geldt ook bij:

- Groepsaansprakelijkheid.
  - Als verzekerde niet zelf maar wel iemand in een groep waarvan verzekerde deel uitmaakt iets doet of niet doet.
- Alcohol en drugs.
  - Als verzekerde zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat verzekerde zijn eigen wil niet meer kon bepalen. Of als iemand in een groep waarvan verzekerde deel uitmaakt zoveel alcohol, drugs of andere (bedwelmende) stoffen heeft gebruikt dat hij of zij de eigen wil niet meer kon bepalen.

IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.

- Maar niet een dienstverlener:
  - Voor stroomvoorziening;
  - Voor telecommunicatie;
  - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

Schade doordat de verzekerde seksueel of seksueel getint gedrag vertoont.

- Geldt alleen voor de verzekerde die het gedrag vertoont.
- Alleen of in een groep.
  - Ook niet verzekerd: als verzekerde zelf niets doet.
  - Maar wel deel uitmaakt van een groep die dit gedrag vertoont.

Als u niet goed samenwerkt met de toezichthouder.

- Om te voorkomen dat een cyberincident of gegevensinbreuk plaatsvindt.
- Om te voorkomen dat aanspraak tegen u wordt ingediend.
- Om te voorkomen dat de toezichthouder u een straf of maatregel oplegt.
  - Als gevolg van een cyberincident, gegevensinbreuk of aanspraak.

Als u niet betaalt voor diensten of producten.

- En daardoor ontstaat schade of ontstaan kosten voor u of een ander.
- Bijvoorbeeld als u een leaseovereenkomst of licentie niet verlengt.
- Ook niet verzekerd als een IT dienstverlener van u niet betaalt.
  - IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
    - Maar niet een dienstverlener:
      - Voor stroomvoorziening;
      - Voor telecommunicatie;
      - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
        - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

11. Telefoonhacking

vervolg

147. Bij welk gedrag bent u niet verzekerd?

Als u zich niet houdt aan de preventieafspraken.

En de schade is hierdoor veroorzaakt of verergerd.

Preventieafspraken =

- U heeft een wachtwoordbeleid
  - Iedere gebruiker heeft een eigen account.
  - Alleen IT-administrators hebben toegang tot administrator accounts of privileged accounts.
  - Alle standaardwachtwoorden of standaardtoegangscodes worden bij het eerste gebruik direct gewijzigd en veilig bewaard.
  - Wachtwoorden bestaan uit 8 of meer tekens.
    - En bestaan uit een combinatie van minimaal drie van de volgende elementen: hoofdletters, kleine letters, speciale symbolen, cijfers.
  - U vermijdt gebruik van:
    - Woordenboekwoorden (bijvoorbeeld: “wachtwoord”).
    - Opeenvolgende of herhalende tekens (bijvoorbeeld “1234”, “1111”, “abcde”).
    - Toetsenbordpatronen (bijvoorbeeld “asdfgh”).
    - Persoonlijke informatie van de gebruiker (bijvoorbeeld een geboortedatum of een naam).
- U gebruikt een firewall om uw netwerk en computersystemen te beveiligen.
- U gebruikt anti-virus-, anti-spyware- en firewallsoftware die automatisch worden geüpdatet.
  - Of vergelijkbare malware-beveiligingssoftware.
  - Als het nodig is wordt deze software wekelijks handmatig geüpdatet.
- U past updates op uw computersystemen en computernetwerken automatisch toe.
  - Of u past deze handmatig toe als dat nodig is.
  - Als die updates zijn uitgegeven om uw computersystemen of computernetwerken te beschermen.
  - Voor computersystemen of computernetwerken die met internet zijn verbonden past u de update toe binnen 30 dagen nadat de update is gepubliceerd.
  - Voor Operationele technologie (OT) en Embedded systems past u de update toe binnen 90 dagen nadat de update is gepubliceerd.
  - Of binnen de periode die de betreffende fabrikant aanbeveelt.
- Voor andere computersystemen past u de update toe binnen 60 dagen nadat de update is gepubliceerd.
- U maakt wekelijks backups van digitale data op uw computersystemen.
- U test regelmatig herstelprocedures van uw computersystemen.
- U bewaart de back-up apart van uw computersystemen waarop de originele digitale data staat.
  - Bijvoorbeeld op een andere server op een andere locatie of bij een andere clouddienst.
- U vervangt software en hardware uiterlijk 3 maanden nadat de fabrikant stopte met de ondersteuning.
  - Of u zorgt voor een upgrade.

Als u één of meerdere van bovengenoemde maatregelen aan een ander bedrijf uitbesteedt:

- Dan staat in de overeenkomst met het andere bedrijf dat het verplicht is om de bovengenoemde maatregelen uit te voeren.
  - Wel verzekerd als u bewijst dat u zich per ongeluk niet hield aan de preventieafspraken.
    - Bijvoorbeeld als de schade wordt veroorzaakt of verergerd omdat u in de week van de gebeurtenis geen back-up maakte.
    - En u bewijst dat u in de periode voor de gebeurtenis wel altijd een back-up maakte.
    - En u bewijst dat de back-up tijdens de gebeurtenis niet gemaakt is door een technische storing waar u niets aan kon doen.

11. Telefoonhacking

vervolg

147. Bij welk gedrag bent u niet verzekerd?

- Computersysteem = hardware, software, elektronische media, infrastructuur en telefoonsysteem.
  - Elektronische media zijn bijvoorbeeld externe schijven, USB-sticks, cd-roms of dvd-roms.
  - Infrastructuur = de apparaten die ervoor zorgen dat uw computersysteem blijft werken.
  - Telefoonsysteem = uw telefooncentrale, telefoonlijnen, webcams, handsets, softphones en mobiele telefoons.
- Operationele technologie (OT) = een verzameling hardware en software die de werking van een industrieel proces kan beïnvloeden.
  - OT houdt meestal toezicht op fysieke processen zoals productie, energie, geneeskunde, gebouwenbeheer en ecosystemen.
- Embedded systems = een computersysteem met een specifieke taak en ingebed in een groter systeem.
  - Bijvoorbeeld een computersysteem in medische apparatuur.
- IT dienstverlener = een leverancier van diensten om uw hardware, computersoftware, infrastructuur en digitale data te laten werken, te verwerken, te beschermen of op te slaan.
  - Maar niet een dienstverlener:
    - Voor stroomvoorziening;
    - Voor telecommunicatie;
    - Voor IT diensten of leveren van apparaten om het gebruik van internet mogelijk te maken:
    - Bijvoorbeeld een internet service provider, een aanbieder van domeinnamen, exploitant van kabelnetwerken.

11. Telefoonhacking

Bij schade

148. Wanneer meldt een verzekerde een gebeurtenis?

Zo snel mogelijk.

- Meld een gebeurtenis bij ons.
  - Een verzekerde meldt het ook als hij een gebeurtenis vermoedt.

149. Wat doet een verzekerde bij schade?

- De verzekerde meldt de schade zo snel mogelijk.
- De verzekerde werkt mee aan de afhandeling van de schade.
- De verzekerde doet alles om de schade zo veel mogelijk te beperken.
- De verzekerde geeft ons alle informatie die nodig is om de omvang en de oorzaak van de schade vast te stellen.
- De verzekerde bewaart alle hardware, software en gegevens.
  - En geeft die voor onderzoek aan ons of een expert als dat nodig is.
- De verzekerde doet aangifte bij de politie bij een strafbaar feit.
  - Bijvoorbeeld bij cyberafpersing.
- De verzekerde helpt ons de betaalde schadevergoeding bij een ander terug te halen.
- De verzekerde geeft alle verzekeringen op die deze schade verzekeren.
- De verzekerde tekent een geheimhoudingsverklaring als de incident response provider daarom vraagt.
  - Tekent u niet? Dan kunnen wij uw schade mogelijk niet of niet volledig afhandelen.

150. Wat is het verzekerd bedrag?

Het verzekerd bedrag staat op het polisblad.

- Dit is het totale verzekerd bedrag per gebeurtenis of aanspraak voor deze verzekering.
- Dit is ook het maximale bedrag dat we per verzekeringsjaar uitkeren.
  - Voor alle schades en kosten bij elkaar.
  - Hieronder vallen ook betalingen van ons aan een expert.
  - Dit geldt voor alle rubrieken samen.

151. Wie bepaalt de hoogte van het schadebedrag?

Of: wij.

Of: onze expert.

Of: onze expert met een expert van de verzekerde.

- Voor zij starten, kiezen zij een 3e expert.
  - Die bepaalt de schade als zij het oneens zijn.
  - Hij bepaalt de schade tussen het laagste en hoogste bedrag.
- Alle experts zijn ingeschreven in het register van het Nederlands Instituut Van Register Experts (NIVRE).
  - Of bij een vergelijkbare beroepsorganisatie.
    - En in de statuten en reglementen van deze organisatie:
      - Staat een duidelijke klacht- en tuchtprocedure.
      - Zijn de eisen beschreven voor permanente opleiding van experts.
  - Alle experts houden zich aan de Gedragscode schade-expertiseorganisaties van het Verbond van Verzekeraars.

Let op: dat wij het schadebedrag bepalen, betekent niet dat we de schade betalen.

11. Telefoonhacking

152. Wat als een verzekerde ook op een andere verzekering is verzekerd?

De andere verzekering gaat voor.

- Als de verzekerde daarop verzekerd is of verzekerd zou zijn als onze verzekering niet zou bestaan.
- Wij betalen de schade boven het maximale bedrag van de andere verzekering.
  - Wij betalen niet uw eigen risico bij de andere verzekering.

153. Wat als bij schade blijkt dat deze verzekering in strijd is met wet- en regelgeving?

Wij houden ons altijd aan de wet- en regelgeving die van toepassing is.

- We zoeken dan naar een oplossing die in lijn is met deze verzekering.

Heeft u vragen?

Neem contact op met uw accountmanager. Hij of zij helpt u graag.

Avéro Achmea
Postbus 101
7300 AC Apeldoorn
Nederland
www.averoachmea.nl