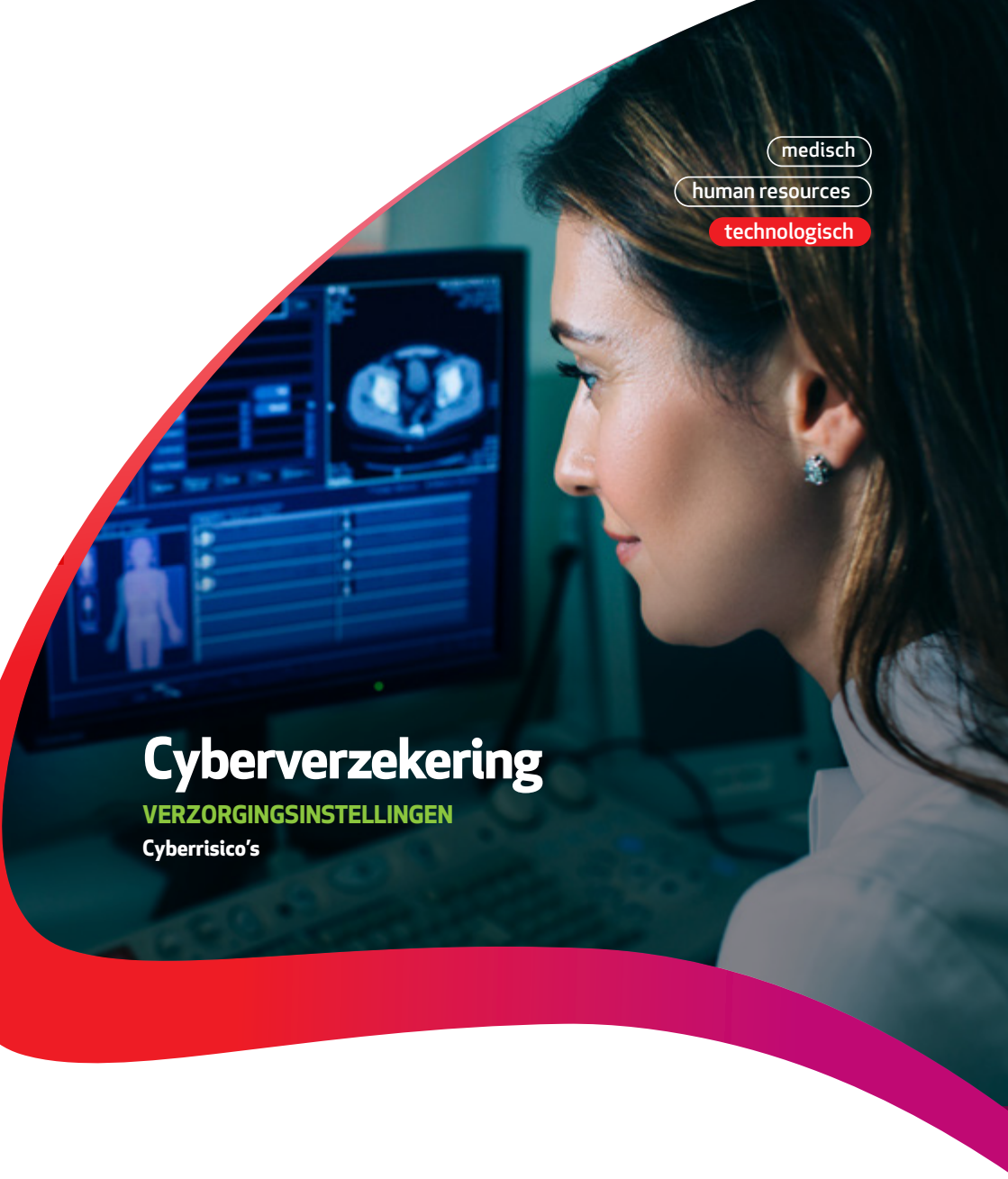

Cyberverzekering

VERZORGINGSINSTELLINGEN

Cyberrisico's

amma
verzekeringen sinds 1944
voor en door de zorgsector

relyens
GROUPE MUTUALISTE EUROPÉEN
ASSURANCE ET MANAGEMENT DES RISQUES

Cyberaanvallen, belangt het u aan?

De digitalisering van de zorg voor patiënten en het gebruik van digitale technologieën ten dienste van uw organisatie stellen u bloot aan nieuwe bedreigingen.

Andere verzekeringen Burgerlijke Aansprakelijkheid en 'alle risico-verzekeringen Informatica' bieden u geen specifieke Cyberdekking.

Relyens, de risicomanager en expert in de gezondheidszorg en in de medisch-sociale sector, biedt u een **globale oplossing voor preventie, bescherming en herstel** in geval van een cyberaanval.

Wat zijn de risico's bij een cyberincident?

Computercriminaliteit spaart zorginstellingen niet. Wat de modus operandi ook is, het kan **zware gevolgen hebben voor de werking van uw organisatie**:

- **Verlies van vertrouwen van uw patiënten, patiënten**
- **Poging tot afpersing**
- **Verlamming van het informaticasysteem**
- **Verspreiding en commercialisatie van medische, bank-, financiële gegevens ...**
- **Stillegging van de geconnecteerde medische apparaten**
- **Imago-en reputatieschade**

WAT ZEGT DE WET?

Uw instelling is verantwoordelijk voor de gegevens die ze heeft en die haar zijn toevertrouwd volgens de bepalingen van de GDPR*:

- ↗ Bij tekortkoming kunnen de boetes oplopen tot € 20 miljoen of 4% van de wereldwijde omzet.
- ↗ In geval van schending van de persoonsgegevens en indien het incident een risico inhoudt voor de rechten en vrijheden van de personen, dient u een melding te doen bij de Gegevensbeschermingsautoriteit(GBA).
- ↗ U moet technische en organisatorische maatregelen treffen om persoonlijke gegevens en het IT-systeem te beveiligen.

De NIS2-wet verplicht zorginstellingen om risicobeheersmaatregelen te nemen op het vlak van cyberbeveiliging en de rapportering van incidenten.

**General Data Protection Regulation*

Cyberverzekering: De oplossing voor u

Relyens biedt u in samenwerking met AMMA **een aanbod op maat voor alle cyberrisico's**. Het omvat een pakket dekkingen en maatregelen **om u een oplossing te bieden op maat** van het blootstellingsniveau van uw instelling.

OMGAAN MET EEN CYBERAANVAL
- 24/7 assistentie.
- Ondersteuning bij crisisbeheer.
- Dekking van honoraria van deskundigen en consultants en verdedigingskosten.

UW GEGEVENS EN SOFTWARE HERSTELLEN
Betaling van de kosten voor het herstellen, opschonen en virusvrij maken van gegevens en software.

DE NETWERKEN EN SYSTEMEN VAN DERDEN BEVEILIGEN
Dekking van de financiële gevolgen van de burgerlijke aansprakelijkheid van de instelling in geval van schade aan de IT-systemen van derden ten gevolge van een cyberbeveiligingsincident.

DE AANSPRAKELIJKHEID VAN UW VESTIGING BESCHERMEN
IN HET GEVAL VAN EEN INBREUK OP UW VERTROUWELIJKE GEGEVENS
Dekking van de financiële gevolgen van de burgerlijke aansprakelijkheid van de instellingen en de verdedigingskosten.

EEN ANTWOORD BIEDEN OP CYBERFRAUDE
Betaling van honoraria en kosten van deskundigen, terugbetaling van te veel in rekening gebrachte telefoonkosten.

DE NETWERKEN EN SYSTEMEN VAN DERDEN BEVEILIGEN
Dekking van de financiële gevolgen van de burgerlijke aansprakelijkheid van de instelling in geval van schade aan de IT-systemen van derden als gevolg van een cybersecurity-incident.

BEDRIJFSSCHADE VERZEKERN
Wanneer deze veroorzaakt wordt door een volledige of gedeeltelijke onderbreking (van de IT-systemen) of een vrijwillige onderbreking ingeval van nood.

DE VOORDELEN VAN RELYENS EN AMMA DIE HET VERSCHIL MAKEN:

1. Aanvullende expertise voor spelers in de gezondheidszorg in België: kennis van het ecosysteem van zorginstellingen in België gecombineerd met expertise op het gebied van cyberrisico.

2. Complete oplossing: assistentie, herstel van schade en aansprakelijkheid.

3. 24/7 bijstand bij crisisbeheer door een multidisciplinair team van experts.

4. Rekening houden met de uitbesteding van informatiesystemen (IS) van instellingen en de bundeling hiervan in specifieke structuren.

5. Rekening houden met vrijwillige onderbrekingen die noodzakelijk zijn om uw activiteiten en de veiligheid van patiënten te beschermen.

6. Een specifiek aanbod voor gezondheidszorg, sociale en medisch-sociale spelers en hun partners.

Cyberaanvallen, wat zijn de gevolgen?

STOPZETTING VAN DE ACTIVITEIT

Een universitair ziekenhuis werd het slachtoffer van een grootschalige cyberaanval met ransomware, die een grote impact had op het IT-systeem en daarmee op de bedrijfsvoering. De aanval, waarbij een groot deel van de werkstations en IT-servers werden versleuteld, legde alle diensten van het universitair ziekenhuis lam, waardoor de meeste bedrijfsapplicaties ontoegankelijk werden.

VERSTORING VAN DE ACTIVITEIT

3 Franse ziekenhuizen waren het doelwit van cyberafpersing. De aanval heeft deze ziekenhuizen ernstig ontwricht, waardoor ze genoodzaakt waren om bepaalde medische procedures te annuleren en ziekenwagens naar andere instellingen te sturen.

VERLIES VAN VERTROUWEN BIJ DE PATIËNT

De scanners, computers en medicatiebeheersoftware van een ziekenhuis werden geblokkeerd door een virus. De persoonlijke gegevens van patiënten werden gestolen en de cybercriminelen eisten een losgeld van 3 miljoen euro.

FINANCIËLE GEVOLGEN

Het hacken van de telefooncentrale van een Frans ziekenhuis leidde tot het teveel in rekening brengen van telefoniekosten voor een bedrag van €40.000.

Een Belgisch ziekenhuis, gehackt in 2019 en 2021, schatte de kosten van dit laatste incident op €300.000, met 70 van zijn 120 servers versleuteld en 100 miljoen bestanden geïnfecteerd in slechts enkele uren.

120

incidenten met ransomware aangegeven in België*

11 %

van de ziekenhuizen wordt getroffen door een cyberincident in België **

** Bron Centre for Cybersecurity Belgium-cijfers voor 2023 gebaseerd op gerapporteerde incidenten.*

*** Bron Federale Politie, 2022.*

3 goede redenen om voor het partnerschap Relyens/AMMA te kiezen

EEN ANDERE KIJK OP VERZEKERINGEN

Door hun benadering op het vlak van risicobeheer biedt Relyens u innovatieve oplossingen op maat.

EEN EXPERT IN DE GEZONDHEIDS-, SOCIALE

Meer dan 5.000 bedrijven hebben al voor Relyens gekozen, sluit u bij hen aan!

EEN PARTNER DICHTBIJ U

Een bevoorrechte, toegewijde en reactieve klantenrelatie.

Deze preventieve oplossingen kunnen worden aangevuld met een aanbod om restrisico's te dekken via onze Cyberverzekering.

AMMA is marktleider in burgerlijke aansprakelijkheid voor (para)medische beroepen en vertegenwoordigt momenteel de belangen van ongeveer 50% van de Belgische ziekenhuizen en 62.000 zorgverleners. AMMA wil deze positie bevestigen door haar leden en de zorgsector te ondersteunen bij het beheer van medische risico's en door oplossingen te bieden tegen cyberrisico's (dankzij de samenwerking met Relyens).

Neem voor meer informatie contact op met onze AMMA-experts

NL: 0032 474 66 74 97
FR: 0032 492 11 21 47
cyberinfo@amma.be

Vandaag anticiperen om morgen te beschermen.

Bij Relyens zijn we veel meer dan verzekeraars, we zijn risicomanagers. Het beheren, voorkomen en verzekeren tegen risico's is onze inzet om zorginstellingen en lokale overheden in Europa een effectievere bescherming te bieden. Samen met hen handelen en innoveren we ten gunste van een steeds veiligere dienst van algemeen belang voor iedereen.

relyens.eu

Relyens Mutual Insurance
Maatschappelijke zetel: 18 rue Edouard Rochet - 69372 LYON Cedex 08 - FRANKRIJK - Tel.: +33 (0)4 72 75 50 25 - www.relyens.eu Onderlinge verzekeringsmaatschappij met vaste bijdragen. Onderneming die valt onder de verzekeringswet - 779 860 881 RCS Lyon. Beroepsopleidingsorganisatie geregistreerd bij de prefect van de regio onder nr. 82690051369. Intracommunautair btw-nummer: FR 79779860881.

amma verzekeringen sinds 1944 voor en door de zorgsector

relyens GROUPE MUTUALISTE EUROPÉEN ASSURANCE ET MANAGEMENT DES RISQUES

Document ontworpen en geproduceerd door de communicatieafdeling van Relyens - 50159-24A -10/2024
Fotocredits: © Vadim - © NDABCREATIVITY - © Damian - © Seventyfour - © Gorodenkoff - stockadobe.com