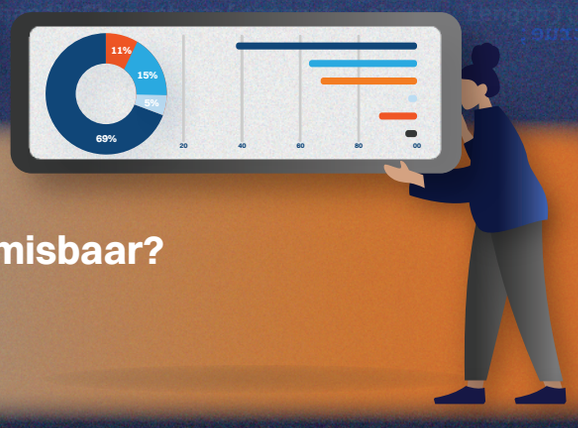
Waarom een Cyberverzekering?

& Risico's van Cybercrime

Wat is cybercrime precies?

Cybercrime omvat alle digitale misdrijven zoals hacks, ransomware, phishing en datadiefstal. Criminelen proberen via ICT-systemen gevoelige informatie te stelen of bedrijfsprocessen te saboteren.



Voor wie is een cyberverzekering onmisbaar?

Voor elk bedrijf dat werkt met digitale processen.

- **Verlies van producten/diensten** Bedrijf tijdelijk offline, met omzetverlies.
- **Gestolen persoonsgegevens** Schade aan privacy én reputatie.
- **Boetes & juridische gevolgen** Datalekken kunnen leiden tot hoge boetes.
- **Verlies van klantvertrouwen** "Wie wil zijn/haar gegevens afstaan aan een bedrijf dat deze niet goed beveiligt?"

Waarom een cyberverzekering?

Een cyberverzekering beschermt tegen de financiële gevolgen van cyberincidenten zoals datalekken, hacks en ransomware. Ze helpt uw bedrijf bij:

Financiële bescherming: Herstel van systemen, dataherstel, juridische kosten en losgeld.

Aansprakelijkheid: Dekking van schade aan derden (bv. door een datalek).

Bescherming bij datalekken: Dekking van herstel, communicatie en meldingen bij Autoriteit Persoons-gegevens.

Vergoeding bij systeemuitval: Herstel en omzetcompensatie.

Juridische ondersteuning: Hulp bij privacyzaken en boetes.

24/7 hulp: Technische en juridische bijstand bij incidenten.

Crisismanagement: Ondersteuning bij communicatie en reputatieherstel.

Preventieve diensten: Audits, risicoanalyses en trainingen.

Hoe kunt u zich beschermen?

Ook zonder verzekering zijn deze maatregelen cruciaal

Sterke wachtwoorden: Uniek, lang en met tekens.

Antivirus & updates: Installeer betrouwbare software en update alles regelmatig.

Back-ups: Bewaar belangrijke data extern en veilig.

Let op phishing: Klik niet zomaar op bijlagen of links.

Altijd up-to-date: Werk software direct bij.

Train medewerkers: Laat hen cyberrisico's herkennen en correct handelen.

Twee-stapsverificatie: Extra beveiliging voor accounts.

Beperk toegang: Alleen toegang voor wie het echt nodig heeft.

Monitor systemen: Gebruik tools voor snelle detectie.Maak een noodplan: Leg vast wat te doen bij een aanval.