Ins & Outs
Cyberrisico's

Zo managet u cyberrisico's in uw bedrijf

De digitale wereld is niet meer weg te denken uit uw onderneming. U slaat informatie op in de cloud, wisselt gegevens uit via e-mail en doet bestellingen online. Bovendien werken uw medewerkers steeds vaker vanuit huis. Deze digitale infrastructuur brengt voor uw bedrijf vele voordelen, maar ook grote risico's met zich mee.

Lees meer over:

- De meest voorkomende cyberrisico's
- De impact van cybercrime voor uw onderneming
- Maak uw bedrijf weerbaarder tegen cybercriminaliteit
- Verzekeren van cyberrisico's
- Feiten en cijfers

VLC & PARTNERS

verkennen
voorkomen
verzekeren

De meest voorkomende cyberrisico's

Nieuwe technologie helpt u beter en efficiënter ondernemen. Businessmodellen van ondernemingen worden steeds afhankelijker van de beschikbaarheid van data en technologie. Hieraan kleven ook risico's. Denk aan het uitvallen van systemen, maar vooral aan aanvallen van buitenaf door cybercriminelen. De risico's kunnen uit verschillende en soms onverwachte hoeken komen. We zetten de belangrijkste cyberrisico's voor uw onderneming op een rij.

Kwaadwillende aanvallen

Het komt steeds vaker voor dat computersystemen, persoonlijke accounts, computernetwerken of digitale apparaten worden gekraakt voor criminele doeleinden. Bijvoorbeeld om uw computersysteem binnen te dringen en malware te verspreiden die bestanden verwijdert of beschadigt. Of om uw computers of bestanden te gijzelen via ransomware, waardoor het hele bedrijf platligt.

Insider threat

Bij een zogenaamde insider threat komt de dreiging vanuit de eigen organisatie. Een werknemer, voormalig werknemer of zakenpartner doet iets waardoor kwaadwillenden toegang krijgen tot de IT-systemen en mogelijk gevoelige informatie. In heel veel gevallen zijn medewerkers bedoeld of onbedoeld de oorzaak van een dergelijk incident. Bijvoorbeeld doordat zij op een linkje in een e-mail klikken (phishing), of doordat iemand binnen de organisatie onbedoeld toegang heeft tot gevoelige informatie.

BEC (Business Email Compromise)

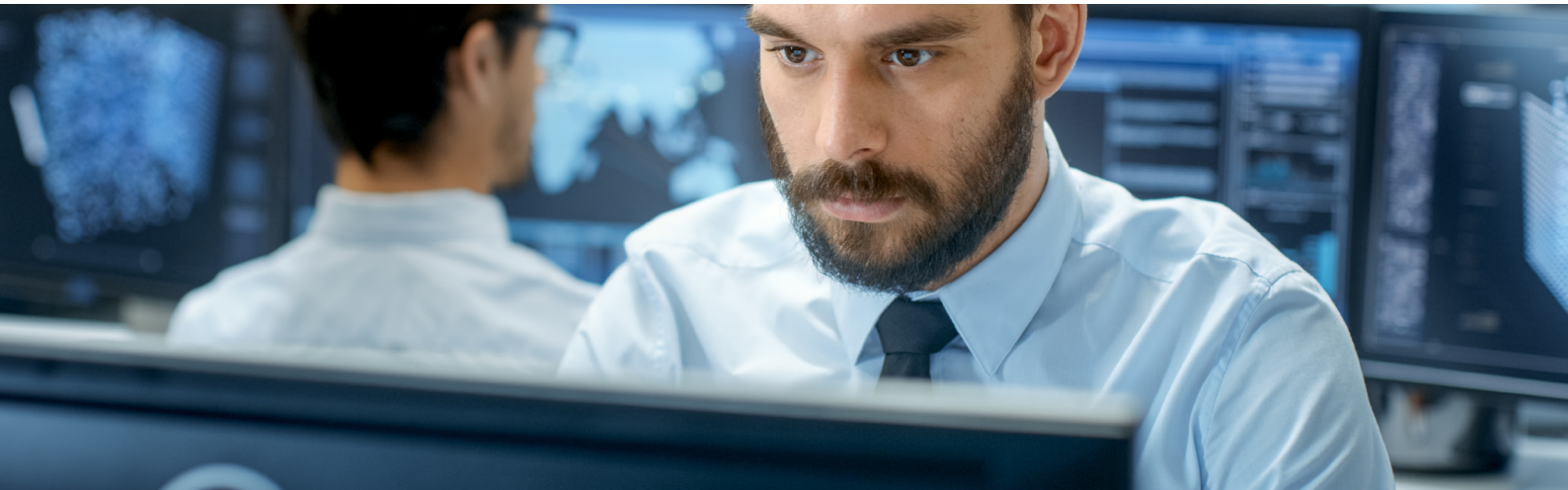
Hierbij maken criminelen gebruik van e-mailcontact binnen bedrijven. Bijvoorbeeld door een e-mailadres te gebruiken dat sterk lijkt op die van de CEO en waarmee een betalingsopdracht wordt gegeven, of door het sturen van nepfacturen.

IT-Leveranciersrisico

Cybercriminelen voeren steeds vaker geavanceerde aanvallen uit op IT-leveranciers om via de geleverde applicaties bij bedrijven binnen te dringen. Deze zogenoemde supply chain attack kan leiden tot gijzeling of spionage met een behoorlijke impact.

Storingen en ongelukken

Een ongeluk zit in een klein hoekje en ook 'normale' incidenten kunnen altijd voorkomen. Denk aan menselijk falen of programmeerfouten. Maar ook weersinvloeden kunnen schade toebrengen, zoals een spanningspiek door blikseminslag. Of uw IT-leverancier kan een fout maken, waardoor uw activiteiten stagneren.



De impact van cybercrime voor uw onderneming

De gevolgen van cybercriminaliteit kunnen groot zijn. Denk aan stagnatie van uw bedrijfsprocessen of reputatieschade. Criminelen weten dat ook en daarom slaan ze steeds vaker toe bij bedrijven. Dit zijn mogelijke gevolgen:

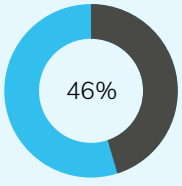
- Klantgegevens komen op straat te liggen en worden mogelijk verhandeld.
- Uw administratie wordt gegijzeld door malware en is daardoor niet meer toegankelijk.
- Gegevensbestanden raken beschadigd of zijn niet meer toegankelijk.
- U moet klanten of opdrachtgevers informeren dat hun privacy niet gegarandeerd is (geweest).
- U moet extra kosten maken omdat processen en/of diensten zijn uitgevallen.
- U loopt inkomsten mis omdat u geen producten of diensten kunt leveren.
- U krijgt te maken met kosten om geïnfecteerde bestanden en systemen te herstellen.
- U krijgt te maken met cyberincidentkosten doordat u externe deskundigen moet inschakelen voor forensisch onderzoek, consultancy of hulp op PR- en juridisch gebied.
- U ontvangt schadeclaims of boetes van derden.
- U moet losgeld betalen.
- U moet een boete betalen.

In de praktijk komen verschillende gevolgen bij elkaar en stapelen deze zich op. Daardoor wordt de financiële impact van een cyberincident op uw organisatie snel heel groot.

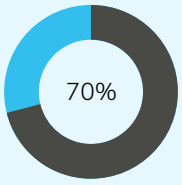
Feiten en cijfers

- Jaarlijks vinden tienduizenden moedwillige en niet-moedwillige datalekken plaats. In 2020 zijn er 23.976 datalekmeldingen gedaan bij de Autoriteit Persoonsgegevens.
- In 2020 schatte Help Net Security naar aanleiding van een enquête onder meer dan 500 leidinggevenden binnen het internationale MKB dat 46 procent van het MKB ooit slachtoffer is geweest van ransomware.
- Volgens schattingen wordt in zo'n 70 procent van alle ransomeware-aanvallen losgeld betaald door het slachtoffer.
- De Nationale Beheersorganisatie Internet Providers (NBIP) stelt in haar jaarlijkse DDoS Datarapport dat DDoS-aanvallen in 2020 krachtiger en complexer zijn geworden, terwijl ook het aantal en de duur van de aanvallen toenam.

Datalekmeldingen



Slachtoffer van ransomware



Losgeld betaald door het slachtoffer

Krachtigere en complexere DDoS aanvallen

Bron: Cybersecuritybeeld Nederland 2021 | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)

Maak uw bedrijf weerbaarder tegen cybercriminaliteit

Cybercriminaliteit volledig voorkomen is eigenlijk onmogelijk. Daarvoor gaan technologische ontwikkelingen te snel, net als de manieren die cybercriminelen vinden om daarvan misbruik te maken. Maar u kunt uw onderneming wél beter weerbaar maken tegen cybercriminelen. Via een mix van technologische en organisatorische maatregelen vermindert u niet alleen de kans dat uw onderneming slachtoffer wordt, maar verkleint u ook de gevolgen van cybercriminaliteit.

U kunt op drie manieren weerbaarder worden tegen cybercriminaliteit:

Uw interne beleid verbeteren

- Beleg het cyberbeleid binnnen het directieteam en draag het actief uit.
- Stel een functionaris gegevensbescherming aan of maak iemand hier verantwoordelijk voor. Deze persoon zorgt er ook voor dat het bedrijf steeds voldoet aan de AVG.
- Zorg voor een goedgekeurd en geïmplementeerd privacy-beleid.
- Laat medewerkers een bewustwordingstraining volgen en informeer hen steeds over nieuwe dreigingen en risico's.
- Hanteer een beleid voor kritische updates en patches om deze steeds zo snel als mogelijk uit te voeren.
- Maak intern afspraken over autorisatiebeheer en leg deze duidelijk vast.

Technologische aanpassingen doorvoeren

- Zorg voor goede firewalls en antivirusprogramma's die up-to-date zijn.
- Stel Multi-Factor Authenticatie (MFA) in voor remote access en admin accounts.
- Zorg voor encryptie van gevoelige data.
- Investeer in detectie- en responssystemen.
- Als er verouderde software wordt gebruikt, vervang of isoleer deze.
- Zorg voor goede back-upsystemen en test deze regelmatig.

Zorgen voor risicomanagement

- Maak een bedrijfscontinuïteitsplan, en vergeet ook niet het incident Response Plan en Crisisherstelplan (Disaster Recovery Plan).
- Regel contracting- en verwerkersovereenkomsten en laat deze toetsen door een jurist.
- Doe een kwetsbaarheidsscan en voer pentesten uit.
- Doe een risk assessment om risico's te identificeren en analyseren.

De experts binnen VLC & Partners kunnen u hierbij ondersteunen. Daarnaast werken we nauw samen met diverse gerenommeerde partners die u kunnen helpen met de cybersecurity van uw onderneming.

Verzekeren van cyberrisico's

Cyberrisico's verminderen is de eerste stap voor uw onderneming. Vervolgens kunt u met een Cyberverzekering via VLC & Partners de financiële schade afdekken. Zo'n verzekering biedt uw onderneming verschillende dekkingen.

Eigen schade

Cyberverzekeringen geven dekking voor uw eigen schade bij cyberincidenten. Zo ontvangt u een vergoeding voor de kosten voor onderzoek, opsporing, herstel, communicatie en PR. Daarnaast is er zelfs dekking voor de eigen kosten die u maakt voor reconstructie en herstel van gegevens of het virusvrij maken van uw systeem. In de meeste gevallen is er ook dekking voor bedrijfsschade als gevolg van stagnatie van de werkzaamheden.

Schade aan derden

U bent verzekerd voor de aansprakelijkheid van uw onderneming voor schade die is geleden door derden, inclusief verweerkosten. Daarbij is het wel van belang dat er sprake is van een onrechtmatige daad die betrekking heeft op privacy-aansprakelijkheid, aansprakelijk voor netwerkbeveiliging of media-aansprakelijkheid.

Eigen Cyber Incident Manager 24/7

Misschien wel het belangrijkste onderdeel van onze cyberverzekeringsoplossing: uw eigen Cyber Incident Manager. Daardoor profiteert u van 24/7 professionele begeleiding bij een (vermoeden van) cyber incident. En dit zonder eigen risico. De Cyber Incident Manager ondersteunt u bij de dilemma's die komen kijken na een cyberincident. Denk aan het doen van een melding, communicatie naar derden of het oplossen van IT-problemen. De Cyber Incident Response Service denkt daarin mee en schakelt desnoods andere experts in die hier ondersteuning kunnen bieden.

Wat is er niet verzekerd?

Gevolgen van BEC
Omdat cybercriminelen bij BEC (Business Email Compromise) uw medewerkers misleiden om fouten te maken zonder dat ze zelf doordringen in de IT-systemen, is hier géén sprake van cybercrime die gedekt wordt door een cyberverzekering. Een van de bekendste voorbeelden van BEC is de zogenaamde 'directeursfraude'. Een medewerker met toegang tot de bankzaken van het bedrijf, ontvangt een e-mail om snel een groot geldbedrag over te maken om een dringende reden.

U kunt dit risico zelf op een aantal manieren beperken. Bijvoorbeeld door deze vorm van fraude intern te bespreken en het op de bedrijfsagenda te zetten. Ook kunt u medewerkers leren dat ze zich niet moeten laten imponeren door de status van de aanvrager. Verder is het belangrijk betalingen te controleren door contact op te nemen met de aanvrager en te zorgen voor heldere regels in het betalingsverkeer. Tot slot raden we u aan afspraken te maken over wie betalingen mogen initiëren en altijd meerdere personen te betrekken bij de betaling; oftewel het vierogenprincipe te hanteren.

Fysieke schade
Zaak- en letselschade als gevolg van cybercrime zijn ook niet verzekerd op een cyberverzekering. Denk daarbij aan een machine die een bedrijfshal beschadigt als gevolg van een cyberincident.

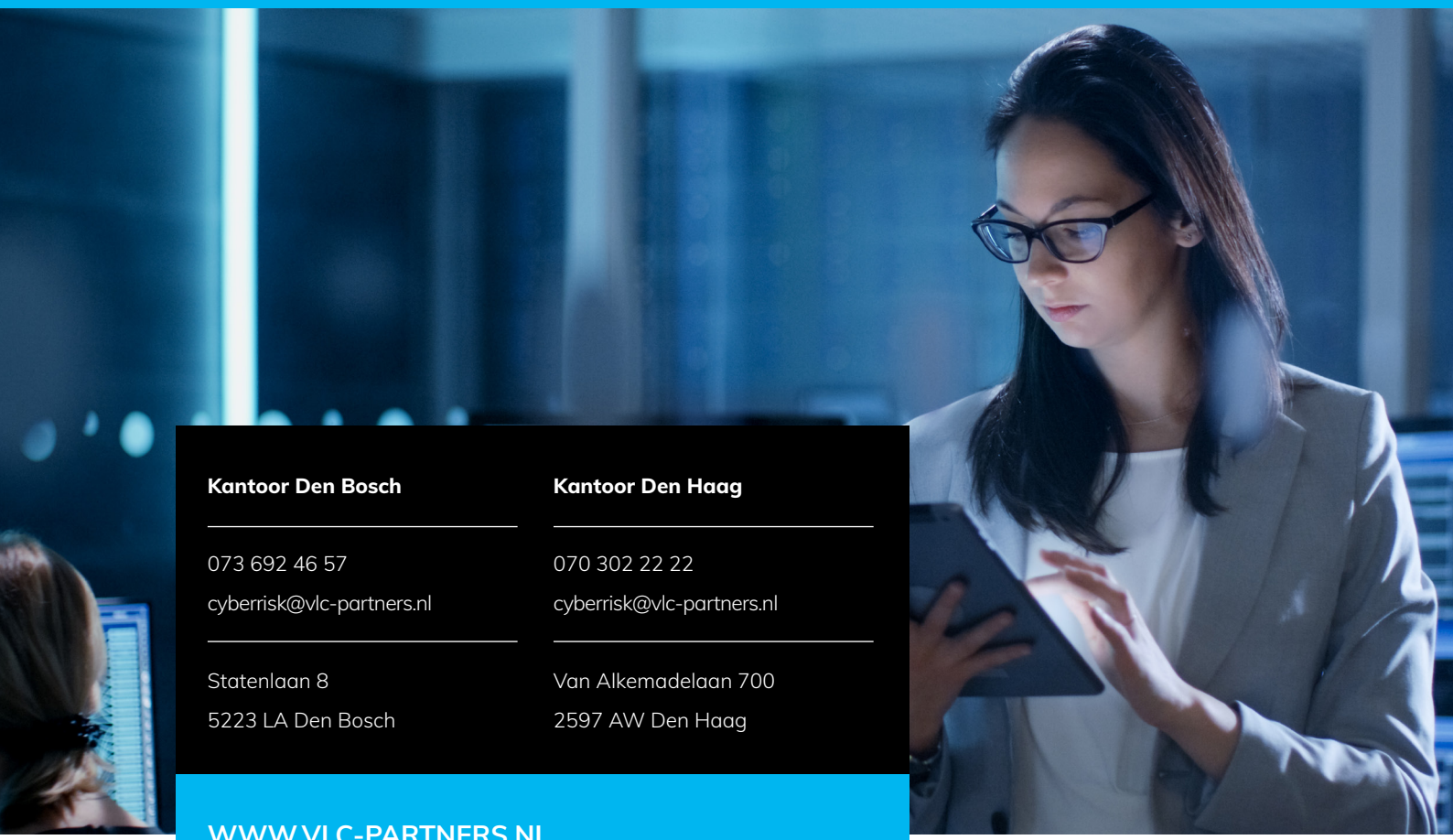
Verbeteringen en vervanging van computersystemen
Update, upgrade, verbetering of vervanging van een computersysteem waarmee het op een hoger niveau wordt gebracht. Schade door onderbreking of storing bij een leverancier van infrastructuur zoals een internetprovider, schade veroorzaakt door opzet of bewuste roekeloosheid door handelingen van bestuurders of directieleden en contractuele aansprakelijkheid en garanties zijn niet verzekerd.

Lege schappen in de supermarkt

Een logistiek bedrijf was in 2021 het slachtoffer van een ransomeware-aanval. Daardoor konden supermarkten niet meer bevoorraad worden met kaas. De hackers maakten gebruik van een lek in Microsoft Exchange, dat veel bedrijven gebruiken voor hun e-mail. De hackers eisten losgeld om de systemen weer vrij te geven. De hack kostte het bedrijf uiteindelijk veel geld. Producten die over de datum waren moesten worden weggegooid. Experts werden ingehuurd om de hele IT-infrastructuur te vernieuwen: nieuwe servers en firewalls, andere verbindingen met klanten. Daarnaast zit de schrik er bij de eigenaar en medewerkers van het bedrijf voorlopig goed in.

Over VLC & Partners

VLC & Partners is dé Nederlandse risicomanager. Onze specialisten zijn actief op het gebied van verzuim, pensioen en private insurance. We werken vanuit de drie stappen: Verkennen, Voorkomen en Verzekeren. Wij bedienen met 285 medewerkers heel Nederland vanuit onze vestigingen in Den Bosch en Den Haag. Onze adviseurs stellen hun diepgaande kennis en ervaring op het gebied van risicomanagement, pensioenadvies en zorg en verzuim beschikbaar voor zakelijke klanten. Ook voor Private Insurance, specifiek verzekeringsadvies en financial planning voor welgestelde particulieren, DGA's, zakelijke en medische professionals hebben we de beste adviseurs aan boord.



Kantoor Den Bosch

073 692 46 57
cyberrisk@vlc-partners.nl

Statenlaan 8
5223 LA Den Bosch

Kantoor Den Haag

070 302 22 22
cyberrisk@vlc-partners.nl

Van Alkemadelaan 700
2597 AW Den Haag

WWW.VLC-PARTNERS.NL

202108V1CYBI&O

VLC & PARTNERS

verkennen
voorkomen
verzekeren