

## CISO-CHECKLIST: VERBINDINGEN MET DERDEN BEVEILIGEN

### LEVERANCIERS KIEZEN MET CYBERBEVEILIGING IN GEDACHTEN

Elke keer dat u een potentiële leverancier evalueert, moet u voor uzelf de volgende vragen beantwoorden:

- Hoeveel ervaring hebben ze met klanten die vergelijkbaar zijn met uw organisatie?
- Geven ze aan de gangbare cyberbeveiligingsnormen na te leven (zoals het NIST Framework of ISO 27001, of kunnen ze een SOC-2rapport tonen)?
- Tot welke van uw gegevens en/of bedrijfsmiddelen moeten ze toegang hebben om hun diensten te kunnen leveren, en vragen ze om kennelijk onnodige toegang?
- Hoe willen ze de bedrijfsmiddelen en gegevens van uw organisatie die in hun bezit zijn beschermen?
- Hoe beheren ze hun eigen cyberrisico's van derden, en kunnen ze informatie geven over de beveiliging van hun toeleveringsketen?
- Wat is hun plan voor herstel na noodgevallen en bedrijfscontinuïteit in geval van een incident dat invloed heeft op uw organisatie?
- Hoe houden ze uw organisatie op de hoogte van trends, dreigingen en veranderingen binnen hun organisatie?

### RISICO'S VIA DERDEN IDENTIFICEREN

Voer een cyberrisicobeoordeling van derden uit en volg hierbij de volgende stappen:

- Houd een actuele lijst bij van alle relaties met leveranciers en de bedrijfsmiddelen en gegevens die in elk van deze relaties worden blootgesteld.
- Controleer de gegevens waartoe elke leverancier of derde toegang heeft en zorg ervoor dat elk toegangsniveau tot het strikte minimum wordt beperkt (principe van 'least privilege').
- Classificeer uw relaties met leveranciers en derden (laag, gemiddeld, hoog) op basis van de impact die een inbreuk op hun systemen zou hebben op uw organisatie.
- Evalueer in hoeverre de leveranciers cyberbeveiliging waarborgen en relevante normen naleven, en begin daarbij met de leveranciers met het hoogste risico.
- Ontwikkel een plan voor regelmatige veiligheidsbeoordelingen. Het kan soms zinvol zijn om leveranciers met het hoogste risico en/of de meest uitgebreide toegang tot klantgegevens ter plaatse te beoordelen.

## BEVEILIGING DOOR DERDEN BEHEREN

- Voer grondige due diligence uit. Neem in al uw offerteaanvragen, contracten, bedrijfscontinuïteit, incidentrespons en service level agreements met leveranciers de verwachtingen van uw organisatie ten aanzien van cyberbeveiliging op. Leg samen vast wie verantwoordelijk en aansprakelijk is in geval van een cyberincident.
- Informeer naar de cyberbeveiligingspraktijken van financiële organisaties en andere entiteiten waarmee u samenwerkt of gegevens deelt, en vergewis u ervan dat uw leveranciers en derden ook eventuele cyberbeveiligingseisen naleven waaraan uw organisatie moet voldoen.
- Gebruik vastgestelde en overeengekomen maatregelen om de naleving van de cyberbeveiligingsnormen van uw leveranciers te controleren.
- Controleer bij uw leveranciers die gevoelige gegevens behandelen of ze gebruikmaken van tweeledige verificatie, encryptie of andere beveiligingsmaatregelen voor de accounts die u bij hen hebt.
- Zorg ervoor dat alle door u geïnstalleerde software en hardware van derden een beveiligingshandshake heeft zodat de opstartprocessen beveiligd zijn via verificatiecodes en niet worden uitgevoerd als codes niet worden herkend.
- Als u leveranciersproducten tegenkomt die namaak zijn of niet voldoen aan de specificaties, werk dan samen aan een oplossing of anders een exitstrategie.
- Evalueer leverancierscontracten jaarlijks en zorg ervoor dat ze blijven voldoen aan uw strategische koers en de wettelijke vereisten inzake gegevensbeveiliging. Bij beëindiging van het contract moet u bepalingen opnemen over het retourneren van uw bedrijfsmiddelen of gegevens, nagaan of de bedrijfsmiddelen of gegevens die in het bezit waren van de leverancier volledig zijn gewist en zorgen dat hij niet langer toegang heeft tot uw systemen of servers.

## INFORMATIE DELEN

- Zorg ervoor dat u duidelijke communicatiekanalen en contactpunten hebt om te communiceren over beveiligingsproblemen met de leveranciers en concurrenten van uw organisatie.
- Deel betrouwbare, bruikbare cyberbeveiligingsinformatie tijdig met interne en externe belanghebbenden (inclusief organisaties en overheidsinstanties binnen en buiten de financiële sector).
- Volg relevante updates over de ervaringen van andere organisaties met hun derden op het gebied van dreigingen, zwakke plekken, incidenten en respons door deel te nemen aan informatie-uitwisseling met andere organisaties, bijvoorbeeld in het kader van FS-ISAC, en door andere bronnen van informatie over dreigingen te zoeken.



[CarnegieEndowment.org](https://CarnegieEndowment.org)

