Checklist cyberveiligheid

Third Party Risk Management (TPRM)
voor het midden- en kleinbedrijf

ABN·AMRO

Hebben leveranciers, klanten en andere partners hun cyberveiligheid op orde? Zet in op Third Party Risk Management (TPRM) om cyberrisico's bij anderen te voorkomen, die ook uw organisatie raken. Gebruik onze checklist waarop u iedere samenwerking in ieder geval wilt controleren.

Werkt de andere partij cyberveilig?

Leveranciers, distributeurs, agenten, klanten en andere samenwerkingspartners verwerken allerlei gegevens, ook van uw bedrijf en medewerkers. U wilt zeker weten dat dit veilig gebeurt. Richt u bij de beoordeling van potentiële partners daarom op de digitale veiligheid van:

IT en netwerk

Gebruikt het bedrijf SSL-protocollen en andere belangrijke beveiligingsstandaarden voor het inkomende en uitgaande dataverkeer, haar website en het IT-netwerk?

Applicaties

Zitten er geen gaten in de beveiliging van (web) applicaties, domeinen en andere online systemen die van buitenaf bereikbaar zijn?

Medewerkers

Zijn medewerkers van partnerbedrijven zich bewust van cyberdreigingen, bijvoorbeeld via e-mail, social media en andere communicatiekanalen?

Tip!

Breng de eigen veiligheidsstandaarden in kaart

Breng op een vergelijkbare manier de veiligheids-standaarden binnen uw bedrijf en het bewustzijn bij eigen medewerkers in kaart. Zorg dat u cyberveilig werkt, om vervolgens de Third Party Risks in kaart te brengen.

Checklist TPRM voorkom cyberrisico's bij partners

Gebruik deze checklist om leveranciers, klanten en andere partners op hun cyberbeveiliging te controleren.

Checklist ✓

1. Toegang tot data
2. Vergelijk met branchebenchmarks
3. Authenticatie: veilige wachtwoorden
4. Applicatie- en systeemontwikkeling
5. Beheer van (gedeelde) data
6. Medewerkers en hun cyberbewustzijn
7. Vraag naar Endpoint Security
8. Assetmanagement
9. Third Party Security Risk
10. Security Incident Management

1. Toegang tot data

Wie heeft er toegang tot welke data (van uw bedrijf)? Beoordeel de beschikbaarheid, betrouwbaarheid en vertrouwelijkheid van data. Hoe slaat het partner-bedrijf (jouw) gevoelige bedrijfsdata op? En wie houdt de toegang tot deze data bij en is er een duidelijk proces ingericht voor joiners, movers en leavers?

Onderzoek wie, op welke manier, waarom en wanneer toegang heeft tot data. Houdt de leverancier met regelmaat de systeemtoegangsrechten bij? En wat gebeurt er bij een duidelijke scheiding van rechten? Controleer of de leverancier het principe van least privilege gebruikt.

2. Vergelijk met branchebenchmarks

Vergelijk de werkwijze bij de partner met de benchmark binnen de branche.

Is de organisatie ISO 27001-gecertificeerd? Controleer of een bedrijf werkt volgens het NIST Cyber Security Framework, volgens de ISO 22307-norm voor privacy en de CoBIT-norm voor IT governance. Of hebben organisaties zelfs een ISAE3401-certificering die de effectiviteit van maatregelen test?

3. Authenticatie: veilige wachtwoorden

Gebruiken medewerkers bij het partnerbedrijf unieke en sterke wachtwoorden voor authenticatie? Vraag naar de manier waarop medewerkers (op afstand) toegang krijgen tot systemen en data.

Stuur aan op multifactor-authenticatie (MFA) en SSO/SAML-beveiliging voor medewerkers en klanten. Dat is extra belangrijk voor medewerkers en klanten die internet en kritische systemen gebruiken of toegang nodig hebben tot kritische data.

4. Applicatie- en systeemontwikkeling

Documenteert en implementeert de leverancier processen en normen over de veilige levenscyclus van softwareontwikkeling (SDLC: Software Development Life Cycle)?

Controleer daarnaast of leveranciers beveiligingsvereisten en -controles hebben gedefinieerd en geïmplementeerd als zij ontwikkeling uitbesteden.

Controleer ook specifiek welke richtlijnen het bedrijf gebruikt voor API-beheer. Let bijvoorbeeld op:

- API rate limiting
- API-sleutelopslag
- IP-vrijstelling voor API-toegang
- API-gebruikersauthenticatie

5. Beheer van (gedeelde) data

Wordt data versleuteld volgens de veilige standaarden voor data-encryptie? Stuur aan op versleutelde data, om te voorkomen dat cybercriminelen die kunnen onderscheppen. Controleer ook wat er gebeurt bij afsluiting van een contract. Zal de leverancier de data vernietigen?

6. Medewerkers en hun cyberbewustzijn

Maakt het bedrijf haar medewerkers regelmatig bewust van de bestaande en nieuwe cyberrisico's? Pas bij voldoende security awareness rondom cybercrime vormen medewerkers niet langer de traditioneel zwakke schakel. Ook management-betrokkenheid is cruciaal voor het ontwikkelen en handhaven van effectieve cyberbeveiligingsstrategieën en waarborgen van bedrijfscontinuïteit bij incidenten.

Heeft het bedrijf een security officer en gebruikt de organisatie een programma om cyberrisico's blijvend in kaart te brengen en medewerkers daarin te trainen?

Controleer ook of medewerkers een VOG moeten aanvragen en of er andere achtergrondchecks worden uitgevoerd. Zorg dat u weet wie er met (uw) data werkt.

7. Vraag naar Endpoint Security

Vraag om de maatregelen voor Endpoint Security die het bedrijf neemt. Het gaat bijvoorbeeld om richtlijnen voor gebruik van smartphones, tablets en laptops voor onderweg en thuis. Denk bijvoorbeeld aan Endpoint Detection & Response (EDR) en een Virtual Private Network (VPN) voor versleuteling van de communicatie. M.a.w., is er sprake van voldoende beveiliging om gegevens te beschermen?

8. Asset management

Hoe beheren en identificeren leveranciers, klanten en andere partijen hun assets en wijzen ze de juiste verantwoordelijkheden toe? Hoe beschermen ze hun assets bij het wijzigen of beëindigen van een dienstverband, contract of overeenkomst? Software die deze partij in eigen beheer heeft dient regelmatig te worden geüpdatet om bescherming te bieden tegen de nieuwe beveiligingsrisico's en om te zorgen dat de functionaliteiten optimaal blijven werken.

Controleer op de veilige verwijdering van apparatuur. En vraag na hoe opslagmedia veilig worden beheerd tijdens de volledige levenscyclus.

9. Third Party Security Risk

Handhaaft een leverancier het overeengekomen niveau voor informatiebeveiliging in hun relaties met derden? Hebben ze een Security Risk Management-proces om beveiligingsrisico's van hun derden te identificeren, continu te bewaken en te minimaliseren? Het is niet alleen van belang dat de leverancier deze afspraken heeft vastgelegd maar ook dat de vastgelegde verplichtingen periodiek worden getoetst, bijvoorbeeld middels een externe audit om te verifiëren dat de verplichtingen worden nageleefd.

Controleer of de informatiebeveiligingsvereisten zijn opgenomen in leverancierscontracten, ook als het gaat om clouddiensten. Specifieke afspraken die hierbij van belang zijn zijn o.a. system hardening, malwareprotectie en patch management..

10. Security Incident Management

Hebben leveranciers processen voor het beheer van beveiligingsincidenten gedefinieerd, gecommuniceerd en geïmplementeerd, inclusief relevante rollen en verantwoordelijkheden? Deze processen moeten betrekking hebben op incidentrapportage, incidentrespons, het verzamelen van bewijsmateriaal en geleerde lessen.

Hoe is uw leverancier in staat om kritieke beveiligingsincidenten te monitoren en te beheren?

Controleer hoe zij omgaan met incidenten en wanneer leveranciers u daarvan op de hoogte stellen. Zorg dat leveranciers u binnen 24 uur op de hoogte brengen van incidenten.

Disclaimer

Copyright © 2024 ABN AMRO Bank. All rights reserved. De informatie in dit document is bestemd voor midden- en kleinbedrijven in Nederland.

Verstrekking aan anderen is niet toegestaan zonder toestemming van ABN AMRO.

ABN·AMRO