HANDLEIDING CISO-NIVEAU: VERBINDINGEN MET DERDEN BEVEILIGEN

RISICO'S VIA DERDEN IDENTIFICEREN

- Houd een actuele lijst bij van alle relaties met leveranciers en de bedrijfsmiddelen en gegevens die in elk van deze relaties worden blootgesteld.
- Bekijk de gegevens waartoe elke leverancier of derde toegang heeft. Zorg ervoor dat dit 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 begin daarbij met de leveranciers met het hoogste risico. Naleving van relevante normen is een goed uitgangspunt. 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 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 andere derden zoals financiële organisaties waarmee u samenwerkt of gegevens deelt .Alle cyberbeveiligingseisen waaraan uw organisatie moet voldoen ,moeten ook gelden voor uw leveranciers en alle andere organisaties waarmee u gegevens deelt of die toegang hebben tot bedrijfsmiddelen.
- 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.
- Het tijdig delen van betrouwbare, bruikbare cyberbeveiligingsinformatie 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 zodat uw organisatie beter gewapend is, zich beter bewust is van de situatie en meer te weten komt. Als uw organisatie deelneemt aan informatie-uitwisseling met andere organisaties, bijvoorbeeld in het kader van de FS-ISAC, kunt u gemakkelijk op de hoogte blijven.

Leveranciers kiezen met cyberbeveiliging in gedachten

Stel potentiële leveranciers de volgende vragen om hun bescherming tegen en bewustzijn van cyberaanvallen te meten en daarmee de impact die ze zouden hebben op het risicoprofiel van uw organisatie:

1. Hoeveel ervaring hebben zij? Achterhaal voor welke klanten de leverancier heeft gewerkt. Have they served clients similar to your organization beåfore?
2. **Geven ze aan de gangbare cyberbeveiligingsnormen na te leven** zoals het NIST Framework of ISO 27001, of kunnen ze een SOC2-rapport tonen?
3. Tot welke van uw gegevens en/of bedrijfsmiddelen moeten ze toegang hebben om hun diensten te kunnen leveren? Vragen ze om kennelijk onnodige toegang?
4. Hoe willen ze de bedrijfsmiddelen en gegevens van uw organisatie die in hun bezit zijn beschermen?
5. Hoe beheren ze hun eigen cyberrisico door derden? Kunnen ze informatie geven over hun toeleveringsketen?
6. **Wat is hun plan voor herstel na noodgevallen en bedrijfscontinuïteit?** in geval van een incident dat invloed heeft op de bedrijfsmiddelen en/of gegevens van uw organisatie?
7. Hoe houden ze uw organisatie op de hoogte? Hoe willen ze trends, dreigingen en veranderingen binnen hun organisatie communiceren?

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE
INTERNATIONAL MONETARY FUND
THE WORLD BANK IBRD • IDA | WORLD BANK GROUP
SWIFT
SWIFT INSTITUTE
FS-ISAC
Standard Chartered
CYBER READINESS INSTITUTE
GLOBAL CYBER ALLIANCE
ICBA Independent Community Bankers of America