# Handleiding incidentrespons

## Voorbereiding

⇒ Werk samen met het senior management van uw organisatie en andere betrokken medewerkers om een incidentrespons en bedrijfscontinuïteitsplan op te stellen op basis van de meest urgente risico's die geïdentificeerd zijn in de cyberrisicobeoordeling van uw organisatie.

- Ontwikkel dreigingsscenario's voor de soorten incidenten die verband houden met de cyberrisico's die binnen uw organisatie de hoogste prioriteit hebben. Focus op capaciteitsopbouw om te reageren op die scenario's.
- Stel een lijst met contactpunten voor incidentrespons samen en verspreid deze binnen uw organisatie.
- Verzamel contactgegevens van relevante lokale en federale wetshandhavingsinstanties en -functionarissen.
- Stel bepalingen vast die aangeven welke soorten incidenten moeten worden gemeld, wanneer ze moeten worden gemeld en aan wie.
- Stel schriftelijke richtlijnen vast die aangeven hoe snel medewerkers moeten reageren op een incident en welke handelingen nodig zijn op basis van relevante factoren zoals de functionele en informatie-impact van het incident en de waarschijnlijkheid van herstel na het incident.
- Laat alle medewerkers contact opnemen met uw technische team – dit zijn meestal de IT-medewerkers en/of de CISO/CIO/een andere vergelijkbare manager – wanneer zich een incident voordoet.
- Implementeer oplossingen om de handelingen van werknemers te monitoren en om dreigingen en incidenten te kunnen identificeren.
- Voeg bedrijfscontinuïteitsplannen toe om de samenwerking van uw organisatie met leveranciers en primaire klanten tijdens een zakelijk noodgeval te coördineren. Vermeld indien nodig ook hoe handmatige of alternatieve bedrijfswerkzaamheden uitgevoerd zouden moeten worden.
- Stel schriftelijke procedures op voor het uitschakelen en herstarten van het systeem in noodgevallen.
- Ontwikkel en test methoden voor het ophalen en herstellen van back-upgegevens; test back-upgegevens periodiek om de validiteit ervan te verifiëren.
- Zorg dat er overeenkomsten en procedures zijn voor het uitvoeren van bedrijfsactiviteiten op een alternatieve locatie.
- Zorg dat er een duidelijk kanaal is voor de verspreiding naar alle klanten.

## Oefening

⇒ Organiseer kleine tafeloefeningen met alle medewerkers of vertegenwoordigers van alle personeelsniveaus, inclusief leidinggevenden van de organisatie, PR/communicatiemedewerkers en juridische en nalevingsteams.
⇒ Zoek tafeloefeningen in de branche die relevant zijn voor uw organisatie en neem hieraan als het even kan deel.
⇒ Stel een proces vast om ervoor te zorgen dat de geleerde lessen van de oefeningen worden opgenomen en aan de orde komen in de cyberbeveiligingsstrategie van uw bedrijf.

## Respons

⇒ Implementeer een incidentresponsplan om de impact te minimaliseren, ook op het vlak van reputatieschade.
⇒ Identificeer betrokken/aangetaste systemen en beoordeel de schade.
⇒ Verminder de schade door de betrokken bedrijfsmiddelen te verwijderen (loskoppelen).
⇒ Begin met het opnemen van alle informatie zodra het team vermoedt dat er een incident heeft plaatsgevonden. Probeer bewijs van het incident te bewaren tijdens het loskoppelen/scheiden van aangetaste geïdentificeerde bedrijfsmiddelen. Verzamel bijvoorbeeld de logboeken van de systeemconfiguratie, het netwerk en inbraakdetectie uit de betrokken bedrijfsmiddelen.
⇒ Breng de juiste interne partijen, externe leveranciers en autoriteiten op de hoogte en vraag indien nodig om hulp.
⇒ Breng klanten op de hoogte en bied ondersteuning in overeenstemming met wet- en regelgeving en richtlijnen tussen instanties.
⇒ Gebruik platforms voor het delen van informatie over dreigingen zoals FS-ISAC of MISP om de branche op de hoogte te stellen van de dreiging.
⇒ Documenteer alle stappen die tijdens het incident werden genomen om deze later te beoordelen.

## Herstel

⇒ Herstel herstelde bedrijfsmiddelen naar periodieke "herstelpunten" (indien beschikbaar) en gebruik back-upgegevens om systemen te herstellen naar de laatst bekende "goede" status.
⇒ Creëer bijgewerkte "schone" back-ups van herstelde bedrijfsmiddelen en zorg ervoor dat alle back-ups van kritieke bedrijfsmiddelen op een fysieke locatie in een veilige omgeving worden opgeslagen.
⇒ Test en controleer of geïnfecteerde systemen volledig zijn hersteld. Bevestig dat de betrokken systemen normaal functioneren.

## Beoordeling

⇒ Voer een discussie over "geleerde lessen" nadat het incident heeft plaatsgevonden – overleg met senior medewerkers, vertrouwde adviseurs en de leverancier(s) van computerondersteuning om mogelijke zwakke plekken te beoordelen of nieuwe stappen aan te bevelen die moeten worden geïmplementeerd.
⇒ Identificeer, indien mogelijk, de zwakke plekken (in software, hardware, bedrijfsactiviteiten of gedrag van medewerkers) die tot het incident hebben geleid en ontwikkel een plan om hierin verbetering aan te brengen.
⇒ Ontwikkel een plan voor controle om soortgelijke of verdere incidenten met betrekking tot de geïdentificeerde problemen te detecteren.
⇒ Deel geleerde lessen en informatie over het incident op platformen voor het delen van informatie over dreigingen zoals FS-ISAC.
⇒ Integreer de geleerde lessen in de protocollen voor respons op incidenten van uw organisatie.