Cyber Chain Resilience Consortium

Eerste hulp Crisiskaart

Cyber Chain Resilience Consortium

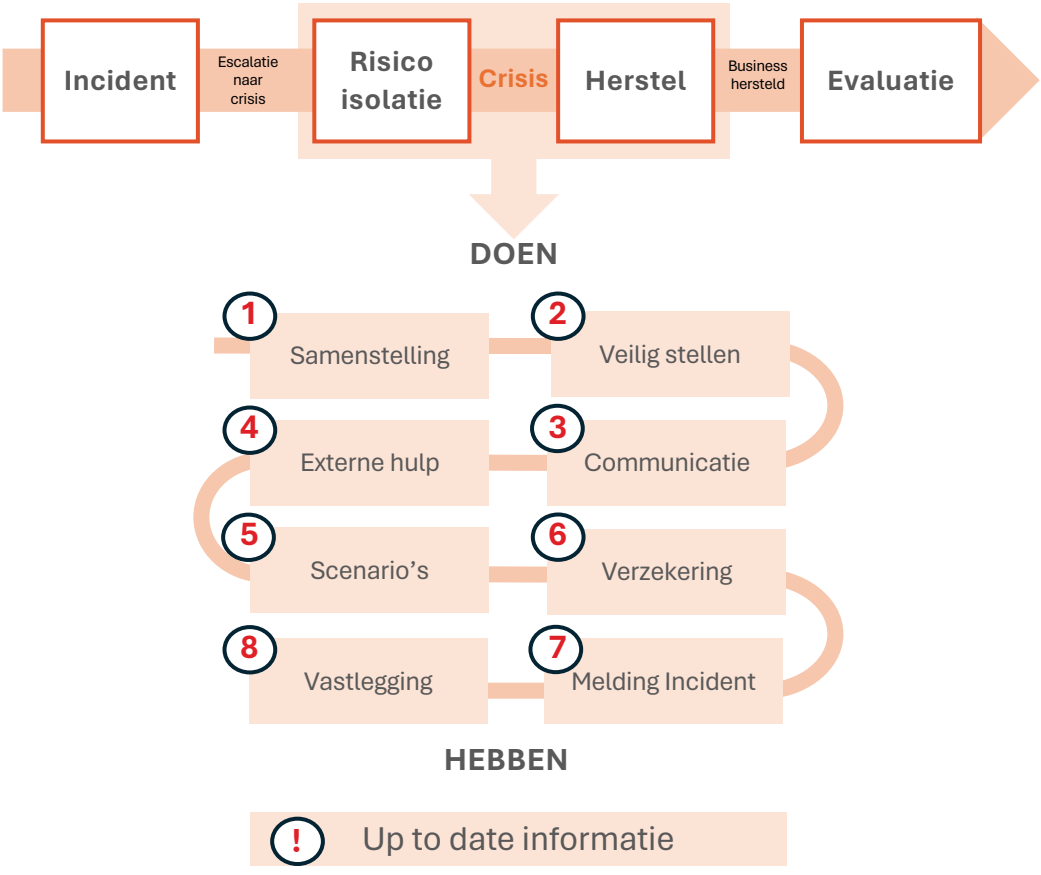
Vraag meer informatie aan!

Cybercrisis? Geen paniek!

Een cyberaanval kan aanzienlijke schade veroorzaken. Door adequaat te handelen met eenvoudige acties kan de impact van de cyberaanval fors beperkt worden. Deze kaarten helpen je daarbij.

Hoe werkt het?

1. Vul de kaarten aan met informatie die relevant is voor jouw organisatie.
2. Zorg ervoor dat zowel fysieke als digitale exemplaren van de kaarten beschikbaar zijn voor het crisisteam.
3. Oefen regelmatig en maak daarbij gebruik van deze kaarten.



Vraag meer informatie aan!

1 Samenstelling Team

De eerste stap bij een crisis is het samenstellen van het crisisteam. Zoek naar een balans tussen expertise en slagvaardigheid en houd het team zo klein mogelijk. De rollen van voorzitter, logger, security / privacy en communicatie zijn altijd aanwezig bij een cyber crisis. De overige rollen zijn enkel aanwezig als dat nodig is.

	Rollen Crisisteam	Naam	Telefoonnr.
Altijd aanwezig	Voorzitter		
	Logger		
	Security / Privacy officer		
	Communicatie expert		
Op verzoek aanwezig	IT Manager		
	Jurist		
	Human Resource mgr		
	Privacy officer		
	Facility manager		

2 Veilig stellen

Tijdens een cybercrisis staan organisaties vaak voor moeilijke beslissingen. Een van de meest voorkomende reacties is het uitschakelen van de systemen, maar dit kan de situatie verergeren. Om effectief te reageren op een cybercrisis, is een doordacht stappenplan essentieel. Volg de onderstaande stappen om de situatie effectief te managen.

☐ Zet de apparatuur niet uit	Zo voorkom je verlies van waardevolle onderzoeksdata.
☐ Verbreek de netwerkverbinding	Schakel wifi uit en ontkoppel de netwerkstekker.
☐ Stel de back-ups veilig	Zorg in overleg met IT dat de back-ups zo snel mogelijk veilig worden gesteld, bij voorkeur volledig losgekoppeld van het netwerk.
☐ Zet automatische back-ups uit	Zorg ervoor dat de automatische back-upprocessen worden stopgezet in overleg met IT, om verdere verspreiding van de besmetting te voorkomen.
☐ Stel logfiles veilig	Logbestanden zijn van cruciaal belang voor forensisch onderzoek. Vraag IT daarom om zoveel mogelijk logs veilig te stellen. (Werkplek-, netwerk- en serverlogs zijn bijzonder waardevol voor dit doel).

3 Communicatie

Aannames of onjuiste informatie met betrekking tot een crisis zorgt voor vertraging van het afhandelen van de crisis omdat veel tijd verloren gaat in het corrigeren van de informatie. Wees proactief in het communiceren en blijf zo baas over de beeldvorming in de omgeving ten aanzien van de crisis.

☐	Communicatie expert	Zorg vanuit het crisisteam altijd voor een communicatie expert die integraal verantwoordelijk is voor alle communicatie rond de crisis.
☐	Kanaliseren communicatie	Forceer alle communicatie in relatie tot de crisis via het crisisteam om grip te houden op communicatie.
☐	Interne communicatie	Medewerkers altijd passend informeren. Zij krijgen vaak als eerste vragen uit de omgeving.
☐	Klant communicatie	Klanten willen vaak niet via-via geïnformeerd worden. Zorg voor heldere informatie naar klanten.
☐	Crisis communicatie	Tijdens de crisis is er intensieve communicatie tussen de leden van het crisisteam. Spreek een communcatieprotocol af en gebruik een mobiel chattool zoals Signal, Threema of WhatsApp.
☐	Openbare communicatie	Zorg ervoor dat je de openbare media van informatie voorziet, in plaats van dat zij hun eigen interpretaties geven aan informatie verkregen via andere kanalen.
☐	Blijf communiceren	Tijdens een crisis gebeurt er veel en is regelmatige communicatie essentieel, zelfs zonder nieuwe ontwikkelingen.

Vraag meer informatie aan!

4 Externe hulp

Er zijn bedrijven die gespecialiseerd zijn in het begeleiden van een cybercrisis. Noteer hieronder de contactgegevens van het door jou gekozen bedrijf. Het is raadzaam om vooraf afspraken te maken voor meer zekerheid. Let op: veel cyberverzekeraars hebben al overeenkomsten met dergelijke bedrijven. Controleer dit altijd eerst! Zie ook kaart 6.

Contactgegevens Incident Response bedrijf	
Bedrijf	
Alarmnummer	
E-mail	
Uurtarief	
Responstijd	

Vraag meer informatie aan!

Belangrijke informatie

Voor het effectief managen van een cybercrisis is het cruciaal om snel vast te stellen of kritische processen zijn getroffen en of er mogelijk een leverancier bij betrokken is. Tijdens een crisis is het verstandig om de verantwoordelijke(n) van deze processen te benaderen voor meer details. Daarom is het essentieel om de contactgegevens van de proceseigenaren vast te leggen.

Kritische bedrijfsprocessen (zie voorbeelden)

Proces	Wie is verantwoordelijk

Essentiele leveranciers

Bedrijfsnaam	Levert welke dienst of product

Belangrijke documenten (zie voorbeelden)

Naam document	Waar kun je het document vinden?

Vraag meer informatie aan!

Telefoon	Betrokken essentiële Leveranciers

Contract eigenaar	Telefoon

Voorbeeld bedrijfsprocessen

Online verkoopkanaal	Productieproces B
IT services	HR proces
Productieproces A	Verkoopproces

Voorbeeld belangrijke documenten

Bedrijfscontinuïteitsplan(nen)
Incidentmanagementplan
Crisiscommunicatieplan

5 Scenario's

Het managen van een crisis wordt efficiënter wanneer dit gebeurt aan de hand van scenario's. Stel 3 scenario's op en werk deze regelmatig bij op basis van nieuwe inzichten gedurende de afhandeling van de crisis.

☐	**Positief** scenario	De dienstverlening komt weer terug zonder al te veel impact en de kosten blijven beperkt.
☐	**Gemiddeld** scenario	Er is flinke impact en de duur van de crisis is enkele dagen tot weken. Maar uiteindelijk kan alles weer hersteld worden ondanks hoge kosten die gemaakt worden.
☐	**Slechtste** scenario	De impact is zo groot dat herstel niet meer mogelijk is omdat er verlies is van kritische data en de dienstverlening ligt vele weken stil.

6 Verzekering

Er zijn verzekeringen die kosten als gevolg van een cybercrisis dekken, zogenaamde cyberverzekeringen. Overweeg of een cyberverzekering zinvol voor je is. Als dat het geval is, noteer dan hieronder de gegevens van de verzekeraar en wanneer je hen moet inschakelen bij een cybercrisis.

Contactgegevens Cyberverzekering	
Naam verzekeraar	
Alarmnummer	
E-mail contactpersoon	
Eigen risico	
Externe hulp	Ja: vul gegevens in bij kaart 4 Nee

Vraag meer informatie aan!

7 Melding Incident

Vanuit verschillende wetten is het verplicht een privacy- of cyberincident te melden. Hieronder volgt een overzicht van de meest voorkomende meldingsplichten en ruimte om aan te vullen met eventuele meldingsplichten voor jouw organisatie / sector.

☐	Datalek	Voor alle organisaties: Binnen 72 uur na ontdekken van datalek incident.	www.autoriteitpersoonsgegevens.nl/datalek-melden
☐	Cyber incident	Voor vitale organisaties: melden zo snel als mogelijk.	www.ncsc.nl/contact/wbni-melding-doen
☐			
☐			
☐			

8 Vastlegging

Tijdens een crisis vinden er vaak veel gebeurtenissen plaats in korte tijd. Het vastleggen van beslissingen, acties en andere relevante zaken is van groot belang voor een efficiënte afhandeling van de crisis. Hieronder vind je een aantal tips voor een goede documentatie.

☐	Wijs een logger aan	Een logger is primair verantwoordelijk voor de vastlegging van alle relevante zaken. De logger bewaakt meestal ook acties en regelt de overleggen.
☐	Logboek goed zichtbaar	Een logboek verhoogt de efficiëntie van het crisisteam als alle leden toegang hebben. Zo is er slechts 1 waarheid en ook een log van acties en voortgang. Dit kan digitaal of fysiek.
☐	Feiten vastlegging	Leg elk relevant feit vast, hoe klein ook. Zet er ook het tijdstip bij van vastlegging. Tijdens elke vergadering komen er meer feiten bij.
☐	SMART Acties	De logger zorgt ervoor dat acties SMART (Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdsgebonden) worden vastgelegd.
☐	Maak een tijdslijn	Zorg voor een goede tijdslijn waarmee een chronologisch verloop van de crisis is te zien.

Het Cyber Chain Resilience Consortium (CCRC) is een platform waar publieke en private organisaties en hun toeleveranciers, cross sectoraal samenwerken om zich te beschermen tegen “Supply Chain Cyberaanvallen”. De partners van CCRC delen gezamenlijk de inspanning en kosten voor het opzetten en uitvoeren van cyberoefeningen in de keten, die geheel gefaciliteerd worden door CCRC. Hiermee worden cyberoefeningen voor bedrijven meer toegankelijk en zorgen we samen voor een hogere cyberweerbaarheid van Nederland.