Cyber Chain Resilience Consortium

Eerste hulp Crisisgids

Beperk schade bij een Cyberaanval

Cyber Chain Resilience Consortium

Colofon

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.

© 2024: Een uitgave van de stichting Cyber Chain Resilience Consortium (CCRC)

Opmaak: Studio Beet Vormgeving – Remco Baars

Redigeren: Kelvin Rorive

De Eerste hulp Crisisgids is gratis te downloaden via www.ccrc.nl.

Eerste hulp Crisisgids

Beperk schade bij een Cyberaanval

Inhoud

Cybercrisis? Geen paniek!

Met deze “Eerste hulp crisisgids”

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

Hoe werkt het?

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

Wat maakt een cybercrisis zo bijzonder?

- Je krijgt vaak te maken met een actieve aanvaller die anticipeert op de verdediging. Het kunnen acteren op gebeurtenissen vereist expertise
- Het kan dagen tot weken duren, 24x7. Fitheid van het crisisteam is belangrijk aandachtspunt
- De situatie is bijna altijd vertrouwelijk en wordt in het geheim afgehandeld. Dit maakt communicatie uitdagend.
- Het herstel van dienstverlening is niet altijd de eerste prioriteit. Stoppen van de aanval is belangrijker.
- Een onderhandeling met een aanvaller kan voor komen. Dit vereist expertise. Vaak is een volledige IT analyse nodig om besmettingen uit te sluiten. Dit kost altijd veel tijd.
- Het proactief uitzetten van ‘gezonde’ systemen hoort bij de aanpak. Dit betekent klantimpact veroorzaken.
- Herstel van dienstverlening vanaf scratch behoort tot realistische scenario’s. Hiervoor moet capaciteit in materiaal en mensen zijn.


Snel handelen
minder schade
Escalatie
naar crisis
Business
hersteld
Incident
Risico
isolatie
CRISIS
Herstel
Evaluatie
DOEN
1
Samenstelling team
2
Veilig stellen
4
Externe hulp
3
Communicatie
5
Scenario's
6
Verzekering
8
Vastlegging
7
Melding incident
HEBBEN
!
Up to date informatie

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 officer en communicatie expert zijn altijd aanwezig bij een cyber crisis. De overige rollen zijn enkel aanwezig als dat nodig is.

Lees ook de volgende pagina met tips over effectief crisis management

Rollen crisisteam

	Naam	*Telefoonnummer*
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.

Actielijst

☐	**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. Door op tijd en duidelijk te communiceren, houd je controle over hoe mensen naar de crisis kijken.

Communicatielijst

☐	**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 communicatieprotocol 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.

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 pagina 16.**

Contactgegevens Incident Response bedrijf

Bedrijf

Alarmnummer

E-mail

Uurtarief

Responstijd

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

- Bedrijfsproces
- Wie is verantwoordelijk
- Telefoon
- Betrokken essentiële leveranciers

- Bedrijfsproces
- Wie is verantwoordelijk
- Telefoon
- Betrokken essentiële leveranciers

- Bedrijfsproces
- Wie is verantwoordelijk
- Telefoon
- Betrokken essentiële leveranciers

Voorbeeld bedrijfsprocessen

- Online verkoopkanaal
- IT services
- Productieproces A
- Productieproces B
- HR proces
- Verkoopproces

Essentiële leveranciers

- Bedrijfsnaam
- Levert welke dienst of product
- Contract eigenaar
- Telefoon

- Bedrijfsnaam
- Levert welke dienst of product
- Contract eigenaar
- Telefoon

- Bedrijfsnaam
- Levert welke dienst of product
- Contract eigenaar
- Telefoon

Belangrijke documenten

- Naam document
- Waar kun je het document vinden?
- Naam document
- Waar kun je het document vinden?
- Naam document
- Waar kun je het document vinden?
- Naam document
- Waar kun je het document vinden?

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.

Scenario's

☐	**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	NEE / JA › vul gegevens in op pagina 12

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.

Incidenten

☐	**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.

Vastlegging

☐	**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.

Effectief crisismanagement

Een aantal tips

Altijd doen!

- Kom op vaste momenten als team bij elkaar.
- Gebruik een vaste crisisagenda, zie Pagina 18.
- Hanteer een overlegstructuur zoals de BOB methodiek; van Beeldvorming naar Oordeelsvorming en Besluitvorming managementmodellensite.nl/bob-model/
- Gebruik een logboek om besluiten en acties vast te leggen en te monitoren.
- Communiceer proactief (altijd feitelijk) richting direct betrokkenen (intern en extern) over feiten, het proces en genomen acties op voorspelbare en regelmatige momenten.
- Probeer verrassingen voor te zijn door het ontwikkelen van 'wat als-scenario's' (zie ook pagina 10).
- Onderhoud deze 'wat-als scenario's' gedurende de ontwikkelingen van de crisis.

Belangrijke besluiten

- Wel/niet preventief uitzetten van "gezonde" systemen.
- Wel/niet ingaan op eisen in het geval van een cyberaanval.
- Wanneer starten met herstel? Is de cybercrisis onder controle ('brand-meester')?

Wat een crisismanager zich moet afvragen bij de start van een incident

- Hoe is de crisis ontdekt?
- Is al bekend wat voor soort aanval het betreft? (aanval op ketenpartij, DDoS, Datadiefstal, Malware / Ransomware, Cyberaanval)
- Wat is het vermoedelijke motief van de aanval? (hacktivisme, financieel gewin, diefstal vertrouwelijke data, ontwrichting maatschappij)
- Is er impact voor de dienstverlening of wordt die verwacht?
- Zijn er andere issues die tegelijkertijd spelen?
- Wie is al op de hoogte? (medewerkers, toezichthouder, klanten, leveranciers, media).
- Zijn er andere partijen (zoals ketenpartijen) betrokken bij de crisis?
- Hebben andere organisaties ook last van de crisis?

Effectief crisismanagement

Een aantal tips

Voorbeeld Crisisagenda

1 – Opening
- Aanwezigen | Vergaderafspraken
- Agenda
- Telefoons op stil en laptops dicht

2 – Acties
- Vorig overleg | status

3 – Beeldvorming
- Belangrijke mededelingen per teamlid:
  a. Gebeurtenissen en genomen maatregelen
  b. Reacties via (social) media
  c. Andere actieve teams

4 – Oordeelsvorming
- Analyse van de situatie (acute situaties, extra teamleden nodig)
  a. Crisisdiagnose
  b. Doelstellingen en uitgangspunten

5 – Besluitvorming
- Vaststelling
- Acties

6 – Communicatie
- Intern en extern

7 – Sluiting
- Vaststelling tijdstip volgende vergadering

Notities

Cyber
Chain
Resilience
Consortium