Crisismanagement

Effectief besturen van een cybercrisis

Cyber Chain Resilience Consortium

CRISIS AGENDA

1 Opening
- Aanwezigen | Vergaderafspraken
- Agenda
- Telefoons op stil

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
- Vaststellen
- Acties

6 Communicatie
- Intern en extern

7 Sluiting
- Vaststelling tijdstip volgende vergadering

Volg de BOB methode!
- Verzamel het feitelijke beeld (beeldvorming)
- Oordeel over knelpunten, vraagstukken en mogelijke ontwikkelingen (oordeelsvorming)
- Neem besluiten en zet acties uit (besluitvorming)

DOELSTELLINGEN CYBER-CRISISTEAM

- Voorkomen en beperken van verlies, beschadiging van data en/of beschermen van persoonsgegevens
- Inzicht krijgen in oorzaak, (mogelijke) effecten en vervolgdreigingen
- Herstellen van functionaliteiten en het waarborgen en herstellen van de bedrijfscontinuïteit
- Behouden en terugwinnen van het vertrouwen van *stakeholders*

WAT MAAKT EEN CYBERCRISIS 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 voorkomen. 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

Eerste checklist voor crisismanager

- Stel een crisisteam samen en bepaal welke rol en verantwoordelijkheid iedereen heeft. Gebruik daarvoor de crisisteamlijst
- Bepaal de positionering van het crisisteam in de organisatie en welk (besluit)mandaat hierbij hoort
- Zorg dat je goed bent geïnformeerd over de situatie. Gebruik de vragenlijst in dit document
- Bepaal welke externe expertise nodig is en betrek deze in een vroeg stadium (externe specialisten/ experts zoals Forensisch bureau, Nationaal Cyber Security Center (NCSC), Autoriteit Persoonsgegevens)

Altijd doen bij afhandeling van crisis

- Kom op vaste momenten als team bij elkaar
- Gebruik een vaste crisisagenda (zie kader)
- Hanteer een overlegstructuur zoals de BOB methodiek
- 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'
- Onderhoud deze 'wat-als scenario's' gedurende de ontwikkelingen van de crisis

Mede mogelijk gemaakt door COT - Instituut voor Veiligheids- en Crisismanagement

Crisismanagement

Inhoudelijke aspecten bij crisisafhandeling

Cyber Chain Resilience Consortium

START CRISISAFHANDELING

Bekendheid

Wat is er al bekend over de crisis?

- 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?

Betrokkenheid

Wie zijn betrokken en wie ervaren impact? Zijn ze ingelicht?

- Cyberexpertise?
- Slachtoffers en verwanten (bij dataverlies)?
- Medewerkers, inhuur, onderaannemers?
- Klanten, opdrachtgevers, partnerbedrijven?
- Toezichthouder, inspecties?
- Verzekeraar?
- Maatschappij in zijn geheel?

TIJDENS CRISISAFHANDELING

Belangrijke momenten

Belangrijke moment die van invloed zijn op aanpak van de crisis

- Media start berichtgeving over de crisis
- Kritieke systemen van de organisatie moeten (uit voorzorg) offline
- Wel of geen datalek met gegevens van klanten/medewerkers
- Wel of geen datamanipulatie
- Wel of geen moedwil/chantage of anders
- Duidelijkheid over wel of geen laakbaarheid/falen van organisatie

Relevante besluiten

Kritieke besluiten

- Uitzetten en/of beperken van kritieke systemen en toepassingen met impact op dienstverlening
- Wel of niet ingaan op eisen in het geval van een cyberaanval
- Wel of geen back-up uitvoeren (ook in relatie met opsporing mogelijke dader)
- Opstarten herstelmaatregelen (inclusief eventuele risico's)
- Communiceren van de duiding van oorzaak en (mogelijke) impact op omgeving
- Bepalen verhaallijn over de gebeurtenis; volledige of beperkte openheid
- Vaststellen naar welke partijen gecommuniceerd moet worden (medewerkers, toezichthouder, klanten, leveranciers, media)
- Vaststellen dat de situatie 'veilig' en/of 'hersteld' is

Crisismanagement

Belangrijke gegevens bij crisisafhandeling

Cyber Chain Resilience Consortium

Samenstelling crisisteam

Naam	Rol in crisisteam	E-mail	Telnr
<Voor- en achternaam>			

Contactgegevens essentiële leveranciers

Bedrijf	Relatie	Contactpersoon	Functie	E-mail	Telnr
<Naam bedrijf>	*<Functie van bedrijf>*				

Communicatielijst

Belanghebbende	Aard betrokkenheid	Vorm van communicate
<Naam betrokkene, bedrijf, klant>	*<Waarom geïnformeerd worden?>*	*<Acties uitvoeren of informeren?>*

Beschikbare crisisplannen

Crisisplan	Te gebruiken wanneer?	Waar te vinden
<bv: DDoS crisisplan of Ransowmare crisisplan>	*<Kort beschrijven wanneer dit plan gebruikt moet worden>*	*<Locatie waar dit plan is opgeslagen (digital en eventueel fysiek)>*