



Hoe overleef je een hack als je bent gehackt ?

28-6-2022

Edwin Moraal
CISO





Voorkomen is beter
dan genezen!

Probleemstelling

- Cybercriminaliteit
- Nieuwe Modus Operandi
- Mens en Security



Awareness



Phishing



Phishing mail



Pakket Gemist

Geachte Heer/Mevrouw,

'S middags om 13:00 op 11-21-2021 kon de bezorging niet in ontvangst genomen worden. Er was niemand aanwezig volgens de pakketbezorger.

Uw bestelling ligt klaar bij een van onze afhaal punten.

Bij een post nl in de buurt dient u uw bestelling op te halen. Bekijk uw [track en trace informatie](#). Aangeraden is dat u uw Track and Trace code aanwezig hebt. Ook vragen we een geldig legitimatie te zien voor we het pakket kunnen overhandigen. Word de zending niet binnen 14 dagen opgehaald word het pakket geretourneerd.

Hoogachtend,

Team postnl

Wij vertrouwen erop u hiernee volkomen te zijn geïnformeerd en van dienst te zijn geweest.

Alvast hartelijk dank voor uw medewerking.

Met vriendelijke groet,
ABN AMRO Bank N.V.

Bas Bisschops
Hoofd Klantcommunicatie

Deze e-mail is verzonden door ABN AMRO Bank N.V., statutair gevestigd te (1082 PP) Amsterdam aan de Gustav Mahlerlaan 10, ingeschreven bij de Kamer van Koophandel van Amsterdam onder nummer 34334259 (hierna te noemen 'ABN AMRO'). ABN AMRO en haar groepsmaatschappijen zijn niet aansprakelijk voor de onjuiste en onvolledige overdracht van de informatie in dit bericht noch voor haar groepsmaatschappijen zijn niet aansprakelijk voor de onjuiste en onvolledige overdracht van de informatie in dit bericht behouden is gebleven noch dat dit bericht, ABN AMRO en haar groepsmaatschappijen staan er niet voor in dat de integriteit van dit bericht behouden is gebleven noch dat dit bericht vrij is van virussen, niet is onderschept of valbaar is geweest voor tussenkomst (door derden).



Rabobank

Geachte klant,

U ontvangt dit automatisch bericht om 14.05 en wordt automatisch in rekening gebracht.

Hoe vraag ik een nieuw bankpas aan?

Klik op de knop 'aanvragen'.

Dit bericht is verzonden op 11-21-2021 om 14.05.

Uw huidige bankkaart binnenkort wordt vervangen door een nieuwe bankkaart. Deze kost u 14,95 en wordt automatisch in rekening gebracht. Doet u mee met ons recycleprogramma? Dan ontvangt u de nieuwe bankpas geheel gratis. Na de aanvraag komt u op de laatste pagina waar ons Recycle programma is. Ontvangen wij uw bankkaart niet binnen 3 werkdagen? Dan ontvangt u de nieuwe bankpas na 5 werkdagen. Uw oude bankkaart is in die tussentijd niet meer geldig.

[aanvragen](#)

CEO fraude

Van: S.I. Bijlhout [s.i.bijlhout@blgbussiness.com]

Verzonden: maandag 14 oktober 2019 12:08

Aan: R. Ylmaz [r.ylmaz@bigbussiness.com]

Onderwerp: Saldo

Urgentie: Hoog

Roy,

Kun je me per omgaande vertellen of onze kredietrekening voldoende saldo bevat om vandaag nog een betaling van 35.000 euro te doen?

Graag een snelle reactie.

Met vriendelijke groet,

Sheryda I. Bijlhout

CEO Bigbussiness

Security Solutions

- Next Generation Firewall
- End Point protection
- Security updates

9/11



9/12



Gehacked, wat nu?



Triage

- Het ontdekken en notificeren dat er een hacker actief is op uw netwerk
- Vaststellen van de signalen
- Eerste stappen zijn cruciaal

Containment

- Het beperken van de schade nadat u geconcludeerd hebt dat uw organisatie gehackt is.
- Maar wat betekent dat inhoudelijk?

Containment

- Backup “isoleren” en veiligstellen
- Connectiviteit uitzetten
- De aanvaller buiten houden



Analyse

- Het beoordelen van de schade die is toegebracht door een derde
- Status van de backup
- Beoordelen wat “als gecompromitteerd” moet worden beschouwd



Recovery

- Het herstellen van de 'crisisituatie' naar de 'normale' situatie
- Communicatie aspect
- Structuur is van groot belang



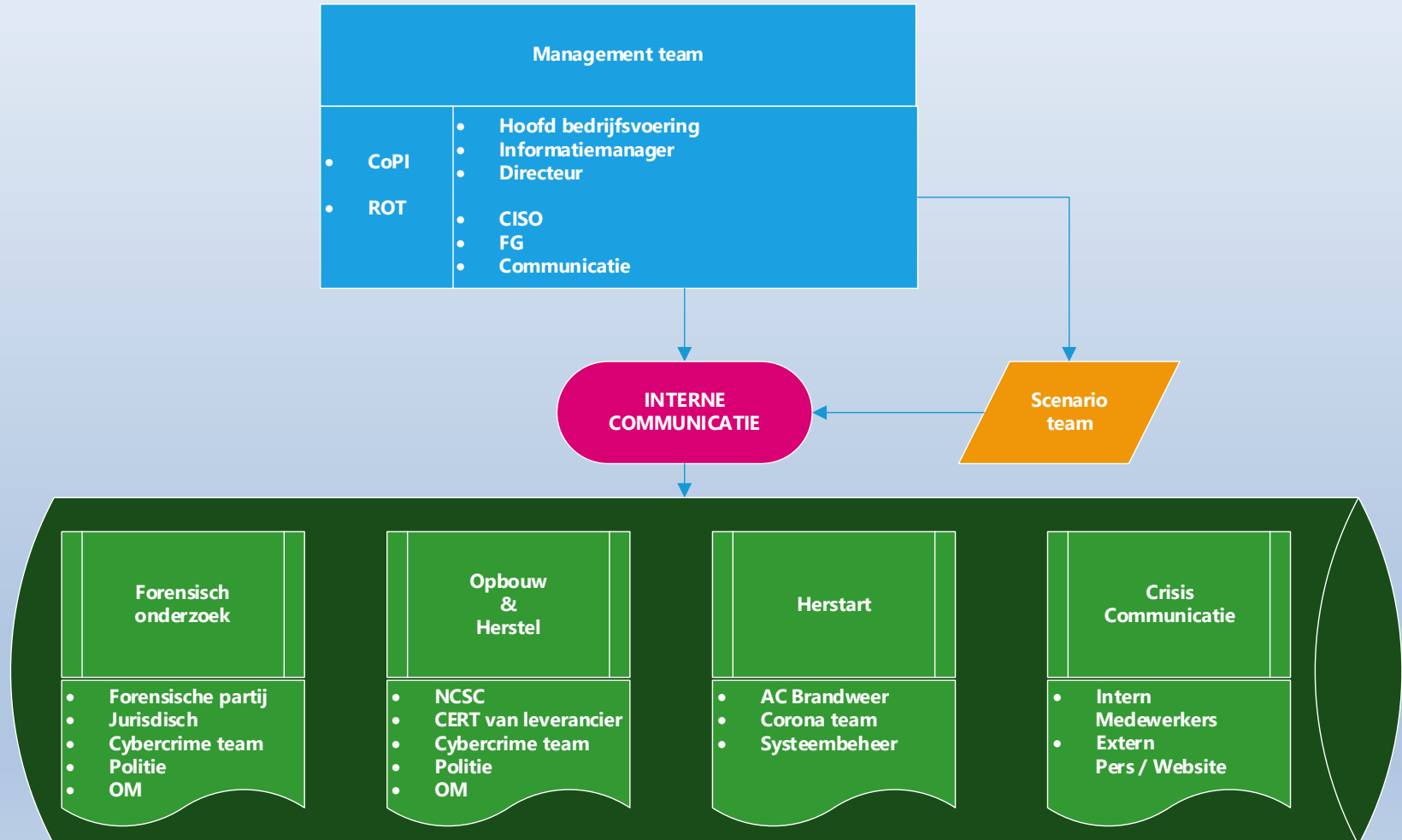
Communicatie & Crisis structuur

- Opschaling naar GRIP structuur
- CoPI - ROT
- Netcentrisch Werken

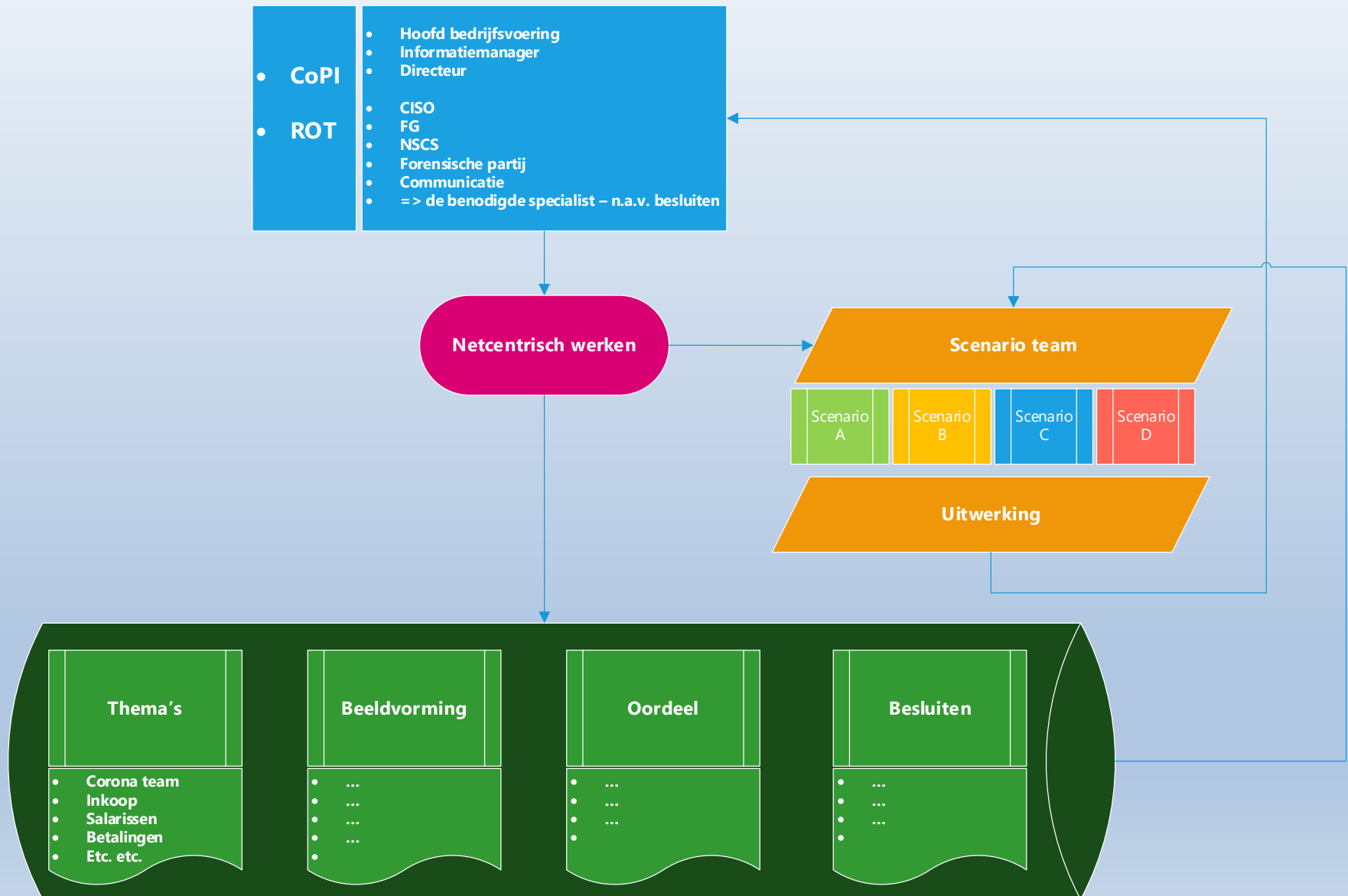
Het is geen wedstrijd,
...het is een marathon!!



Communicatie



Crisis structuur



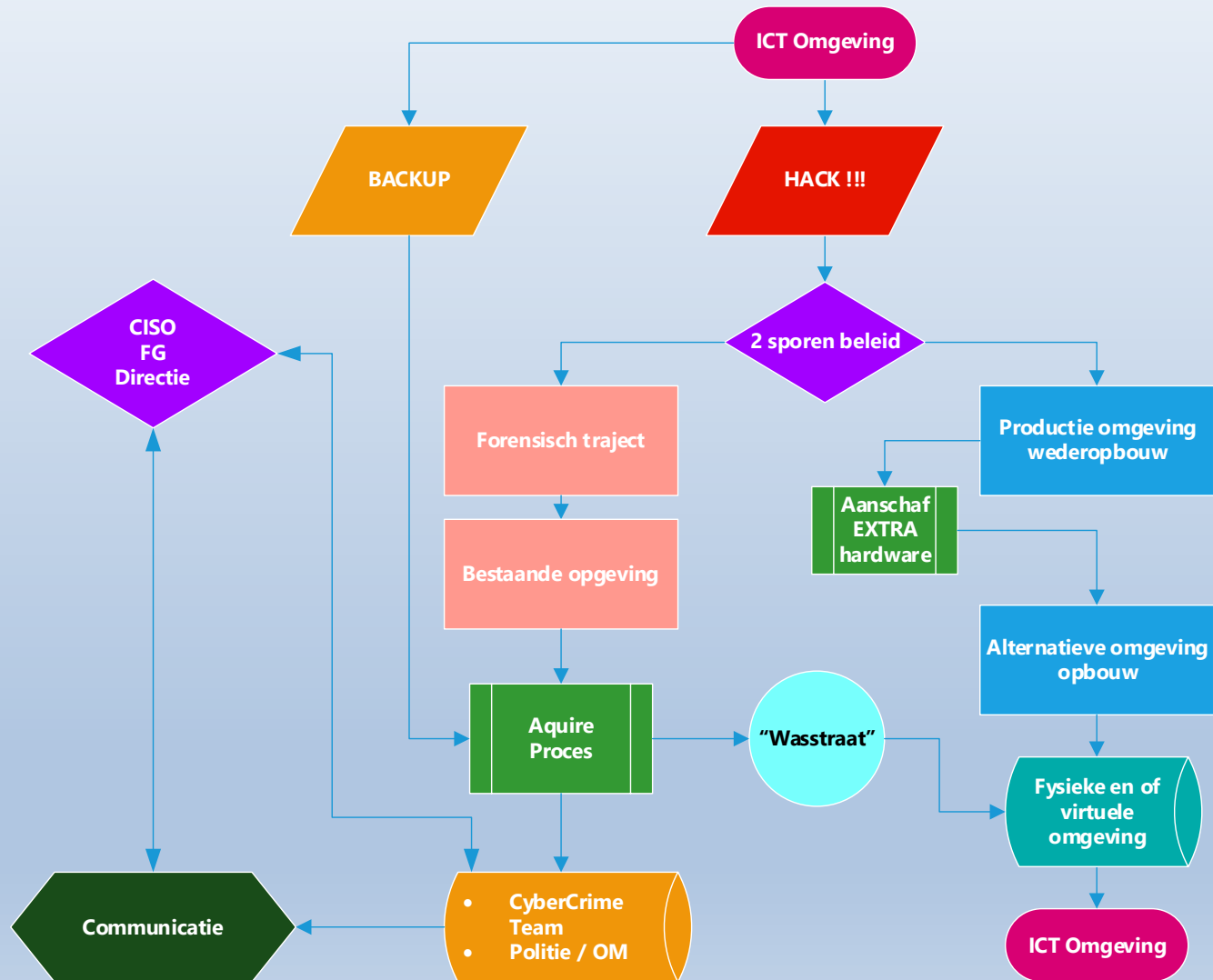
2 Sporen beleid



2 Sporen beleid

- Het herstellen van de “crisissituatie” naar de “normale” situatie
- Forensisch traject & Juridisch aspect
- Communicatie

2 Sporen beleid



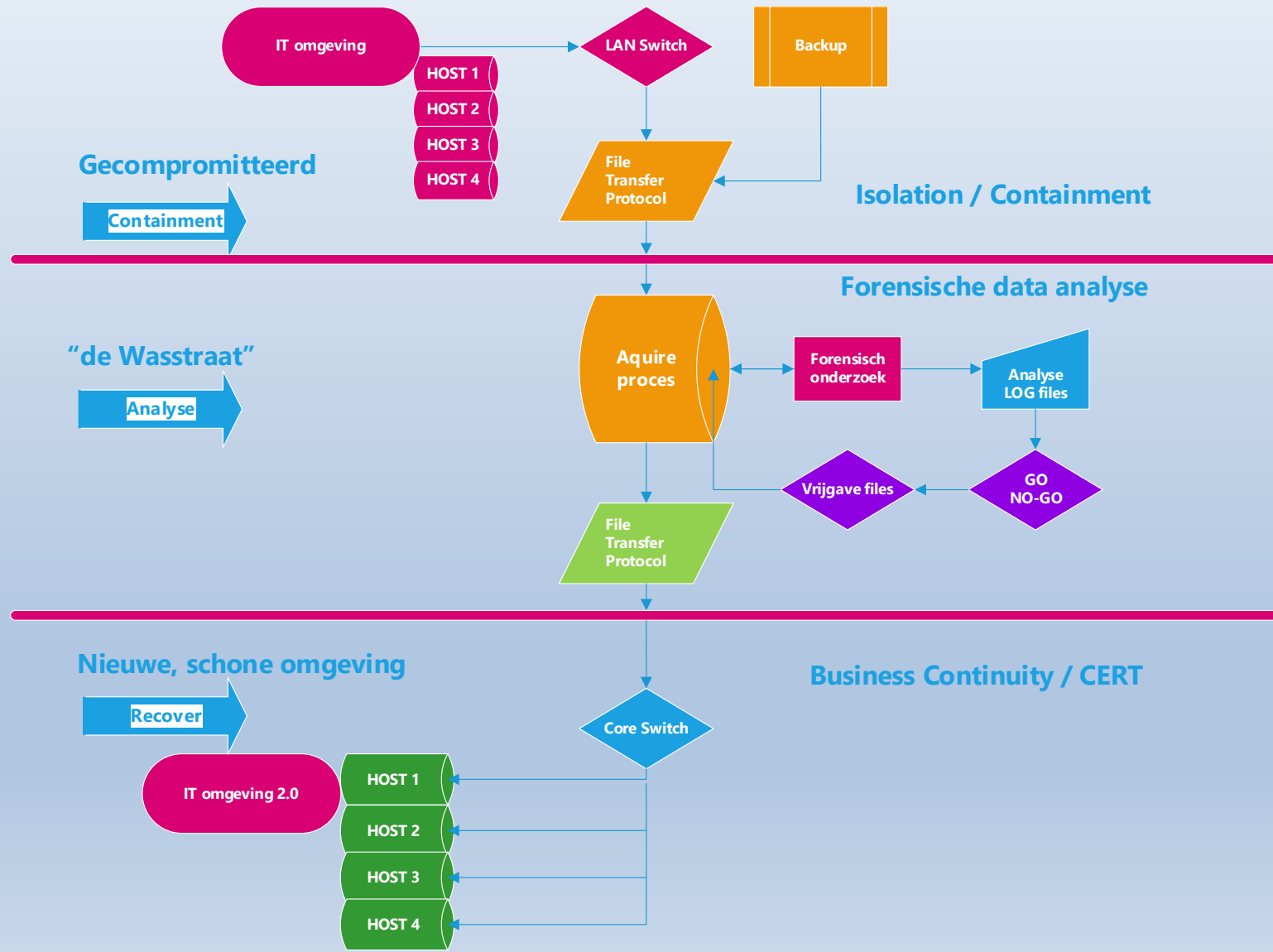
De "Wasstraat"



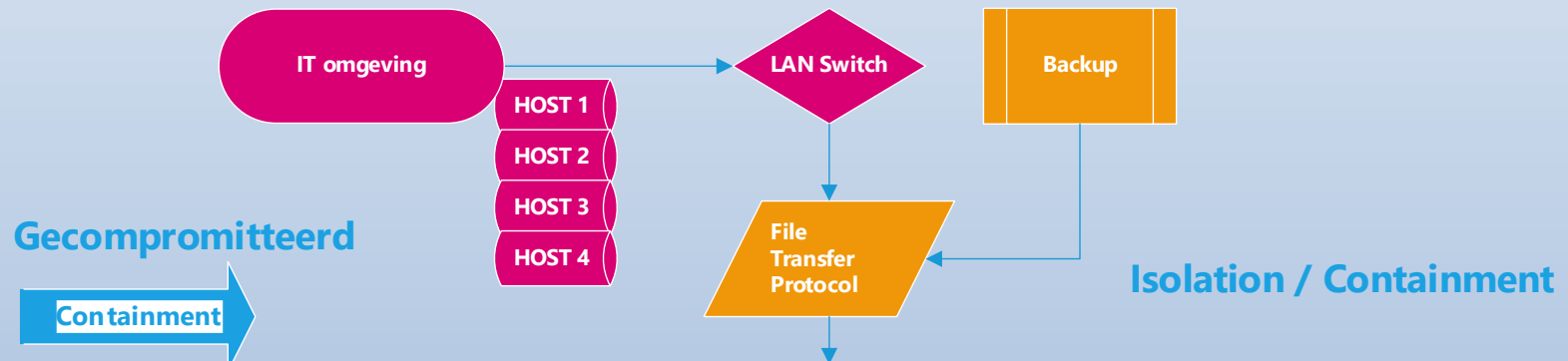
De “Wasstraat”

- Structuur om van “niet vertrouwd” naar “vertrouwd” te gaan
- Aquire proces
- Opbouw Business Continuity i.c.m. CERT

De "Wasstraat"



De "Wasstraat"

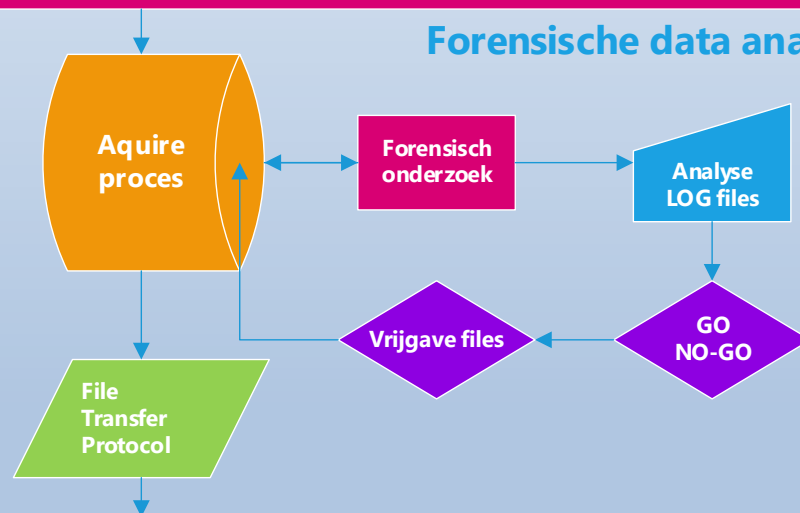


De "Wasstraat"

"de Wasstraat"

Analyse

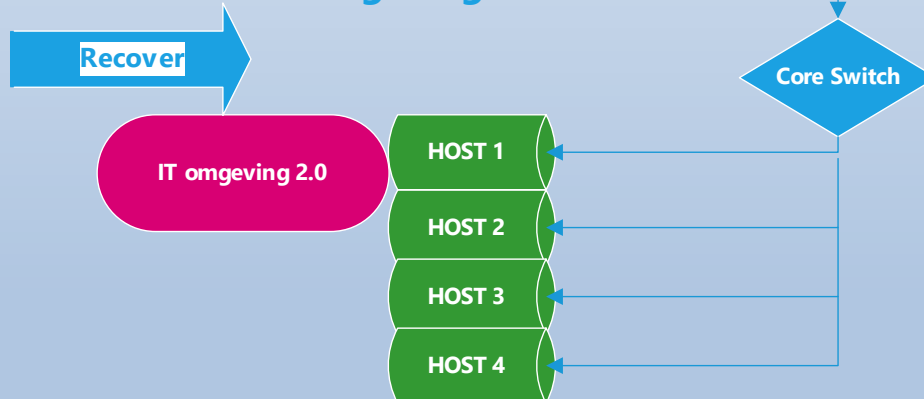
Forensische data analyse



De "Wasstraat"

Nieuwe, schone omgeving

Business Continuity / CERT



Business Continuity

- ISAC
- CERT
- RTO, RPO & MTD



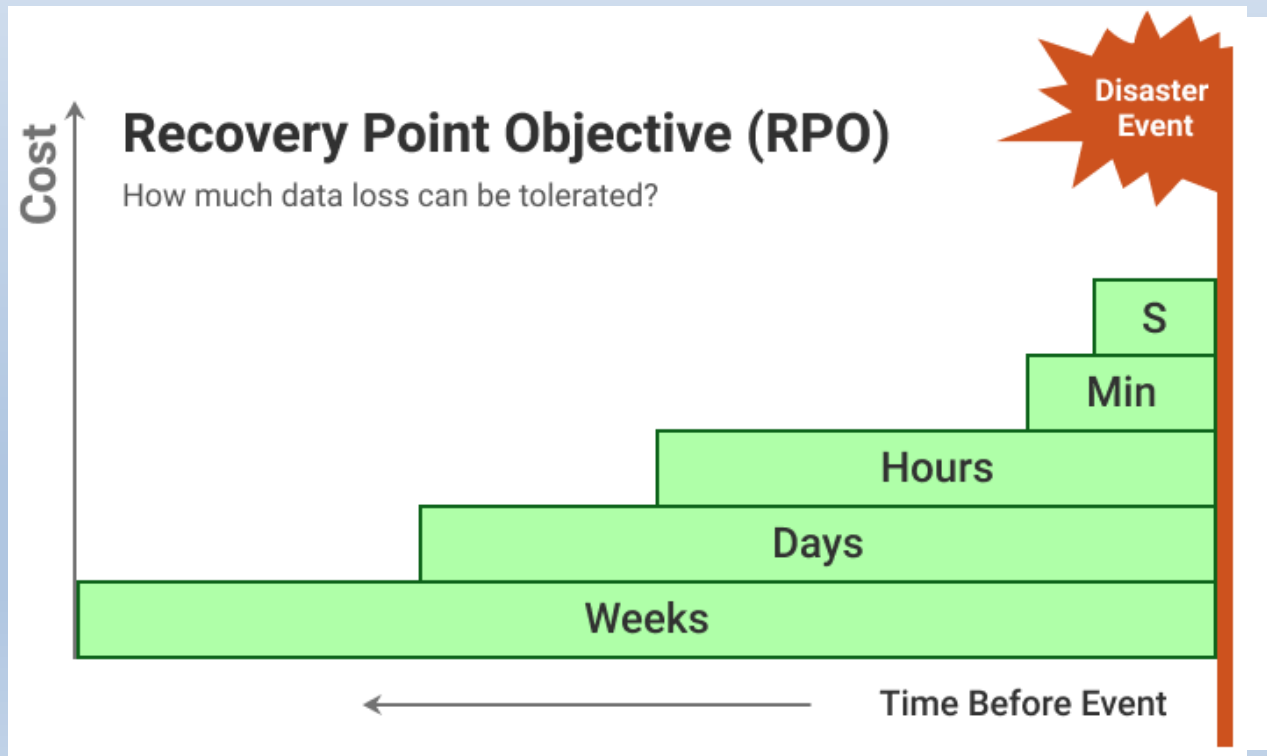
Business Continuity & Disaster Recovery

- Backup **3-2-1(0)** regel !!!
- Zorg voor minimaal **3** kopieën
- Waarvan er minimaal **2** op verschillende media
- Waarvan er **1** op een externe locatie (offline)
- '**0**-fouten' tijdens de herstelbaarheidsverificatie

Business Continuity & Disaster Recovery: RTO



Business Continuity & Disaster Recovery: RPO



Samenvattend

- Huidige ontwikkelingen
- Belang van bewustwording
- Be Prepared!



Lessons Learned:

- Ga niet op zoek naar de schuldige in je organisatie, maar **focus** je **op herstel**.
- Het is **geen wedstrijd**, maar **een marathon**!
- Kennis is **goed**.
- Kennissen zijn **beter**!

Lessons Learned:

- Ga niet op zoek naar de schuldige in je organisatie, maar **focus** je **op herstel**.
- Het is **geen wedstrijd**, maar **een marathon**!
- Kennis is **goed**.
- Kennissen zijn **beter**!

Vragen?



Bedankt! Stay safe!



Edwin Moraal

CISO, Adviseur ICT

e.moraal@vnog.nl

<https://linkedin.com/in/edwinmoraal>

