# Een cyberaanval? Laat je niet verrassen!

Door Lucinda Sterk


Lucinda Sterk

Zelfstandig communicatie adviseur

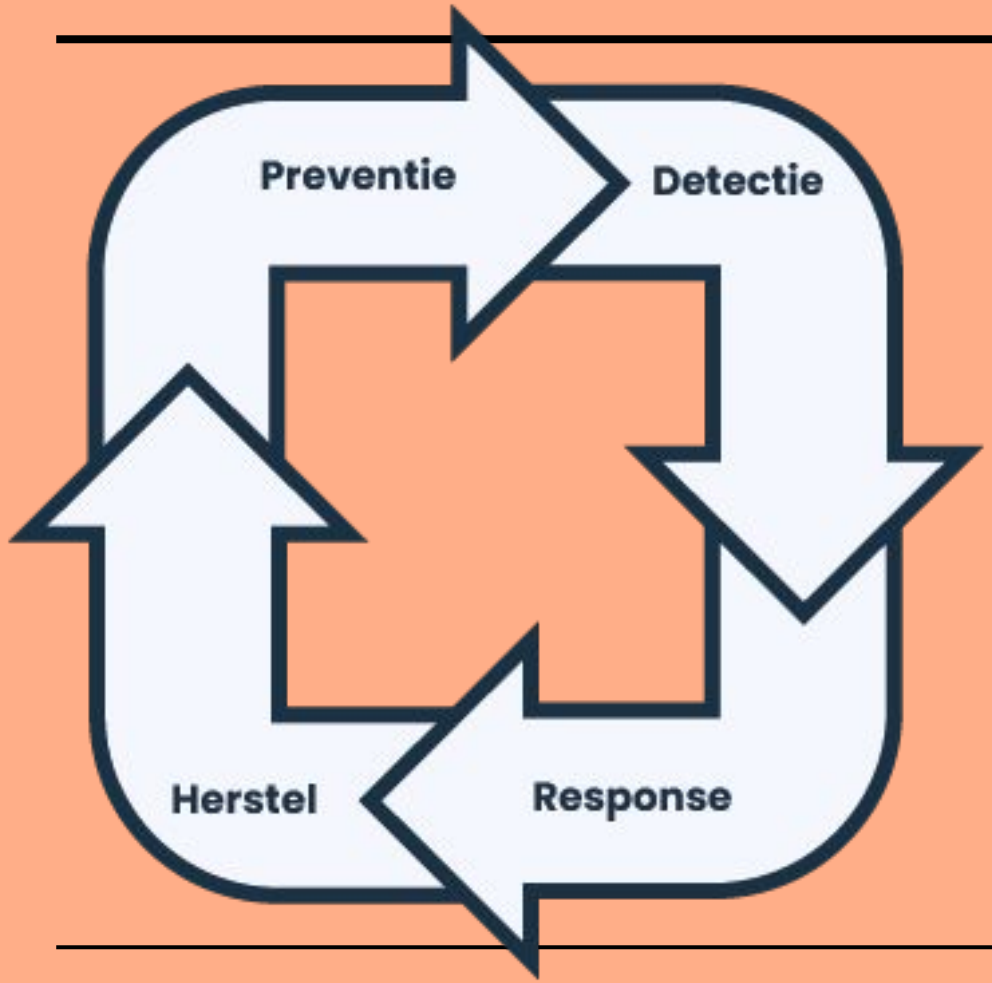
NCSC
Fox-IT
Z-CERT
KPN Security / DIVD

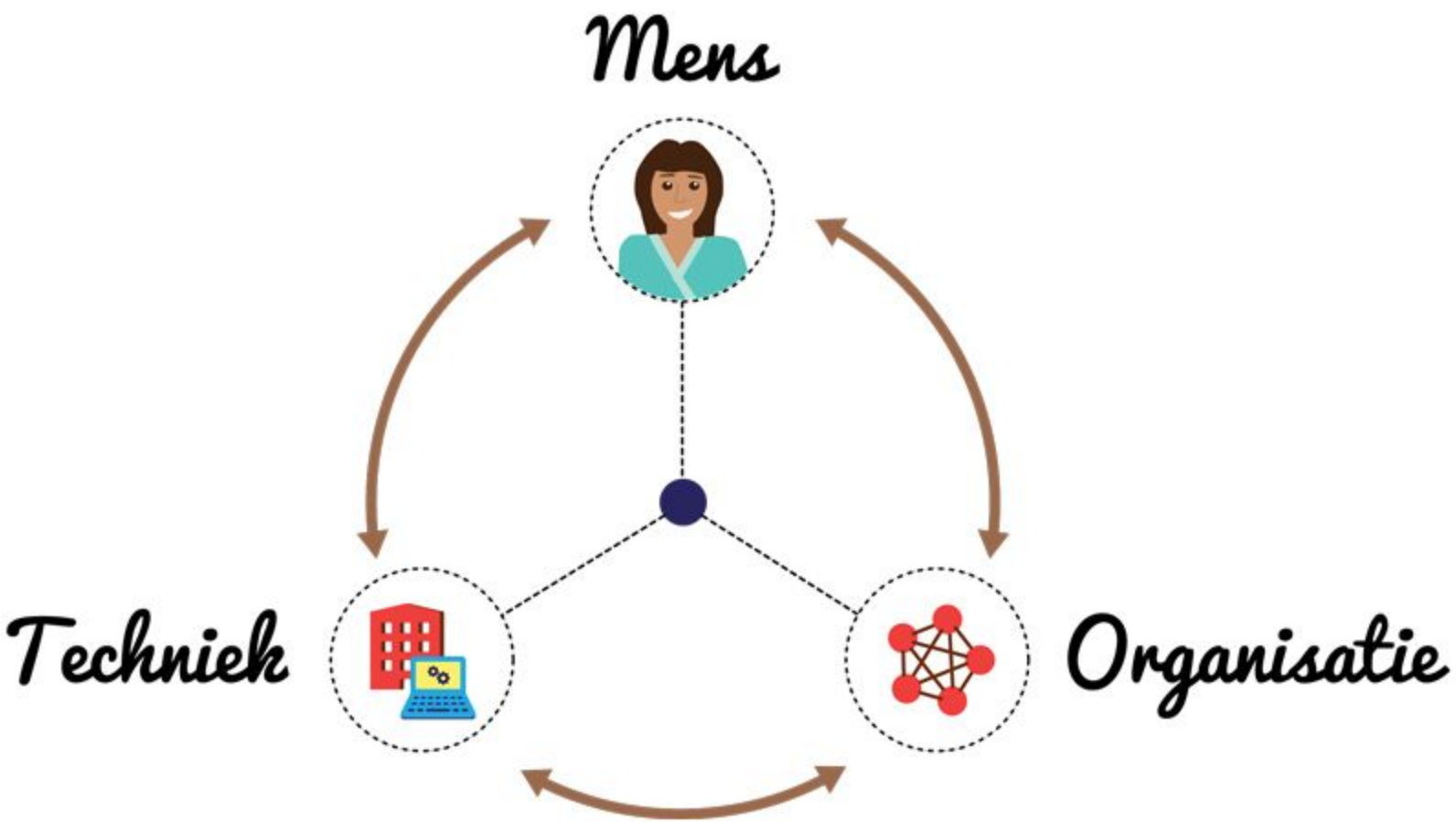

Een goede
voorbereiding
is het halve
werk

Stress!

Maar geen zorgen, we zijn nog niet zo ver

We gaan ons voorbereiden  op een incident


Preventie
Detectie
Response
Herstel


Mens
Techniek
Organisatie

# Preventie

Voorkomen van een aanval / inbraak begint bij het kijken en inventariseren van wat je hebt..

# Het huis..

Hoe beveilig je een huis?

- Inventariseren
- Dure spullen?
- Slecht sluitende deuren?
- Kiepraampje?
- Achterdeur?

# Het netwerk

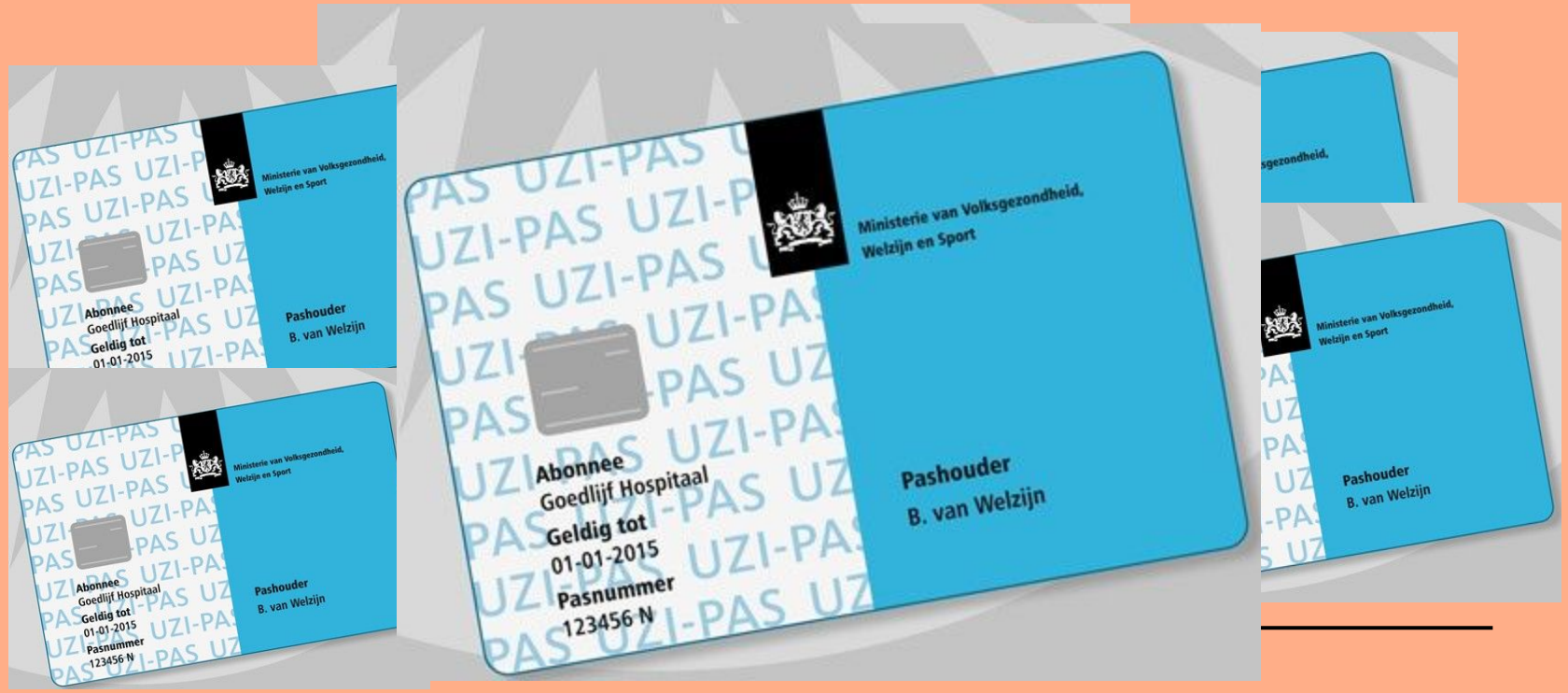
Hoe beveilig je een netwerk?

- Inventariseren
- Dure spullen?
- Slecht sluitende deuren?
- Kiepraampje?
- Achterdeur?

# Risico-inventarisatie

Waar zitten je

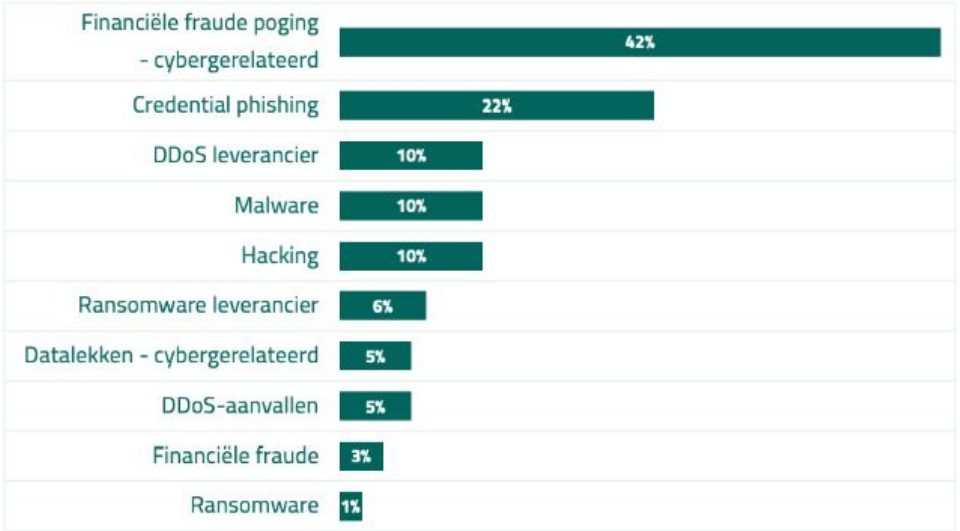
# Wie heeft er toegang tot de kroonjuwelen?

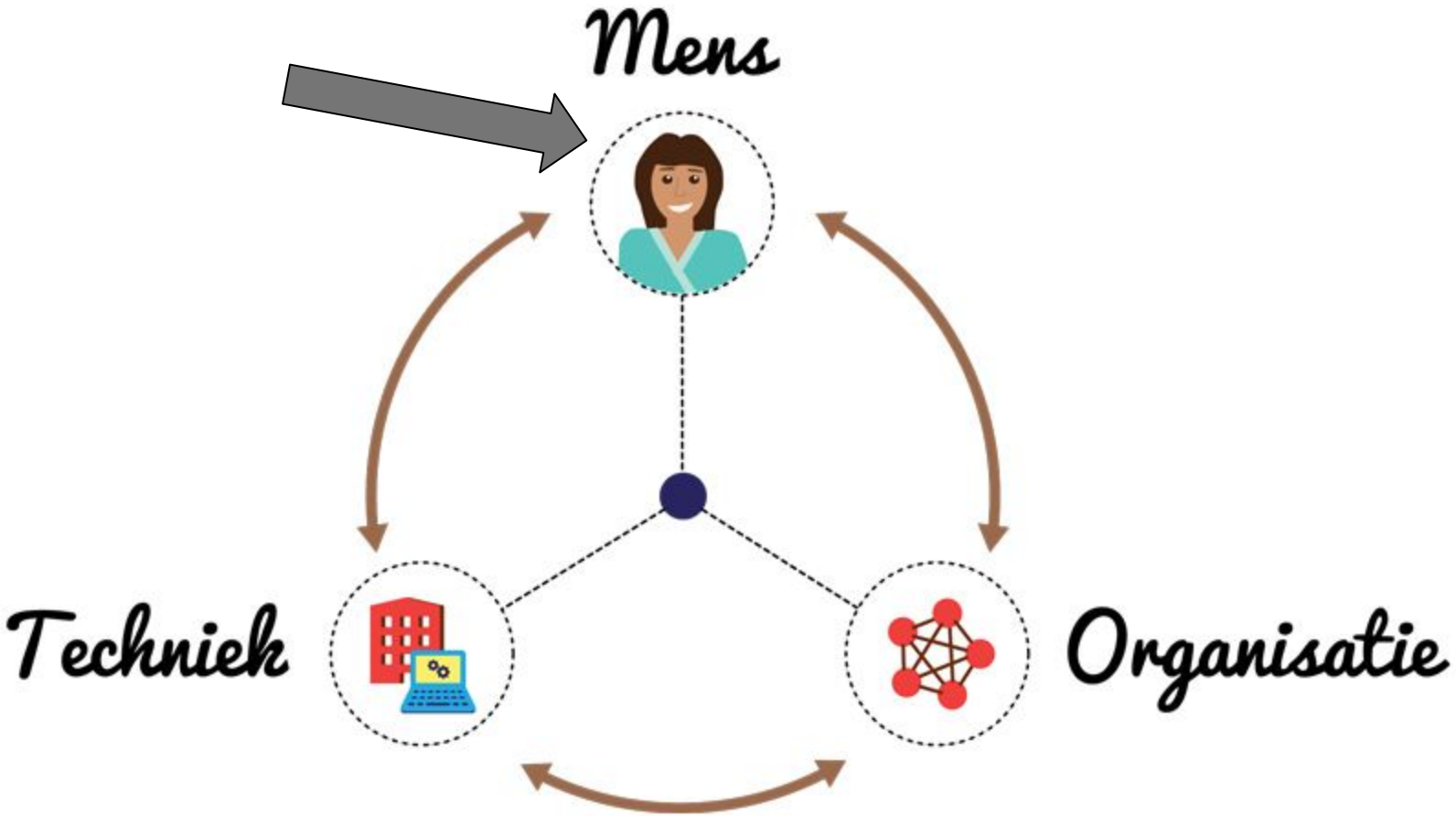


# Onderzoek naar risico's

*Figuur 1*

**Meest voorkomende soorten security-incidenten bij ondervraagde Nederlandse zorginstellingen**




Mens
Techniek
Organisatie

# Mens

Zwakke of sterke schakel?

- Awareness
- Herkennen van phishing
- Cyber hygiene

(wachtwoorden niet op een briefje, netjes afsluiten van de computers, geen pasjes uitlenen)

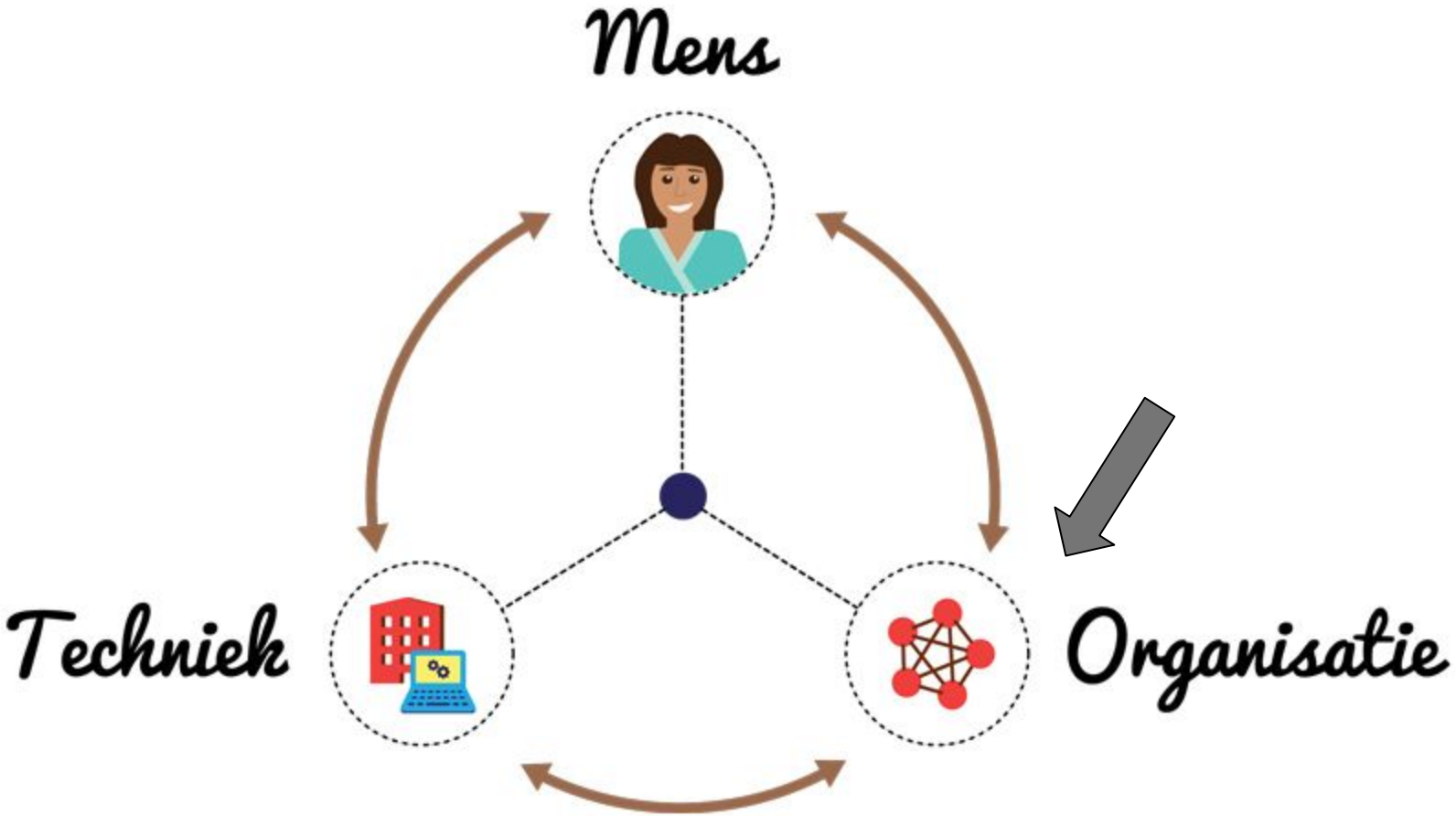
# Awareness

Bewust zijn van eigen gedrag

Controle mechanisme inbouwen bij financiele transacties

Wachtwoordbeleid afdwingen


THIS
IS A
SAFE
SPACE


Mens
Techniek
Organisatie

# Organisatie

Met wie doe je zaken?  Ken je partners.

Hoe is hun security geregeld?

Ketenkwetsbaarheden (supply chain attack)

Heb je een SLA met je leverancier?

Wie heeft er toegang tot je netwerk?

Hoeveel domeinnamen zijn er geregistreerd?

Crisisteam samenstellen

Wie zitten er in het cmt (CISO, FG, Voorzitter, Coms adviseur, jurist?)

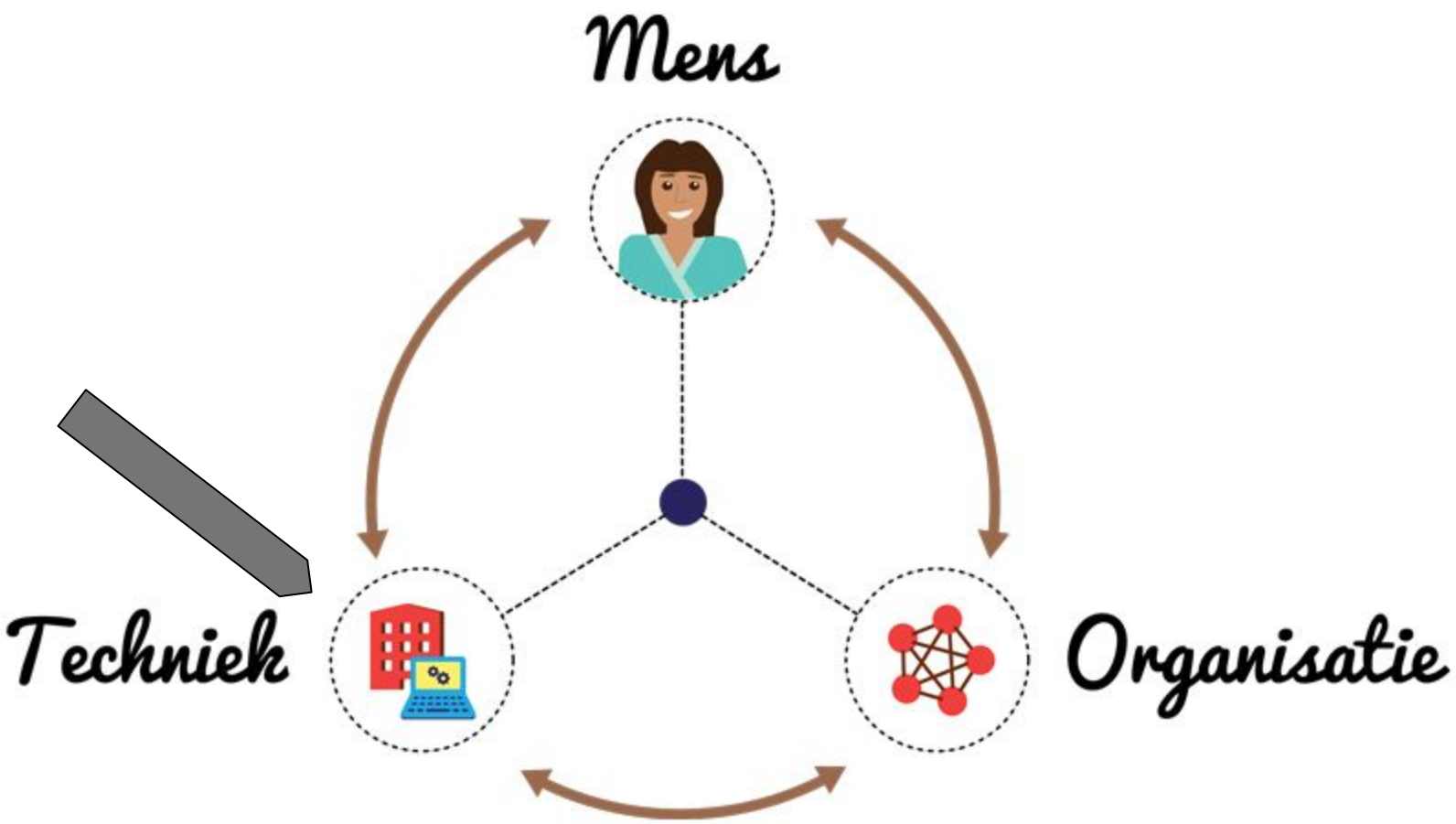
Regelmatig oefenen

Kent iedereen zijn/haar taak?

Is er sprake van piket?

Mandaten vastgelegd?

Is er een crisiscommunicatieplan?


Mens
Techniek
Organisatie

# Techniek

Weet wat je aan techniek hebt draaien

Patchen, updaten

Hangen er producten aan het internet en zo ja waarom?

Wie heeft er toegang tot je netwerk?

# Is dat voldoende?

# Wat zou je nog meer kunnen doen?

Meetings met gelijke organisaties in de sector

Trainen en oefenen

Pentesten / red teaming

Table top

Rapporten en documenten lezen van oa Z-CERT


NO TIME TO LOSE

Maak morgen nog een begin met een crisisplan, als je dat nog niet had.

Want het is geen kwestie van of, maar een kwestie van wanneer.