Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Nationaal Detectie Netwerk (NDN)

Onderwerpen:

- Waarom Nationaal Detectie Netwerk?
- Hoe werkt het?
- Wat doet het wel en niet?

Aanleiding

- MinVenJ coördinerend bewindspersoon voor cyber security
- Departementen zelf verantwoordelijk voor informatiebeveiliging
- Vanuit coördinerende rol is aangeven dat de detectiecapaciteit versterkt zal worden
- Aanvulling en aansluitend op reeds gebruikte middelen

Proces

- Toelichting huidige stand van zaken politiek-bestuurlijk process

- Min WenR tekent voor opdrachtgever
- SIB
- ICCIO (met advies RPPF)
- SGO t.a.v. positie OR

Waarom Detectie?

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

- Detectie is altijd een belangrijk onderdeel van je beveiliging, naast firewalls, virusscanners etc. wil je immers weten of er iets aan de hand is. Één geslaagde cyberaanval kan jouw werk en van al jouw collega's compleet ontwrichten.

- Toegang tot kwalitatieve dreigingsinformatie is moeilijk te realiseren. Het probleem is simpelweg te groot om individueel op te lossen
  - Te kostbaar, te complex, groot tijdsbeslag
  - Te weinig publiek beschikbare kennis, te weinig techniek en resources
  - Onvoldoende brede blik, dus geen sectorbeeld of trendanalyse

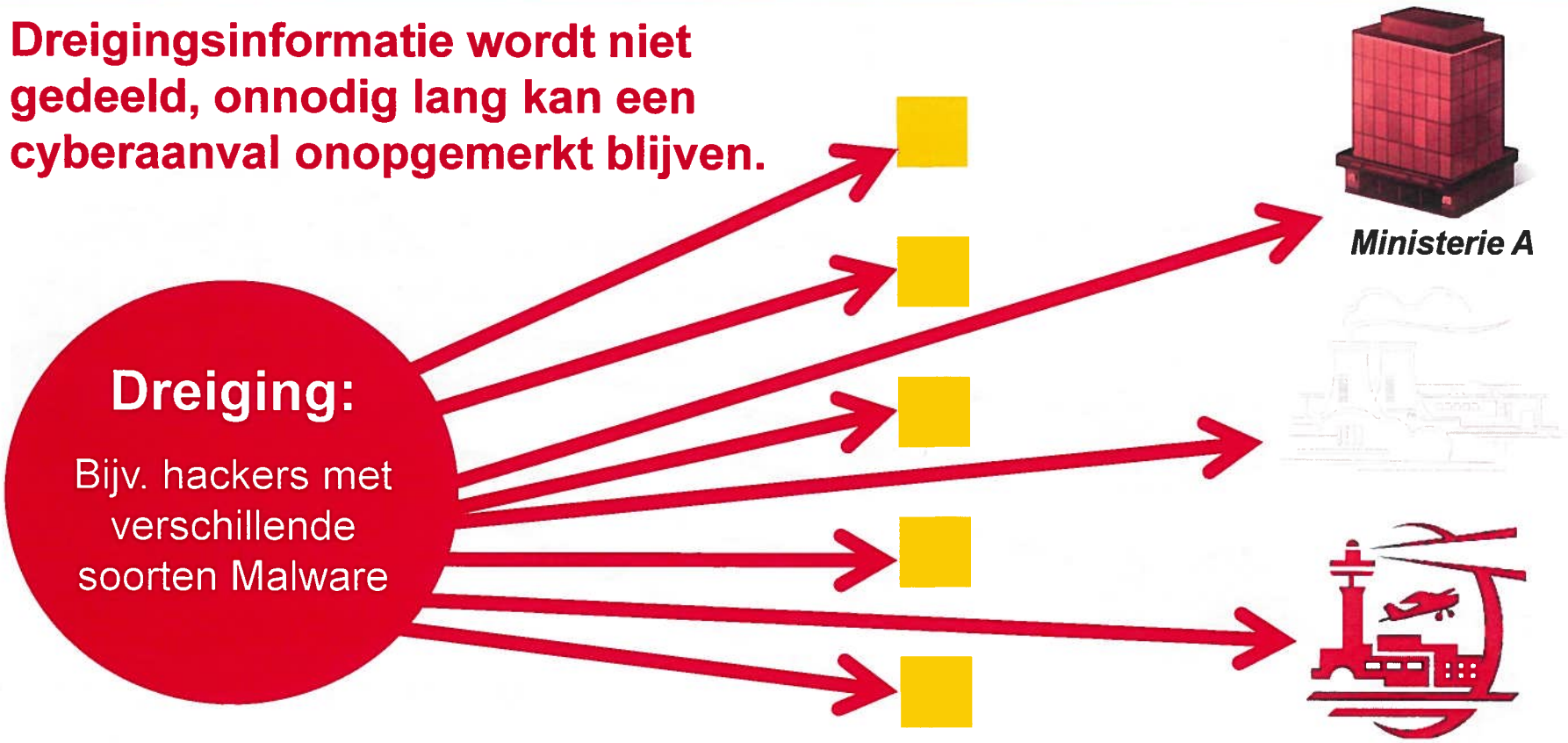
- Door de beschikbare informatie te delen ontstaat een gezamenlijk gedragen beeld van de dreigingen op dit moment. Samenwerken is de sleutel!

- "Signalering bij de een, werkt als preventie bij de ander"

Huidige situatie

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

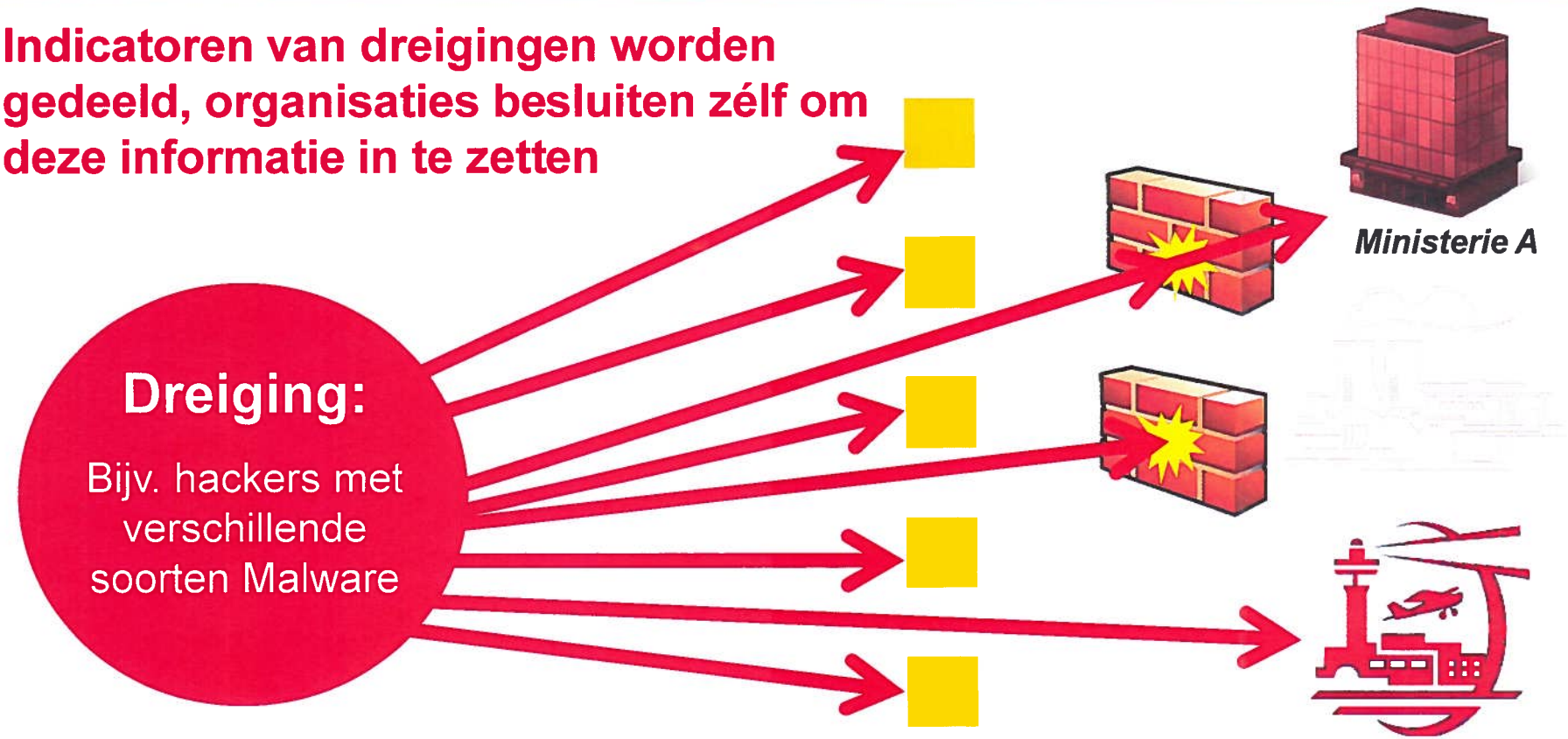
Dreigingsinformatie wordt niet gedeeld, onnodig lang kan een cyberaanval onopgemerkt blijven.



Pilot voor NDN

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Indicatoren van dreigingen worden gedeeld, organisaties besluiten zélf om deze informatie in te zetten



Dreiging:

Bijv. hackers met verschillende soorten Malware

Barrière:

Bv. virusscanner

Doelwitten:

Rijksoverheid en vitale sectoren

Hoe werkt het delen?

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Aanvallen met malware X

Ministerie A

NDN Melding:

Malware X gedetecteerd

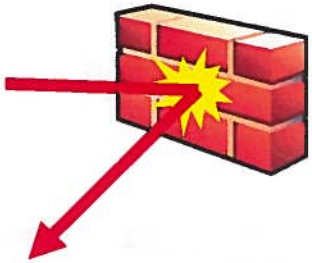
Nationaal Detectie Netwerk

AIVD & NCSC

Levert actuele database met (on)bekende cyber aanvallen

NDN Alerting:

Bescherm jezelf tegen malware X



Ministerie B

Wat doet het?

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Doet WEL

Waarschuwen voor cyber aanvallen

Alléén gedrag van cyber aanval opslaan

Digitaal verkeer scannen op malware

Delen hoe mogelijke aanvallen eruit zien

Beschermen tegen spionage

Meer kennis dan virusscanners toepassen

Bestaande informatie gebruiken

Veiliger maken

Doet NIET

Dader van aanval opsporen

Gedrag en verkeer van personeel opslaan

Digitaal verkeer scannen op inhoud

Delen wie er hoe is aangevallen

Zelf personeel bespioneren

Meer data dan virusscanners gebruiken

Op zoek naar nieuwe informatie

Privacy aspect negeren

Waarborgen

- Voor AIVD toezicht via CTIVD
- Voor NCSC wordt gekeken naar rol voor Auditdienst Rijk
- Nadere betrokkenheid RPPF?