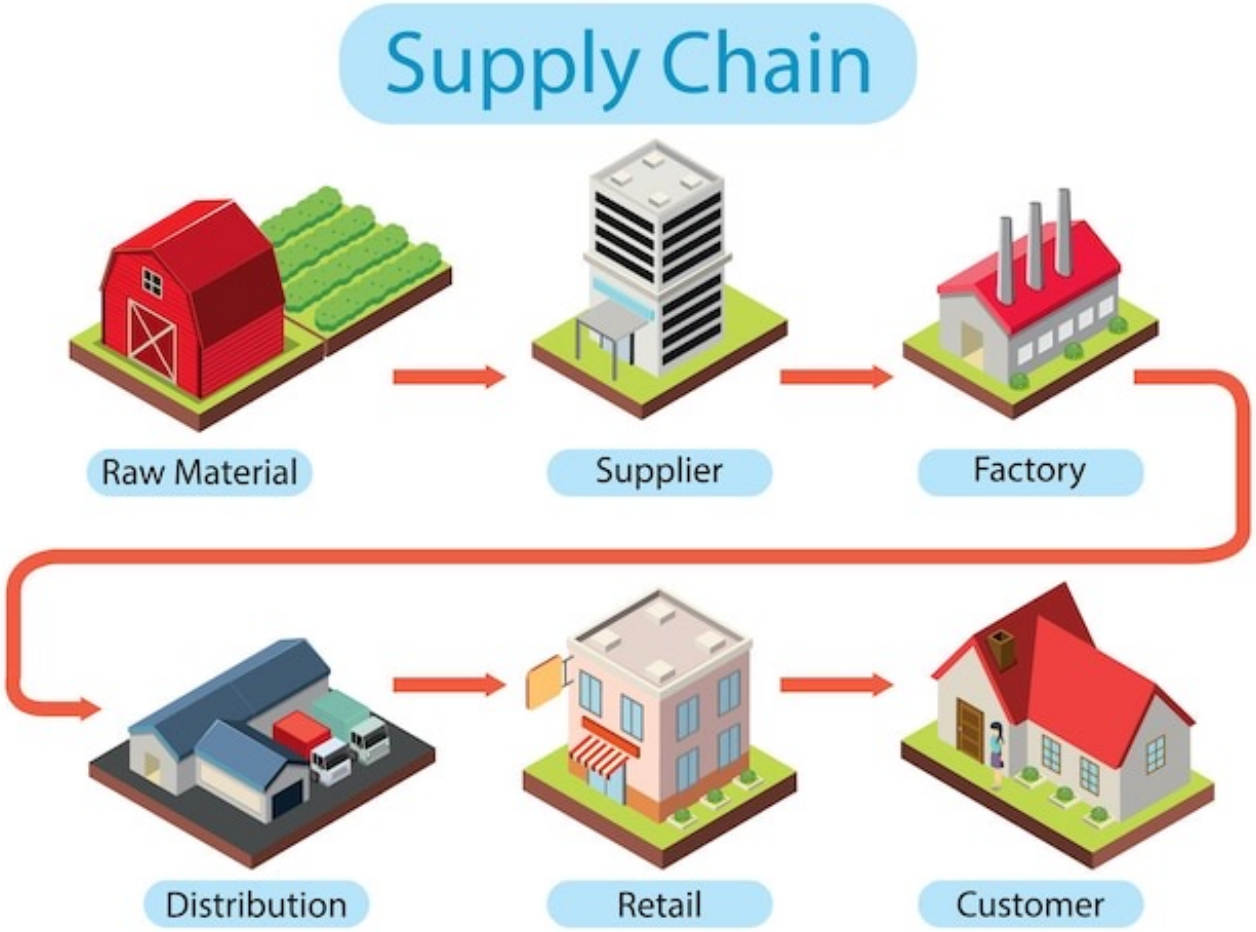
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Cybercheck: ook jij hebt supply chain risico's!

Larissa Kalle & Bart Snijdelaar

Platform voor Informatie Beveiliging (PvIB), 03-04-2024

NCSC



De cybercheck

Inhoudsopgave

1. Aanleiding Cybercheck
2. De cybercheck: wat is het idee?
3. Het inventariseren van mogelijke supply chain risico's met behulp van de cybercheck
4. De aanvullende risicoanalyse
5. Conclusie

rtl nieuws

0 ° | 204 km | 6

Vrees voor spionage

Chinese douanescanners Schiphol en Rotterdamse haven onder vuur: 'Dit is onbegrijpelijk'

Door Chris Koenis
22 januari 2022 08:00 • Aangepast 22 januari 2022 13:52

NOS Nieuws • Dinsdag 8 februari 2022, 12:00 •
Aangepast dinsdag 8 februari 2022, 14:34

Omstreden Chinese camera's hangen overal in Nederland, ook bij ministeries

rtl nieuws

Vanwege spionage

Kabinet: TikTok liever niet op werktelefoon ambtenaren

21 maart 2023 12:30 • Aangepast 21 maart 2023 15:08

Aanleiding

Waar zorgt deze aandacht voor?

- **Kamervragen:** waarop tijdig een antwoord moet komen
- **Vragen uit de praktijk:** CI(S)O's, inkoop of beleid.

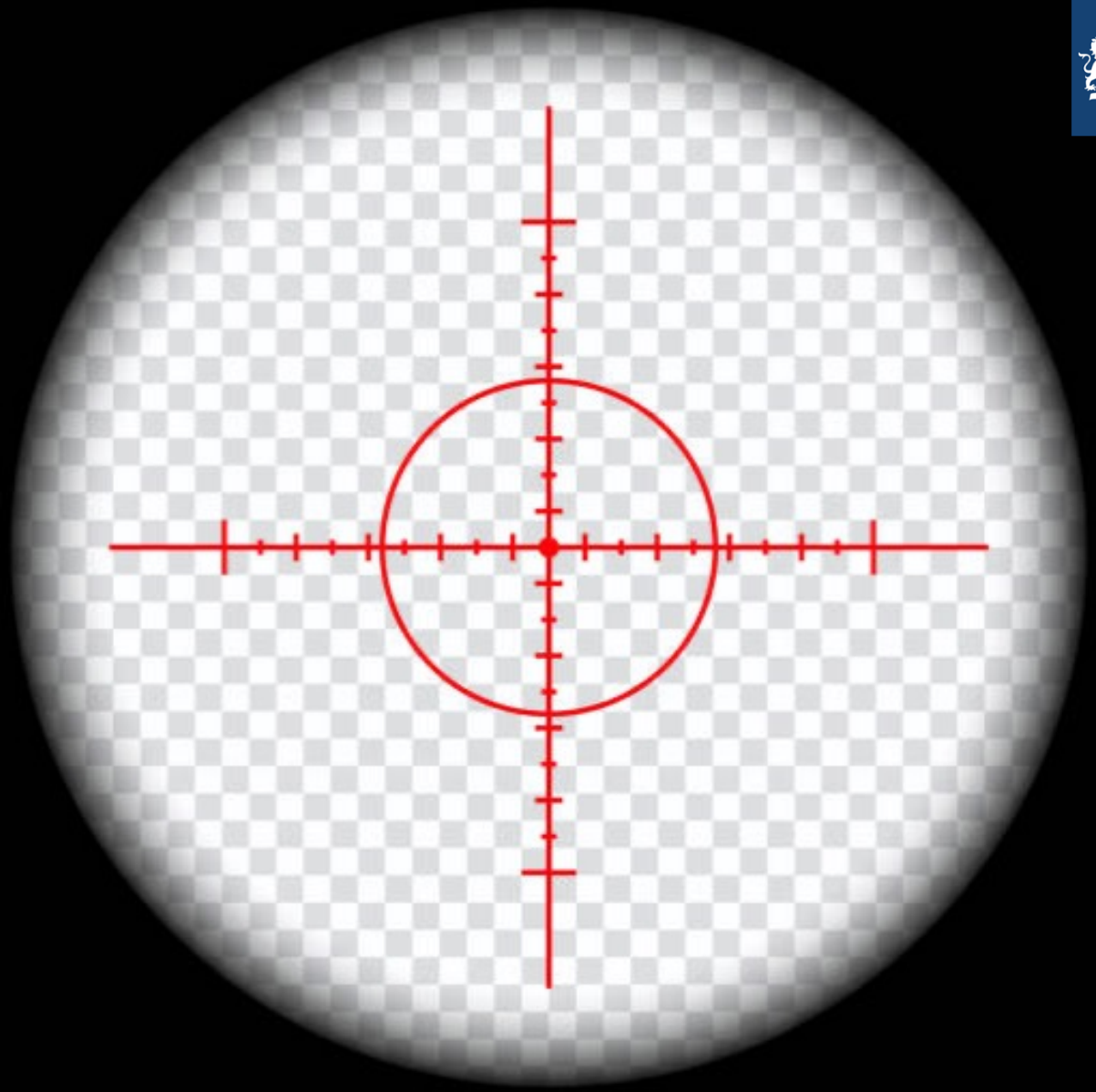
Hoe pakken we dit op:

- **Expertiseteam Veilige Digitale Overheid (EVDO)** krijgt opdracht om een risicoanalyse te doen.
- **Opvolging advies:** in maatregelen, inkoop of aanpassing beleid.
- **Beantwoorden kamervragen:** op basis van de risicoanalyse.

Aanleiding

Rode draden in de risicoanalyses

- **Een product of dienst afkomstig uit een land met een offensief cyberprogramma** dat wordt gebruikt door een (semi-)overheidsorganisatie
- **Maatschappelijke en politieke druk om te weren:** maar is dit wel de beste oplossing?
- **EVDO gebruikt steeds dezelfde methode:** kunnen we dit niet omzetten in een kennisproduct?



De cybercheck: wat is het idee?

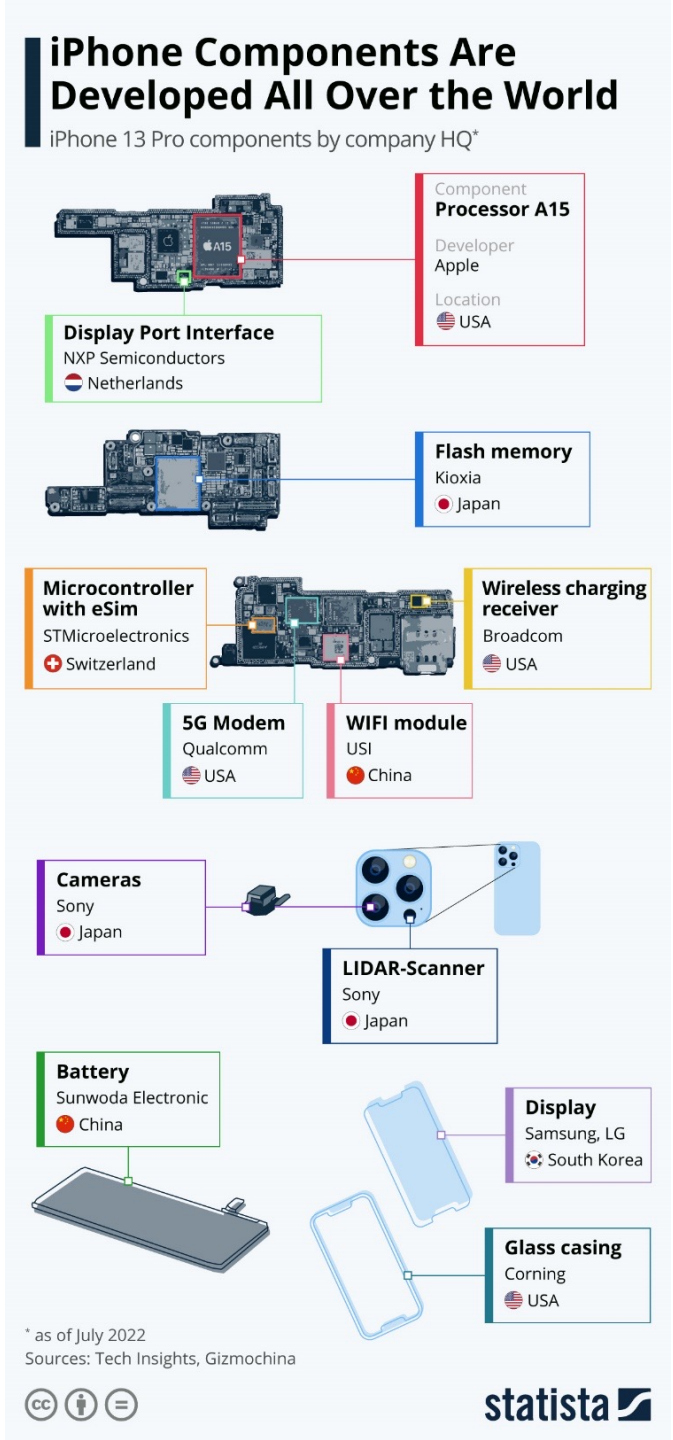
Scope en doel

- **Richt zich op producten en diensten die raken aan TBB-NV**
- **Implementeer eerst een algemeen risicomanagement proces** voordat je aan de cybercheck begint
- **Organisaties blijven zelf verantwoordelijk** voor het uitvoeren van risicoanalyse en besluiten zelf hoe ze met deze risico’s omgaan
- **Doel:** een hulpmiddel om mogelijke supply chain risico’s te inventariseren en hoe je vervolgens een aanvullende risicoanalyse kan aanpakken

De cybercheck: wat is het idee?

Wat doet de cybercheck niet?

- De cybercheck is **geen Zwitsers zakmes**
- Focus ligt op ‘cyber security’
- Vraagstukken zoals ethiek en strategische afhankelijkheden worden niet meegenomen in de cybercheck



Het inventariseren van mogelijke supply chain risico's

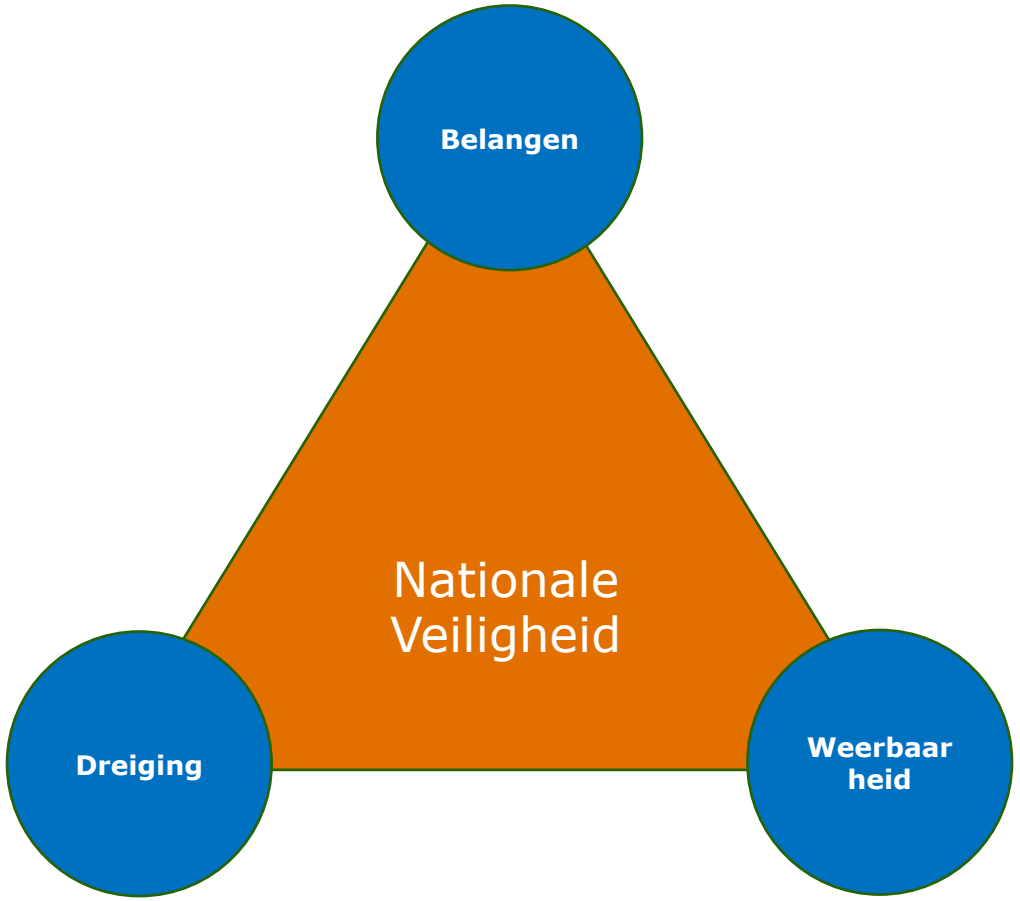
Hoe weet je of een product of dienst uit land X komt?

- Producten en diensten bestaan uit verschillende componenten. Elk component heeft weer zijn eigen supply chain.
- **Belangrijk:** wat gebeurt er met de data die het product of dienst verwerkt?
- Hoe bepaal je of een product of dienst afkomstig is uit land X?
- **Voorbeeld**: Is een iPhone een Amerikaans product?

Het inventariseren van mogelijke supply chain risico's

De cybercheck

- **De Technology Stack** bestaat uit verschillende lagen
- **Per laag is de vraag:** Wordt deze ontwikkeld of onderhouden door land X?
- Als het antwoord 'Ja' is, kan dit aanleiding zijn voor een aanvullende risicoanalyse.



De aanvullende risicoanalyse

Onderdelen van de aanvullende risicoanalyse

- **Dreiging:** in kaart brengen door middel van aanvalsscenario's.
- **Te Beschemen Belangen**: dit zou de organisatie al in kaart moeten hebben gebrachten als onderdeel van het algemene risicomanagementproces.
- **Weerbaarheid:** Is er een passend niveau van weerbaarheid?

De aanvullende risicoanalyse

Aanvallers kiezen de weg van de minste weerstand

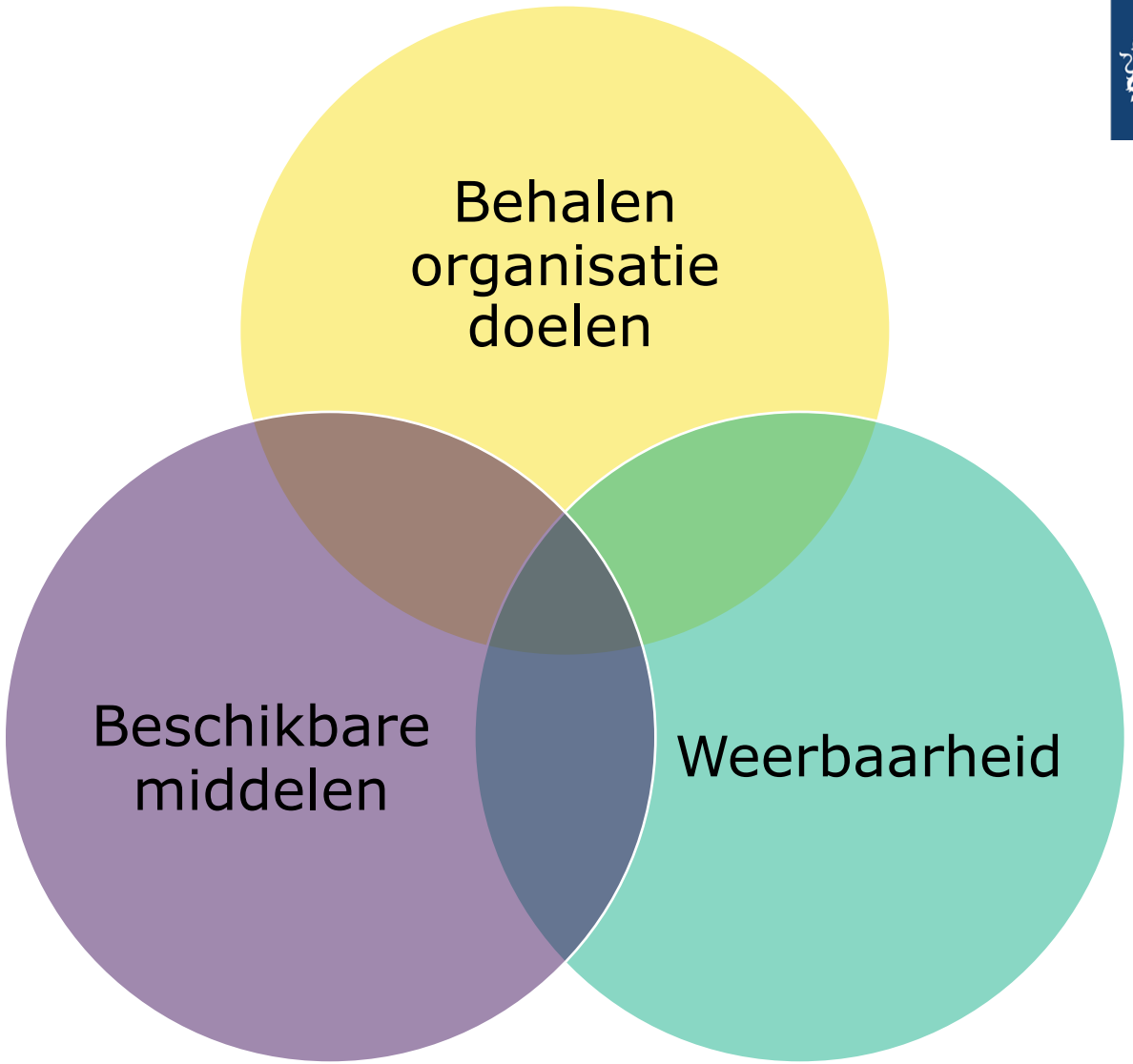
- De cybercheck richt zich op een zeer speficieke set aan risico’s
- Er zijn ook andere manieren om een succesvolle aanval uit te voeren: bijvoorbeeld phishing of misbruik van een kwetsbaarheid.
- Het is belangerijk om naar het **‘Grotere Plaatje’** te kijken

De aanvullende risicoanalyse

Het opstellen van aanvalscenario's

Voorbeeld aanvalsscenario	Fase	Beschik-baarheid	Integriteit	Vetrouwelijkheid
1. Bewust geplaatste backdoor of kwetsbaarheid	In	√	√	√
2. Kwaadaardige update van software	In	√	√	√
3. Insider threat via onderhoudsmonteur	In	√	√	√
4. Misbruik van een product of dienst voor toegang tot een ander product of dienst	Through	√	√	√
5. Spionage op data die standaard naar de leverancier verzonden wordt	Out	-	-	√
6. Heimelijke beïnvloeding van het functioneren van een product of dienst	Out	-	√	-
7. Sabotage van een product of dienst	Out	√	-	-

- Maak onderscheid tussen de verschillende aanvalsfases: in, through, out.
- Hoe raken de scenario's de beschikbaarheid, integriteit, vetrouwelijkheid van data, informatie en/of processen?
- **Doel:** mogelijke aanvalspaden van een malafide actor (via de supply chain) in beeld brengen.

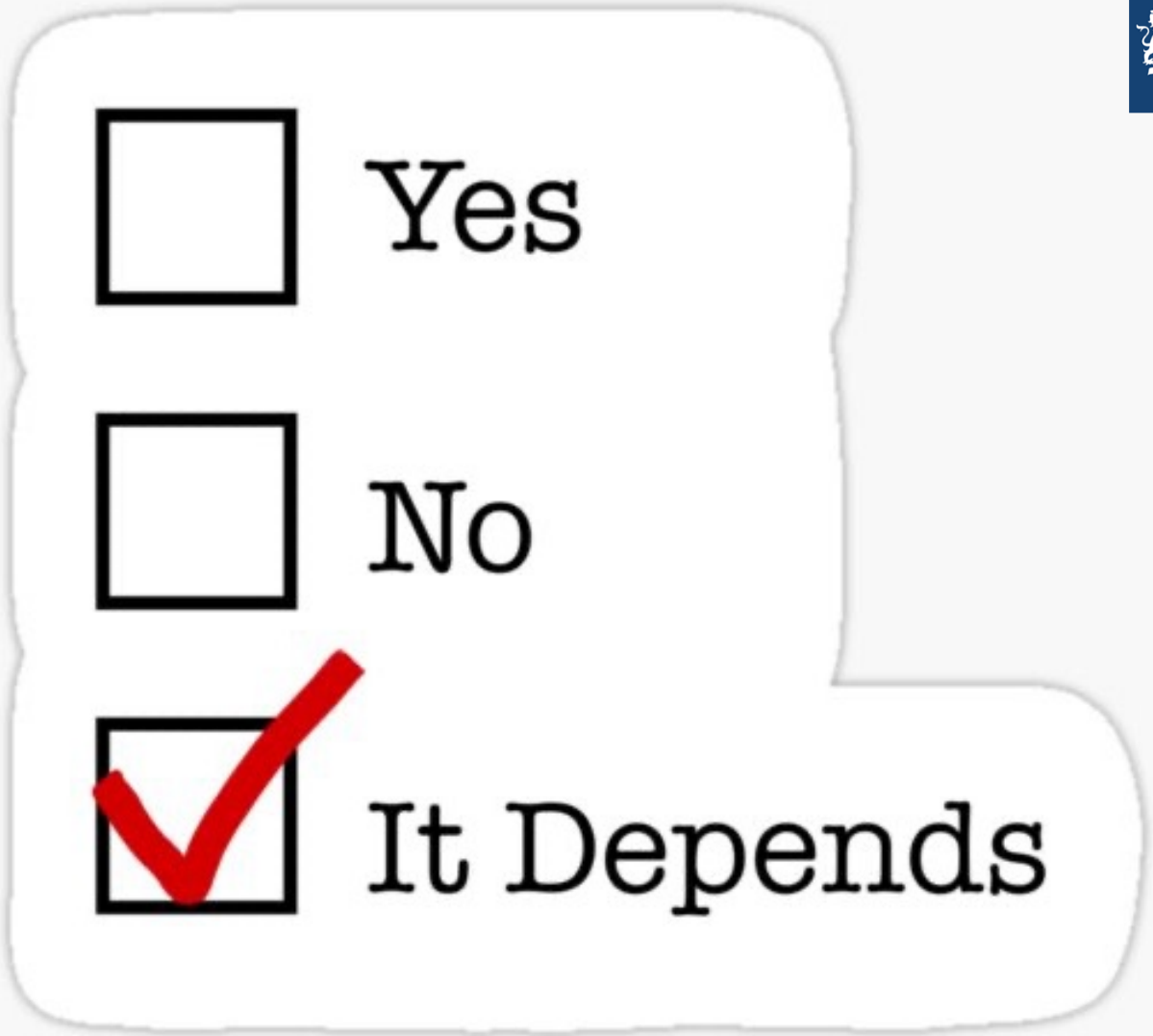


De aanvullende risicoanalyse

Een passend niveau van weerbaarheid

- Weerbaarheid gaat niet alleen over **identify en prevent**, maar ook over ook over **detect, respond en recover.**

- Passend niveau van weerbaarheid = afweging tussen verschillende belangen.



Conclusie

Main Takeaways

- Is het erg dat producten & diensten uit landen met een offensief cyber programma worden gebruik door (semi-)overheidsorganisaties in Nederland?
  - **Well, it depends…**

- De cybercheck is handreiking die structuur biedt bij het beantwoorden van de bovenstaande vraag.