

# Operationele KPI's en restrisico's als doelstelling voor de cybersecurity van OT-systemen

Metro en Tram

Gemeente Amsterdam

Dit document beschrijft de causaliteit hoe cybersecurity-incidenten kunnen leiden tot operationele incidenten. Het is een raamwerk voor risico-analyses. Het geeft de relaties weer tussen operationele kpi's en incidenten.

Het is bedoeld om contractmanagers, assetmanagers, projectmanagers, ontwerpers, ontwikkelaars, beheerders en cybersecurity-medewerkers de handvatten te geven om de cybersecurity van de OT handen en voeten te geven.

**! Dit document is een onderdeel van het CS aanpak voor de OT van MET.  
Zie [4] CS-Voorschrift CEB-OVG-21876.**

## **Vertrouwelijkheid.**

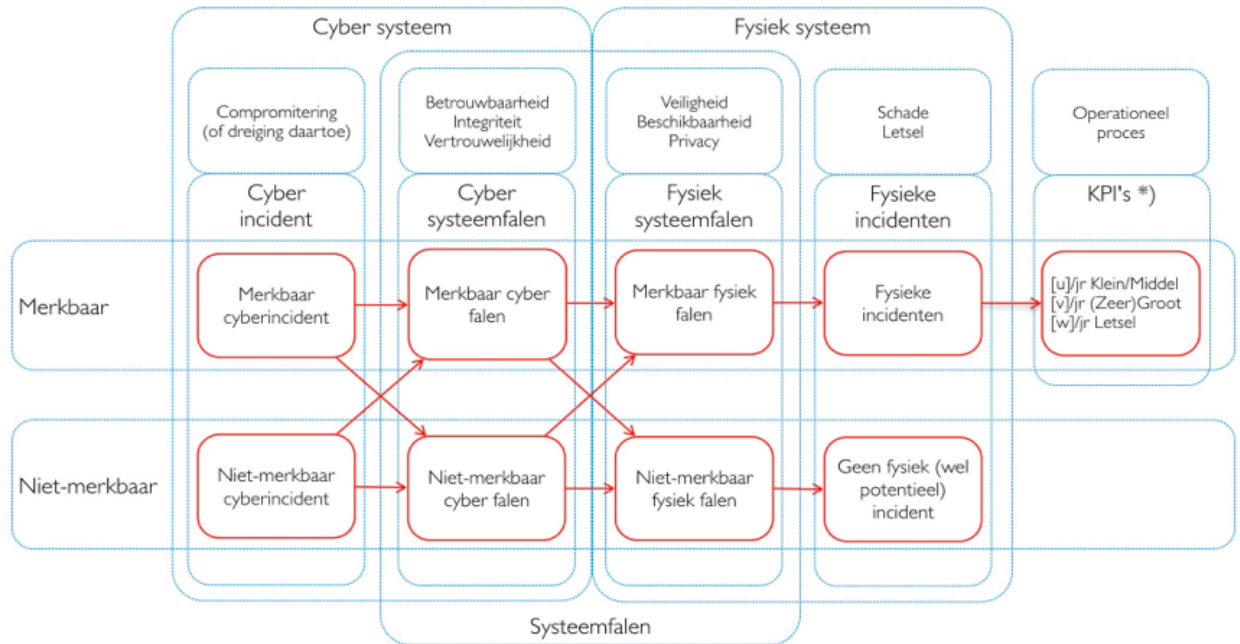
Dit document is niet-vertrouwelijk.

## **Documentnummer**

Join	CEB/OVG/21172
Datum	21 februari 2020
Versie	1
Status	Definitief
Door	Wim van Asperen, Cybersecurity & Privacy Officer OT MET

# 1. Causaliteiten

Deze tabel geeft de causaliteit tussen cyberincident en operationele incidenten. Uitgangspunt is dat de operationele kpi's zijn vastgesteld. Zoals gegeven in [4].



Er is sprake van

- merkbare en niet-merkbare incidenten en van
- merkbare en niet-merkbare systeemfalen.

Met het cyber systeem wordt bedoeld: de software en firmware van een OT systeem.

Met fysiek systeem wordt bedoeld: de hardware van een OT-systeem, inclusief de operationele installaties en apparaten.

*Voorbeelden zijn IO-systemen, servers, maar ook camera's, liften en verlichting(systemen).*

Een merkbare cyberincident kan leiden tot merkbare cyber systeemfalen.

*Een infectie met ransomware (beschikbaar- en integriteitsinbreuk) kan leiden tot een ontoegankelijke stuurgegevens van het scada-systeem.*

Een merkbare cyber systeemfalen kan leiden tot merkbare fysiek systeemfalen.

*Een ontoegankelijke database kan leiden tot beschikbaarheidsverlies van een centrale bedieningssysteem.*

Een merkbare fysiek systeemfalen kan leiden tot een fysieke incident.

*Een niet beschikbare bedieningssysteem van camera's en uitval van de verlichting, kan leiden tot paniek en chaos, verdringing en letsel.*

Niet-merkbare cyberincidenten kunnen leiden tot merkbare cyber systeemfalen. Dan is het wel merkbare, alleen is de oorzaak nog niet bekend.

Niet-merkbaar cyberincident kan leiden tot niet-merkbaar cyber systeemfalen.

Niet-merkbaar cyber systeemfalen kan leiden tot merkbaar fysiek systeemfalen. Dan is het wel merkbaar, alleen is de oorzaak nog niet bekend.

Niet-merkbaar cyber systeemfalen kan leiden tot niet-merkbaar fysiek systeemfalen Het falen van een systeem of installatie blijft in dat geval onopgemerkt en is een potentieel incident.

## 2. Kwantitatieve operationele kpi's

Voor Metro en Tram kan de VUS/BOGT-matrix [10] als kader fungeren voor het stellen van kwantitatieve operationele KPI's. Op basis van de VUS/BOGT-criteria.

>> Voor andere type OT systemen kan een soortgelijk raamwerk worden gebruikt.

### Geaccepteerde restrisico's

Voor de restrisico's kan een stramien worden gekozen waarbij vastgesteld wordt wat het maximum aantal (te accepteren) operationele incidenten (merkbaar en fysiek) per jaar is:

- maximaal [u] van het VUS/BOGT-type: Klein en/of Middel, zonder lichamelijk letsel;
- maximaal [v] van het VUS/BOGT-type: Groot en Zeer groot, zonder lichamelijk letsel;
- maximaal [w] met lichamelijk letsel

Voorbeeld: [incidenten/jaar]  
u = 4 zijn geaccepteerde restrisico's  
v = 1  
w = 0

### Conclusie1

De tabel toont dat alleen **fysieke merkbare operationele incidenten** meetellen in het jaarlijks vaststellen of de cybersecurity doelstellingen worden/zijn gehaald.

### Conclusie2

Cyberincidenten en cybersysteemfalen (al of niet merkbaar) die niet leiden tot merkbare fysieke operationele incidenten – feitelijk zijn dit potentiële cyberincidenten of cyberdreigingen – tellen niet mee in het vaststellen of de cybersecurity doelstellingen zijn gehaald.

### Conclusie3

Voor een Systeem dient te worden vastgesteld wat de vigerende operationele eisen zijn; als VS1-eisen. De integrale veiligheidsdoelstellingen, beschikbaarheidsdoelstellingen en de AVG (privacy) zijn dan de basis. De integrale veiligheidsdoelstellingen (c.q. te accepteren restrisico's t.a.v. veiligheid) zijn te bevragen bij Veiligheidscoördinator van MET.

De doelstellingen voor beschikbaarheid en privacy (c.q. te accepteren restrisico's t.a.v. beschikbaarheid en privacy) dienen te worden opgesteld door de Opdrachtgever van MET.

### **3. Vaststellen van cybersecuritymaatregelen**

De kwantitatieve operationele KPI's zijn de meetbare doelstelling van een OT-systeem en worden gebruikt voor het vaststellen van (de soort en de mate van) de cybersecuritymaatregelen aan de hand van de Risicomanagementaanpak voor cybersecurity [1].

De eis aan cybersecurity [6] geldt dat

- aangetoond moet worden dat de cyberrisicomaatregelen de kwantitatieve operationele KPI's faciliteren en
- de kwantitatieve operationele KPI's moeten worden gebruikt voor de cyber-risicomanagement.

## 4. Bronnen en referenties

[1] Cybersecurityrisicomanagementaanpak MET, CEB-OVG-18786

[2] Cybersecuritybeleid OT MET, CEB-OVG-20961

[3] Integrale incidentmanagementprocedure cybersecurity, CEB-OVG-20126

[4] CS-Voorschrift CEB-OVG-21876

[5] Vertrouwelijkheid MET, CEB/OVG/20264

[6] CS-eisen MET, CEB/OVG/18908

[7] CS-dossier voor een systeem/project, CEB/OVG/20265

[8] Meerjaren cybersecurityplan MET, CEB/OVG/20960

[9] -

[10] VUS/BOGT-matrix van GVB is een tabel met calamiteitenindeling ten behoeve voor opschaling: Verstoring, Uitval, Storing, Brand, Ongeval, Gevaarlijke stoffen, Terrorisme met een classificatie en de periode van Klein (lokaal), Middel (een OV-lijn), Groot (meerdere OV-lijnen, Zeer groot (alle OV-lijnen in de regio). Zie CEB-OVG-18786.