

# **Cybersecurityrisicomanagementaanpak OT MET 1/3 Uitleg**

voor operationele technologie

Metro en Tram

Gemeente Amsterdam

**Vertrouwelijkheid.**

Dit document is niet vertrouwelijk.

**Documentnummer**

Join                    CEB/OVG/18786

## Inhoudsopgave

1. Cybersecurityrisicomanagement .....	3
1.1. Definities en begrippen .....	3
1.2. Keuzes maken. Van generiek naar specifiek .....	4
1.3. Situationeel risicosturing: effectief en efficiënt .....	4
1.4. Cybersecurityrisicomanagement van OT-systemen .....	4
1.5. Cybersecuritydoelen en -eisen .....	4
1.5.1. Kwantitatieve cybersecuritydoelen .....	5
1.5.2. Kwalitatieve cybersecuritydoelen .....	6
1.6. Van dreigingsbeeld naar hazards .....	6
1.7. Assetmanagement .....	8
1.8. Cybersecurity in het ontwerpproces (By-design) .....	8
1.9. Stapgewijze aanpak .....	9
2. Bronnen en referenties .....	10

### Versiebeheer

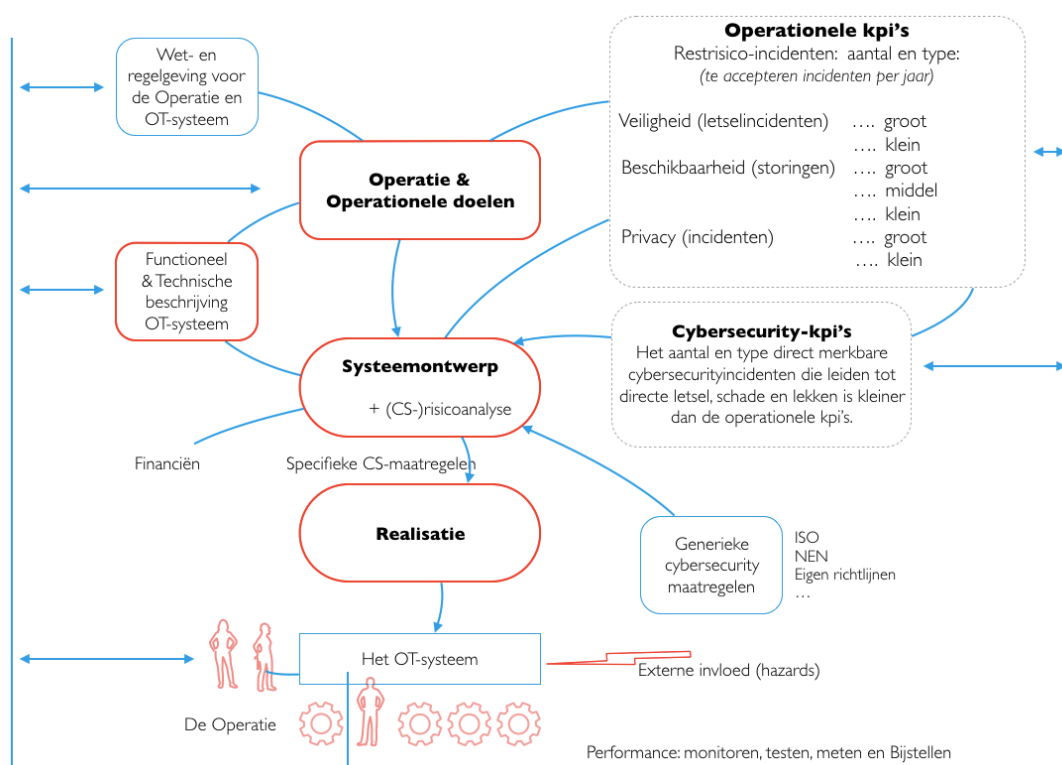
19 dec 2019 , Versie 1.1, Uitleg stappen risicoanalyseproces uitgewerkt, W.L. van Asperen  
18 sep 2019 , Versie 1.0, Definitief, W.L. van Asperen

# 1. Cybersecurityisicomanagement

Dit document beschrijft hoe MET voor de bedienings- en bewakingsystemen de beveiliging organiseert op basis van specifieke risicoanalyses. Dit document beslaat het proces van vaststellen of afleiden van cybersecurity-doelen tot en met het vaststellen van de preventieve en regressieve cybersecuritymaatregelen.

Cybersecurityrisicomanagement vormt een onderdeel van een integrale aanpak, dat beschreven is in **CS-Voorschrift** [10]. Het CS-Voorschrift is het top-document voor de cybersecurity van de OT van MET.

Cybersecurityrisicomanagement is een centraal onderdeel van het ontwerpproces van systemen en wordt ook bij veranderingen aan bestaande ict-systemen toegepast (changes).



## 1.1. Definities en begrippen

Voor definities en begrippen (OT, cyberincident, cybersecuritymaatregelen, cybersecuritydoelen) wordt verwezen naar  
 [2] Cybersecuritybeleid en  
 [10] Cybersecurityvoorschrift

## 1.2. Keuzes maken. Van generiek naar specifiek.

Er bestaat een veelheid aan informatie in de wereld over generieke cybersecurity-maatregelen in de vorm van best practices, internationale en nationale normen, algemene richtlijnen, checklists en richtlijnen van de fabrikant. In algemene termen geldt dat voor een specifiek OT-systeem in een specifiek omgeving en voor een specifiek operationeel doel keuzes worden gemaakt (in het ontwerpproces) voor specifieke cybersecuritymaatregelen, als een subset van generieke maatregelen.

## 1.3. Situationeel risicosturing: effectief en efficiënt

Cybersecurityrisicomanagement faciliteert situationeel risicosturing en bewerkstelligt dat cybersecuritymaatregelen adequaat precies voldoende (niet te veel en niet te weinig) gericht zijn op de beoode operatie en de operationele doelstelling (effectief) en tegen zo min mogelijk kosten (efficiënt) kunnen worden bewerkstelligd.

## 1.4. Cybersecurityrisicomanagement van OT-systemen

Cybersecurityrisicomanagement beheerst de risico's van cyberincidenten, dat begint met een cybersecurityrisicoanalyse,

- is een onderdeel is van het **ontwerpproces** van een OT-systeem
- uit te voeren in alle fasen van de levenscyclus (nieuwbouw, onderhoud en renovatie);
- dat op basis van een reële dreigingsbeeld (en hazards) en de kwetsbaarheid van het specifieke systeem en organisatie
- specifieke cybersecuritymaatregelen vaststelt
- die bruikbaar, betaalbaar (efficiënt en effectief) zijn;
- en die de specifieke operationele doelstellingen van het systeem en de beoogde operatie faciliteren op basis van ontwerpkeuzes tussen de tegenstrijdige overwegingen, als
  - de technische mogelijkheden en beperkingen,
  - de operationele bruikbaarheid;
  - de organisatorische en financiële mogelijkheden en beperkingen;
- bedoeld om de kans te verminderen (preventief) op het optreden van een cyberincident en/of
- het effect op het systeem en de impact op de operatie te verminderen;
- dat inzichtelijk maakt wat de restrisico's zijn (de kans en de mate van impact op operatie);
- wat de herstelmaatregelen zijn van het systeem en van de operatie (repressief);
- en waarbij de restrisico's en de herstelmaatregelen geaccepteerd (geëvalueerd, bevestigd en begrepen) zijn door de stakeholders
- en geoefend zijn door de gebruikers en beheerders.

## 1.5. Cybersecuritydoelen en -eisen

Eisen worden afgeleid van de doelen. De operationele doelen van een OT-systeem dienen te worden vertaald naar cybersecuritydoelen.

Vanuit het gezichtspunt van de cybersecurity betreffen de **operationele doelen** tav het beoogde gebruik en beheer:

Titel. Cybersecuritymanagementaanpak MET  
Classificatie Niet-vertrouwelijk  
Document: CEB/OVG/18786  
Versie 19 december 2019

- Veiligheid (alle type van veiligheid ondermeer: tunnelveiligheid, spoorveiligheid, publieksveiligheid, arbo-veiligheid en milieuveiligheid)
- Beschikbaarheid (volledig/partiëel, permanente/tijdelijk, (on)merkbaar systeemfalen)
- Privacy

Cybersecuritydoelen op systeemniveau betreffen (in generieke zin):

- beschikbaarheid,
- integriteit en
- vertrouwelijkheid

van het systeem (software en hardware) en van de gegevens (data).

### 1.5.1. Kwantitatieve cybersecuritydoelen

De beschikbaarheid, integriteit en vertrouwelijkheid van systemen en gegevens zijn een subset van de RAMSSHEEP-eigenschappen van een systeem en kunnen respectievelijk worden uitgedrukt in %-verminderde gebruikstijd van een (partieel of volledig) systeem, aantal en mate (gering tot kritisch) van integriteitsincidenten per periode en aantal en mate (gering tot kritisch) van vertrouwelijkheidsincidenten per periode.

Kwantitatieve cybersecurityeisen kunnen ook worden vastgelegd in combinaties van beschikbaarheid, privacy (gelijk de vertrouwelijkheidsseis) en veiligheid (gelijk de integriteitseisen). Kwantitatieve cybersecuritydoelen komen in de praktijk (nog) nauwelijks voor, omdat de harde correlatie tussen de operationele doelstellingen en cybersecurityeisen (nog) nauwelijks wordt gemaakt.

De operationele kpi's voor Veiligheid, Beschikbaarheid en Privacy is gelijk aan de geaccepteerde fysieke restrisiko's in termen van het aantal te accepteren incidenten per jaar van een bepaalde omvang.

!! Het is de bedoeling dat voor elk (type)systeem de kpi's worden vastgesteld door de opdrachtgever en/of (toekomstig) beheerder.

Zie het document CS Operationele KPI's OT MET [11].

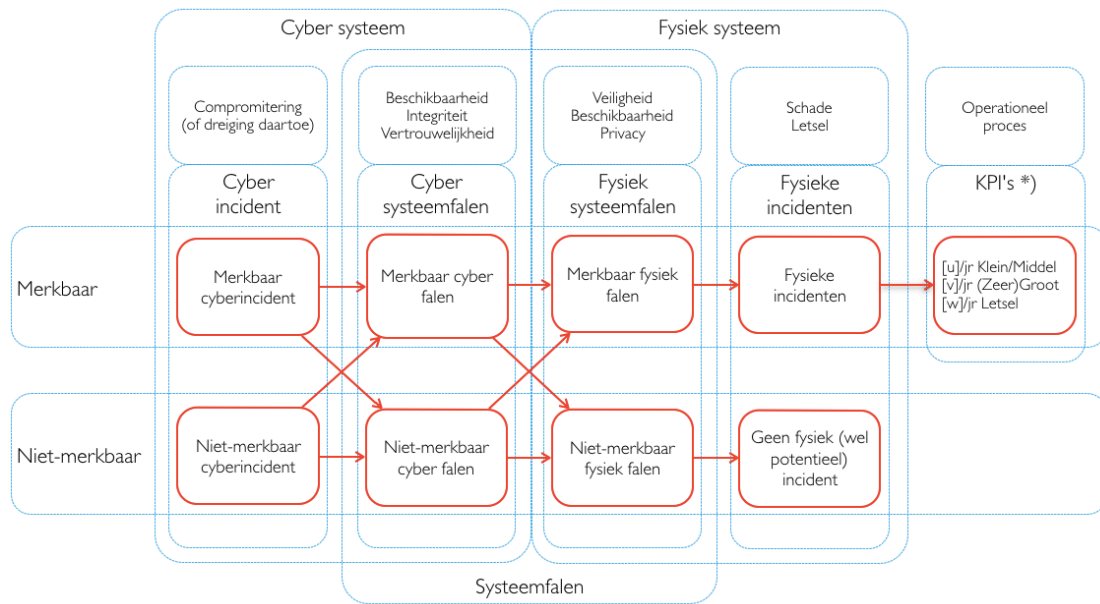
!! Als geen doelen en kpi's zijn vastgesteld, kan het project 'eigen' doelen en kpi's opstellen en die - expliciet - als aannames en uitgangspunten.

Deze worden opgenomen in de CS-eisen (voor een nieuw project) en/of vastgelegd in het CS-Dossier van het betrokken object.

Het aantal en soort cyberincidenten die leiden tot fysieke incidenten, is dus maximaal kleiner dan het aantal operationele VBP-kpi's; omdat andere oorzaken ook kunnen leiden tot fysieke falen en incidenten.

Het aantal en soort cyberfalen en -incidenten (per jaar) kunnen veel hoger zijn dan de het aantal VBP-kpi's omdat cyberincidenten ook kunnen leiden tot niet-merkbaar falen.

In de figuur hieronder wordt de relatie getoond tussen (merkbare en niet-merkbare) cyberincidenten die kunnen leiden tot fysieke incidenten t.a.v. de veiligheid, beschikbaarheid en privacy.



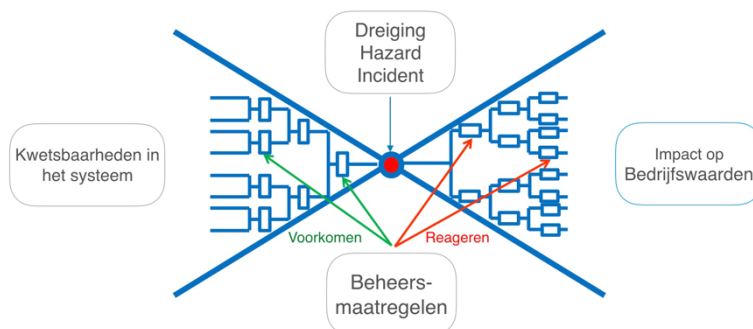
Figuur. Causaliteit tussen cyberincidenten en merkbaar falen en fysieke incidenten

### 1.5.2. Kwalitatieve cybersecuritydoelen

Cybersecurityeisen worden dikwijls vertaald naar voorgeschreven cybersecuritymaatregelen en organisatorische of proces-eisen. De ISO27001 en ISO27002 bevatten gezamenlijk ca 340 (generieke) maatregelen die veelal specifiek gemaakt worden per systeem. Een (globale) correlatie met de operationele doelstellingen wordt gemaakt in de vorm van een cybersecurityclassificatie van OT-systemen. OT-systemen krijgen een cybersecurityindeling van 'zeer kritische' tot 'gering kritische' op basis van de mate van impact op de operatie. Per classificatieniveau wordt een subset van de 340 maatregelen voorgeschreven als eis.

## 1.6. Van dreigingsbeeld naar hazards

MET heeft een eigen **CS Dreigingsbeeld OT MET** [9] dat vooral gebaseerd is op de jaarlijks update van het NCSC: het algemene dreigingsbeeld van cyberincidenten in Nederland.



Cybersecurityhazards en hazardlog is een manier om het dreigingsbeeld voor een specifiek systeem in te vullen. Cybersecurityhazards worden dikwijls door cybersecurityexperts bepaald. Het is verstandig om deze door 'peers te challengen' op realiteitswaarde en door opdrachtgevers en gebruikers te worden geëvalueerd ten aanzien van de impact op de operatie.

- De ongewenste gebeurtenis (dreiging/hazard) is het wegnemen, toevoegen of aanpassen van informatie of systeemgedrag; uit balorigheid, chantage, sabotage of terrorisme, gov-threats, van binnen (intern) of van buiten (extern).
- De kwetsbaarheid van het systeem (hardware, software, organisatie, mens en omgeving) bepaalt de kans dat de ongewenste gebeurtenis optreedt. Maar niet alleen dat; de kans van optreden is ook gekoppeld aan de impact van de gebeurtenis. Een ongewenste gebeurtenis kan met verschillende kansen impact hebben op verschillende bedrijfswaarden met verschillende ernst. Kwetsbaarheden worden gedetecteerd door: virus-scanners, risico-analyses, surveillance/monitoring, pentesten, compromise assessments
- De bedrijfswaarden zijn imago, fysieke veiligheid, beschikbaarheid, sociale veiligheid, privacy, kosten, milieu, toegankelijkheid (stations), reizigersinformatie.
- Restrisico's zijn risico's die impact kunnen hebben op de operatie en die geaccepteerd zijn door de opdrachtgever en de beheerder en de exploitant en die gemitigeerd worden door het herstellen van de operatie en waarvan de mitigatie- en herstelprocedures geoefend zijn. Een handbediende operatie kan een maatregel zijn om een restrisico te mitigeren.

Impact	waarde	Imago	fysieke veiligheid	beschikbaarheid	sociale veiligheid	privacy	kosten	toegankelijkheid	reizigersinformatie	milieu
gering	1	negatieve aandacht in de plaatselijke pers	licht gewonde	dispuntualiteit	reizigers voelen zich niet veilig. <10 klachten	gegronde klachten zonder juridische gevolgen	€ 1k < kosten <= € 10k	Mindervalden hebben moeite bij de trein te komen; 1 of meer liften en/of roltrappen werken niet	gebrekige of geen informatievoorziening op 1 of meer stations	bepaalde gevolgen voor het milieu; lokaal en binnen beheergebied; beperkte en kortdurende overschrijding
bepaald	2	negatieve aandacht in de regionale pers; zorg bij lokale overheid; vergoeding bedruid	licht gewonde(n) met verzuin	rituval(en)	Aanzienlijk gevoel van onbehagen; vandalsisme en criminaliteit; >10 klachten	Klachten met juridische gevolgen	€ 10k < kosten <= € 100k	reizigers hebben moeite bij de trein te komen; uitval liften, roltrappen en OVCP	Verhoorde of tegenstrijdige reizigersinformatie op 1 of meer stations	gevolgen voor het milieu; lokaal; bodemverontreiniging; g die sanering behoeft; beperkte overschrijding normen; <= 10 klachten
aanzienlijk	3	korte negatieve aandacht in de nat. Pers; zorg bij prov. overheid of een stakeholder; vergoeding ingetrokken	x	vollidige stremming metroverkeer zonder ontbruimng stations	Ernstig gevoel van onbehagen; gewaelijk; reizigers midden locatie	x	€ 100k < kosten <= € 1 mio	x	x	grootaachlijke verontreiniging van o.a. Bodem en opp./ grondwater; langdurige overschrijding normen; >10 klachten
hoog	4	negatieve aandacht in nat. Pers; vermeldingen in internationale pers; zorg bij nat. overheid en/of div stakeholders	letale slachtoffers en/of zwaargewonde	stremming metroverkeer en ontbruimng stations	x	x	€ 1 mio < kosten <= € 10 mio	Station(s) moeten ontbruimd; uitval verlichting	Ontbruim Alarm installatie van station(s) is langdurig defect	Ernstige milieuschade; ingrijpende herstellende maatregelen nodig; langdurige impact; schade voor omwonenden; vele klachten
kritiek	5	langdurige negatieve aandacht in de (inter)nationale pers; langdurige zorg bij overheid en div Stakeholders; dreiging voor concessie	letale slachtoffers en/of zwaargewonden	herhaakelijke langdurige stremming metroverkeer en ontbruimng stations	x	x	kosten > €10 mio	herhaakelijk ontbruimng van stations; langdurige uitval veiligheidssystemen	x	milieuschade met (mogelijk) blijvende schade; impact; schade voor de hele regio

Een risico is de kans op een dreiging [9] met een bepaalde impact. Maatregelen kun je nemen om de oorzaken van de dreiging voor te zijn, of om de gevolgen van die dreiging te beperken. Bepalend voor het nemen van maatregelen is het maximale risico dat veroorzaakt wordt door de dreiging op basis van de bedrijfswaarden. Immers een ongewenste

gebeurtenis kan met verschillende kansen impact hebben op verschillende bedrijfswaarden met verschillende ernst. Hoe eenduidiger en objectiever de risico's worden ingeschat hoe eenvoudiger prioriteiten kunnen worden gesteld aan het nemen van maatregelen. Zie ook het document Dreigingsbeeld voor OT van MET [9].

		impact	trage	fysieke veiligheid	beschikbaarheid	sociale veiligheid	privacy	kosten	loggeerbaarheid	redigerbaarheid	milieu	Waarschijnlijkheid (over Tijdenster van 3 jaar)				
												zeer onwaarschijnlijk 1 (<0.0%)	onwaarschijnlijk 2 (0.0% < x < 0.1%)	mogelijk 3 (0.1% < x < 0.5%)	waarschijnlijk 4 (0.5% < x < 5%)	zeer 5 (>5%)
Impact	gering	1	negatieve aandacht in de plaatselijke pers	licht gevorderd	dispuiteerbaar	relatieve waken acht met veilig <10 kVacten	gevoelige kVacten zonder juridische gevolgen	€1k < kosten <= 10k	Minderwaarden hebben moeite bij de train te komen; 1 of meer stations of roltrappen werken niet	gebruik van geen informatievoorziening op 1 of meer stations	gevoelige voor het milieu; leed en slecht beheer; beperkte en kortlopende vernieuwing	zeer onwaarschijnlijk	onwaarschijnlijk	mogelijk	waarschijnlijk	zeer
	beperkt	2	negatieve aandacht in de regionale pers; zorg bij lokale overheid; vergoeding bedrag	licht gevorderd met verarm	risicovol	Aanzienlijk gevoel van onveiligheid; verduidelijke en onduidelijke >10 kVacten	KVacten met juridische gevolgen	€10k < kosten <= 100k	relatieve hebben moeite bij de train te komen; uitsluiting van roltrappen en OVP	Verkeerde of tegevoelige redigerbaarheid op 1 of meer stations	gevoelige voor het milieu; leed bodemverontreiniging die sanering behoeft; beperkte vernieuwing; normen <=10 kVacten	zeer onwaarschijnlijk	onwaarschijnlijk	mogelijk	waarschijnlijk	zeer
	aanmerkelijk	3	forte negatieve aandacht in de nat. Pers; zorg bij provincie of een staatsrechter; vergoeding ingetrokken	x	voldoende strooming met roovermeer onder omringing stations	Eenlig gevoel van onveiligheid; relaties met lokale	x	€100k < kosten <= €1 mio	x	x	grote schade; vernieuwing van i.s. System en ego-groenwater; langdurige vernieuwing; normen >10 kVacten	zeer onwaarschijnlijk	onwaarschijnlijk	mogelijk	waarschijnlijk	zeer
	hoog	4	negatieve aandacht in nat. Pers; vermeldingen in internationale pers; zorg bij nat. overheid en/of staatsrechter	zeer slecht of zeer gevorderd	stremming met roovermeer en omringing stations	x	x	€1 mio < kosten <= €10 mio	Station(s) moeten ontruimd; uitsluiting vernieuwing	Ontruim. Alarm installatie van station(s) is langdurig defect	ernstige milieuschade; ingrijpende herstellende maatregelen nodig; langdurige impact; hinder voor omwonenden; vele kVacten	zeer onwaarschijnlijk	onwaarschijnlijk	mogelijk	waarschijnlijk	zeer
	extrem	5	langdurige negatieve aandacht in de internationale pers; langdurige zorg bij nat. overheid en/of staatsrechter; dreiging voor concessie	zeer slecht of zeer gevorderd	herhaalbare stremming met roovermeer en omringing stations	x	x	kosten > €10 mio	herhaalbare ontruiming van station(s); langdurige uitsluiting veiligheidssystemen	x	ernstige milieuschade; ingrijpende herstellende maatregelen nodig; langdurige impact; hinder voor de hele regio	zeer onwaarschijnlijk	onwaarschijnlijk	mogelijk	waarschijnlijk	zeer

Zie ook [1] Cybersecurity Risico-analyse Bedrijfswaardenmatrix

## 1.7. Assetmanagement

OT-Cybersecurityrisicomanagement dient te zijn ingebed in het assetmanagement van een specifiek systeem (object of asset). De ISO55000 is een bruikbare richtlijn voor assetmanagement en betreft alle levenscycli van een asset.

## 1.8. Cybersecurity in het ontwerpproces (By-design)

Cybersecurity is (idealiter) een onderdeel is van het **ontwerpproces** van een OT-systeem, zoals beschreven in de paragraaf Cybersecurityrisicomanagement van OT-systemen. Cybersecurity is een RAMSSHEEP-aspect. Zie het CS-Voorschrift [10].

## 1.9. Stapgewijze aanpak

Gebruik het Cybersecurity **CS Risicomgt 3/3 Sjabloon** [1] en volg de onderstaande stappen. In het sjabloon zijn de te hanteren indicaties gegeven.

Kwetsbaarheden betreffen bestaande systemen en processen of systemen en processen waarvoor nog geen maatregelen voor zijn ontworpen of geïmplementeerd.

Plan (bijvoorbeeld) een dagdeel voor de onderstaande stappen (afhankelijk van de complexiteit). Stap 1 en Stap 5 kan vooraf worden voorbereid.

In beginsel is het een proces van experts (-judgement): systeemexperts en cybersecurity-experts.

Rollen:

- Facilitator van de sessie
- Systemengineers, kennen techniek, het gebruik en het beheer van systeem
- Cybersecurityexpert
- Veiligheidsexpert, optioneel, kan ook nadien worden geraadpleegd

De restrisico's dienen te worden afgestemd met en geaccordeerd door de veiligheidsexperts.

Het resultaat dient te worden afgestemd c.q. vastgesteld door de opdrachtgever/beheerder en/of gebruiker.

### A. Inventariseer

- Stap 1 Verzamel technische informatie (ontwerp)(fysiek, hardware, software)
- Deze stap kan vooraf

### B. Identificeer kwetsbaarheden in bestaand systeem

- Stap 2 Identificeer technische configuratie
- Stap 3 Identificeer functionele configuratie o.b.v. de indicaties
- Stap 4 Identificeer kwetsbaarheidsniveau o.b.v. de indicaties

### C. Bepaal hazards

- Stap 5 Leidt van de indicaties de potentiële dreigingen (hazards) af
- Stap 6 Bepaal de waarschijnlijkheid a.d.h.v. Bedrijfswaardenmatrix (2/3)

### D. Bepaal waarschijnlijkheid en impact t.a.v. de kwetsbaarheid

- Stap 7 Bepaal soort en mate van systeem falen
- Stap 8 Bepaal impact op operatie a.d.h.v. Bedrijfswaarden-matrix
- Stap 9 Bepaal het operationeel doel cq de bedrijfswaarde dat aangetast wordt

### E. Adviseer/Bepaal maatregelen voor aanvaardbare restrisico's

- Stap 10 Verzamel generieke mitigerende maatregelen.
- Stap 11 Adviseer of Ontwerp mitigerende maatregelen
- Stap 12 Bepaal te accepteren restrisico's (met opdrachtgever/beheerder, gebruiker)

### F. Zet acties uit.

- Stap 13 Neem hoofdpunten over in CS-Dossier. Zet acties uit.

## 2. Bronnen en referenties

- [1] Cybersecurity Risicomgt 1/3 Toelichting CEB-OVG-18786  
Cybersecurity Risicomgt 2/3 Bedrijfswaardenmatrix CEB-OVG-18786  
Cybersecurity Risicomgt 3/3 Sjabloon CEB-OVG-18786
- [2] Cybersecuritybeleid MET, CEB-OVG-20961
- [3] Integrale incidentmanagementprocedure cybersecurity, CEB-OVG-20126
- [4] Charter Cybersecurity Board, CEB-OVG-19094, w.van.asperen@amsterdam.nl
- [5] Vertrouwelijkheid, CEB/OVG/20264
- [6] Cybersecurityeisen MET, CEB/OVG/18908
- [7] Cybersecuritydossier(sjabloon) voor een systeem/project, CEB/OVG/20265
- [8] Cybersecurity Meerjarenplan MET (beveiligd), CEB/OVG/20960
- [9] Cybersecurity Dreigingsbeeld OT MET (beveiligd), CEB/OVG/22124
- [10] CybersecurityVoorschrift OT MET, CEB/OVG/21876
- [11] CS Operationele KPI's OT MET, CEB/OVG/21172
- [12] Bronnen en referenties voor cyberrisicomanagement:
- Handreiking Risicoanalyse, door Navi (Nationaal Adviescentrum Vitale Infrastructuur)
  - ISO27001, paragrafen 6.1.2 en 6.1.3 en 8.2 en 8.3
  - ISO31000 Risicomanagement (in het algemeen)
  - EN62443-4-2- Technical security requirements
  - ISO27035 Incidentresponse