

Integrale incidentmanagementprocedure cybersecurity

voor de operationele ICT-systemen voor metro- en tram

door Peter van Gestel
onder auspiciën van de
Cybersecurity Board MET/GVB

Versie 1.4 Datum 26 maart 2019
Join: CEB/OVG/18784

Inhoud

Managementsamenvatting	3
Versiebeheer	3
1. Inleiding	4
2.0 Het doel en organisatie	5
2.1 Het doel van de cybersecurity	5
2.2 Organisatie van de cybersecurity	5
2.3 Sleutelfunctionarissen en informatie delen	6
2.4 Integraal incidentmanagementprocedure cybersecurity	6
3.0 Cybersecurity incidenten	8
3.1 Hoe definiëren we cybersecurity incidenten?	8
3.2 Wanneer is sprake van een cybersecurity dreiging?	8
4.0 De procedure	10
5.0 Toelichting op de procedure	11
6.0 Referenties	13
Bijlage A Gegevens sleutelfunctionarissen	14

Managementsamenvatting

Deze procedure beschrijft wie wat moet doen als een cyber security incident is opgetreden of als een (vermoeden van een) incident dreigt op te treden in één of meer van de operationele ICT-systemen van metro- en tram.

Deze procedure is van belang in verband met:

- het delen van bevindingen tussen sleutelfunctionarissen van de betrokken organisaties: de leveranciers, GVB en MET;
- het gezamenlijk oplossen van het incident of het wegnemen dan wel verminderen van de dreiging;
- het centraal registreren van incidenten en dreigingen;
- het evalueren van de afhandeling;
- de rapportage en het advies over de inhoud en het gevolgde proces.

Deze procedure bevat in bijlage A de actuele contactgegevens van de sleutelfunctionarissen van de betrokken organisaties.

Deze procedure is ontwikkeld onder auspiciën van de Cybersecurity Board MET/GVB.

Versiebeheer

Versie 1.4 dd 26 maart 2019, kleine aanpassingen door Wim van Asperen. Definitie aangescherpt en identiek gemaakt tussen integrale incidentprocedure en MET incidentprocedure.

Versie 1.3 dd 28 november 2018, kleine aanpassingen door Wim van Asperen nav opmerkingen in MT E&B overleg dd 19 november.

Versie 1.2.1 dd 22 oktober 2018, kleine aanpassingen door Wim van Asperen ter nadere verduidelijking van de tekst.

Versie 1.2 dd 3 september 2018, opgesteld door Peter van Gestel (MET/E&B) na verwerking reviewcommentaar van de leden van de Cybersecurity Board MET/E&B.

1 Inleiding

Deze Incidentmanagementprocedure is bedoeld voor medewerkers en sleutelfunctionarissen van leveranciers c.q. opdachtnemers die werkzaamheden verrichten en verantwoordelijk zijn voor (de ontwikkeling, het beheer en onderhoud van) de operationele ICT-systemen (OT) van metro en tram [12].

Doel van deze procedure is te beschrijven wat de sleutelfunctionarissen moeten doen als een cybersecurityincident is opgetreden of als een incident dreigt op te treden in één of meer van de systemen en samenwerking noodzakelijk is.

Leeswijzer

In hoofdstuk 2 wordt de organisatie [1] rondom cybersecurity besproken, worden de sleutelfunctionarissen genoemd, wordt de positie en de rol van de Cybersecurity Board MET/ GVB, de Werkgroep Security MET/E&B/GVB en de Integraal Cybersecurity Board leveranciers MET besproken.

In hoofdstuk 3 wordt ingegaan op de soorten van cybersecurity incidenten en dreigingen en hoe de desbetreffende sleutelfunctionaris moet acteren na een melding.

Hoofdstuk 4 betreft de procedure zelf, met het proces, de taken en verantwoordelijkheden.

In hoofdstuk 5 wordt een toelichting gegeven op de procedure.

2 Doel en organisatie cybersecurity

2.1 Doel van cybersecurity

Het doel van de Cybersecurity Board MET/GVB is het realiseren en in stand houden van een geaccepteerd en beheerst cybersecurity-niveau van het Metro- en Tramsysteem Amsterdam, gedurende de gehele levenscyclus van metro en tram, met aandacht voor de belangen van de verschillende stakeholders. Lees verder in Doel, Scope en Beleid [12] en de charter van de Cybersecurity-organisatie [1].

2.2 Organisatie van cybersecurity

Het doel van de Cybersecurity Board MET/GVB is het realiseren en in stand houden van een geaccepteerd en beheerst security-niveau van het Metro- en Tramsysteem Amsterdam, gedurende de gehele levenscyclus van metro en tram, met aandacht voor de belangen van de verschillende stakeholders. Lees verder in de charter van de Cybersecurity-organisatie [1].

De Cybersecurity Board MET/GVB richt zich op het beoordelen en monitoren van de cybersecurity-aspecten van de operationele bediening- en bewaking van de metro en tram systemen. Ook wel Operationele Technologie (OT) genoemd. De Cybersecurity Board MET/GVB kan gevraagd en ongevraagd de directie van E&B, GVB en VRA adviseren over security betreffende metro en tram.

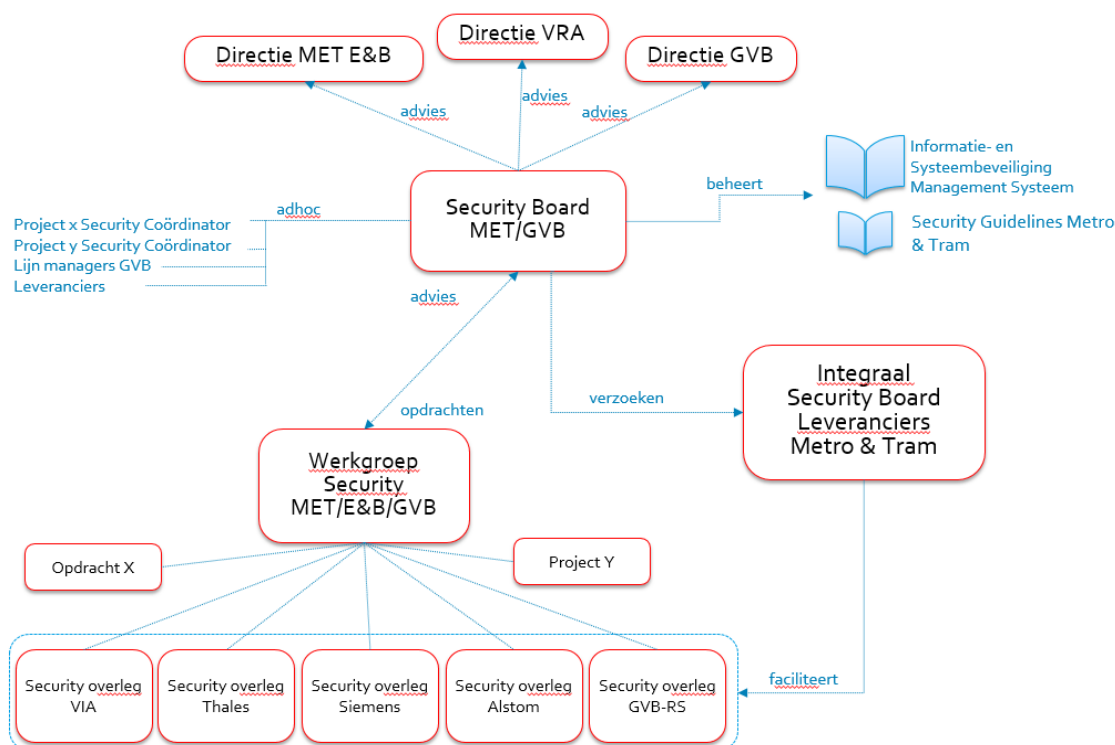
De Cybersecurity Board MET/GVB vindt zijn legitimatie in het feit dat beveiliging conditioneel is voor veiligheid (spoor, arbo, publiek, milieu), privacy (reizigers en personeel) en beschikbaarheid (dienstregeling) en is bedoeld ter voorkoming van schade en letsel. De lijnorganisaties borgen dat de beveiliging deze doelstellingen haalt en behoudt (accountable), de Cybersecurity Board MET/GVB geeft richting aan het resultaat (consulted en supportive).

Een van de activiteiten van de Cybersecurity Board MET/GVB is regievoering op te nemen maatregelen en ondersteuning hiervan in de betreffende lijnorganisatie(s). Daartoe kan de Cybersecurity Board MET/GVB opdrachten geven aan werkgroepen. Op het gebied van cybersecurity is dat de werkgroep security MET/GVB.

De werkgroep security behandelt vraagstukken op inhoud, onderzoekt, discussieert en adviseert de Cybersecurity Board MET/GVB. Daarnaast voert zij opdrachten uit en werkt aan verbetermaatregelen in opdracht van de Cybersecurity Board MET/GVB. Verder gaat de werkgroep in gesprek met de leveranciers van de systemen over de invulling van het cybersecurity beleid, procedures en te nemen maatregelen.

In verband met de vertrouwelijkheid worden inhoudelijke zaken in afzonderlijke overleggen met de leveranciers behandeld. Voor ketenvraagstukken worden speciale overleggen met de betrokken leveranciers belegd. Elke leverancier voorziet in een security-vertegenwoordiger die te raadplegen is in geval van een incident.

Naast de Cybersecurity Board MET/GVB is de Integrale Cybersecurity Board Leveranciers MET ingericht, waarin met de formele vertegenwoordigers van de leveranciers de security gezamenlijk en als een keten aan te pakken. Dit overleg faciliteert de conditionele, commerciële en contractuele zaken om de inhoudelijke samenwerking te laten plaatsvinden.



Opmerking: VIA is nu VisserSmitBouw (VSB).

Opmerking: De Werkgroep Cybersecurity houdt zich voornamelijk bezig met cybersecurity aspecten.

2.3 Sleutelfunctionarissen en informatie delen

MET/E&B, GVB en leveranciers kennen diverse functionarissen die binnen de eigen organisatie taken en verantwoordelijkheden hebben op het gebied van cyber security of security in het algemeen. De functionaris die als eerste verantwoordelijk is voor het behandelen en afhandelen van cybersecurity incidenten zijn in deze procedure de sleutelfunctionarissen. Naast de taken en verantwoordelijkheid die sleutelfunctionarissen hebben binnen de eigen organisatie hebben zij de taak om de collega-sleutelfunctionarissen te informeren over dreigende en opgetreden incidenten, over de maatregelen die genomen zijn en hoe hierover gecommuniceerd wordt. Zie bijlage A voor de actuele gegevens van sleutelfunctionarissen. Omdat de sleutelfunctionarissen van GVB Exploitatie en MET/E&B lid zijn van de Cybersecurity Board MET/GVB, wordt de Cybersecurity Board MET/GVB via hen gevoed. De werkgroep security kan in opdracht van de Cybersecurity Board MET/GVB nader onderzoek (laten) verrichten, of met verbetervoorstellen komen.

2.4 Integraal incidentmanagementprocedure cybersecurity

Incidentmanagement is het geheel aan organisatorische, technische en procedurele maatregelen dat ervoor zorgt dat een incident of dreiging van een incident adequaat wordt gedetecteerd, gemeld en behandeld om uitval en de kans op schade of nadelige gevolgen te minimaliseren of te voorkomen.

MET, GVB en leveranciers hebben allen een eigen incidentmanagementprocedure. In voorliggende procedure wordt aan elk van deze organisatiespecifieke procedures gerefereerd. De organisatiespecifieke procedures worden beoordeeld door de Cybersecurity Board MET/GVB.

Opmerking: Van belang is dat we in de keten dezelfde begrippen hanteren; zie hoofdstuk 3.

Minimaal dient de organisatiespecifieke procedure te vermelden:

- wat een cybersecurity incident is;
- wanneer een incident of dreiging moet worden gemeld;
- wie de functionaris is aan wie het incident of de dreiging wordt gemeld en hoe de melding bij de sleutelfunctionaris (zie bijlage A) terecht komt;
- wat de taken van de sleutelfunctionaris zijn, mede in relatie met de Cybersecurity Board MET/GVB.

Deze incidentmanagementprocedure start bij de sleutelfunctionaris van één van de betrokken organisaties die op de hoogte is gesteld van een cybersecurity incident of dreiging daarvan. De sleutelfunctionaris meldt (telefonisch) het incident bij de Cybersecurity Board MET/GVB, informeert zo nodig in acute situaties andere sleutelfunctionarissen en laat het incident registreren in de beveiligde omgeving van de Cybersecurity Board. De secretaris van de Cybersecurity Board MET/GVB houdt de registraties bij. De werkgroep security beoordeelt onder leiding van de voorzitter en in opdracht van de Cybersecurity Board MET/GVB of en hoe (Q&A [9]) hierover namens de Cybersecurity Board MET/GVB gecommuniceerd wordt en/of nader onderzoek noodzakelijk is. De behandeling van de melding is uiteraard strikt vertrouwelijk.

Opmerking: Er is sprake van een meertrapsproces afhankelijk van de soort dreiging en het soort incident, maar in alle gevallen dient het incident of de dreiging te worden gemeld en geregistreerd. Zie ook hoofdstuk 5 Toelichting procedure.

Uitgangspunt is dat de lijnorganisaties en uiteindelijk de directie van MET/E&B eindverantwoordelijk is voor de beveiliging van OT-systemen. Afstemming vindt plaats tussen MET en GVB Exploitatie, omdat GVB Exploitatie verantwoordelijk is voor het gebruik van de OT-systemen en de communicatie hierover. De Cybersecurity Board MET/GVB adviseert.

3 Cybersecurity incidenten

In dit hoofdstuk wordt nader ingegaan op cybersecurity incidenten en dreigingen.

3.1 Hoe definiëren we cybersecurity incidenten?

Een cybersecurityincident van de operationele metrosystemen is een (on)bedoelde (kans of een dreiging op een) inbreuk op de

- a. de vertrouwelijkheid van informatie,
- b. de integriteit van informatie en systeemgedrag,
- c. de betrouwbaarheid van informatie en systeemgedrag.

Mede op basis van de RI&E die op de OT-systemen [12] zijn en worden uitgevoerd kunnen hier voorbeelden worden genoemd, zoals:

- de ontruim- en alarminstallatie van station De Pijp is gesaboteerd door een hack-aanval, waardoor de installatie niet werkt of moet worden uitgezet;
- een virus is geplaatst op een van de OT-systemen, waardoor het systeem niet meer betrouwbaar functioneert en moet worden uitgezet;
- het treinverkeer moet worden stilgelegd als gevolg van een langdurige externe WIFI-verstoring van het BRN signaal;
- door een hack zijn live camerabeelden van het perron van station Rokin te zien op internet.

De handleiding van NCSC beschrijft cybercrime in termen van diefstal van gegevens, identiteitsdiefstal, onbevoegde beïnvloeding, verstoringen en manipulatie gericht op het belemmeren, aanpassen of verstoren van een bedrijfsproces. Voorbeelden van cybercrime in enge zin zijn:

- het ongeoorloofd toegang verschaffen tot een geautomatiseerd systeem;
- het ongeoorloofd verwijderen of aanpassen van computergegevens;
- het ongeoorloofd uitschakelen of onbruikbaar maken van systemen;
- het versturen van computervirussen;
- het onderscheppen en/of veranderen van computerberichten.

Een cybersecurity-incident leiden tot schending van de privacy, maar er zijn ook andere oorzaken denkbaar, zoals kapotte apparatuur of menselijk falen anders dan intentioneel. Dat geldt trouwens ook voor veiligheid en beschikbaarheid. Niet al het falen moet gekenmerkt worden als een cybersecurity incident. Uitgangspunt is dat ergens in de keten van handelingen leidend tot een incident sprake is van intentioneel handelen, zoals het fabriceren van een virus. Elke schending van de privacy, elke onveilige gebeurtenis en ook elke verstoring van de dienstregeling moet worden onderzocht, maar niet allemaal vanuit het oogpunt van cybersecurity.

Bijvoorbeeld het per ongeluk delen van camerabeelden, foto- of filmmateriaal is geen onderwerp voor cybersecurity, maar wel voor privacy (Algemene verordening gegevensbescherming). Het onbewust verspreiden van computervirussen is wel een cybersecurity onderwerp, dat door de sleutelfunctionaris moet worden behandeld.

3.2 Wanneer is sprake van een cybersecurity dreiging?

Er is sprake van een dreiging als bekend is of wordt gemaakt dat een cybersecurity incident zal of zou kunnen optreden met OT-systemen met effect op de bedrijfswaarden (imago, fysieke veiligheid, beschikbaarheid, sociale veiligheid, privacy, kosten, toegankelijkheid, reizigersinformatie en milieu). Het gewicht van de dreiging is afhankelijk van de termijn dat de dreiging manifest wordt, de mate waarin beveiligingsmaatregelen nog intact zijn (de actuele kwetsbaarheid) en de ernst van het potentiële incident in termen van de bedrijfswaarden.

Opmerking: Inbreken in een technische ruimte is op zichzelf geen cybersecurity incident, maar kan wel gezien worden als een dreiging indien in die ruimte OT-systemen geïnstalleerd zijn. Een afwijkende afloop van een toegangsprocedure, wijzigingsprocedure, een backupprocedure of een logprocedure kan al een cybersecurity incident zijn.

Mede op basis van de RI&E die op de OT-systemen zijn en worden uitgevoerd kunnen hier voorbeelden worden genoemd, zoals:

- via media is bekend gemaakt dat binnen 1 week de ontruim- en alarminstallatie van station De Pijp wordt gesaboteerd door een hack-aanval;
- een toegangsdeur van een technische ruimte, waar OT-systemen zijn opgesteld, is geforceerd zonder zichtbare schade aan de systemen;
- een laptop van een leverancier, die gebruikt wordt bij werkzaamheden aan OT-systemen, bevat een virus;
- GVB wordt gechanteerd dat op elke maandagochtend gedurende 2 uur het treinverkeer wordt stilgelegd door een langdurige verstoring van het BRN signaal;
- De afdeling communicatie heeft een dreigbrief ontvangen dat live camerabeelden getoond zullen worden op internet.

4 De procedure

1. Het incidentmanagementproces start bij een van de sleutelfunctionarissen die een incident of dreiging zelf constateert of gemeld krijgt van een van zijn collega's van dezelfde organisatie.
Zie de Bijlage A voor de organisatie- en contactgegevens.
Opmerking: Bij een dreiging van buitenaf (bijvoorbeeld de media) kunnen verschillende functionarissen een en dezelfde dreiging constateren.
2. Bij een incident, dus een direct gevaar voor Veiligheid, Beschikbaarheid of Privacy, neemt de desbetreffende sleutelfunctionaris telefonisch contact op met de sleutelfunctionarissen van MET/E&B en GVB.
3. Bij een major incident (te beoordelen door GVB Exploitatie en indien van toepassing aan de hand van de VUS/BOGT criteria) treedt de calamiteitenprocedure [10] van GVB in werking.
4. De desbetreffende sleutelfunctionaris meldt het incident of de dreiging tevens bij de sleutelfunctionaris van de Cybersecurity Board MET/GVB. Zie de Bijlage A voor de contactgegevens.
5. De secretaris van de Cybersecurity Board MET/GVB registreert de melding en legt bij de registratie vast:
 - a. Datum en tijdstip van de melding;
 - b. Datum en tijdstip van de constatering;
 - c. Korte beschrijving van het incident of de dreiging;
 - d. Datum en tijdstip aangifte (indien van toepassing);
Opmerking: NCSC adviseert om in geval van cybercrime altijd aangifte te doen. Schakel voor strafrechtelijke procedures direct de autoriteiten (politie) in. Bij twijfel kunt u deskundige hulp inschakelen, bijvoorbeeld van een beveiligingsadviesbureau of een particulier recherchebureau, om het onderzoek te begeleiden of het beveiligingsincident op te volgen. Zie ook punt 9 hieronder.
 - e. Actuele stand van zaken op het moment van de melding:
 - i. waaronder genomen acties en actoren;
 - ii. en nog te nemen acties en actiehouders;
 - f. De initiële sleutelfunctionaris in beginsel is dat de sleutelfunctionaris die de melding heeft gedaan.
6. De secretaris informeert de overige betrokken sleutelfunctionarissen dat een melding heeft plaatsgevonden. Dat kan een Share-board-melding zijn, maar in acute situaties is telefonisch overleg ook mogelijk.
7. De voorzitter van de werkgroep Security bepaalt in overleg met de leden van de werkgroep en de overige sleutelfunctionaris(en) en op basis van bestaande RI&E-resultaten (impact classificatie) van het OT-systeem de urgentie van de melding (dreiging).
8. Afhankelijk van de urgentie en reeds genomen maatregelen worden – als dat al niet eerder is gebeurd - operationele beheerders geïnformeerd en geadviseerd met betrekking tot het nemen van (acute) mitigerende maatregelen.
9. Als besloten is dat nader of aanvullend onderzoek noodzakelijk is, wordt door de werkgroep en samen met de initiële sleutelfunctionaris documentatie en bewijsmateriaal verzameld.
10. Indien een vermoeden van malversatie is vastgesteld, wordt het verzamelen van forensisch bewijs in gang gezet door de sleutelfunctionaris van MET/E&B.
11. Binnen de werkgroep, de Cybersecurity Board MET/GVB en samen met de andere sleutelfunctionarissen wordt de communicatie over de melding afgestemd (Q&A [9]).
12. De voorzitter van de werkgroep rapporteert na afronding van het onderzoek de resultaten en het advies voor eventuele verbetermaatregelen aan de Cybersecurity Board MET/GVB en de initiële sleutelfunctionaris.

5 Toelichting op de procedure

Deze procedure begint bij de situatie dat een incident, dan wel dreiging bekend is bij een sleutelfunctionaris. Deze procedure maakt geen onderscheid tussen minor en major incidenten. In alle gevallen dient een incident of dreiging te worden gemeld.

Taken en verantwoordelijkheden die hieraan voorafgaan of geen directe relatie hebben met de Cybersecurity Board MET/GVB staan beschreven in organisatiespecifieke procedures [2], [3], [5], [6], [7] en [8].

Bijvoorbeeld:

1. Afspraak is dat een MET-medewerker de sleutelfunctionaris van MET informeert en een GVB medewerker de sleutelfunctionaris van GVB. Zo ook de medewerkers van leveranciers zullen hun eigen sleutelfunctionaris moeten informeren.
2. Een sleutelfunctionaris zorgt binnen de eigen organisatie voor een achterwacht of vervanging bij afwezigheid. Dit staat beschreven in de organisatiespecifieke procedure.
3. Een sleutelfunctionaris zorgt binnen de eigen organisatie dat de procedure bij alle medewerkers van de organisatie bekend is: de medewerkers zijn alert op bewuste en onbewuste onregelmatigheden die kunnen leiden tot een cybersecurity incident en weten hoe zij een incident na constatering moeten melden aan de sleutelfunctionaris. Dit staat beschreven in de organisatiespecifieke procedure.
4. Als sprake is van een datalek met privacygevoelige informatie, dan zal in de organisatiespecifieke procedure opgenomen zijn dat de melding moet worden geregistreerd via Topdesk-C en doorgezet naar de Privacy Officer van het cluster waar Metro en Tram onder valt. Zie de betrokken procedure van de gemeente Amsterdam.
5. Als een dreiging of incident betrekking heeft op de systemen van Communicatie Centrum Vervoer (CCV), dan zal het aanspreekpunt de sleutelfunctionaris van GVB zijn. Overleg zal dan al plaatsvinden met desbetreffende leveranciers voordat het incident bij de secretaris van de Cybersecurity Board MET/GVB gemeld wordt. Het is in dit geval (hoge classificatie) de verantwoordelijkheid van GVB om een quick respons team in te stellen.

Differentiatie naar privacy, veiligheid en beschikbaarheid

Omdat aparte afspraken en procedures worden gevolgd met betrekking tot privacy-incidenten zal (om dubbel werk te voorkomen) onderzoek door de werkgroep naar incidenten en dreiging voornamelijk zo niet enkel en alleen te maken hebben met Veiligheid van reizigers en personeel in de breedste zin van het woord en Beschikbaarheid van het Metro- en Tramsysteem.

Meertrapsproces

Bij het optreden van een incident of dreiging wordt het onderzoek en de afhandeling tot en met rapportage gezien als een meertrapsproces, afhankelijk van de soort, de ernst en de urgentie:

1. Het incident of de dreiging is gesignaleerd en wordt zelfstandig opgelost door een van de sleutelfunctionarissen van de verschillende organisatie in de keten. De Cybersecurity Board

MET/GVB wordt (in ieder geval) achteraf geïnformeerd. Van belang is onderscheid te maken tussen veiligheid, beschikbaarheid en privacy. Bij twijfel is van belang zo spoedig mogelijk de bevindingen te delen met de andere sleutelfunctionarissen.

2. Indien het incident niet zelfstandig opgelost kan worden, of de dreiging kan niet zelfstandig worden weggenomen door de sleutelfunctionaris en zijn eigen organisatie, dan zoekt de sleutelfunctionaris hulp bij een of meer andere sleutelfunctionarissen. Gelijktijdig wordt het incident of de dreiging gemeld bij en geregistreerd door de secretaris van de Cybersecurity Board MET/GVB.
3. De werkgroep onderzoekt alle geregistreerde incidenten en evalueert de afhandeling van incidenten en dreigingen nadat Cybersecurity Board MET/GVB geïnformeerd is. De diepgang is afhankelijk van de ernst van het incident in termen van bedrijfswaarden en de waarschijnlijkheid van optreden bij een dreiging overeenkomstig de RI&E van het desbetreffende OT-systeem.
4. De werkgroep rapporteert aan de Cybersecurity Board MET/GVB en de Cybersecurity Board MET/GVB besluit over het te geven advies aan de directies m.b.t. vervolgacties, verbeterpunten en communicatie hierover.

6. Referenties

- [1] Charter Security-organisatie Metro en Tram & GVB, CEB/OVG/19094
- [2] Incidentmanagementprocedure MET, CEB/OVG/18784
- [3] Incidentmanagementprocedure GVB Exploitatie
- [4] Incidentmanagementprocedure GVB RS (nog in te vullen)
- [5] Incidentmanagementprocedure Alstom (nog in te vullen)
- [6] Incidentmanagementprocedure Siemens (nog in te vullen)
- [7] Incidentmanagementprocedure Thales (nog in te vullen)
- [8] Incidentmanagementprocedure VSB (nog in te vullen)
- [9] Q&A voor pers/media omtrent cybersecurity incidenten, Join: CEB/OVG/18784
- [10] Noodplan Calamiteitenbestrijding Metrosysteem Amsterdam versie 3.2
- [11] Hoofddocument van het ISMS: Doel, Scope en Beleid CyberSecurity van de OT van metro en tram, SI/OVG05274.
- [12] ‘Operational technology’ (OT) betreffen de operationele ICT-systemen van metro en tram, zoals CBI, ICS, NMA, CTS etc