Provincie Noord-Holland

1632704

Het leveren en plaatsen van observatiecamera's bij verkeersregelinstallaties

Bijlage 7.3 Cyber security eisen

Revisie: 1.0
Datum: 7 april 2022

Inhoudsopgave

1. Algemeen

Voor de invulling van de Cybersecurity eisen voor camerasystemen die staan opgesteld aan de veldzijde, op een kruispunt of langs een wegkant, volgt Provincie Noord-Holland de aanpak van Rijkswaterstaat zoals uitgewerkt in de Cybersecurity Implementatie Richtlijn (CSIR).

Voor alle camerasystemen hanteert provincie Noord-Holland weerstandsniveau 1. Hieronder zijn deze maatregelen verzameld uit de CSIR versie 1.4 (PNH versie 2016).

Daarbij gelden de volgende uitganspunten:

- 'lokale objectdatanetwerk' moet gelezen worden als het netwerk in (en om) de verkeerskast, dat verschillende lokale componenten (o.a. camera) verbindt. Daarnaast is de verkeerskast verbonden met een verkeerscentrale.
- 'ondersteunde ICT systemen', hiermee worden alle ICT middelen bedoeld, die worden ingezet voor systeemontwikkeling en/of -beheer.
- 'Hulppersonen' zijn alle medewerkers (in- en extern) die vanuit hun taken fysieke of logische toegang hebben tot camerasystemen.

Bron van de eisen:

- De in dit document genoemde eisen komen voort uit: "CSIR – versie 2016/PNH"

2. Fysieke toegangsbeveiliging

Aspect:	**Eistekst**
Toegangsbeheer	Toegang middels een fysieke sleutel (voor normering zie Bouwkundige maatregelen).
Bouwkundige maatregelen	B1 Hang- en sluitwerk met een inbraakwerendheid van 3 minuten volgens BRL3104 of klasse 2 NEN5096.
Compartimentering / Meeneem beperkende Maatregelen	C/M1 Inbraakwerende kast/safe volgens VGW kwalificaties. Of M1 door verankeren, verplaatsen. Of bouwkundig compartiment C1. Alles met inbraakvertraging van 3 minuten.

3. Logische toegang

LTPO1	De Opdrachtgever heeft het recht om controles uit te voeren op de naleving van het logische toegangsproces door de Opdrachtnemer.
LTPO3	De toegangsrechten van Hulppersonen dienen jaarlijks beoordeeld en geactualiseerd te worden in een formeel proces.

LTPO5 Bij remote toegang om beheeractiviteiten uit te voeren dient gebruik gemaakt te worden van de diensten die PNH hiervoor beschikbaar stelt.

LTPO6 De logische toegang dient afhankelijk van de classificatie van het object als volgt te worden ingevuld:
- Lokaal bediening en beheer – minimaal een user-id en wachtwoord combinatie met navolging van de wachtwoordrichtlijn
- Remote toegang voor bediening en beheer - ‘two factor’ authenticatie en uitsluitend via de beveiligde voorzieningen van de provincie.

LTT1 De logische toegang tot informatiesystemen en netwerk dient plaats te vinden na het succesvol doorlopen van het identificatie, authenticatie en autorisatieproces (IAA), waarbij de IAA- gegevens voor zover haalbaar in versleutelde vorm worden uitgewisseld en opgeslagen.

LTT2 De toegang tot camerasystemen is geblokkeerd, tenzij het expliciet is toegestaan.

LTT3 Voor bedienaars en beheerders en systemen worden unieke ID’s gehanteerd zodat uitgevoerde handelingen terug te leiden zijn tot een persoon of systeem.

4. Maatregelen Beveiligingsincidenten en incident Response Plan

BIRPT1 De ingebouwde beveiligingsfuncties, controlemechanismen en waarschuwingen die systemen genereren dienen geactiveerd en benut te worden voor registratie en rapportage van beveiligingsincidenten.

5. Maatregelen Netwerkkoppelingen

NKP01 Opdrachtnemer draagt zorg voor en ziet erop toe dat alle netwerkkoppelingen met het lokale objectnetwerk strikt en uitsluitend plaatsvinden via de beveiligde centrale netwerkvoorzieningen en koppelpunten van PNH. Rechtstreekse toegang tot camerasystemen vanuit een publiek netwerk - waaronder het gebruik van internet en e-mail - is verboden.

NKP05 Opdrachtnemer draagt zorg voor en ziet erop toe dat het lokale objectdatanetwerk gehardend is door niet noodzakelijke netwerkservices uit te zetten (voor hardening zie ‘Maatregelen bescherming tegen malware, hardening en patching’).

NKT1 Wanneer configuratie van camerasystemen op afstand plaatsvindt, dient dit altijd over beveiligde verbindingen plaats te vinden. Het gebruik van onveilige communicatieprotocollen zoals FTP, Telnet, VNC en RDP dient vermeden te worden. Indien dit niet haalbaar is, mogen deze enkel gemotiveerd worden ingezet wanneer een additioneel encryptiekanaal wordt toegepast (zoals SSL, TLS of IPSEC).

NKT2 Camerasystemen en besloten (lokale) objectnetwerken mogen geen directe verbindingen hebben met kantoornetwerken.

6. Maatregelen bescherming tegen malware, hardening en patching

MHPP02 Opdrachtnemer dient over een geborgde procedure te beschikken voor het (laten) hardenen van de camerasystemen door:

- niet noodzakelijke datanetwerkservices uit te zetten;
- het verwijderen (patchen) van bekende kwetsbaarheden;
- alle poorten die niet nodig zijn te deactiveren/blokkeren;
- alle default “access points” te verwijderen;
- de default accounts uit te schakelen conform het wachtwoord policy;
- Indien beschikbaar gebruik te maken van de security opties van leveranciers.

MHPPO3 De Opdrachtnemer dient zorg te dragen dat zijn ICT systemen, die gekoppeld worden aan de ICT en IA van Opdrachtgever voorzien zijn van alle recente beveiligingsupdates en patches.

MHPPO8 Opdrachtnemer dient te beschikken over een herstelplan na een besmetting met malware, waaronder alle nodige voorzieningen voor back-up, kopieën van gegevens en programmatuur evenals herstelmaatregelen.

MHPPO10 Opdrachtnemer draagt zorg voor en ziet erop toe dat gegevensdragers, beheer- en onderhoudsapparatuur altijd vooraf op malware gecontroleerd worden voordat deze worden gekoppeld aan de camerasystemen en lokale objectdatanetwerken.

MHPT1 Indien mogelijk dienen camerasystemen zodanig (her)geconfigureerd te worden dat auto-run van USB-tokens, USB harde schijven, mounted network shares of andere removable media niet wordt toegestaan.

7. Maatregelen Logging en Monitoring

LMPO1 De handelingen van medewerkers, beheerders, meldingen vanuit systemen en eventlogs dienen te worden vastgelegd in auditlogbestanden waarbij een logregel minimaal de volgende gegevens bevat:

- de gebeurtenis zelf;
- een tot een natuurlijk persoon herleidbare gebruikersnaam of een (systeem)-ID
- het object waarop de handeling werd uitgevoerd
- het resultaat van de handeling
- de datum en het tijdstip van de gebeurtenis
- optioneel de identiteit van het werkstation of de locatie
- een doorlopende en unieke nummering per logregel.

LMPO2 Opdrachtnemer draagt zorg voor en ziet er op toe dat:

- de loggegevens in een apart bestand worden weggeschreven en opgeslagen die alleen toegankelijk is voor speciaal hiertoe geautoriseerd personeel;
- de logbestanden van bediening- en besturingssystemen, beveiliging en ondersteunende ICT-systemen en –netwerkelementen beschermd worden voor verlies of wijziging;
- van systemen met logvoorzieningen de logbestanden drie maanden bewaard worden;
- loggegevens die gebruikt zijn voor incidentonderzoeken conform de bewaartermijnen die de (feiten)onderzoekers aangeven langer worden bewaard.

LMT2 In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden zoals wachtwoorden, inbelnummers, e.d.

LMT4 De loginstellingen en -bestanden worden zodanig beschermd dat deze niet gewijzigd of gewist kunnen worden door ongeautoriseerden.

8. Maatregelen Bewustwording en Training

<u>Voor alle betrokken medewerkers van opdrachtnemer:</u>

BTME5 Bij het constateren van een security incident dienen Hulppersonen dit direct als een security incident te melden bij de verantwoordelijke objecteigenaar/ -beheerder. Er is sprake van een security incident bij het manifest worden van een (dreigend of reeds opgetreden) security risico als gevolg van een (mogelijke) overtreding van het cybersecurity beleid of onregelmatigheid.

Voorbeelden van security incidenten zijn:

- verlies van dienst, apparatuur of voorzieningen;
- systeemstoringen of overbelasting;
- menselijke fouten die leiden tot functionele verstoring of uitval van systemen;
- inbreuk op fysieke en logische beveiligingsvoorzieningen van het object;
- inbreuk op de bediening en beheer;
- ongeautoriseerde systeemwijzingen;
- niet-naleving van beleid of gedragsregels;
- virusmeldingen;
- verlies of diefstal van bedrijfsmiddelen;
- oneigenlijk gebruik van bevoegdheden;
- vandalisme, moedwillige beschadiging.

BTME8 Hulppersonen gaan zorgvuldig om met de verstrekte persoonsgebonden fysieke toegangsmiddelen voor het object en de (systeem, bedien, technische) ruimten hierbinnen en delen deze niet met collega’s.

BTME9 Hulppersonen creëren geen eigen netwerkkoppelingen op het object en melden dit als een beveiligingsincident als er een zelf aangelegde netwerkkoppeling wordt geconstateerd.

BTME10 Hulppersonen nemen de wachtwoordrichtlijn voor de logische toegang tot camerasystemen in acht.

BTME12 Voor Hulppersonen is toegang tot internet vanaf camerasystemen strikt verboden.

BTME13 Hulppersonen mogen de beschikbaar gestelde toegangsmiddelen (tokens, pasjes) tot camerasystemen en –netwerken alleen gebruiken voor het doel waarvoor ze ontworpen zijn. Hierbij mogen de getroffen beveiligingsmaatregelen niet omzeild worden.

BTME14 Hulppersonen houden hun accountgegevens strikt geheim; zij gebruiken hun account en uitgegeven autorisaties alleen zelf en staan niet toe dat anderen onder hun account kunnen inloggen. Handelingen zijn altijd te herleiden naar de voor dat account geautoriseerde persoon.

BTME15 Hulpersonen dienen op camerasystemen en -netwerken de standaard/default/fabrieks accounts en/of wachtwoorden bij ingebruikname te wijzigen conform de wachtwoordrichtlijn.

BTME17 Ongeautoriseerd aan- of afkoppelen van removable apparatuur of usb-sticks aan het netwerk of camerasystemen is strikt verboden.

BTME18 Alleen geautoriseerde Hulppersonen mogen systemen die voorzien zijn van de laatste security updates, patches en actuele viruscontroleprogrammatuur koppelen aan objectdatanetwerken of camerasystemen.

BTME19 Gegevensdragers worden altijd vooraf op malware gecontroleerd voordat deze worden gekoppeld aan camerasystemen en netwerken.

BTME22 Hulppersonen van Opdrachtnemer zorgen ervoor dat onbeheerde camerasystemen en overige ICT-apparatuur – zo mogelijk - wordt gelocked.

<u>Voor verantwoordelijke managers van opdrachtnemer:</u>

BTMA6 Opdrachtnemer dient bij het constateren van onregelmatigheden in de logische toegang tot camerasystemen uit voorzorg in dergelijke situaties het betreffende account en wachtwoord altijd te laten wijzigen.

BTMA7 De Opdrachtnemer dient zijn Hulppersonen nadrukkelijk te informeren over het feit dat het doorgeven van informatie over de werking, inrichting, organisatie rondom de objecten in welke vorm dan ook NIET zal geschieden dan na uitdrukkelijke toestemming van de Opdrachtgever.

9. Maatregelen gecontroleerd wijzigen

GWPO9 Opdrachtnemer ziet erop toe dat naar aanleiding van een wijziging uitgeschakelde beveiligingsmaatregelen weer zijn geactiveerd alvorens de wijziging te sluiten.

GWT1 Alle CI's met bijbehorende settings/configuraties en de wijzigingen hierop worden geregistreerd in een CMDB.

GWT2 Voor zover beschikbaar wordt gebruik gemaakt van testvoorzieningen.

10. Maatregelen beheer en onderhoud

BOPO4 Opdrachtnemer draagt zorg voor de beschikbaarheid en onderhoud van (technische) beheerdocumentatie, gebruikers- en/of installatiehandleidingen voor de camerasystemen alsmede procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen.

BOT1 Voor de fysieke toegang (ICT-deel) van bedienaars, beheerders en overig ondersteunend personeel zowel van PNH als die van Opdrachtnemer tot objecten en de ruimten hierbinnen wordt gebruikt gemaakt van de producten en diensten van PNH.

BOT2 Voor (remote) logische toegang van bedienaars en beheerders tot het netwerk en camerasystemen wordt gebruikt gemaakt van de producten en diensten van PNH.

11. Maatregelen Back-Ups

BUPO2 De integriteit en beschikbaarheid van de laatste drie versies van de camerasystemen dient gewaarborgd te worden door het maken en testen van back-ups, conform een geborgde procedure:

- systeemimages/back-ups worden gemaakt vooraf en na iedere (functionele) systeemwijziging. Met deze back-up moet men in staat zijn een volledige roll-back naar de werkende situatie terug te kunnen gaan;
- Deze back-ups worden opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade aan de back-up kan worden aangericht als een calamiteit zich voordoet op de locatie waar het camerasysteem zich bevind;
- Back-ups en de ruimte waarin ze zijn opgeslagen behoren fysiek goed te worden beschermd volgens dezelfde normen die gelden voor de hoofdlocatie en zijn alleen toegankelijk voor bevoegden;
- Back-ups worden bewaard tot het moment van uitdienstname van betreffend camerasysteem.