Van: " [redacted] " <[redacted]@politie.nl>
Verzonden: woensdag 4 september 2024 15:31
Aan: " [redacted] " <[redacted]@politie.nl>
Cc: " [redacted] " <[redacted]@gemeentealtena.nl>; " [redacted] " <[redacted]@gemeentealtena.nl>
Onderwerp: FW: Belverzoek
Bijlage(n): (Openbaar) Checklist_leverancier cameratoezicht 151c 1_3.docx

Dag [redacted],

Een poosje terug heb ik al met je gesproken over het feit dat de gemeente Altena bezig is met het netjes regelen van cameratoezicht. Zie voor nu bijgevoegd document. Wil jij contact leggen met [redacted] voor een aantal vragen vanuit hun zijde? Hij is te bereiken op 06[redacted].

Met vriendelijke groet,

[redacted]

0900 – 88 44
[redacted]@politie.nl
Werkdagen: onregelmatig

POLITIE

Eenheid Zeeland West-Brabant | Baronie | Team Dongemond | Cluster Altena
Bureau Nieuwendijk, Doornseweg 2, 4255 GZ, Nieuwendijk
Bureau Oosterhout, Europark 30, 4904 SX, Oosterhout NB
Postbus 8050, 5004 GB Tilburg

Meer informatie? Kijk op politie.nl

Van: [redacted] <[redacted]@gemeentealtena.nl>
Verzonden: woensdag 4 september 2024 16:14
Aan: [redacted] <[redacted]@politie.nl>
CC: [redacted] <[redacted]@gemeentealtena.nl>
Onderwerp: RE: Belverzoek

Hallo [redacted],

Aanvullend op het onderstaande, hierbij het volledig ingevulde formulier door Trigion.

Met vriendelijke groet,

[redacted]
Gemeente Altena
Bibob coördinator & Projectleider Brabantse Norm Weerbare Overheid | Team Veiligheid, Toezicht & Handhaving
Sportlaan 170 | 4286 ET Almkerk
Postbus 5 | 4286 ZG Almkerk

T: 0183 - [redacted]
www.gemeenteAltena.nl

Aanwezig: ma, di, wo, do, vr (bereikbaar)

Van: [redacted]
Verzonden: woensdag 4 september 2024 12:25
Aan: [redacted] <[redacted]@politie.nl>
Onderwerp: Belverzoek

Hallo [redacted],

Wil jij mij even bellen wanneer het jou uitkomt. Ik heb wat vragen over het formulier van de toetsing van het cameratoezicht. Graag stem ik het even telefonisch af t.b.v. de efficiëntie. Bedankt!

Met vriendelijke groet,

[redacted]
Gemeente Altena
Bibob coördinator & Projectleider Brabantse Norm Weerbare Overheid | Team Veiligheid, Toezicht & Handhaving
Sportlaan 170 | 4286 ET Almkerk
Postbus 5 | 4286 ZG Almkerk

T: 0183 - [redacted]
www.gemeenteAltena.nl

Aanwezig: ma, di, wo, do, vr (bereikbaar)

Checklist Leverancier

[

Veilige implementatie Cameratoezicht 151C Gemeentewet

Sector Informatiebeveiliging

Volgnr: ***2023-11-29 –1.3***

Welke beveiligingseisen toe te passen bij de inrichting van Cameratoezicht 151C

Cameratoezicht 151C

Gemeenten hebben de mogelijkheid om cameratoezicht in te zetten om de openbare orde te handhaven. Bijvoorbeeld in uitgaansgebieden, rond voetbalstadions en treinstations. De mogelijkheden hiervoor zijn geregeld in artikel 151c van de Gemeentewet. Cameratoezicht op grond van 151c heeft als eerste een signalerende functie en mogen alleen toezichthouden op openbare plaatsen en andere bij verordening aan te wijzen plaatsen (artikel 151c lid 1). Voor iedereen moet duidelijk zijn dat gemonitord wordt met camera's. Met behulp van de camerabeelden kunnen de politie en andere hulpdiensten op straat worden aangestuurd, met het doel het handhaven van de openbare orde. Maar in geval van een concrete aanleiding mogen de beelden (indien dit noodzakelijk is) ook worden gebruikt om een strafbaar feit op te sporen.

Terminologie

Er is een verscheidenheid in de organisatie, inrichting en naamgeving van cameratoezicht 151c. Daarbij worden termen als "Gemeentelijk cameratoezicht", "Cameratoezicht centrum", "Openbare orde cameratoezicht" of "Veiligheid cameratoezicht" gebruikt.

Verwerkingsverantwoordelijk

De Gemeentewet stelt dat de verwerking van de camerabeelden t.b.v. 151c valt onder de Wet Politiegegevens (Wpg). Daarmee is niet de burgemeester maar de (korpschef van de) politie de verwerkingsverantwoordelijke.

Eisen verwerking

De verwerking van gegevens uit cameratoezicht 151c moet voldoen aan alle eisen die in de Wpg worden gesteld aan de verwerking van politiegegevens. Als deze gegevens een hoog privacy risico opleveren, dient een GEB uitgevoerd te worden. De gegevens moeten worden beschermd door passende technische en organisatorische maatregelen, afgestemd op het risico van ongeoorloofde of onrechtmatige verwerking en van opzettelijk verlies, vernietiging of beschadiging van politiegegevens. Zie ook maatregelen en eisen genoemd in de Baseline Informatiebeveiliging Overheid (BIO), de Addendum BIO politie en de maatregelen van de top 8 van het Nationaal Cybersecurity Center (NCSC).

Checklist Informatiebeveiliging

Om te bepalen welke beveiligingseisen van toepassing zijn is de checklist Cameratoezicht 151C opgesteld, zie daarvoor bijlage 1:

- Stel in samenwerking met de ICT-leverancier/projectleider een rapportage op die inzicht geeft in de huidige maatregelen rekening houdend met de genoemde dreigingen/eisen;
- Stem de rapportage af met de sector Informatiebeveiliging via de informatiebeveiligingsliaison van de eenheid.

Pentest/audit

Neem in het contract met de ICT-leverancier de eis op dat de politie het recht heeft op het uitvoeren van een pentest en of audit.

Vragen?

Bij vragen over deze checklist of een andere vraag over informatiebeveiliging kunt u contact opnemen met uw contactpersoon binnen de politie.

Bijlage 1: Checklist informatiebeveiliging Cameratoezicht Gemeentewet 151C

Onderwerp	Beveiligingseis	Wettelijk kader	Bevindingen + maatregelen
Camera (Leverancier)	1. Camera is geïsoleerd in beveiligd en apart netwerk/VLAN 2. Inregelen patchproces 3. Hardening wordt toegepast 4. Camera's zijn beschermd tegen onbevoegde toegang 5. Bij MCU wordt data SD-card na einde inzet gewist	BIO 11.1.4.2,11.2.4 / WPG BPG Art 6:1a	1. Ja, er worden routers geleverd met VPN verbinding. Alle aangeboden apparatuur zit in hetzelfde beveiligde netwerk. 2. Ja, is aanwezig dient te worden vastgelegd in SLA. 3. Ja. 4. Montage buiten bereik en alle camera's zijn voorzien van detectie van afscherming en vandalisme. 5. Dit dient door gebruiker te worden uitgevoerd of door Trigion vastgelegd in SLA.
	1. **Camera's** zijn fysiek beschermd en voldoen aan beschikbaarheidseisen 2. Beschikbaarheidseisen zijn in SLA vastgelegd	BIO 11.2	1. Camera's zijn type IK10 en geplaatst buiten normaal bereik. Tevens is er detectie op afdekken en vandalisme aanwezig op elke camera. 2. ?
	Aanvullende maatregelen ten aanzien van ICT-systemen uit landen waarvan is vastgesteld dat zij een offensief cyberprogramma tegen Nederland voeren	BIO 12.6, 13.1	Niet van toepassing, apparatuur is van Axis (Zweeds leverancier en producent) bovendien bevat het een Trusted Platform Module (TPM) die FIPS 140-2 level 2 gecertificeerd is.
	Beeldmateriaal is van goede kwaliteit zoals contractueel is vastgelegd	BIO 15.1.	Alle camera's zijn 4K UHD-resolutie. Het beschikt over IR-verlichting en dag/nacht-functionaliteit voor bewaking in pikkedonker. Met een ingebouwde laser, 31x optische zoom.
Leverancier	Er mag geen Wpg data op een externe commerciële hostingsite geplaatst worden. Bovendien moeten eventuele sub-leveranciers aan dezelfde eisen voldoen als de hoofdleverancier en de hoofdleverancier is hiervoor verantwoordelijk.	WPG, BIO 9, 15.1	Eigenlijk is de installateur of IT-er verantwoordelijk omdat zij verantwoordelijk zijn voor de hiërarchie van het netwerk. De Axis camera's bieden de keuze om gebruik te maken van het IP-adres, Hostname (Met en zonder DNS ondersteuning), My-Axis P2P of 3e partij oplossingen. Bij het gebruik van het IP-adres of Hostname tussen de camera en VMS, is er absoluut geen data die het Subnet of Vlan verlaat. Omdat Axis en ADI de configuratie niet uitvoeren, kan er geen verantwoording door deze partijen genomen worden.
	Procedurele afspraken worden m.b.t. screening, geheimhoudingsverklaring, logfiles van beheerders worden volgens contractkaders vastgelegd.	WPG, BPG Art 6:1a	- Screening is een administratieve actie. Uitvoering hiervan via software of documentatie wordt bepaald door de keuzen door de klant en de producten. Axis en ADI hebben hier geen oplossing voor. - Geheimhouding: Het akkoord voor geheimhouding ontstaat door ondertekening van formulieren, contracten of andere documentatie. Wanneer taken uitgevoerd worden door de betrokken partijen zullen deze ondertekend worden.

			Deze aanvraag valt voor ADI onder de AVG/GDPR en is alleen in te zien door betrokken personeel van ADI. Gezien de contractkaders niet in de aanvraag zijn gespecificeerd. Daardoor kunnen wij dit niet bevestigen. Wel kan ik aangeven, dat de klant zelf kan bepalen wie op welke manier toegang tot de verschillende logs kunnen krijgen. * Windows logs en applicatie logs: Systeem beheer inlog in Windows op de server of Active Directory. VMS logs zijn afhankelijk van de gekozen toepassing. Deze is niet genoemd in de aanvraag en kan hierdoor niet beantwoord worden. Camera logs zijn beveiligd achter de camera login. Welke wordt bepaald door de graad van Authenticatie beveiliging en Hardening
	De producten zijn getest op cyberaanvallen en geaccrediteerd. Aanvullende maatregelen ten aanzien van ICT-systemen uit landen waarvan is vastgesteld dat zij een offensief cyberprogramma tegen Nederland voeren	BIO 12.6, BPG Art 6:1a	Ja, en periodiek wordt deze test herhaald.
	1. Beheer en onderhoudsafspraken zijn in SLA vastgelegd 2. Na onderhoud controle hardening	BIO 15.1	1. Ja, akkoord 2. Akkoord
	1. Remote beheer mag alleen via een beveiligde verbinding plaats vinden en geen gebruik maken van het politienetwerk. 2. Remote beheer moet beperkt blijven tot beheerwerkzaamheden 3. Remote beheer mag zich geen toegang verschaffen tot live- of opgenomen camerabeelden.	BIO 9, 15.1	1. Akkord. Kan worden ingesteld, alleen vanaf RSA-afdeling Trigion. 2. Akkoord. Wordt vastgelegd in SLA en middels autorisatie afgebakend. 3. Akkoord. Zie antwoord 2.
Onderwerp	**Beveiligingseis**	**Wettelijk kader**	**Bevindingen + maatregelen**
Verbindingen (Leverancier)	Communicatieverkeer is beveiligd en versleuteld	BIO 8.3, 14.1	Ja
	Manipulatie/wijzigen dataverkeer / Communicatieverkeer is beveiligd en versleuteld	BIO 13.1	Ja
	Authenticatie en registratie van apparatuur	BIO 9.1.2.1	Ja
	1 Inregelen patchproces software en hardware	BIO 12.6	Akkoord, vastleggen in SLA.

	2 Inregelen hardening software		
	De beschikbaarheidseisen zijn in een SLA vastgelegd.	BIO 15.1	Akkoord
Server (Leverancier)	Als de server in de ICT omgeving van de gemeente staat (b.v. in het gemeentehuis) dan is het beleid van fysieke toegang van de gemeente van toepassing. Als de server voor cameratoezicht extern is opgeslagen, is de leverancier contractueel verplicht dat de server in de serverruimte aantoonbaar logisch en fysiek beveiligd is.	BIO 11.1	Uitgangspunt is plaatsing server op locatie gemeente.
	Logging op fysieke toegang tot de serverruimte en logische toegang tot de server is ingeregeld en opvraagbaar.	BIO 9.4, BPG Art 6:1a	Verantwoordelijkheid gemeente.
	Toegang wordt geregeld via authenticatie en autorisatie	BIO 9.4, BPG Art 6:1a	Akkoord
	Kwetsbaarheden worden niet aangepakt 1. Inregelen patchproces sotware en hardware 2. Inregelen hardening software	BIO 12.6, 15.1	1. Akkoord, vastleggen in SLA. 2. Akkoord, vastleggen in SLA
	Uitval apparatuur (storingen, nutsvoorzieningen, zwakke componenten). De status van de ICT-Infrastructuur Infrastructuur is verouderd of niet up to date. Beschikbaarheidseisen zijn in SLA vastgelegd.	BIO 11.2, 15.1	Aangeboden decentrale apparatuur is voorzien van UPS, server op locatie gemeente dient door gemeente te worden voorzien van noodstroomvoorziening. Aanname dat de serverruimte gemeente is voorzien van UPS.
	Ontbreken bescherming malware Beheersmaatregelen tegen malware implementeren	BIO 12.2, 15.1	Eigen VPN-netwerk risico's laag
	DDoS-aanval DDoS mitigatieoplossing is aanwezig	BIO 13.1	
Onderwerp	**Beveiligingseis**	**Wettelijk kader**	**Bevindingen + maatregelen**
Opslag gegevens (Leverancier)	Gegevens worden versleuteld opgeslagen		
	1. Backup afspraken met operatie die in verhouding staan met de noodzakelijke beschikbaarheid. 2. Afspraken in SLA vastleggen	BIO 12.1, 15.1	1. Akkoord, wens gemeente is leidend 2. Akkoord
	Bij opslag beelden lokaal op de camera, worden deze vernietigd zodra cameratoezicht wordt stopgezet.	BIO 8.3	Akkoord, vastleggen in SLA
Software	Software anders dan door leverancier ondersteund kan worden geïnstalleerd. Software van derden kan niet	BIO 12.5.1	Het ROOT account van AXIS camera's kan niet gedeactiveerd of

(Leverancier)	zelfstandig door gebruikers worden geïnstalleerd		vervangen worden. Firmware upgrades kunnen alleen via die account uitgevoerd worden. Axis heeft het deactiveren van dit account op firmware niveau geblokkeerd. Axis verwacht dat bij het opstarten van hun devices een nieuw wachtwoord ingevoerd wordt. Hiervoor verschijnt dan ook in de web interface de functie voor. Het is aan de installateur of beheerder op dat moment om te bepalen welk wachtwoord toegekend wordt. De Axis camera's ondersteunen HTTPS en Radius oplossingen. Hierdoor heeft de klant zelf de keuze om de graad van beveiliging te bepalen.
	Kwetsbaarheden in software 1. Inregelen patchproces software 2. Inregelen hardening software	BIO 12.6	1. Akkoord, vastleggen in SLA. 2. Akkoord, vastleggen in SLA
Personeel (Leverancier)	Ontbreken autorisatieproces, geen beheer op beheer-accounts, autorisatieprofielen ontbreken. 1. Autorisatieproces en profielen zijn vastgelegd, rekening houdend met functiescheiding 2. Autorisaties worden periodiek gecontroleerd 3. Maak gebruik van het modelcontract m.b.t. beheerregeling	WPG art.6, BIO 9.2, BPG Art 6:1a	1. Akkoord, inrichten bij installatie na vooraf overleg. 2. Akkoord, vastleggen in SLA 3. Akkoord.
	Betrouwbaarheid extern personeel wordt niet vastgesteld. 1. Geldig VOG overleggen en leg dit vast bij de aanstellingseisen. 2. Geheimhoudingsverklaring wordt getekend 3. Controleer inhuurcontracten en een actuele lijst met namen van geautoriseerde personen zodat het traceren en aanspreken van medewerkers mogelijk is.	BIO 7.1	1. Alle medewerkers van Trigion in binnen- en buitendienst zijn in het bezit van een geldig VOG. Wordt door HR up-to-date gehouden. 2. Akkoord. 3. Er wordt geen gebruik gemaakt van extern personeel. Alleen vooraf aangemelde personen van Trigion zullen werkzaam zijn op dit project. Bestaande uit een projectteam
	Menselijke factor: bewust/ onbewust handelen tegen regels in. 1. Inzet van personeel (camera-operateurs) met de juiste wettelijke vakbekwaamheidseisen gesteld in de Regeling Beveiligingsorganisaties & particuliere recherchebureaus 2. Loggingsproces is ingeregeld	BIO 7.2, BPG Art 6:1a	1. Akkoord, onze mensen zijn vakkundig en gedegen opgeleid. 2. Worst aan de voorkant besproken en vastgelegd.

Begrippen:

Hardening: het aanpassen van veiligheidsconfiguraties om risico's te verkleinen door veilige instellingen te kiezen. Het gaat hierbij onder andere om:

- Het uitschakelen of verwijderen van overbodige functies en gebruikersaccounts.
- Het toekennen van veilige waarden aan beveiligingsinstellingen.
- Het wijzigen van standaard wachtwoorden op systemen.

Patchproces: het patchproces bestaat uit een aantal stappen:

- Het inventariseren of documenteren van welke systemen welke software draaien.
- Het in de gaten houden van nieuwe lekken in software en beschikbare patches van geïnventariseerde systemen.
- Als een lek wordt ontdekt, dan is er een vast proces om te patchen (testen, plannen, distribueren en implementatie)
- De laatste stap bestaat uit het volgen en vastleggen van een eventuele nieuwe patches.

Malware: is elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot (private) computersystemen.

DDos: met een (Distributed) Denial-of-Service aanval (DDos-aanval wordt de capaciteit van onlinediensten of de ondersteunende servers en netwerkapparatuur aangevallen. Het resultaat van deze aanval is dat diensten slecht of helemaal niet meer bereikbaar zijn voor medewerkers of klanten. In de praktijk krijgt de getroffen server tijdens een DDos-aanval enorm veel verzoeken vanaf meerdere computers tegelijk te verwerken. Daardoor wordt het netwerkverkeer van en naar de website geblokkeerd en kan zelfs de server van de dienst crashen of down gaan.

IoT: Het Internet of Things (IoT) is het netwerk van fysieke objecten of "dingen", waarin sensoren, software en andere technologieën zijn ingebouwd om ze met internet te verbinden en gegevens uit te wisselen met andere apparaten en systemen.

Man in the middle: Een **man-in-the-middle-aanval** (MITM-aanval) of **person-in-the-middle-aanval** (PITM-aanval) is een aanval waarbij informatie tussen twee communicerende partijen onderschept wordt zonder dat beide partijen daar weet van hebben. Hierbij bevindt de computer van de aanvaller zich tussen de twee communicerende partijen. De berichten kunnen daarbij mogelijk gelezen en veranderd worden. Ook kunnen berichten worden verzonden die niet door de andere partij zijn geschreven. De naam van de aanval verwijst naar de derde persoon die in het midden tussen de twee partijen *staat* en de langskomende berichten bekijkt en aanpast.

MCU: Mobiele Camera Unit

Pentest: Een pentest is een test waarbij ethical hackers systemen onderzoeken op kwetsbaarheden. De ethical hackers proberen op verscheidene manieren zwakke plekken in systemen aan het licht te brengen. Door een combinatie van geautomatiseerde tooling en creativiteit trachten de ethical hackers ongeautoriseerd toegang tot krijgen tot informatie en/of systemen. Een pentest vindt altijd plaats in opdracht en met toestemming van de eigenaren van de systemen die getest worden. Als er geen vrijwaringsverklaring, is er namelijk sprake van computervredebreuk.

Toelichting grondslagen

In dit document kunt u secties vinden die onleesbaar zijn gemaakt. Deze informatie is achterwege gelaten op basis van de Wet open overheid (Woo). De letter die hierbij is vermeld correspondeert met de bijbehorende grondslag in onderstaand overzicht.

J Art. 5.1 lid 2 sub e

Het belang van de openbaarmaking van deze informatie weegt niet op tegen het belang van de eerbiediging van de persoonlijke levenssfeer van betrokkenen