Memo

Betreft: **Beleid t.a.v. buitenlandse surveillance (IP-)camera's**

Datum: 28 maart 2022

Door: CISO GVB, Daniel Wunderink
Cybersecurity-officer OT, Wim van Asperen

Status: Vastgesteld door Cybersecurity Board OT op 28 maart 2022

Vertrouwelijkheid: Bedrijfsvertrouwelijk: uitsluitend bestemd voor intern en extern betrokkenen

Samenvatting
De Cybersecurityboard OT sluit het gebruik van (buitenlandse) IP-camera's voor surveillance c.q Camera Ondersteund Toezicht (COT) niet uit, maar schrijft wel stringente beveiligingsmaatregelen voor (ongeacht het land van herkomst) ter bescherming van de eigendommen van GVB en de gemeente Amsterdam en de privacy en de veiligheid van reizigers en personeel.

NB. Deze memo is een aanvulling op het Handboek Cameradekking Metro en Tram (Ref. 2). Dit handboek is en blijft onverkort van toepassing op het gebruik van COT.

Achtergrond
IP-camera's zijn veelal van buitenlandse (zoals Chinese) makelij. Er is een politiek-maatschappelijke discussie over het misbruik van systemen (waaronder camera's) en het weren van producten van niet-westerse afkomst. Fabrikanten zouden (gesteund door overheden) misbruik kunnen maken van 'achterdeurtjes' om informatie weg te sluizen voor spionage-doeleinden. Hoewel die praktijken voorkomen in de wereld, passen die 'hazards' niet in het 'Dreigingsbeeld OT' (ref 3.) dat gebaseerd is op het risicoprofiel van het OV-systeem in Amsterdam. Bovendien (en vooral) kan met passende beveiligingsmaatregelen misbruik worden voorkomen en de privacy (datalekken en gezichtsherkenning) effectief worden beschermd. Het is sowieso beter om goede beveiligingsmaatregelen te treffen in plaats van zekere landen uit te sluiten van levering, om uit voldoende gunstige producten te kunnen kiezen en omdat ook andere (zelfs westerse) landen 'achterdeurtjes' kunnen (laten) creëren die de privacy schenden of misbruik faciliteren. Tenslotte zijn alle (embedded) systemen, waaronder ook camera’s aan kwetsbaarheden onderhevig ongeacht de afkomst. Beter jezelf beschermen (tegen welk misbruik door wie dan ook), dan keuzes uitsluiten.

De beveiligingsmaatregelen
De beveiligingsmaatregelen zijn erop gericht om inkomend verkeer (stuurinformatie en patches inclusief eventuele malware) en uitgaand dataverkeer (camerabeelden) te voorkomen en

eventuele pogingen (toch nog) worden gesignaleerd. Daarnaast dient (eventueel aanwezige gezichts)-herkenningsoftware in de camera(-systemen) te worden verwijderd (of op z'n minst adequaat te worden disabled).

De uitvoerders van deze beveiligingsmaatregelen

Deze beveiligingsmaatregelen zijn in de volgende paragraaf in detail gegeven en hebben betrekking op de volgende actoren.

- Opdrachtgevers en projectmanagers van nieuwe camera-systemen en van uitbreidingen van bestaande camera-systemen
- Beheerders, areaal- en assetmanagers, verantwoordelijk voor het correct aansluiten, beheren en gebruik van de (camera-)systemen en de netwerken waarop de camera's zijn/worden aangesloten
- aan beheerleveranciers van GVB voor het uitvoeren van beheer- en onderhoud van systemen en assets en in het bijzonder van de camera-systemen
- aan beheerleveranciers van GVB voor het uitvoeren van beheer- en onderhoud van netwerk/communicatie-systemen waarop IP-camera-systemen zijn aangesloten.

De beveiligingsmaatregelen in details

- IP-camera's mogen alleen worden aangesloten op een apart onderdeel van een netwerk ('camera-VLAN'), waar geen andere servers (dan de camera-servers) of ander soortige endpoints zijn aangesloten (isolatie/segmentatie)
- IP-camera's en camera-systemen (servers) dienen gehardend te worden/zijn.

    NB. Specifieke hardeningsvoorschriften voor IP-camera's zijn in de maak en worden later (2022) toegevoegd aan dit document. Vooralsnog geldt de algemeen geldende hardeningsvoorschrift van het IBD, InformatieBeveiligingsDienst van de Vereniging van Nederlandse Gemeenten.

- Al het inkomend- en uitgaand verkeer van/naar de camera-VLAN dienen expliciet te worden disabled/uitgesloten.

    NB. Vaak zoekt de software in camera's by-default en periodiek verbinding met de leverancier voor geautomatiseerde nieuwe updates en patches. Ook die geautomatiseerde verbindingen(functies) dienen te worden verwijderd of uitgezet.

- Functies voor object- of gezichtsherkenning in IP-camera's (in software of hardware/‘on the chip’) of in de camera-systemen/servers volledig dienen te worden verwijderd of uitgeschakeld, tenzij voor het gebruik van herkenningssoftware expliciete en schriftelijk toestemming is gegeven door de privacy-office en cybersecurity-office van GVB.

    NB. Dergelijke systemen hebben vaak 'undocumented features' waaronder objectherkenning. Die features dienen - in overleg met de leverancier - gedectecteerd en verwijderd te worden, vooraf aan implementatie. Zie ook bij hardening.

- Voor de railinfra van GVB geldt dat IP-camera's uitsluitend op het NMA mogen worden aangesloten.
- In het camera-VLAN dienen uitgaande of inkomende verkeer te worden disabled.

- In het netwerk dienen pogingen voor uitgaande of inkomende verkeer van en naar camera's te worden gelogd, gedetecteerd en daarover gerapporteerd als events aan de cybersecurity-office van GVB.
- In het netwerk dient het ingaande en uitgaand verkeer te worden matcht tegen de actuele kwetsbaarheids- en dreigingsbronnen (monitoring op basis van threat-intell: vulnerabilities, indicators of compromise en tactics, techniques, and procedures (TTP's)).
- Er dient een vulnerability- en patchmanagement proces te zijn ingericht om patches/upgrades te beoordelen, daarover te beslissen en te (laten) implementeren.
- Patches/updates in camera's en camera-systemen dienen altijd vooraf aan de implementatie te worden gecontroleerd op virussen/malware (reguliere 'wasstraat' met -waar mogelijk- aandacht voor 'achterdeurtjes'). De mogelijkheden voor een ‘wasstraat’ worden op het moment van schrijven onderzocht.

Referenties/bronnen:

1. Memo Camerabewakingsystemen Facilitair Beheer, CISO 9 september 2019
2. Handboek Cameradekking Metro en Tram, 11-1-2011
3. Cyber Dreigingsbeeld OT, 05-01-2021

Versiebeheer:

28 maart 2022 De versie van 15mrt22 is vastgesteld door Cybersecurity Board OT dd 28mrt22
15 maart 2022 Opmerkingen van technisch projectleider NMA (Louis de Wolff) verwerkt.
4 maart 2022 Opmerkingen van CISO GVB (Daniel Wunderink) verwerkt.
3 maart 2022 Eerste versie Cybersecurity Officer OT (Wim van Asperen)