Onderzoeksvoorstel

Kwetsbaarheden in het [IP-cameramodel van bedrijf X]: analyse en proof-of-concept in een retailomgeving.

Bachelorproef, 2025-2026

Emiel Smith

E-mail: emiel.smith@student.hogent.be

Samenvatting

In veel retailomgevingen, waaronder meubel- en zetelwinkels, worden IP-camera's ingezet voor diefstalpreventie, operationeel inzicht en veiligheid. Toch tonen recente rapporten aan dat netwerkcamera's vaak onveilig geconfigureerd zijn en daardoor kwetsbaar zijn voor cyberaanvallen. In deze bachelorproef wordt onderzocht hoe een [IP-cameramodel van bedrijf X] zich gedraagt binnen het interne netwerk van een zetelwinkel, welke kwetsbaarheden aanwezig zijn en hoe deze misbruikt kunnen worden binnen een gecontroleerde testopstelling. Het onderzoek vertrekt vanuit gekende CVE's, een uitgebreide literatuurstudie en een technische analyse van netwerkverkeer en configuratie. Via proof-of-concepttesten worden potentiële aanvalsscenario's nagebootst, waarna beveiligingsmaatregelen worden geformuleerd. Het eindresultaat bestaat uit een praktisch toepasbaar beveiligingsadvies voor de winkel, een kwetsbaarhedenrapport en een reproduceerbare testomgeving. Dit biedt winkelketens, IT-beheerders en security-professionals inzicht in risico's en aanbevelingen om hun cameranetwerk robuuster te beveiligen.

Keuzerichting: System & Network Administrator

Sleutelwoorden: Cybersecurity, IP-camera's, Retail, CVE-analyse, Threat modeling

Inhoudsopgave

1. Introductie

Retailbedrijven maken steeds vaker gebruik van IP-camera's voor beveiliging, analyse van klantenstromen en operationeel beheer. Ook in zetelwinkels is videobewaking ondertussen een essentieel onderdeel van de dagelijkse werking. Deze camera's worden doorgaans aangesloten op het interne netwerk van de winkel, vaak zonder strikte segmentatie of geavanceerde beveiligingsinstellingen. Hierdoor vormen ze een mogelijk toegangs- of escalatiepunt voor aanvallers (Naprys, 2024).

Het [IP-cameramodel van bedrijf X] wordt door de betrokken zetelwinkel ingezet als primair bewakingsmiddel. Vaak blijkt dat configuratie en firmwarebeheer eerder beperkt zijn uitgevoerd bij bedrijven, een situatie die in de literatuur vaak gelinkt wordt aan verhoogde veiligheidsrisico's (AlfredCamera, 2022). De combinatie van retailnetwerken, beperkte IT-ondersteuning en wijdverspreide IoT-apparaten creëert een omgeving waarin zelfs kleine misconfiguraties aanzienlijke impact kunnen hebben.

De centrale probleemstelling luidt dat de winkel een IP-camera gebruikt waarvan niet duidelijk is of deze veilig geconfigureerd is, up-to-date is of correct gesegmenteerd is binnen het netwerk. Indien kwetsbaarheden aanwezig zijn, kan dit leiden tot ongeautoriseerde toegang tot camerabeelden, manipulatie van instellingen of zelfs gebruik van de camera als toegangspunt voor bredere netwerktoegang.

Deze bachelorproef richt zich op IT-professionals, netwerkbeheerders en security-consultants die in een retailcontext verantwoordelijk zijn voor het veilig inzetten van camerabewaking.

Centrale onderzoeksvraag

Welke kwetsbaarheden vertoont het [IP-cameramodel van bedrijf X] binnen de retailomgeving van een zetelwinkel, hoe kunnen deze in een gecontroleerde omgeving worden aangetoond, en welke beveiligingsmaatregelen zijn nodig om misbruik te voorkomen?

Vanuit deze centrale vraag worden volgende deelvragen onderzocht:

- Welke bekende CVE's en risico's bestaan er voor vergelijkbare IP-camera's?
- Hoe communiceert het toestel binnen een retailnetwerk (open poorten, protocollen, standaardinstellingen)?
- Kunnen bekende exploits of misconfiguraties effectief worden misbruikt in een gecontroleerde testomgeving?
- Welke beveiligingsmaatregelen zijn noodzakelijk om de winkelomgeving beter te beschermen?

De doelstelling van dit onderzoek is het opleveren van een onderbouwd beveiligingsadviesrapport op basis van technische analyse, exploitatiepogingen en threat modeling. Daarnaast worden een reproduceerbare proof-of-concept-testomgeving en technische documentatie voorzien, zodat resultaten herhaalbaar zijn binnen dezelfde of gelijkaardige retailomgevingen.

2. State-of-the-art

De beveiliging van netwerkkamera's blijft een actueel onderzoeksdomein, zeker binnen sectoren waarin deze apparaten intensief worden gebruikt, zoals retail. Onderzoeken tonen aan dat IP-camera's vaak kwetsbaarheden bevatten door gebrekkige firmware, zwakke standaardconfiguratie en beperkte beveiligingsfunctionaliteit (Butun et al., 2019). In een winkelomgeving, waar camera's vaak zonder netwerksegmentatie worden geplaatst, vergroot dit risico aanzienlijk.

Recente kwetsbaarheden tonen structurele problemen bij diverse camerafabrikanten. In de literatuur worden verschillende ernstige kwetsbaarheden beschreven, waaronder API-kwetsbaarheden zoals CVE-2024-13130, waarbij configuratiebestanden toegankelijk worden zonder geldige authenticatie. Andere kwetsbaarheden, zoals CVE-2021-33045, tonen aan dat brute-force-aanvallen mogelijk blijven wanneer rate limiting en account lockout ontbreken.

Daarnaast wijzen verschillende bronnen erop dat gebruikers zelden standaardwachtwoorden wijzigen of firmware-updates toepassen (Alfred-Camera, 2022). In een retailcontext, waar dagelijkse operationele druk hoog is en IT-ondersteuning vaak beperkt, wordt deze problematiek nog versterkt. Camera's worden in de praktijk vaak rechtstreeks op het productienetwerk aangesloten, samen met kassasystemen, kantoorpc's en andere kritieke systemen.

Onderzoek naar IoT-beveiliging toont aan dat apparaten zoals IP-camera's vaak minimale beveiliging implementeren, beperkte rekenkracht hebben en afhankelijk zijn van correcte configuratie door de eindgebruiker (Butun et al., 2019). Hierdoor zijn zij gevoelig voor aanvallen zoals:

- credential stuffing en brute force op inlogginterfaces;
- sniffing van ongeëncrypteerde videostreams (bijvoorbeeld RTSP zonder TLS);
- misbruik van debuginterfaces of verborgen API-endpoints;
- firmware-manipulatie of analyse op zoek naar backdoors.

Binnen de literatuur ligt de focus vaak op brede productlijnen of meerdere merken tegelijk. Er is echter een duidelijke tekort in onderzoek dat zich specifiek richt op één camera gebruikt in een reële retailomgeving, met een concrete casus en aanbevelingen op maat van die omgeving. Deze bachelorproef probeert dat gat te vullen door het [IP-cameramodel van bedrijf X] centraal te stellen in een zetelwinkelcontext.

3. Methodologie

Het onderzoek wordt uitgevoerd in vijf iteratieve sprints van telkens tien dagen. Elke sprint levert concrete deliverables op die als input dienen voor de volgende fases. De aanpak is daar-

door adaptief en laat toe om tussentijdse inzichten snel te verwerken.

Sprint 1: literatuurstudie en CVE-inventaris

In de eerste sprint wordt een gestructureerd overzicht opgebouwd van alle publiek gedocumenteerde kwetsbaarheden die relevant zijn voor het type IP-camera dat in de zetelwinkel wordt gebruikt, aangevuld met informatie over vergelijkbare modellen. Hiervoor worden onder meer de NVD-database, vakartikels en securityblogs geraadpleegd. Elke vondst krijgt een plek in een tabel met onder andere:

- CVE-identificatie;
- CVSS-score;
- type aanval (bijv. authenticatie-omzeiling, remote code execution, informatielek);
- vereiste toegangsrechten;
- potentiële impact in een retailomgeving.

De sprint wordt afgerond met een risico-matrix die per kwetsbaarheid de impact en de exploitatiemoeilijkheid weergeeft, toegespitst op de winkelcontext.

Sprint 2: analyse winkelomgeving en opzetten testlab

Parallel aan de literatuurstudie wordt de huidige situatie in de zetelwinkel in kaart gebracht:

- netwerktopologie: plaats van de camera ten opzichte van andere systemen (kassa's, kantoor, guest Wi-Fi);
- gebruikte protocollen: HTTP/HTTPS, RTSP, ONVIF, eventuele cloudkoppelingen;
- huidige configuratie: gebruikersaccounts, wachtwoordenbeleid, firmwareversie, loginstellingen.

Op basis hiervan wordt een gecontroleerde testomgeving opgezet die de winkelconfiguratie zo goed mogelijk benadert, maar volledig afgescheiden is van het productienetwerk. Deze labomgeving bevat onder andere:

- een fysiek exemplaar van het [IP-cameramodel van bedrijf X];
- een virtuele Kali Linux-aanvalsmachine;
- een management-VM voor configuratie en logging;
- netwerkmonitoring met Wireshark;
- documentatie van VLAN's en firewallregels die de winkelsetup simuleren.

De deliverable van deze sprint is een gedetailleerd netwerkschema van zowel de reële winkelomgeving als de testlabconfiguratie, inclusief motivering van eventuele vereenvoudigingen.

Sprint 3: proof-of-conceptexploitatie en logging

In de derde sprint worden de belangrijkste kwetsbaarheden uit de CVE-inventaris en de geobserveerde configuratie getest in de labomgeving. De nadruk ligt op aanvallen die in de praktijk relevant zijn voor retail, zoals:

- brute-force- of credential-stuffingaanvallen op de webinterface van de camera;
- misbruik van onbeschermde of zwak beschermde API-endpoints;
- sniffing van videostreams op zoek naar ongeëncrypteerde data;
- misbruik van te ruime netwerktoegang (bijvoorbeeld toegang vanaf guest-netwerk).

Elke test wordt uitgebreid gelogd:

- PCAP-bestanden van het netwerkverkeer;
- consolelogs van tools (Nmap, hydra, eigen scripts, ...);
- screenshots van geslaagde en mislukte aanvallen;
- eventuele wijzigingen in de configuratie of firmware.

De sprint resulteert in een dataset van proof-of-concept-scripts, configuratiebestanden en logbestanden die later gebruikt worden voor analyse en rapportage.

Sprint 4: threat modeling (STRIDE) en mitigatieontwerp

Op basis van de bevindingen uit sprint 1–3 wordt een STRIDE-analyse uitgevoerd. Voor elke vastgestelde kwetsbaarheid of misconfiguratie wordt nagegaan welke bedreigingen aanwezig zijn op het vlak van:

- Spoofing;
- Tampering;
- Repudiation;
- Information Disclosure;
- Denial of Service;
- Elevation of Privilege.

Bij iedere bedreiging hoort een set van concrete mitigaties, specifiek afgestemd op de zetelwinkel. Mogelijke aanbevelingen zijn:

- segmentatie van cameraverkeer in een apart management-VLAN;
- afdwingen van sterke wachtwoorden en het uitschakelen van standaardaccounts;
- beperken van externe toegang via firewallregels;
- opzetten van een procedure voor tijdige firmware-updates;
- waar mogelijk inschakelen van versleutelde streams en beheerinterfaces (bijv. HTTPS, TLS).

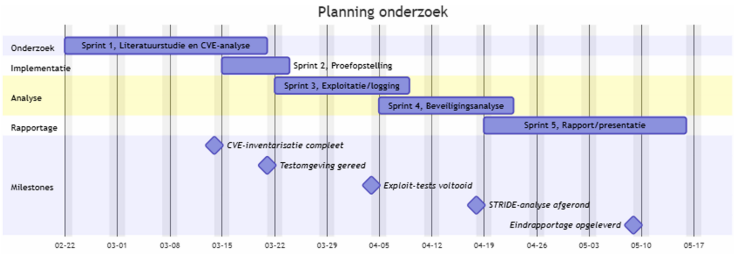
De output van deze sprint is een STRIDE-matrix en een conceptversie van het beveiligingsadvies.

Sprint 5: eindrapport en presentatie

In de laatste sprint worden alle resultaten samengebracht in een eindrapport voor bedrijf X. Dit rapport bevat:

- een samenvatting van de context en onderzoeksvragen;
- een overzicht van de relevante kwetsbaarheden en testresultaten;
- de STRIDE-analyse en prioriteitenlijst van risico's;
- een praktisch stappenplan met aanbevolen maatregelen.

Daarnaast wordt een presentatie uitgewerkt waarin de belangrijkste bevindingen en aanbevelingen in begrijpelijke, maar technisch onderbouwde taal worden toegelicht. De technische artefacten (scripts, configuraties, PCAP's) worden in een versiebeheersysteem opgenomen zodat verdere opvolging mogelijk is.



Figuur 1: Planning van het onderzoek met de vijf sprints en milestones.

4. Verwachte resultaten en conclusie

Op basis van de literatuur en praktijkervaring verwachten we aan te tonen dat het [IP-cameramodel van bedrijf X] minstens één of meerdere kwetsbaarheden of misconfiguraties vertoont die relevant zijn voor een retailomgeving. Dit kunnen onder andere zijn:

- zwakke of ongewijzigde standaardcredentials;
- ongefilterde netwerkpoorten die van buiten het camerasegment bereikbaar zijn;
- onversleutelde videostreams of beheerinterfaces;
- onvoldoende logging en monitoring van beheeracties.

De proof-of-concepttesten zullen naar verwachting aantonen dat sommige van deze kwetsbaarheden in de labomgeving misbruikt kunnen worden zonder dat dit onmiddellijk merkbaar is voor winkelpersoneel. De mate waarin deze aanvallen ook in de echte winkelomgeving mogelijk zijn, zal afhangen van de effectieve segmentatie en firewallconfiguratie.

Wat de visualisatie betreft, wordt voorzien om resultaten onder meer als volgt voor te stellen:

- een vergelijking van de beveiligingsstatus vóór en na implementatie van de voorgestelde maatregelen.

De meerwaarde voor de zetelwinkel en soortgelijke retailers ligt in:

- een concreet kwetsbaarhedenrapport op maat van hun omgeving;
- duidelijke, haalbare aanbevelingen om de camerabeveiliging te verbeteren;
- een reproduceerbaar testscenario dat later opnieuw kan worden gebruikt bij configuratiewijzigingen of vervanging van hardware.

Tabel 1: Verwachte meetgegevens

Parameters	**Eenheid**	**Toelichting**
Aantal succesvolle logins	Aantal	Via standaard-aanvallen of brute-force-aanvallen
CVE's toepasbaar op toestel	Aantal	Met bewijs van de impact die deze kwetsbaarheden kunnen hebben
Poorten die extern zichtbaar zijn	Aantal	Gedetecteerd via Nmap-scans
Reactietijd op een loginpoging	Milliseconden	Meetbaarheid van brute-force-detectie of login-vertraging

Deze bachelorproef levert dus niet alleen academische inzichten op, maar ook direct toepasbare output voor de praktijk. Indien bepaalde kwetsbaarheden al door recente firmware-updates opgelost blijken te zijn, is dat eveneens een relevante conclusie: het toont aan dat proactief patchbeheer ook in retailomgevingen een doorslaggevende rol speelt in de beveiliging van IoT-apparaten zoals IP-camera's.

Referenties

AlfredCamera. (2022). *How to Protect Your Security Camera from Hackers*. Geraadpleegd op 23 mei 2025, van https://alfred.camera/blog/how-to-protect-security-cameras-from-hackers/

Butun, I., Osterberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *arXiv preprint*, *arXiv:1910.13312*.

Naprys, E. (2024). *Security flaws in cameras being actively exploited*. Geraadpleegd op 21 mei 2025, van https://cybernews.com/security/security-flaws-in-dahua-cameras-being-exploited/

National Vulnerability Database (diverse CVE's voor IP-camera's) [Geraadpleegd via nvd.nist.gov]. (2025).