



Resultaten Omgevingsanalyse

Wijknetwerk Batau-Zuid

Door aspiranten van
Basisteam Lekpoort
30 oktober 2023

Agenda

Onderdelen van de presentatie

1. Interne analyse
2. Probleemomschrijving
3. Probleemanalyse
4. Probleemoplossing



1. Interne analyse Batau-Zuid

Enkele zaken die opvallen

- Wij zien na een jarenlange stijging weer een **daling** in het **totale aantal incidenten** voor Batau-Zuid;
- Het aantal incidenten bevat **veel snelwegmeldingen van de A2**. Deze zijn niet kenmerkend of behorend bij het gebied en hebben wij opgeschoond van onze dataset.
- Het type meldingen in Batau-Zuid varieert van huiselijk geweld en burenruzies tot de opkomst van **gedigitaliseerde criminaliteit**
- De **criminaliteit in Batau-Zuid** is net als in de rest van Nederland **aan het digitaliseren** en traditionele criminaliteit daalt. Procentueel gezien stijgt online en aan- en verkoopfraude het hardst.
- **Ondermijning** is niet direct tastbaar en dit is moeilijk in kaart te brengen, ook in onze wijk Batau-Zuid.
- In **ons advies** focussen wij op het **voorkomen/ aanpakken van online aan en verkoopfraude**. Dit misdrijf staat op nummer 4 van de misdrijven die hebben plaatsgevonden in Batau-Zuid in de periode (afgelopen jaar) die wij hebben onderzocht.



2. Probleemomschrijving

Welk probleem willen we aanpakken?

*Wij focussen ons op het probleem van **online aan- en verkoopfraude** of **internetoplichting**:*

Bij aankoopfraude maak je geld over naar een persoon of bedrijf zonder de dienst of het product te ontvangen waarvoor is betaald. Bij verkoopfraude worden goederen wel geleverd maar betaalt de ontvanger daar niet voor. Online betekent dat dit voornamelijk op internet handelsplaatsen gebeurt.



3. Probleemanalyse

Wat valt onder aan- en verkoopfraude?

- Onder **gedigitaliseerde criminaliteit** vallen delicten die buiten de digitale wereld ook plaats vinden. Denk bijvoorbeeld aan oplichting door middel van babbeltrucs of **verkoopfraude**. Onder **cybercrime** vallen delicten die zich richten op ICT (Informatie- en Communicatie Technologie), denk aan hacking, malware, DDOS aanvallen.
- Wij focussen dus op gedigitaliseerde criminaliteit, en dan met name op **online aan- en verkoopfraude**. Internetoplichting, waarbij goederen, geld en/of gegevens van nietsvermoedende gebruikers afhandig gemaakt worden.
- Slachtoffers voelen zich **schuldig & schamen** zich voor het voorval. Het gebeurt daarom best vaak dat er geen **aangifte** wordt gedaan. Naar onze mening is dit type criminaliteit ook goed te **voorkomen** met voldoende kennis en communicatie, werkend vanuit **preventie** door een samenwerking tussen **gemeente en politie**.
- De belangrijkste partijen die betrokken bij online aan- & verkoopfraude zijn naar onze mening **benadeelde burgers**, de **oplichters** of **georganiseerde criminelen**, de **postorderbedrijven** en de **digitale platformen en webshops**.
- Daarnaast zijn politie (reactief en proactief) en de gemeente betrokken. In onze optiek is wellicht frappant genoeg de **burger** zelf de belangrijkste betrokken partij.



4. Probleemoplossing

Korte termijn gericht op de burger

- **Bewaar bewijsmateriaal**

Maak screenshots of kopieën van alle relevante communicatie, transactiedetails en eventuele andere bewijzen van de fraude. Let op: delete geen accounts uit emotie. Lees hier meer informatie: <https://internetsporen.nl/is/>

- **Neem contact op met jouw bank**

Let op: dit kan vaak online, via de app of telefonisch

- **Meld de fraude bij het platform**

Dit kan ook vaak online of via een button op de site, bijv. bij Marktplaats of AutoTrack. Op marktplaats staan bijvoorbeeld heel veel tips voor veilig handelen én je kunt gebruikmaken van een veilige Marktplaats betaalmethode.

- **Doe aangifte bij de politie**

Dit kan online, mocht er meer informatie nodig zijn, kunt u worden uitgenodigd op het bureau. Via politie.nl/aangifte-of-melding-doen kunt u kiezen voor internetoplichting en zo gericht online aangifte doen.

- **Wees waakzaam voor verdachte activiteit**

Reageer niet op anonieme kopers of bellers bij het kopen of verkopen van goederen. Als het te mooi lijkt om waar te zijn, dan is dit ook zo.

- **Meld de fraude aan relevante instanties**

Meldpunt Internetoplichting (in Nederland).



4. Probleemoplossing

Middellange termijn gericht op de burger

- **Educatie en bewustwording**

Blijf op de hoogte van de nieuwste oplichtingstechnieken en leer hoe je ze kunt herkennen. Dit kan via de handelsplatforms, maar ook via voorkom internetoplichting, internetsporen.nl of via Marktplaats veiligheidscentrum.

- **Wees voorzichtig met het delen van persoonlijke informatie**

Door complexe en unieke wachtwoorden te gebruiken voor verschillende handelsaccounts wordt phishing moeilijker. Tweestapsverificatie vermindert de kans op misbruik nog meer waar mogelijk.

- **Gebruik beveiligde betaalmethoden**

Vaak zijn hier al gebruikers, telefoon-, rekeningnummers van verkopers die betaalverzoeken gebruiken gecontroleerd.

- **Controleer de verkoper of de koper en /of de webshop**

Door beoordelingen en recensies van de persoon met wie je handelt te controleren. Ook de webshop kun je controleren. Via politie.nl is er een lijst met malafide handelsbedrijven, onbetrouwbare webshops en verkopers.

- **Houd financiële transacties bij of maak een overzicht**

Verdachte transacties, of uitblijven van betaling is dan snel duidelijk!



4. Probleemoplossing

Lange termijn gericht op de burger

- **Digitale geletterdheid en bewustzijn**

Blijf zelf op de hoogte van cybercrime en gedigitaliseerde criminaliteit. Dit geldt voor burgers, politie & justitie en lokale of landelijke gemeente.

- **Cyberbeveiligingstraining**

Volg cursussen of workshops over cyberbeveiliging om dieper inzicht te krijgen in veiligheidsmaatregelen en -praktijken. Daarnaast wordt er door politie en justitie toezicht gehouden op digitale handelsplatforms.

- **Pas op voor phishing en social engineering**

Hier worden heel veel burgers door verrast, van jong tot oud, van laag- tot hoog opgeleid. Wij zijn tegenwoordig 24/7 online, gewend om direct iets te kopen / bestellen of ontvangen, online geeft gevoel van controle (ik doe het zelf) maar vaak is er een gebrek aan kennis.

- **Meld verdachte activiteiten direct**

En dit bij de juiste autoriteiten en initiatieven. Hoe meer dit gedeeld wordt, hoe beter er centraal kan worden gemeten en/of vervolgd.

- **Blijf zelf op de hoogte van wetgeving en beleid**

Houd jezelf op de hoogte van de wetgeving met betrekking tot online handel en fraudepreventie via overheidswebsites. Let op: wetgeving loopt altijd achter op de praktijk, maar er komt nieuwe wetgeving ten aanzien van online aan- & verkoopfraude.



4. Probleemoplossing

Een handig stappenplan

1. *Als het te goed klinkt om waar te zijn, dan is dit waarschijnlijk ook zo...*
2. *Google de URL*
3. *Google het bedrijf*
4. *Controleer het KvK nummer*
5. *Bel de klantenservice*
6. *Lees reviews*
7. *Betaalmiddel bekend en gewend?*
8. *Controleer de gebruiker of verkoper*
9. *Check de partijen zoveel mogelijk bij de politie via de bestaande oplichtingslijsten*
 - <https://www.politie.nl/aangifte-of-melding-doen/bekende-malafide-handelspartijen.html>
 - <https://www.politie.nl/aangifte-of-melding-doen/controleer-handelspartij.html>





« waakzaam en dienstbaar »