DIGITAAL VEILIGHEIDSBEELD AMSTERDAM

Versie 2019

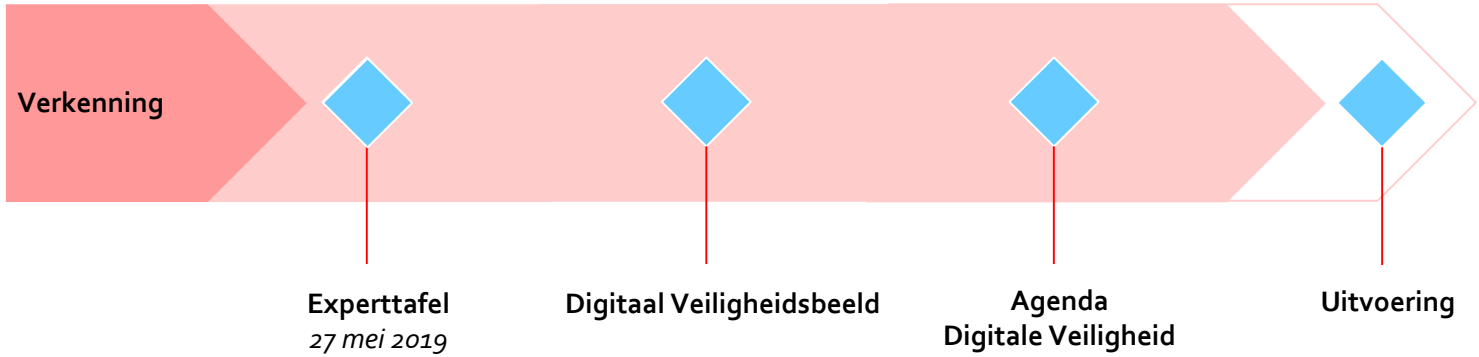
Inhoud

Klik op de hoofdstukken om er naar toe te bewegen. Je kunt overal in het document via de Home-button terug naar deze slide!

Doel van dit document: verkenning Digitaal Veilige Stad

Deze verkenning levert een eerste Digitaal Veiligheidsbeeld voor Amsterdam; met de belangrijkste digitale dreigingen, en een verkenning naar de mogelijke effecten en weerbaarheid. Daaruit volgen vragen voor verdieping, en de noodzaak tot een Agenda Digitale Veiligheid te komen om Amsterdam zo digitaal veilig mogelijk te maken.

Tijdens een experttafel (27 mei 2019) zijn de eerste uitkomsten gevalideerd en verder aangevuld door de aanwezige (externe) experts. Daarnaast zijn de domeinexperts gevraagd om met oplossingen en aanbevelingen te komen om de Amsterdamse weerbaarheid te vergroten. Als logisch vervolg is op basis van het veiligheidsbeeld de Agenda Digitale Veiligheid opgesteld waarin de aanpak en acties in beschreven staan.



Disclaimer: dit document is gebaseerd op een verkenning die breed opgezet is en alleen (kwalitatief) gebruik heeft gemaakt van bestaand onderzoek en gesprekken met experts. Het veiligheidsbeeld zal met de start van de Agenda Digitale Veiligheid in de toekomst steeds verder verbeterd worden.

Managementsamenvatting

Managementsamenvatting

Inleiding

Thema
Eigen huis op orde

Thema
Het individueel welzijn van burgers

Thema
Private en maatschappelijke organisaties

Thema
Vitale infrastructuur

Thema
Democratie en bestuurlijke stabiliteit

Thema
De openbare orde en veiligheid

Klik op de hoofdstukken om er naar toe te bewegen. Je kunt overal in het document via de Home-button terug naar deze slide!

Managementsamenvatting (1/2)

Door de snelle digitalisering en door nieuwe technologie is digitale veiligheid steeds belangrijker. De gemeente wil **Amsterdam zo digitaal veilig mogelijk maken voor haar burgers, ondernemers en bezoekers**: het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Digitale veiligheid is steeds meer in het geding omdat digitale aanvallen een laagdrempelig wapen zijn waartegen een doelwit zich lastig kan verweren. Ook leidt op dit moment bij **cybercrime slechts 1,4% van de registraties tot een eindbeslissing bij de rechter**.

Het Amsterdamse veiligheidsbeeld beslaat de volgende thema's:

- Eigen huis op orde: gemeente heeft een significante digitale "footprint" en kent 26 vitale processen. **Voornaamste dreigingen worden veroorzaakt door menselijke fouten,** maar er moet ook rekening gehouden worden met **verstoring, ransomware en sabotage/diefstal van data** of geld door criminelen of hacktivisten. Jaarlijks worden beveiligingstests en audits uitgevoerd om vast te stellen of beveiliging op orde is. Het informatiebeveiligingsbeleid is gebaseerd op de VNG-standaarden, met daarbinnen toepassingsbeveiliging o.b.v. risico-inschatting. College rapporteert jaarlijks aan de raad en externe toezichthouders hierover. Aan de hand van het veiligheidsbeeld kan het gemeentebestuur hierin **prioriteiten stellen op welke risico's te focussen**.
- Burgers: vooral jongeren hebben last van cyberpesten. Hacking en koop- en verkoopfraude zijn andere **cybercrimes waar in totaal jaarlijks ~11% van de Amsterdammers slachtoffer van worden**. Met name cyberpesten kan significante welzijnsschade tot gevolg hebben. Vanuit overheid en op scholen is hier dan ook al veel aandacht voor door het stimuleren van digitale bewustwording (en opbouwen digitale vaardigheden). Een ander veelgenoemd risico voor burgers is de **lage weerbaarheid van (individuele) IoT-apparaten**.
- Private & maatschappelijke organisaties: verstoringsaanvallen komen voor bij alle organisaties (bijv. met ransomware), datadiefstal/-lek heeft grote privacy-impact bij financiële instellingen en ziekenhuizen. Zorgt ook voor financiële schade: **in Amsterdam kost cybercrime bedrijven naar schatting €600 mln per jaar,** naast maatschappelijke onrust bij data-ontvreemding. Weerbaarheid vooral laag bij MKB door laag bewustzijn van risico's, en in de zorg door relatief lage digitale vaardigheden medewerkers. Overheid/gemeente probeert

Managementsamenvatting (2/2)

weerbaarheid te verhogen door bewustwordingscampagnes

- Vitale infrastructuur A'dam: beslaat 17 vitale processen. Grootste digitale dreigingen zijn **langdurige verstoring van elektriciteit, sabotage van waterkeringen, scheepvaart of verkeer**. Huidige schaal/aantal incidenten vooralsnog niet beschikbaar maar iedere betrokkene geeft aan **regelmatig aanvallen te ondervinden**. Primaire verantwoordelijkheid voor deze vitale processen ligt vaak buiten de gemeente maar **samenwerking en goede (crisis)communicatie is essentieel** om weerbaarheid te vergroten
- Democratie & bestuurlijke stabiliteit: **ca. ~50% van burgers komt wekelijks in contact met nepnieuws**. Verdergaande digitalisering (bijv. verdere verspreiding van algoritmes) brengt risico's op maatschappelijke verkokering en polarisatie met zich mee. Belangrijk dilemma welke rol overheid/gemeente zou moeten spelen om weerbaarheid te vergroten. Daarnaast is landelijke verkiezingssoftware kwetsbaar en dus ook in A'dam. Bij nieuwe vormen van stemmen zal robuustheid afhangen van zwaarte stemming
- De openbare orde en veiligheid: wanneer een digitale dreiging zich manifesteert kan de Amsterdamse openbare orde in het geding komen. Daarom dient de gemeente direct ingelicht te worden / significant cyberincident te herkennen, goed voorbereid te zijn en te beschikken over de juiste middelen en commmunicatielijnen om (de gevolgen van) een cybercrisis te beheersen. Cruciaal dat gemeente met belangrijke partijen intern en in het Amsterdamse speelveld, en met NCSC **duidelijke afspraken maakt over verantwoordelijkheid en communicatielijnen, en deze regelmatig oefent**. Hiervoor en voor een hogere inzet op de preventie en aanpak van cybercrime is Directie OOV al gestart met een plan van aanpak

De uitkomsten/vragen uit het veiligheidsbeeld vereisen een Agenda Digitale Veiligheid die de belangrijkste vragen op ieder thema adresseert en (indien specifiek nodig voor A'dam) de gekozen oplossingen uitvoert. Cruciaal hierin is dat de **primair verantwoordelijken voor elk thema en elke actie** duidelijk zijn, juist omdat de elementen van digitale dreigingen vaak door de gehele gemeentelijke organisatie heen lopen én niet altijd primair bij de gemeente liggen.

Een eerste Digitaal Veiligheidsbeeld Amsterdam: de belangrijkste dreigingen

Inschattingen o.b.v. kwalitatieve research en expertvalidatie

Eigen huis op orde

- Systeem- of menselijke fouten
- Ransomware of verstoring door criminelen of hacktivisten
- Onzorgvuldig of frauduleus handelen

Individueel welzijn burgers

- Cyberpesten
- Hacken IoT-apparaten
- Hacken computers

Private en maatschappelijke organisaties

- Hacken of verstoren van apparaten / systemen binnen zorginstellingen
- Datalek bij zorginstellingen
- Mal- of ransomware aanval op groot bedrijf, (m.n. financiële sector)
- Datadiefstal bij grote bedrijven

Vitale infrastructuur

- Langdurige (ver)storing elekriciteit / gas in geheel A'dam
- Uitzetten gemalen en openzetten waterkeringen
- Langdurig platleggen / saboteren vitale transport-infrastructuur
- Langdurig verstoord telefoon- / dataverkeer in geheel A'dam

Democratie en bestuurlijke stabiliteit

- Nepnieuws door staten en belangengroepen
- Beïnvloeding d.m.v. trollen door staten en belangengroepen
- Hacks bij politieke partijen

Impact

Waarschijnlijkheid

Klik op een thema om de dreigingsmatrix te bekijken

Bron: Expert interviews, Analyse projectteam

Een eerste Digitaal Veiligheidsbeeld Amsterdam: de belangrijkste dreigingen

Inschattingen o.b.v. kwalitatieve research en expertvalidatie

	Eigen huis op orde
Systeem- of menselijke fouten	*Veroorzaken langdurige uitval gemeentelijke ICT-systemen waardoor dienstverlening in vitale processen niet mogelijk is. Langdurige uitval onwaarschijnlijk maar als het gebeurt is mogelijke impact groot (schade door keteneffecten en onrust bij burgers die afhankelijk zijn)*
Ransomware of verstoring door criminelen of hacktivisten	*Veroorzaken langdurige uitval gemeentelijke ICT-systemen waardoor dienstverlening in vitale processen niet mogelijk is. Langdurige uitval onwaarschijnlijk maar als het gebeurt is mogelijke impact groot (schade door keteneffecten en onrust bij burgers die afhankelijk zijn)*
Onzorgvuldig of frauduleus handelen	*Directe financiële schade bij bijv. per abuis verhoogde uitgekeerde bedragen en kans op maatschappelijke ophef bij nalatigheid of fraude. In verleden aantal keer voorgekomen bij gemeenten in NL*

Impact

Waarschijnlijkheid

Klik op een thema om de dreigingsmatrix te bekijken

Bron: Expert interviews, Analyse projectteam

Een eerste Digitaal Veiligheidsbeeld Amsterdam: de belangrijkste dreigingen

Inschattingen o.b.v. kwalitatieve research en expertvalidatie

	Individueel welzijn burgers	Private en maatschappelijke organisaties	Vitale infrastructuur	Democratie en bestuurlijke stabiliteit
Eigen huis op orde				
Systeem- of menselijke fouten	Cyberpesten			Nepnieuws door staten en belangengroepen
Ransomware of verstoring door criminelen of hacktivisten	Hacken IoT-apparaten			Beinvloeding d.m.v. trollen door staten en belangengroepen
Onzorgvuldig of frauduleus handelen	Hacken computers	Datadiefstal bij grote bedrijven	Langdurig verstoord telefoon- / dataverkeer in geheel A'dam	Hacks bij politieke partijen

Op individueel niveau kan het zeer ernstig effect hebben (enkele zelfmoordgevallen bekend), en heeft op de samenleving als geheel ook relatief grote impact vanwege laagdrempeligheid. Vooral jongeren hebben ermee te maken

Beveiliging IoT-apparaten vaak minimaal, impact kan groot zijn wanneer hackers kwaadwillend zijn en apparaten overnemen die fysieke schade kunnen aanrichten

Gebeurt op redelijk grote schaal, impact voornamelijk economisch op individueel niveau

Impact

Waarschijnlijkheid

Klik op een thema om de dreigingsmatrix te bekijken

Bron: Expert interviews, Analyse projectteam

Een eerste Digitaal Veiligheidsbeeld Amsterdam: de belangrijkste dreigingen

Inschattingen o.b.v. kwalitatieve research en expertvalidatie

Private en maatschappelijke organisaties	
Hacken of verstoren van apparaten / systemen binnen zorginstellingen	*Wanneer zorginstellingen doelwit zijn van hacken van apparaten kan dat grote consequenties hebben voor patiënten, geen gevallen hiervan bekend*
Datalek bij zorginstellingen	*Grootste aantal meldingen bij Autoriteit Persoonsgegevens zijn in de zorgsector*
Mal- of ransomware aanval op groot bedrijf, (m.n. financiële sector)	*Grote bedrijven vaker doelwit dan MKB, met name financiële sector. Schade voornamelijk in reparatie en beveiligingskosten*
Datadiefstal bij grote bedrijven	*Financiële sector is belangrijkste doelwit van hackers, financiële gegevens zijn waardevol. Grote bedrijven hebben in vergelijking met MKB wel betere weerbaarheid tegen cyberdreigingen*

Impact

Waarschijnlijkheid

Klik op een thema om de dreigingsmatrix te bekijken

Bron: Expert interviews, Analyse projectteam

Een eerste Digitaal Veiligheidsbeeld Amsterdam: de belangrijkste dreigingen

Inschattingen o.b.v. kwalitatieve research en expertvalidatie

Eigen huis op orde	Individueel welzijn burgers	Private en maatschappelijke organisaties	**Vitale infrastructuur**	Democratie en bestuurlijke stabiliteit
Systeem- of menselijke fouten				Nepnieuws door staten en belangengroepen
Ransomware of verstoring door criminelen of hacktivisten				Beïnvloeding d.m.v. trollen door staten en belangengroepen
Onzorgvuldig of frauduleus handelen				Hacks bij politieke partijen

Significante fysieke (keten)effecten en economische schade mocht elektriciteitsvoorziening langdurig (meerdere dagen) uitvallen. Waarschijnlijkheid laag gegeven historie en eventuele uitwijk/steun van buiten A'dam	Langdurige (ver)storing elekriciteit / gas in geheel A'dam	Impact: hoog Waarschijnlijkheid: laag
Significante fysieke effecten en economische schade mocht waterbescherming daadwerkelijk gesaboteerd worden. Waarschijnlijkheid laag gegeven historie	Uitzetten gemalen en openzetten waterkeringen	Impact: hoog Waarschijnlijkheid: laag
Impact verschilt per transporthub / type infrastructuur maar kan beperkt tot groot zijn, vooral economische schade. Regelmatig aanvallen bekend op bijv. openbaar vervoersnetwerken in buitenlandse steden	Langdurig platleggen / saboteren vitale transport-infrastructuur	Impact: hoog Waarschijnlijkheid: middel
Impact steeds groter vanwege steeds toenemende digitalisering en gebruik van data voor fysieke handelingen. Waarschijnlijkheid laag vanwege veelheid aan netwerken en infrastructuur	Langdurig verstoord telefoon- / dataverkeer in geheel A'dam	Impact: hoog Waarschijnlijkheid: laag

Impact

Waarschijnlijkheid

Klik op een thema om de dreigingsmatrix te bekijken

Bron: Expert interviews, Analyse projectteam

Een eerste Digitaal Veiligheidsbeeld Amsterdam: de belangrijkste dreigingen

Inschattingen o.b.v. kwalitatieve research en expertvalidatie

Impact

Waarschijnlijkheid

Klik op een thema om de dreigingsmatrix te bekijken

Bron: Expert interviews, Analyse projectteam

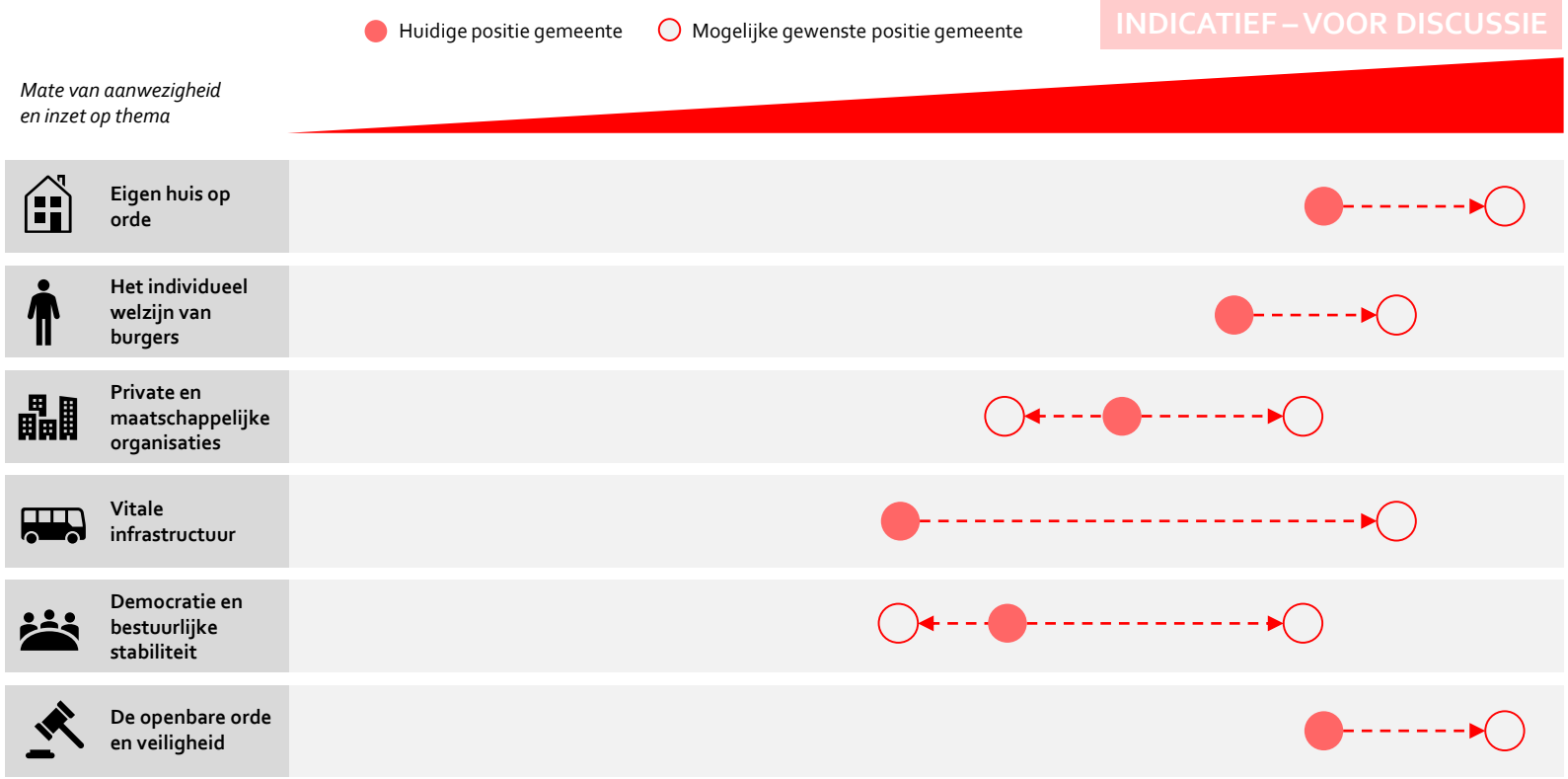
Overheid voert vanuit verschillende niveaus initiatieven uit om weerbaarheid te verhogen

	Preventie	Crisis
Eigen huis op orde	▪ Nationaal: gemeenten door NCSC niet aangeduid als vitale infrastructuur maar geregeld via IBD ▪ Lokaal: Amsterdam volgt landelijke standaarden VNG/IBD en werkt samen in G4	▪ Nationaal: ondersteuning door IBD ▪ Lokaal: Amsterdam heeft eigen Security Operations Center dat in verbinding staat met IBD, interne samenwerking en communicatie met OOV kan geintensiveerd worden
Het individueel welzijn van burgers	▪ Nationaal: vanuit VNG/CCV ondersteuning en uitwisseling voor lokale weerbaarheidsinitiatieven ▪ Lokaal: gemeente (voornamelijk Onderwijs, GGD) heeft aantal initiatieven om weerbaarheid te vergroten	▪ Lokaal: hulp en ondersteuning slachtoffers door politie en evt. nazorg
Private en maatschappelijke organisaties	▪ Nationaal: vanuit VNG/CCV ondersteuning en uitwisseling voor lokale weerbaarheidsinitiatieven ▪ Lokaal: gemeente heeft in regionale samenwerking Platform Veilig Ondernemen om weerbaarheid te vergroten	▪ Nationaal: datalekken dienen gemeld te worden bij Autoriteit Persoonsgegevens ▪ Lokaal: hulp en ondersteuning slachtoffers door politie
Vitale infrastructuur	▪ Nationaal: aard en beleid statelijke dreigingen (zoals huidige discussie rondom China-Huawei) worden onderzocht en bepaald door rijksoverheid/NCSC, gemeente volgend ▪ Lokaal: geen specifiek beleid t.a.v. A'damse vitale infra	▪ Nationaal: nationale vitale infra in verbinding met NCSC ▪ Lokaal: t.a.v. digitale dreigingen A'damse vitale infra dient gemeente met hen communicatie en crisisaanpak af te stemmen en regelmatig te oefenen
Democratie en bestuurlijke stabiliteit	▪ Internationaal: G7 (incl. EU) plan tegen cyberaanvallen en manipulatie sociale media door Rusland en China, EU bezig met nepnieuws ▪ Nationaal: beleid tegen bijv. nepnieuws in ontwikkeling ▪ Lokaal: geen specifiek beleid	
De openbare orde en veiligheid	▪ Lokaal: bezig met inventarisatie of specifieke Amsterdamse dreigingen specifieke preventie behoeft	▪ Lokaal: hoofdverantwoordelijk voor lokale (fysieke) openbare orde en bezig met betere voorbereiding op digitale dreigingen en digitale elementen van crisis

Bron: Expert interviews, Press search, Analyse projectteam

Belangrijk om rol gemeente in digitale veiligheidsdomein te bepalen en af te bakenen; dilemma om meer/minder te doen op elk thema

INDICATIEF – VOOR DISCUSSIE



Essentieel om rol te bepalen door uit te gaan waar gemeente daadwerkelijk over gaat (bestuurlijke verantwoordelijkheid heeft)

Bron: Expert interviews en experttafel, Analyse projectteam

Schets van actieplan (per thema)

	Acties/maatregelen
Eigen huis op orde	▪ Opstellen intern cybercrisisplan, procedures en communicatie tussen CI(S)O (vooral SOC) en OOV ▪ Verder versterken CIO/informatiebeveiligingsorganisatie waar nodig (te onderzoeken), bijv. in mandaat/capaciteit/budget ▪ Waarborgen continue aandacht en monitoring van veiligheid gemeentelijke sites en webapplicaties ▪ Verder versterken van digitaal bewustzijn directies en medewerkers
Het individueel welzijn van burgers	▪ Continueren (en evt. uitbreiden) campagnes en programma's digitale bewustwording en digitale vaardigheden ter verhoging weerbaarheid bij (vooral kwetsbare) burgers ▪ Onderzoeken of experiment/aanjagen minimum voorwaarden/veiligheidseisen aan IoT-apparaten wenselijk en haalbaar is
Private en maatschappelijke organisaties	▪ Continueren campagnes en programma's verhoging digitale weerbaarheid bedrijven met focus op MKB
Vitale infrastructuur	▪ Starten samenwerking en afstemming crisisaanpak en –communicatie met vitale infrastructuur A'dam (ook vs. nationaal) ▪ Opstellen scenario's en regelmatig oefenen crisisaanpak ▪ Dieper onderzoeken van gevolgen digitale storingen vitale infrastructuur voor A'dam
Democratie en bestuurlijke stabiliteit	▪ Onderzoek verder welke Amsterdammers nu door nepnieuws bereikt worden en hoe de gemeente hen kan bereiken, zonodig met het breed aanbieden van lessen mediawijsheid ▪ Maak scenario's wie en waarom online stemmingen zou willen manipuleren. Overweeg of extra protectie opweegt tegen het opwerpen van een drempel om te kunnen participeren
De openbare orde en veiligheid	▪ Uittekenen en borgen verantwoordelijkheid t.a.v. digitale dreigingen binnen het thema OOV ▪ Opstellen cybercrisisaanpak en –communicatie met landelijke en A'damse spelers (incl. regelmatig oefenen van verschillende scenario's) ▪ Uitvoeren plan van aanpak t.a.v. preventie en impact digitale dreigingen voor OOV-organisatie

Bron: Analyse projectteam

Eventueel vervolgonderzoek / verdieping kan diepere inzichten op elk thema leveren

	Wat weten we niet / waar is nader onderzoek nodig?
Eigen huis op orde	▪ Objectief beeld van weerbaarheid vergt continue bestuurlijke aandacht voor technische assessments en hackersonderzoeken (die ook al plaatsvinden), en evt. een benchmark t.o.v. andere gemeenten/organisaties ▪ Of en in hoeverre er verdere versterking mandaat/capaciteit/budget en bewustwording bij directies nodig is voor verhogen weerbaarheid
Het individueel welzijn van burgers	▪ Beter en betrouwbaarder beeld (over tijd) van incidentie verschillende cybercrimes (wordt onderzocht door OIS) ▪ Verborgen cybercrime (niet of lastig meetbaar, bijv. vanwege slachtoffers buiten A'dam/NL, geavanceerde technieken)
Private en maatschappelijke organisaties	▪ Kwantitatief onderbouwde en specifieke incidentie en vooral kosteninschatting voor Amsterdamse bedrijven en maatschappelijke organisaties (wordt onderzocht door OIS)
Vitale infrastructuur	▪ Huidige schaal/aantal incidenten bij vitale infrastructuur ▪ Inzicht in (mogelijke) keteneffecten bij een significante cybercrisis ▪ Vollediger beeld: projectteam heeft niet kunnen spreken met alle A'damse vitale infra, en ook niet met het NCSC en IBD
Democratie en bestuurlijke stabiliteit	▪ Omvang en impact van dreigingen zeer lastig meetbaar ▪ Mogelijk beleid en maatregelen zijn op alle niveaus nog volop in ontwikkeling – nog geen geijkte methodes ▪ Huidige staat en eventueel beleid t.a.v. informatieveiligheid politieke partijen
De openbare orde en veiligheid	▪ In hoeverre gemeente als crisisorganisatie voorbereid is op digitale dreigingen met gevolgen voor openbare orde ▪ In hoeverre bevoegdheden BM toereikend zijn m.b.t. digitale veiligheid ▪ Wenselijkheid digitaal veiligheidsbeleid en digitale APV

Bron: Analyse projectteam

Inleiding

Managementsamenvatting

Inleiding

Thema
Eigen huis op orde

Thema
Het individueel welzijn van burgers

Thema
Private en maatschappelijke organisaties

Thema
Vitale infrastructuur

Thema
Democratie en bestuurlijke stabiliteit

Thema
De openbare orde en veiligheid

Amsterdam wil digitaal de meest veilige stad zijn

Digitaal veilig zijn betekent het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie. [1]

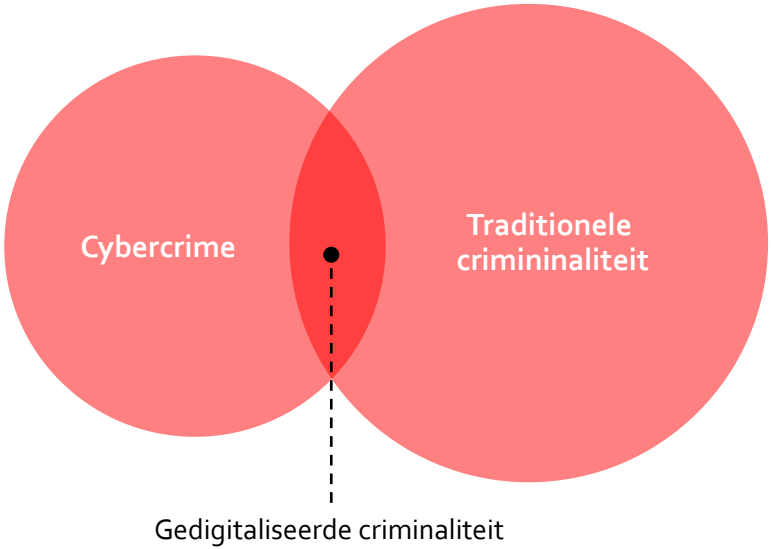
Digitale veiligheid is **relevant voor de hele Amsterdamse samenleving**. Het is belangrijk dat kinderen veilig op het internet kunnen bewegen, ouderen veilig toegang hebben tot zorg, onze energievoorziening veilig en betrouwbaar is, maar ook dat we kunnen vertrouwen op de informatie die via digitale platformen aan ons wordt gegeven.

Door de **toenemende digitalisering en nieuwe technologie** wordt digitale veiligheid steeds belangrijker voor Amsterdamse burgers, ondernemers en bezoekers

1 Gelijk aan de definitie van "cybersecurity" zoals beschreven door NCTV/NCSC - https://www.nctv.nl/organisatie/cs/index.aspx

Bron: NCTV, Analyse projectteam

Bij een aanval op digitale veiligheid spreken we over cybercrime



Cybercrime (in enge zin): strafbare feiten die gepleegd worden met ICT middelen én die gericht zijn op ICT middelen. Onder ICT middelen worden verstaan: computers, computernetwerken, servers, smartphones, tablets etc.

Gedigitaliseerde criminaliteit: klassieke misdrijven die (mede) worden gepleegd met een ICT middel. ICT is hierbij alleen het middel en níét het doel. Bijvoorbeeld aan- en verkoopfraude, oftewel: diefstal.

Landelijk wordt veelal de term **"cybersecurity"** gebruikt i.p.v. digitale veiligheid. In dit document geven we de voorkeur aan de Nederlandse term, maar waar het onpraktisch is gebruiken we ook het woord **"cyber" als synoniem voor "digitaal".** Dit geldt vooral voor de termen **"cybercrime"** en **"cybercrisis"**.

Bron: Politie, Trendbeeld 2019; CBS (2018). *Cybersecuritymonitor 2018*

Digitale veiligheid steeds meer in het geding omdat digitale aanvallen een ideaal wapen zijn waartegen een doelwit zich lastig kan verweren

Kernproblematiek (CSBN) van digitale aanvallen

Vanuit actor - een ideaal wapen

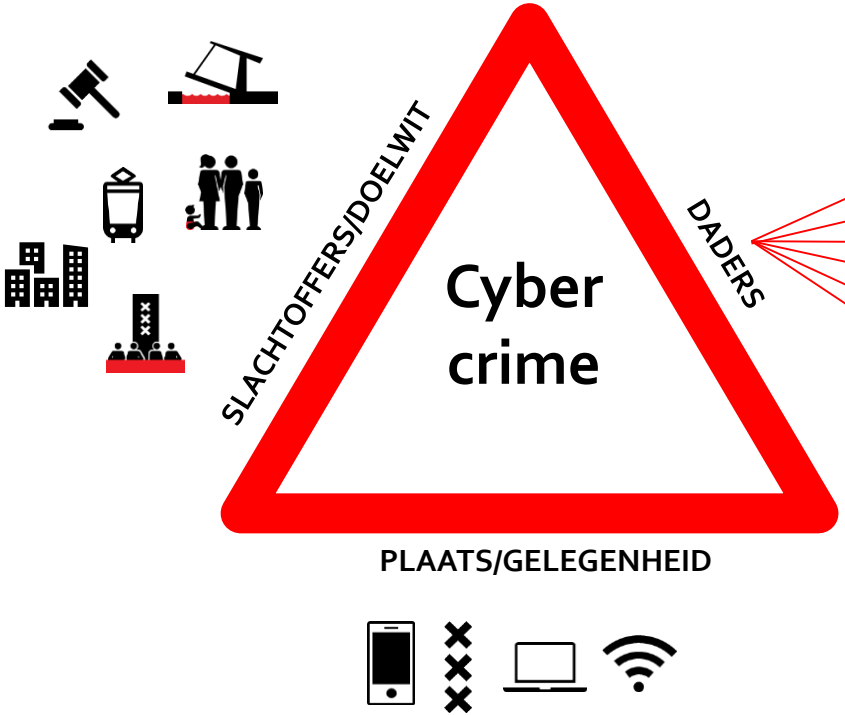
- **Profijtelijk:** ongeacht het motief – persoonlijk, economisch, ideologisch of geopolitiek – is een digitale aanval al jaren een profijtelijk middel voor actoren. Door de nog steeds toenemende digitalisering neemt het profijt (en ook de aangerichte schade) toe
- **Laagdrempelig:**
  - Aanvalsmiddelen zijn eenvoudig toegankelijk door aanvals-facilitatoren. Deze dienstverleners stellen infrastructuur, hulpmiddelen en technieken voor digitale aanvallen tegen betaling beschikbaar. Daardoor hoeft een aanvaller zelf lang niet altijd over veel capaciteiten, ervaring en middelen te beschikken voor een aanval
  - Onveilige producten en diensten maken het voor aanvallers makkelijk om succesvolle aanvallen uit te voeren
- **Weinig riskant:** kans bestaat dat de aanval lange tijd onopgemerkt blijft. Als de aanval wel ontdekt wordt, is de attributie aan en de opsporing van actoren complex. En zelfs als dat lukt blijft het vaak zonder consequenties, zeker in het geval van statelijke of staatsgelieerde actoren (al lijkt dit recentelijk veranderd door het publiekelijk attribueren van digitale aanvallen door overheden)

Vanuit doelwit – uitdagende weerbaarheid

- **Belangentegenstellingen leiden tot concessies:** maatregelen voor meer digitale veiligheid kosten tijd en geld, twee schaarse middelen die ook anders ingezet kunnen worden. Burgers, bedrijven, sectoren en overheden zullen daarom altijd een belangenafweging moeten maken
- **Toenemende complexiteit en connectiviteit:** organische groei en de relatief lange levensduur van systemen zorgen voor een steeds ingewikkelder ICT-landschap. Ook maakt het toegenomen gebruik van gedeelde voorzieningen, zoals clouddiensten, in de vorm van losse bouwblokken, dat het overzicht lastiger te bewaren is
- **Veel buitenlandse producenten en dienstverleners:** Nederlandse organisaties zijn sterk afhankelijk van een beperkt aantal buitenlandse leveranciers van producten en diensten. Hoewel het positief is dat deze bedrijven meer middelen hebben om zich tegen aanvallen te wapenen, kan de maatschappelijke impact bij verstoringen groot zijn, omdat veel verschillende diensten afhankelijk zijn van een klein aantal aanbieders die meestal onder invloed staan van een overheid en wetgeving buiten Nederland

Bron: CSBN

Digitale aanvallen worden gepleegd door veel verschillende type daders met verschillende motieven



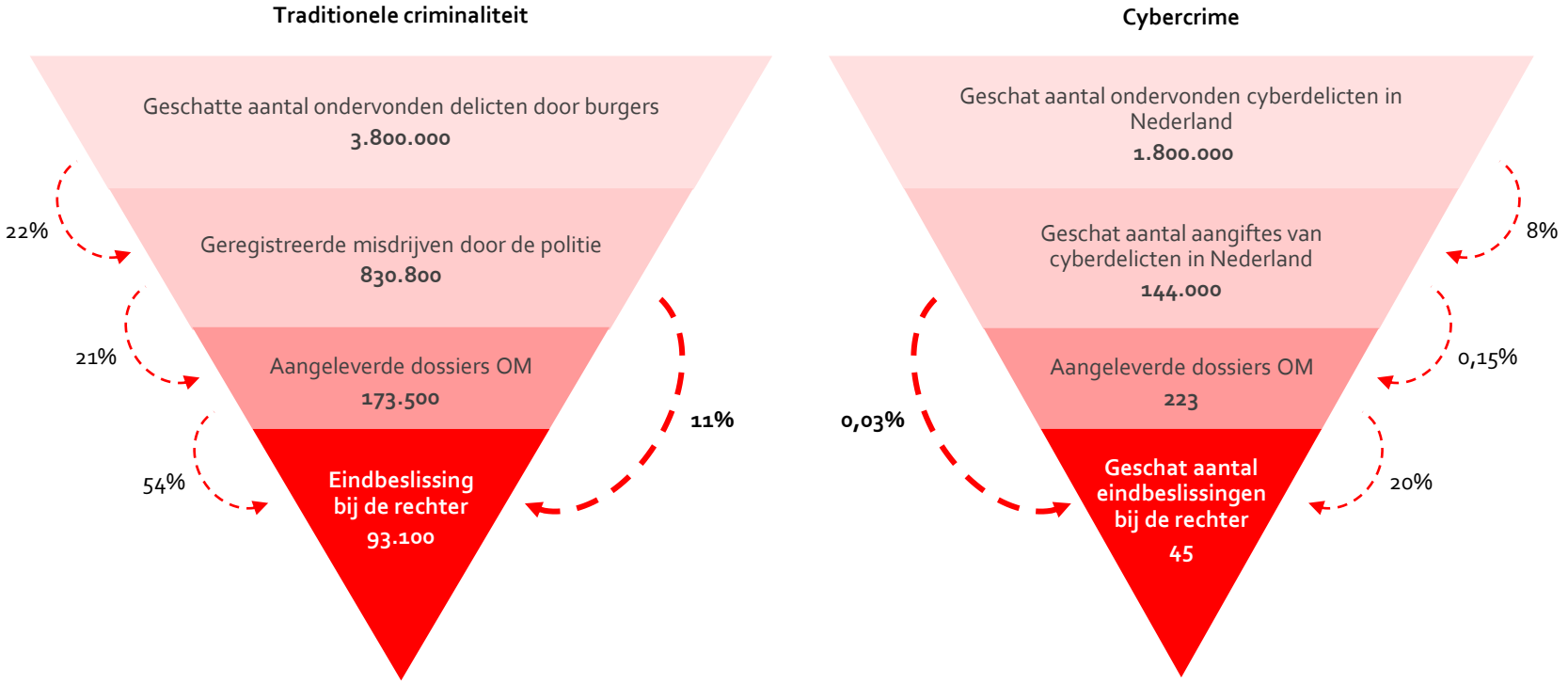
- Staten/staatsgelieerd
- Criminelen
- Terroristen
- Hacktivisten
- Cybervandalen en scriptkiddies
- Insiders

Digitale aanvallen door statelijke actoren en (beroeps)criminelen vormen de grootste digitale dreiging voor de nationale veiligheid volgens CSBN

Bron: CSBN 2018

Cybercrime is lastig aan te pakken (1/2) – Slechts 0,03% van de aangiftes leidt tot eindbeslissing bij rechter

NEDERLAND



Bron: "Criminaliteit en Rechtshandhaving 2017" (WODC 2017); CBS, OM.nl, rechtspraak.nl

Rol van overheid/gemeente verschilt nu fysiek en digitaal: vraag is of gemeente grotere rol zou moeten hebben op digitale veiligheid

INDICATIEF - VOORBEELD

Brandveiligheid

- Brandweer heeft wettelijke taken op het gebied van preventie en voorlichting. De wetgever heeft daarmee vastgesteld dat de brandweer dit regionaal moet uitvoeren (voor digitale veiligheid ontbreekt zo'n kader)
- Externe maatregelen (stad als geheel):
  - Periodieke brandkeuringen en controle brandveiligheid
  - Sluitingen van woningen indien er brandgevaar is
  - Brandweer en politie paraat
- Interne maatregelen (gemeente zelf):
  - Alarmnummer om een calamiteit te melden
  - In geval van explosie of brand kan een handmelder ingedrukt worden
  - Ontruiming; oefeningen voor in geval van nood
  - Aanwezige bedrijfshulpverleners
  - Nooduitgangen

Dit roept vragen op over digitale veiligheid: dient/wil de overheid daar een soortgelijk beleid op voeren als voor brandgevaar?

En wat is de rol van specifiek de gemeente in het waarborgen van digitale veiligheid, en is dat voor alle betrokkenen duidelijk?

Bron: Amsterdam.nl

Onderzoek, Informatie & Statistiek (OIS) kan informatiepositie voor gemeente innemen door publicaties digitale veiligheid te verzorgen

EERSTE IDEEËN – NADER TE BEPALEN

	Fysieke veiligheid	Digitale veiligheid
Bronnen	▪ Veiligheidsmonitor (vragenlijst aan bewoners) ▪ Data Politie, OM en OOV	▪ Veiligheidsmonitor (vragenlijst aan bewoners): opnemen vragen slachtofferschap cybercriminaliteit monitoren (hacken, cyberpesten, koop- en verkoopfraude en identiteitsfraude) ▪ Data Politie, OM en OOV over cybercriminaliteit
Publicaties	▪ Veiligheidsindex (overzicht criminaliteit, overlast en onveiligheidsbeleving naar buurt) ▪ Criminaliteitsbeeld (rapportage met statistieken criminaliteit en verdachten) ▪ Nog vele andere publicaties	▪ Index m.b.t. cybercriminaliteit naar relevante dimensies (bijv. leeftijdsgroepen, SES, opleiding) ▪ Criminaliteitsbeeld (rapportage met statistieken criminaliteit): toevoegen cybercriminaliteit ▪ Lokaal veiligheidsbeeld (waarvan dit document eerste versie is): kwalitatief maar zoveel mogelijk onderbouwd met statistieken en evt. externe databronnen ▪ Eventueel opzetten van een panel waarin ontwikkelingen/impact van interventies op digitale veiligheid gemeten kan worden

Bron: OIS (afdeling Onderzoek, Informatie en Statistiek verzamelt data over Amsterdam en verwerkt/publiceert deze tot informatie) , Analyse projectteam

Amsterdam kan samenwerken met andere (grote) steden op digitale veiligheid en van elkaar leren

Ambities en activiteiten digitale veiligheid

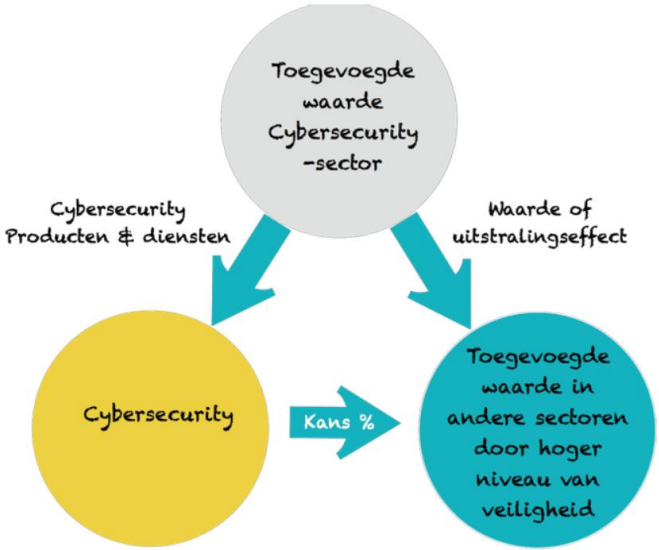
Rotterdam	▪ Uit Coalitieakkoord 2018-2022: - Er wordt een Rotterdams cyberbeeld opgesteld met speciale focus op de Rotterdamse haven - Voorlichting over cybersecurity voor Rotterdammers en ondernemers ▪ Coalitieakkoord stelt ook €500k per jaar beschikbaar voor versterken digitale weerbaarheid ▪ Veiligheidsalliantie regio Rotterdam wil digitale weerbaarheid (met subsidie Ministerie Justitie en Veiligheid) door ontwikkelen van extra materiaal t.a.v. de campagne Digitaal Veilig (www.checklistdigitaalveilig.nl), inrichten pilot meldpunt gemeenten voor het doen van aangifte bij de politie en het organiseren van masterclasses cybercrime en ondersteuning op een lokaal cyberdreigingsbeeld
Den Haag	▪ Ambieert voortrekkersrol op cybersecurity ▪ Heeft voor periode 2019 – 2022 in veiligheidsbeleid extra aandacht voor cybercriminaliteit, geen extra budget gespecificeerd ▪ Richt zich op burgers en MKB weerbaar maken (met extra aandacht voor ouderen en jongeren), beschouwt grootschalige cybercrime niet als een taak voor de gemeente ▪ Wil crisisorganisatie optimaal voorbereid hebben op cyberaanvallen op vitale infrastructuur. In 2019 wordt i.s.m. een drinkwaterbedrijf een crisisoefening gehouden
Utrecht	▪ Stelt vier ambities in integraal veiligheidsplan m.b.t. digitale veiligheid (geen indicatie over (extra) budget): - Opstellen stedelijk weerbaarheidsbeeld cyberveiligheid (met subsidie van Ministerie Justitie en Veiligheid), met daarin kansen en bedreigingen voor alle stedelijke functies. Op basis van weerbaarheidsbeeld moet handelingsperspetief worden opgesteld - Meer inzicht verkrijgen in wie daders en slachtoffers van cybercriminiteit zijn en meldingsbereidheid verhogen - Vergroten van de bewustwording over digitale risico's - Optimaal voorbereiden op cybercrises

Bron: Websites gemeenten, Press search

Koppositie in digitale veiligheid kan ook stimulans geven aan tech / cybersecurity sector in Nederland als geheel

In NL is toegevoegde waarde van de cybersecurity-sector **€ 3,8-4,1 miljard** (2014). De cybersecurity-sector **groeit ook veel sneller** dan de IT-sector zelf. In de periode 2010-2014 is de omzet en de toegevoegde waarde van cybersecurity binnen de IT-sector jaarlijks met 14,5 procent toegenomen. De benaderde IT-bedrijven in de SEO-enquête verwachten een jaarlijkse groei van omzet uit cybersecurity-activiteiten van **~7%**.

Economische betekenis van cybersecurity voor de economie

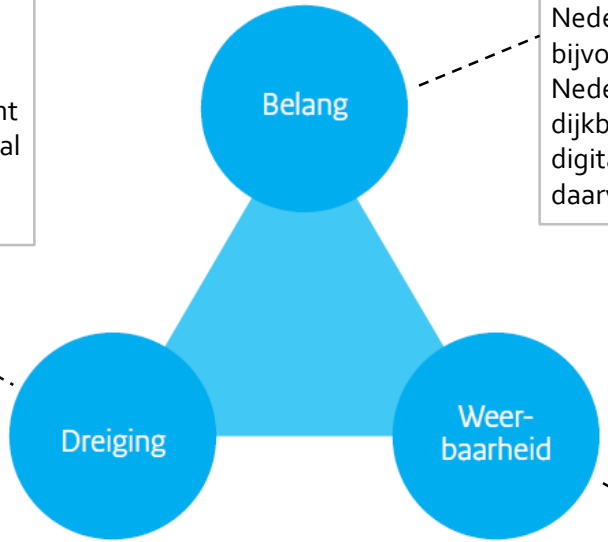


Bron: "Economische kansen Nederlandse cybersecurity-sector" (SEO 2014)

Inleiding
Methodologie verkenning

Om tot een Amsterdams veiligheidsbeeld te komen, gebruiken we de structuur zoals opgesteld door NCTV/NCSC[1]

De digitale dreiging is permanent. Een dreiging is de kans op schade, in dit geval digitale schade. Digitale aanvallen zijn profijtelijk, laagdrempelig en weinig riskant voor aanvallers. Toepassing op grote schaal is relatief makkelijk, waardoor er grote dreigingen zijn



Digitale veiligheid is noodzakelijk voor het functioneren van de sterk gedigitaliseerde Nederlandse samenleving en economie. Net als bijvoorbeeld voor overstromingen, moet Nederland ook in de digitale wereld de dijkbewaking op orde brengen. Een veilige digitale infrastructuur en cybersecurity zijn daarvoor randvoorwaarden

De digitale weerbaarheid van Nederland staat onder druk. Lang niet alle organisaties treffen bijvoorbeeld basismaatregelen. De weerbaarheid staat verder onder druk door een toenemende complexiteit en connectiviteit van het ICT-landschap en weinig aandacht voor digitale veiligheid

1 NCTV = Nationaal Coördinator Terrorismebestrijding en Veiligheid, NCSC = Nationaal Cyber Security Centrum
Bron: CSBN 2018

De 5 nationale veiligheidsbelangen van het CSBN zijn vertaald naar de Amsterdamse context

Type	Nationale omschrijving	In Amsterdam
Territoriale veiligheid	Het ongestoord functioneren van Nederland als onafhankelijke staat in brede zin, dan wel de territoriale integriteit in enge zin. *Dit betreft zowel het fysieke grondgebied en de bijbehorende infrastructuur als het imago en de reputatie van ons land.*	Het ongestoord functioneren van Amsterdam als gemeente en stad, dan wel de territoriale integriteit in enge zin. *Dit betreft zowel het fysieke grondgebied en de bijbehorende infrastructuur als het imago en de reputatie van de stad.*
Fysieke veiligheid	Het ongestoord functioneren van de mens in Nederland en zijn omgeving. *Dit betreft de gezondheid en het welzijn van mensen. Criteria zijn aantallen doden en zwaargewonden en gebrek aan primaire levensbehoeften zoals voedsel, energie, drinkwater en adequate huisvesting.*	Het ongestoord functioneren van de mens in Amsterdam en zijn omgeving. *Dit betreft de gezondheid en het welzijn van mensen. Ook psychische gezondheid scharen we hier onder. Criteria zijn aantallen doden en zwaargewonden en gebrek aan primaire levensbehoeften zoals voedsel, energie, drinkwater en adequate huisvesting.*
Economische veiligheid	Het ongestoord functioneren van Nederland als een effectieve en efficiënte economie. *Dit betreft zowel economische schade (kosten) als de vitaliteit van onze economie (bijvoorbeeld sterke toename werkloosheid).*	Het ongestoord functioneren van de lokale economie van Amsterdam, en het volledig kunnen vervullen van een rol in de (inter)nationale economie. *Dit betreft zowel economische schade (kosten) als de vitaliteit van onze economie (bijvoorbeeld sterke toename werkloosheid).*
Ecologische veiligheid	Het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij Nederland. *Dit betreft aantasting van natuur, milieu en ecosystemen.*	Het ongestoord blijven voortbestaan van de natuurlijke leefomgeving in en nabij Amsterdam. *Dit betreft aantasting van natuur, milieu en ecosystemen.*
Sociale en politieke veiligheid	Het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen kunnen functioneren en groepen mensen goed met elkaar kunnen samenleven binnen de verworvenheden van de Nederlandse democratische rechtsstaat en daarin gedeelde waarden. *Dit betreft aantasting van vrijheid van handelen, de democratische rechtsstaat, de kernwaarden van onze samenleving en het al dan niet optreden van grootschalige sociaal-maatschappelijke onrust en daarmee gepaard gaande emoties (angst, woede, verdriet).*	Het ongestoorde voortbestaan van een maatschappelijk klimaat waarin individuen kunnen functioneren en groepen mensen goed met elkaar kunnen samenleven binnen de verworvenheden van de Nederlandse democratische rechtsstaat en daarin gedeelde waarden. *Dit betreft aantasting van vrijheid van handelen, de democratische rechtsstaat, de kernwaarden van onze samenleving en het al dan niet optreden van grootschalige sociaal-maatschappelijke onrust en daarmee gepaard gaande emoties (angst, woede, verdriet).*

Bron: CSBN 2018, Analyse projectteam

Thema: Eigen huis op orde

Managementsamenvatting

Inleiding

Thema
Eigen huis op orde

Thema
Het individueel welzijn van burgers

Thema
Private en maatschappelijke organisaties

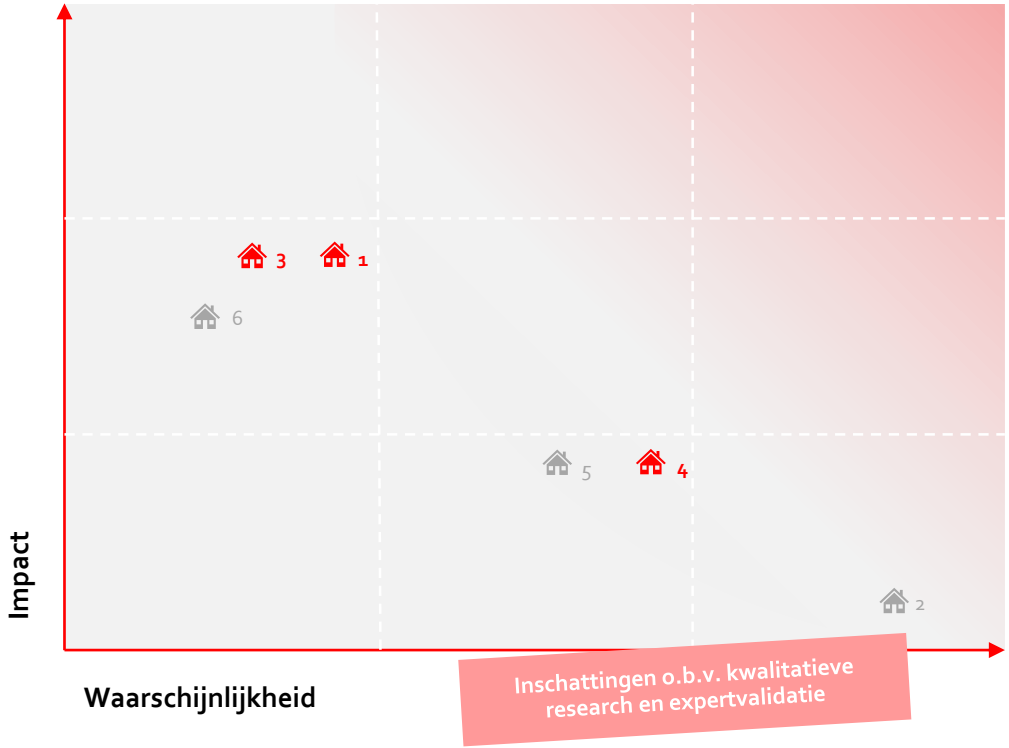
Thema
Vitale infrastructuur

Thema
Democratie en bestuurlijke stabiliteit

Thema
De openbare orde en veiligheid

Digitaal Veiligheidsbeeld A'dam - Gemeentelijke organisatie

Totaal | Eigen huis op orde | Individueel welzijn burgers | Private en maatschappelijke organisaties | Vitale infrastructuur | Democratie en bestuurlijke stabiliteit



Eigen huis op orde

1. **Systeem- of menselijke fouten** veroorzaken langdurige uitval gemeentelijke ICT-systemen waardoor dienstverlening in vitale processen niet mogelijk is
2. Snelle aanvallen door hacktivisten veroorzaken korte verstoringen / vertraging
3. **Ransomware/langdurige verstoring door criminele hackers of hacktivisten** (van gemeentelijke ICT-systemen)
4. **Onzorgvuldig/frauduleus menselijk handelen** veroorzaakt fout / onbetrouwbare informatievoorziening (bijv. in uitkeringsproces)
5. Verlies/diefstal van informatie (menselijke fout of onbevoegde toegang tot vertrouwelijke gegevens)
6. Manipulatie van informatie en/of sabotage van buitenaf voor criminele of activistische doeleinden

Bron: Expert interviews, Analyse projectteam

Waarschijnlijkheid dreigingen

Laag | Medium | Hoog

Nr	Dreiging	Waarschijnlijkheid
1	Systeem- of menselijke fouten veroorzaken langdurige uitval waardoor dienstverlening in vitale processen niet mogelijk is	*Korte uitval komt zo nu en dan voor maar langdurige uitval (>1 dag) onwaarschijnlijk*
2	Snelle aanvallen door hacktivisten veroorzaken korte verstoringen/vertraging	*Laagdrempelige aanvallen maar met geen tot zeer weinig succes / impact*
3	Ransomware/langdurige verstoring van gemeentelijke ICT-systemen door criminele hackers of hacktivisten	*Korte verstoring komt zo nu en dan voor maar langdurige uitval (>1 dag) onwaarschijnlijk*
4	Onzorgvuldig/frauduleus menselijk handelen veroorzaakt fout / onbetrouwbare informatie (bijv. in uitkeringsproces)	*In verleden aantal keer voorgekomen bij gemeenten in NL*
5	Verlies/diefstal van informatie (menselijke fout of onbevoegde toegang tot vertrouwelijke gegevens)	*In verleden aantal keer voorgekomen bij gemeenten in NL*
6	Manipulatie van informatie en/of sabotage van buitenaf voor criminele of activistische doeleinden	*Op grote schaal onwaarschijnlijk, in NL nog niet voorgekomen*

Bron: Expert interviews, Analyse projectteam

Mogelijke impact dreigingen

Beperkt | Medium | Significant

Nr	Dreiging	Territoriaal	Fysiek	Economisch	Ecologisch	Sociaal en politiek
1	Systeem- of menselijke fouten veroorzaken langdurige uitval waardoor dienstverlening in vitale processen niet mogelijk is	*Negatieve media-aandacht, bijv. bij verstoring uitkeringen*	*Onzekerheid over bijv. sociale dienstverlening, reisdocumenten etc. kan leiden tot psychische schade*	*Intern ligt veel werk stil, extern zorgen keteneffecten voor economische schade bij burgers en organisaties*		*Onrust bij medewerkers gemeente en bij burgers die afhankelijk zijn van (vitale) dienstverlening*
2	Snelle aanvallen door hacktivisten veroorzaken korte verstoringen / vertraging			*Lichte vertraging / gedeeltelijke verstoringen zorgen voor inefficiënties intern en extern*		
3	Ransomware/langdurige verstoring van gemeentelijke ICT-systemen door criminele hackers of hacktivisten	*Negatieve media-aandacht, bijv. bij ransomware*	*Onzekerheid over bijv. sociale dienstverlening, reisdocumenten etc. kan leiden tot psychische schade*	*Intern ligt veel werk stil, extern zorgen keteneffecten voor economische schade bij burgers en organisaties*		*Onrust bij medewerkers gemeente en bij burgers die afhankelijk zijn van (vitale) dienstverlening*
4	Onzorgvuldig/frauduleus menselijk handelen veroorzaakt fout / onbetrouwbare informatie (bijv. in uitkeringsproces)	*Negatieve media-aandacht, bijv. bij menselijke fouten uitkeringsproces*		*Directe financiële schade bij bijv. per abuis verhoogde uitgekeerde bedragen*		*Kans op maatschappelijke ophef bij grote fouten of nalatigheid*
5	Verlies/diefstal van informatie (menselijke fout of onbevoegde toegang tot vertrouwelijke gegevens)	*Negatieve media-aandacht*		*Directe financiële schade bij verlies/diefstal*		*Kans op maatschappelijke ophef bij significant verlies/diefstal*
6	Manipulatie van informatie en/of sabotage van buitenaf voor criminele of activistische doeleinden	*Negatieve media-aandacht, met kans op ondermijning territoriale integriteit bij grootschalige sabotage*		*Kans op grote (in)directe financiële schade (bijv. vastgoedfraude met onjuist verkregen informatie)*		*Kans op maatschappelijke ophef en onrust bij grootschalige sabotage*

Bron: Expert interviews, Analyse projectteam

Om weerbaar te zijn heeft gemeente al concrete maatregelen lopen die verder versterkt kunnen worden

Preventie

- Generieke maatregelen (fysieke beveiliging, standaardeisen aan hard- en software)
- Standaarden/eisen nu o.b.v. BIG (Baseline Informatiebeveiliging Gemeenten), vanaf 2020 volgens BIO (Baseline Informatiebeveiliging Overheid)
- Standaardtoetsing van externe leveranciers (na eerste toetsing moet leverancier 1-2 jaarlijks blijven rapporteren)
- Hack & Pentesten op alle nieuwe webapplicaties
- Risicoanalyses bij projecten
- Periodieke rapportages informatieveiligheid en jaarlijks worden de nodige beveiligingstests en audits uitgevoerd om vast te stellen of de beveiliging op orde is
- Meldpunt datalekken ingericht en responsible disclosure op website (gepland)
- Inhaalslag beveiliging SCADA-systemen (industriële automatisering) bezig (met verhoogde aandacht en landelijke aanpak)

Crisis

- Security Operations Center (SOC)
  - Permanente dreigingsmonitoring (24/7 operationeel) om aanvallen te kunnen identificeren en te kunnen afslaan
  - SOC staat in verbinding met IBD. Bij grootschalig incident wordt Communicatie aangehaakt, en bij ontwrichting ook OOV. Crisisorganisaties werken echter nog niet intensief met elkaar samen (zie ook thema De openbare orde en veiligheid)

Bron: CISO office; Expert interviews, Analyse projectteam

Eigen huis op orde
Verdieping

Gemeente Amsterdam heeft een significante digitale “footprint”

(Digitale) informatie over en handelingen door:

Inwoners	> 862.000
Medewerkers	> 15.600

Digitale ondersteuning door middel van:

Werkplekken	> 15.000
Applicaties	> 1.000
Laptops	> 4.000
Servers	> 4.000
Uitgaande e-mails/maand	> 8.000.000
Binnenkomende e-mails/maand	> 9.000.000

Bron: OIS; CISO office

Digitale dreigingen - Gemeentelijke organisatie

Iedere dreiging is relevant voor alle onderdelen van de gemeente

	Type dreiging	Interne Dienstverlening	Dienstverlening en Informatie	Sociaal	Ruimte en Economie	Bestuur en Organisatie	Stadsdelen
Moedwillig	Verstoring	2 Snelle aanvallen door hacktivisten veroorzaken korte verstoringen/vertraging 3 Ransomware/langdurige verstoring van gemeentelijke ICT-systemen door criminele hackers of hacktivisten					
	Sabotage	6 Manipulatie van informatie en/of sabotage van buitenaf voor criminele of activistische doeleinden					
	Systeem-/ informatie-manipulatie						
	Diefstal / spionage	4 Onzorgvuldig/frauduleus menselijk handelen veroorzaakt fout/onbetrouwbare informatievoorziening (bijv. in uitkeringsproces) 5 Verlies/diefstal van informatie (menselijke fout of onbevoegde toegang tot vertrouwelijke gegevens)					
Onopzettelijk	Storing/uitval	1 Systeem- of menselijke fouten veroorzaken langdurige uitval gemeentelijke ICT-systemen waardoor dienstverlening in vitale processen niet mogelijk is					
	Datalek	4 Onzorgvuldig/frauduleus menselijk handelen veroorzaakt fout/onbetrouwbare informatievoorziening (bijv. in uitkeringsproces) 5 Verlies/diefstal van informatie (menselijke fout of onbevoegde toegang tot vertrouwelijke gegevens)					

Bron: CIO office, Expert interviews, Analyse projectteam

Meeste incidenten bij gemeente die uitval veroorzaken komen door menselijke fouten

Voorbeeld periodieke rapportage

		Laag					Middel					Hoog					Totaal				
hoofdcategorie	soort incident	BV	SD	Soc	DI	RE	BV	SD	Soc	DI	RE	BV	SD	Soc	DI	RE	BV	SD	Soc	DI	RE
Onbevoegd menselijk ingrijpen	misbruik van bevoegdheden																0	0	0	0	0
	misbruik van informatie																0	0	0	0	0
	fraude																0	0	0	0	0
	diefstal																0	0	0	0	0
	beschadiging																0	0	0	0	0
Menselijke fouten	onzorgvuldigheid																0	0	0	0	0
	bedieningsfouten																0	0	0	0	0
	beheerfouten																0	0	0	0	0
	invoerfouten																0	0	0	0	0
	lekken van persoonsgegevens																0	0	0	0	0
Hardware	fysieke schade																0	0	0	0	0
	storing in apparatuur																0	0	0	0	0
Software	uitval van programmatuur																0	0	0	0	0
	fout in programmatuur																0	0	0	0	0
Infrastructuur	uitval van communicatielijn																0	0	0	0	0
	verstoring van communicatie																0	0	0	0	0
Personeel	uitval van personeel																0	0	0	0	0
Fysieke beveiliging	inbraak																0	0	0	0	0
	stroomstoring / kortsluiting																0	0	0	0	0
	beschadiging aan gebouw																0	0	0	0	0
Externe factoren	natuurgeweld																0	0	0	0	0
	brand																0	0	0	0	0
	wateroverlast																0	0	0	0	0

- Volgens CISO wordt ~80% van de incidenten veroorzaakt door onopzettelijk handelen danwel menselijke fouten
- Bij de recente interne storingen (25 maart, 7 maart en 18 februari 2019) speelden ook verschillende, onopzettelijke handelingen een rol
- Storingen duren (tot nu toe) echter relatief kort en hebben daarom beperkte impact. Dat verandert als de uitval dagenlang zou duren

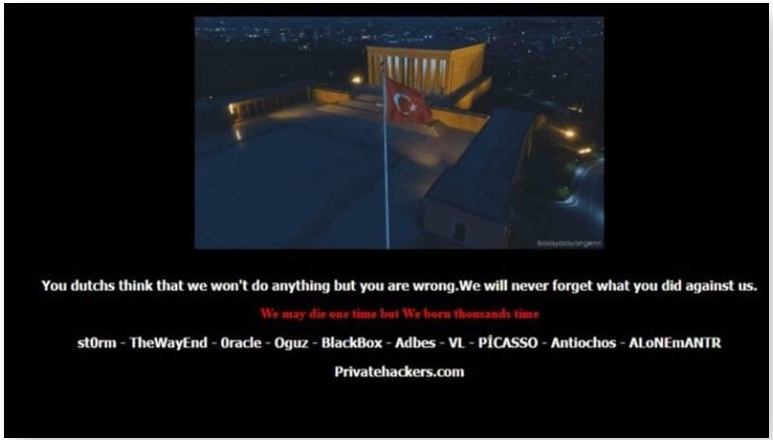
Bron: CISO (Chief Information Security Officer)

Naar aanleiding van een actualiteit zou (gemeente) Amsterdam tijdelijk een specifiek target kunnen worden voor hackers(groepen)

DDoS-aanvallen en websitehacks in 2017 bij bezoek Turkse minister

In maart 2017 mocht de Turkse minister Kaya van Nederland niet landen op Rotterdam The Hague Airport. Direct daarna werd de website van de luchthaven bestookt met een DDoS-aanval. In de dagen daarna werden diverse Nederlandse websites door hackers "defaced" met Turkse teksten

Screenshot van gehackte Nederlandse website



Bron: CISO office; Press search, NOS, FoxIT (https://www.fox-it.com/nl/insights/blogs/blog/nederlandse-banken-en-belastingdienst-geraakt-ddos-aanvallen/)

Ransomware kan een gehele stad langdurig platleggen, zoals Atlanta overkwam in maart 2018

- *In de stad (met bijna 6 miljoen inwoners) versleutelde een virus op 22 maart 2018 bestanden op vele gemeentecomputers. Een hacker eiste 40.000 euro aan bitcoins om de computers weer vrij te geven*
- *"Ik wil duidelijk maken dat dit groter is dan een ransomwareaanval", benadrukte de burgemeester tijdens een persconferentie. "Dit is een aanval op onze overheid. Het is dus een aanval op ons allemaal."*
- *Daphne Rackley, het hoofd van de afdeling informatiemanagement van de stad Atlanta, liet weten dat meer dan een derde van de 424 softwareprogramma's die door de stad gebruikt wordt, helemaal of deels offline is komen te staan door het incident. Daarvan wordt bijna dertig procent beschouwd als "kritisch", waarbij kerndiensten van de stad – waaronder de politie en rechtbanken – in het geding komen*
- *De gemeentelijke diensten raakten dan ook flink ontregeld: politieverslagen moesten met de hand worden uitgeschreven, rechtbanken moesten zaken uitstellen en rekeningen moesten cash worden betaald*

Bron: https://nos.nl/artikel/2225279-atlanta-al-anderhalve-week-in-greep-van-ransomware.html, https://www.techzine.nl/nieuws/405764/atlanta-kan-gevolgen-cyberaanval-bijna-niet-aan.html

Menselijke fouten (of sabotage) kunnen tot grote kostenposten leiden, bijv. bij uitkeringsprocessen

VOORBEELDEN GEBASEERD OP OPENBARE BRONNEN

Woonkostenbijdrage Amsterdam

- *De gemeente Amsterdam heeft in 2013 ca. 9.000 Amsterdamse minima per abuis teveel uitbetaald. Bij de overboeking van de jaarlijkse woonkostenbijdrage is destijds iets misgegaan met komma's en punten. In totaal werd niet 1,88 miljoen maar 188 miljoen euro uitgekeerd, waardoor de betrokken minima enorme bedragen op hun rekening gestort kregen. Anderhalf jaar later, in 2015, stond er nog 1.976.889 euro open*
- *Als gevolg van de fout heeft het college de directie Belastingen onder versterkt toezicht geplaatst en een verbeterprogramma te lanceren (samen met de uitvoering van de WOZ). Dit programma kende een looptijd tot 2018 en was erop gericht de kwaliteit van de waardering structureel op orde brengen en te houden*

Bijstandsuitkeringen Den Haag

- *In april 2019 heeft de gemeente Den Haag per ongeluk 2,5 miljoen euro te veel overgemaakt aan mensen die meededen aan een project rond arbeidsparticipatie. Het betrof 69 Hagenaars met een bijstandsuitkering. De meeste mensen hebben het geld terugbetaald maar er ontbreken nog tienduizenden euro's*
- *Het hoogste bedrag dat per ongeluk op de rekening van een van de 69 mensen verscheen is 108.117 euro en het laagste bedrag is 7.419 euro. De fout is volgens de gemeente ontstaan doordat de bedragen niet goed in het informatiesysteem zijn gezet. Waar een punt stond, had een komma moeten staan*

Bron: Parool (2013), Raadsstuk: Slotrapportage verbeterprogramma's directie Belastingen Nr. BD2018-008528 (2018); Omroep West (2019)

Gemeente heeft organisatie en strategie om informatiebeveiliging te waarborgen

Huidige informatiebeveiligings-organisatie

- 1 CISO, 3 adviseurs informatiebeveiliging
- Ca. 15 ISO's (2-3 per cluster)
- Ca. 10 Privacy Officers (2-3 per cluster)
- Regelmatig overleg en kennisuitwisseling tussen CISO en ISO's bij de clusters via Expertisepool IB

Strategie

- Het Amsterdamse informatiebeveiligingsbeleid is gebaseerd op de VNG-standaarden. Daarbinnen wordt de beveiliging van toepassingen ingericht op basis van risicomanagement. Het college rapporteert jaarlijks aan de raad en externe toezichthouders over informatieveiligheid
- Strategie kent drie pijlers:
  - Betrouwbare, beschikbare en toegankelijke informatievoorziening
  - Aantoonbaar "in control", ook t.a.v. privacy
  - Risicogebaseerde aanpak met als doel voorkomen van schade, misbruik en uitval

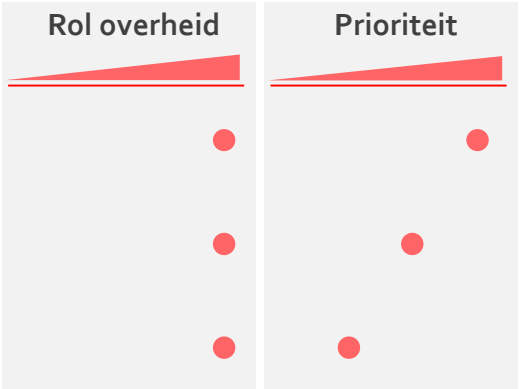
Bron: CISO

Continue aandacht voor digitale veiligheid gemeentelijke processen en versterken beveiligingsbewustzijn is essentieel

AANVULLINGEN UIT VALIDATIE EXPERTTAFEL

Conclusies en aanbeveling(en)

- Waarborgen van continue aandacht en monitoring van de veiligheid van gemeentelijke websites en webapplicaties door het beheer hiervan expliciet in te richten en periodiek beveiligingstests uit te laten voeren
- Verder versterken van het beveiligingsbewustzijn van medewerkers door het uitvoeren van een nieuwe bewustwordingscampagne, gebaseerd op de uitkomsten van een onlangs uitgevoerde 1-meting (n.a.v. de 0-meting in 2017)
- Laat de inkoopcontracten van de gemeente Amsterdam checken op zorgplicht en eerdere voorvallen van cyberincidenten bij de aanbieder



Gestarte acties voor 2019/2020

- Implementeren van het onlangs binnen de gemeente Amsterdam vastgestelde proces voor informatiebeveiligingsincidenten en datalekken, mede gericht op het in staat zijn om incidenten met een grote impact te kunnen afhandelen
- Uitwerken en implementeren van 'Business Continuity Management'

Bron: Experttafel (27-5-2019)

Thema: Het individueel welzijn van burgers

Managementsamenvatting

Inleiding

Thema
Eigen huis op orde

Thema
Het individueel welzijn van burgers

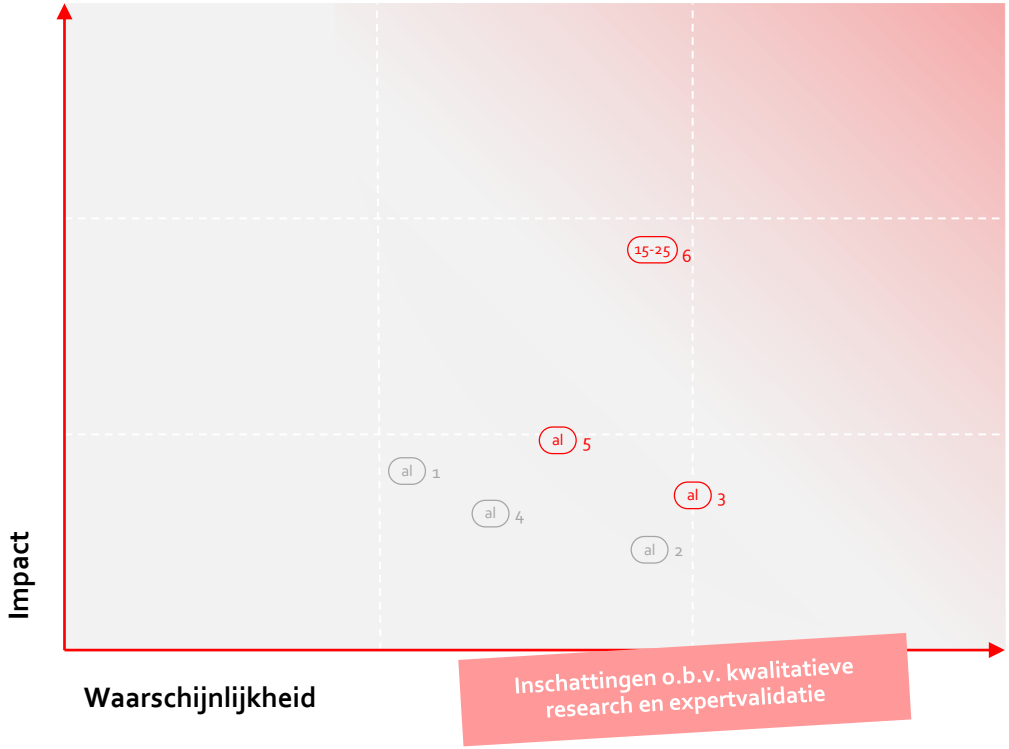
Thema
Private en maatschappelijke organisaties

Thema
Vitale infrastructuur

Thema
Democratie en bestuurlijke stabiliteit

Thema
De openbare orde en veiligheid

Digitaal Veiligheidsbeeld A'dam - Burgers



al Alle leeftijden

1. Phishing
2. Oplichten door webshops
3. **Hacken computers**
4. Hacken social media accounts
5. **Hacken IoT-apparaten**

15-25 Voornamelijk 15-25 jaar

6. **Cyberpesten**

Bron: Expert interviews, Analyse projectteam

Waarschijnlijkheid dreigingen

Laag | Medium | Hoog

Nr	Dreiging	Waarschijnlijkheid
1	Phishing	
2	Oplichten door webshops	
3	Hacken computers	
4	Hacken social media accounts	
5	Hacken IoT-apparaten	
6	Cyberpesten	

Sociale uitsluiting door gebrek aan digitale vaardigheden is een reëel probleem maar valt buiten de scope van digitale veiligheid (zie Agenda Digitale Stad)

Bron: Expert interviews, Analyse projectteam

Mogelijke impact dreigingen

Beperkt | Medium | Significant

Nr	Dreiging	Territoriaal	Fysiek	Economisch	Ecologisch	Sociaal en politiek
1	Phishing		*Traumatische ervaring voor slachtoffer*	*Directe financiële schade*		
2	Oplichten door webshops		*Traumatische ervaring voor slachtoffer*	*Directe financiële schade*		
3	Hacken computers		*Traumatische ervaring voor slachtoffer*	*Mogelijke indirecte financiële schade door bijvoorbeeld gijzeling van bestanden*		*Schade aan sociale positie slachtoffer door ontvreemding gevoelige gegevens*
4	Hacken social media accounts		*Traumatische ervaring voor slachtoffer, mogelijke psychische gevolgen door verspreiden valse berichten*	*Mogelijke indirecte schade door chantage nav hacken social media accounts*		*Schade aan sociale positie slachtoffer door verspreiden gevoelige (nep)gegevens slachtoffer*
5	Hacken IoT-apparaten		*In het ergste geval hacken van apparaten die brand kunnen stichten*	*Mogelijke schade opgelopen beschadigingen door bedienen van apparaten in huis door hackers*		
6	Cyberpesten		*Potentieel ernstige psychische effecten bij (langdurig) cyberpesten, zelfmoordgevallen bekend*	*Mogelijke indirecte schade door chantage*		*Schade aan sociale positie slachtoffer door verspreiden gevoelige (nep)gegevens slachtoffer*

Bron: Expert interviews, Analyse projectteam

Het individueel welzijn van burgers
Verdieping

Digitale dreigingen - Burgers

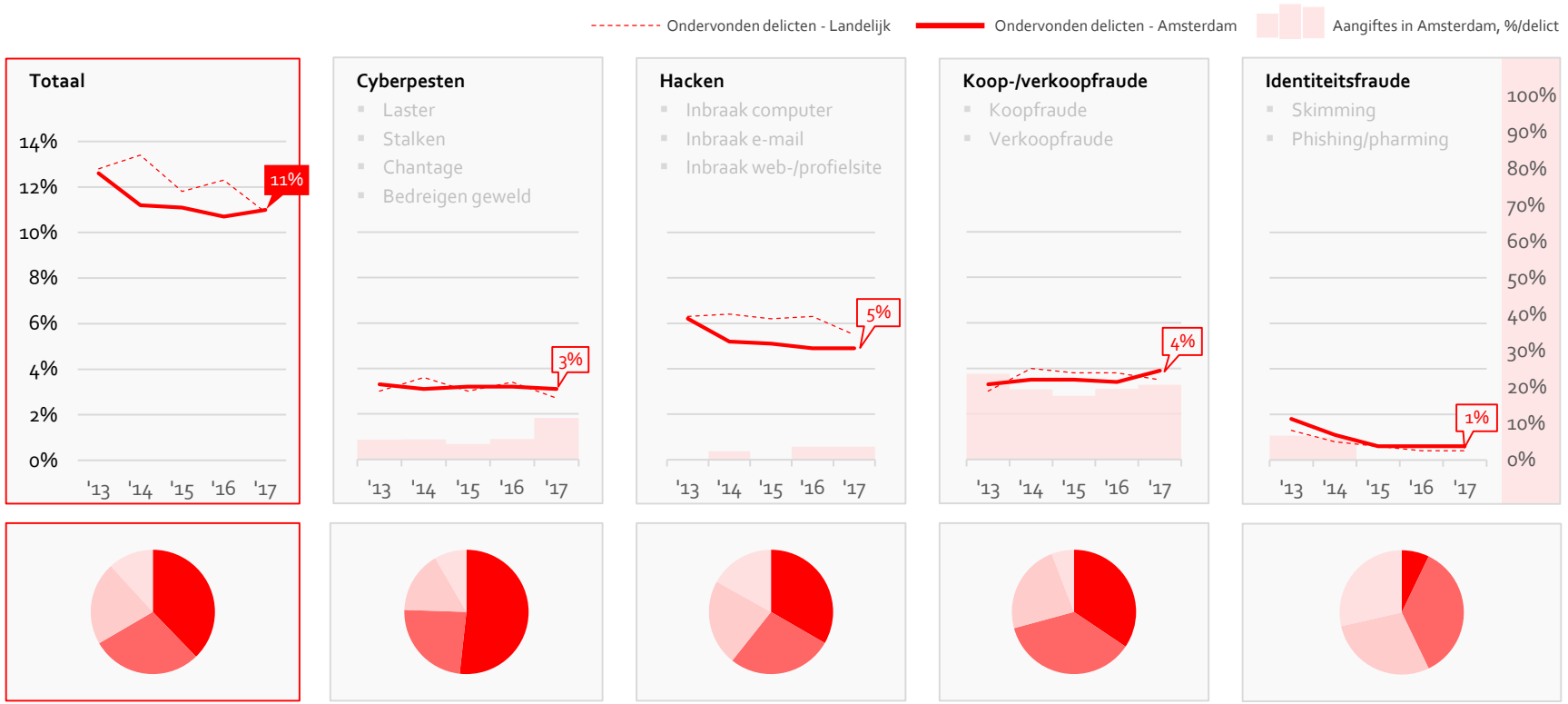
Type aanval	15-25	25-45	45-65	65+
Identiteitsfraude	1	1	1	1
Koop- en verkoopfraude	2	2	2	2
Hacken	3/4/5	3/4/5	3/4/5	3/4/5
Cyberpesten	6			

Belangrijkste dreigingen

1. Phishing
2. Oplichten door webshops
3. Hacken computers
4. Hacken social media accounts
5. Hacken IoT-apparaten
6. Cyberpesten

Bron: CBS, Expert interviews, Analyse projectteam

11% Amsterdammers jaarlijks slachtoffer cybercrime – in totaal neemt percentage over afgelopen jaren licht af in Amsterdam



Politie A'dam is bezig de informatiepositie op het gebied van cybercrime te verbeteren, o.a. meer gedetailleerde data per cyberdelict (aantal, type slachtoffer, schade). Deze is nog niet volledig en vergelijkbaar over de jaren heen. Daarom kiezen wij er voorlopig voor alleen CBS cijfers over ondervonden delicten te gebruiken

[1] Totaalcijfers zijn anders dan de som van de afzonderlijke dreigingen vanwege overlap

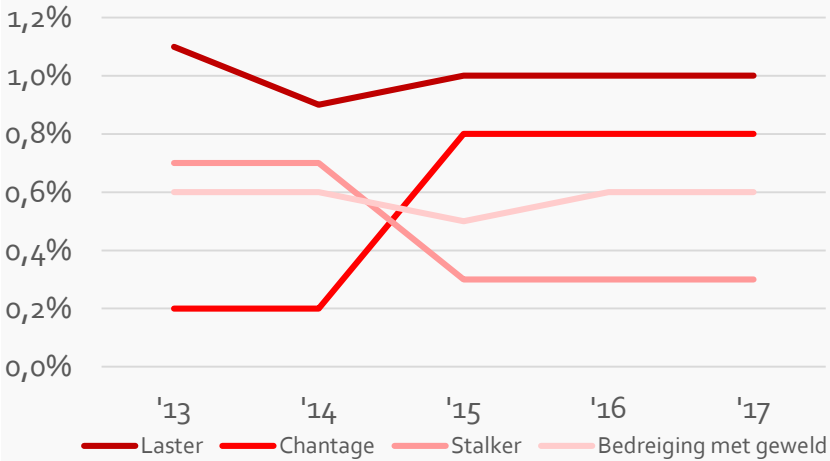
Bron: CBS

Cyberpesten in Amsterdam voornamelijk onder jongeren, betreft vooral laster en chantage

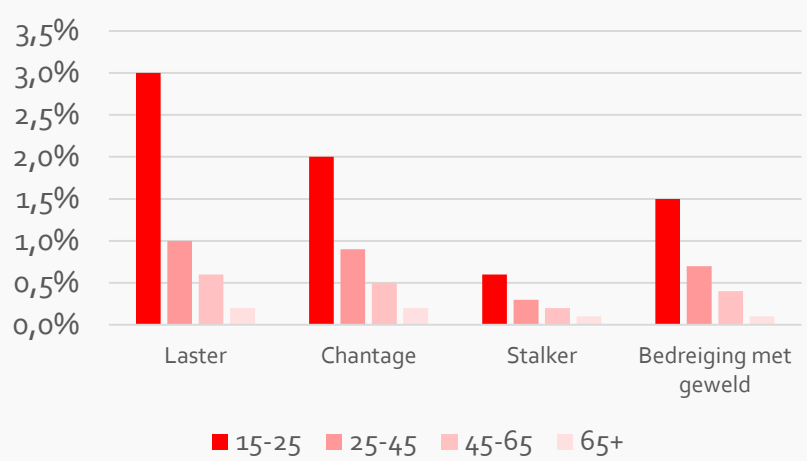
Laster en chantage meestvoorkomende vormen van cyberpesten

Hoewel cyberpesten over de afgelopen jaren heel licht afneemt, neemt chantage wel toe. Samen met laster zijn dat de twee grootste dreigingen, voornamelijk onder jongeren tussen 15 en 25 jaar. Veel van de kennismaking met seksualiteit speelt zich online af, een negatief bij-effect daarvan is de toename van misbruik van o.a. het delen van naaktfoto's en –filmpjes.

Vormen van cyberpesten over tijd



Vormen van cyberpesten per leeftijdsgroep in 2017



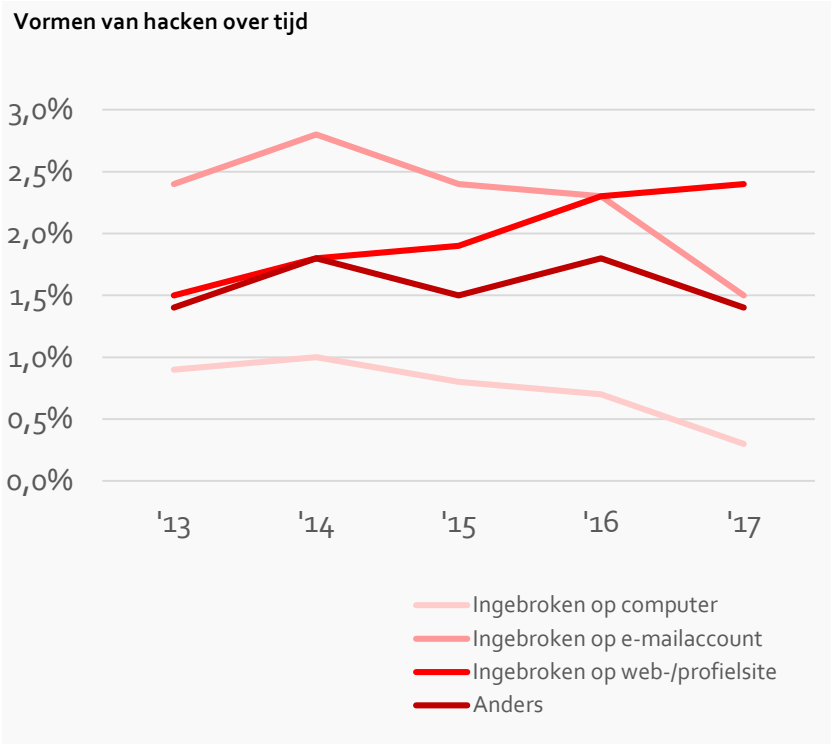
Bron: CBS

Hacken neemt licht af in Amsterdam, web- en profielsites zijn belangrijkste doelwit van hackers

Aantal slachtoffers van hacken licht gedaald

Het aantal Amsterdammers dat een hack heeft ondervonden in 2017 ligt rond de 5% blijkt uit cijfers van het CBS. Het ligt daarmee ongeveer gelijk met het landelijk gemiddelde en is in de afgelopen jaren licht gedaald. Onder hacken wordt verstaan het inbreken op:

- Computer
- E-mailaccounts
- Web- en profielsites



Bron: CBS

Risico van hacken door toename van (slecht beveiligde) IoT-verbindingen

IoT belangrijke pijler in de toekomst

Hoewel de ontwikkeling van aantallen hacks niet zorgwekkend lijkt is er wel grote aandacht voor de toename van Internet of Things (IoT), het gebruik van apparaten die op het internet zijn aangesloten.


Online 26.06.2017

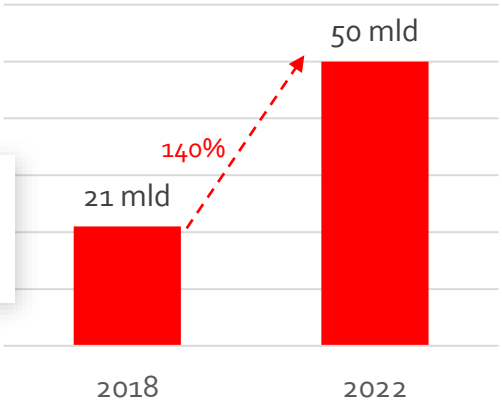
Internet of Things gebruik neemt flink toe in 2021

Het hele internet zit nog altijd in een enorme groeicurve

IDC: 'Investeringen in IoT stijgt in 2019 met dubbele groeicijfers'

De wereld zal dit jaar zo'n 745 miljard dollar uitgeven aan Internet of Things. Dat bedrag zal de komende jaren nog toenemen, zowel in de industrie als thuis.

Toename aantal IoT-verbindingen in komende jaren[1]



Gevaar hacken van IoT-apparaten

In de afgelopen jaren is herhaaldelijk duidelijk geworden hoe makkelijk het is oom IoT-apparaten te hacken.

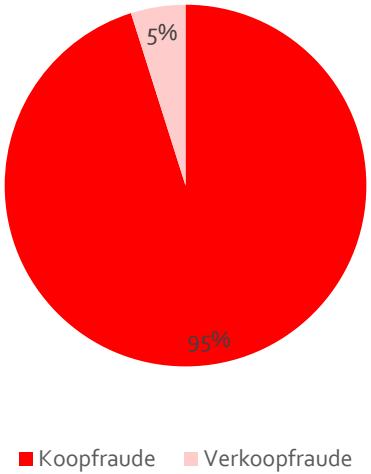
- In 2016 kwam de pop "My Friend Cayla" in het nieuws omdat het zonder veel moeite gehackt bleek te kunnen worden. Alleen de aanwezigheid van een telefoon met bluethooth was daarvoor nodig, waarna hackers de kinderen konden afluisteren en de pop dingen konden laten zeggen tegen de kinderen.[2]
- In 2017 lieten hackers zien hoe gemakkelijk het was om een volledige geautomatiseerde wasstraat te hacken, waarna ze auto's konden beschadigen door op de juiste momenten de deuren dicht te doen of de borstels hard op de auto te laten neerkomen. Het nieuwsartikel stipte het gevaar aan van het hacken van apparaten waarmee brand veroorzaakt kan worden, zoals broodroosters.[3]

Bron: [1] https://telecomnieuwsnet.wordpress.com/2018/06/22/juniper-research-aantal-iot-verbindingen-gaat-snel-toenemen/, [2] https://nos.nl/artikel/2146787-speelgoedpop-my-friend-cayla-blijkt-kinderen-af-te-luisteren.html [3] https://www.dutchcowboys.nl/online/kijk-hoe-een-gehackte-wasstraat-een-auto-aanvalt

Koop- en verkoopfraude voornamelijk oplichting via Marktplaats

Gros gaat om koopfraude

Bij koopfraude betaalt de koper, maar blijft de verkoper in gebreke door niet te leveren. Bij verkoopfraude wordt een artikel geleverd maar wordt het geld niet overgemaakt.



Groot deel van de gevallen vindt plaats via Marktplaats

Ruim de helft van de gedupeerden in het publieksonderzoek deed de aankoop via Marktplaats. Volgens een woordvoerder van Marktplaats komen er dagelijks 75 meldingen binnen van oplichting, op 80.000 dagelijkse transacties.


Online opgelicht? Naar je geld kun je fluiten

29-05-2017, 06:08 AANGEPAST 29-05-2017, 11:36 BINNENLAND

Bronnen: CBS, https://nos.nl/artikel/2175501-online-opgelicht-naar-je-geld-kun-je-fluiten.html

Programma's en initiatieven

Programma: Gezonde School VO, thema Mediawijsheid

Beschrijving	Binnen het programma Gezonde School Amsterdam-Amstelland biedt de GGD scholen ondersteuning aan voor het thema Mediawijsheid. Er wordt gewerkt aan een structurele aanpak op de pijlers Educatie, Signaleren, Omgeving en ouders en Beleid.
Initiatiefnemer	GGD Amsterdam, afdeling EGZ
Doelgroep	VO
Type (eenmalig, terugkerend, website)	Terugkerend
Datum/sinds	2018
Doelstelling/resultaat	Scholen kiezen hun eigen thema uit 7 thema's van de Gezonde School. Andere thema's zijn bijvoorbeeld preventie Genotmiddelen of gezonde Voeding. Nadat een school een thema gekozen heeft wordt in principe in twee leerjaren een structurele en integrale aanpak.
Bereik (mensen/scholen)	Enkele VO scholen per jaar. In juli zijn de bereikcijfers van schooljaar 2018/2019 bekend.
Hoe is het bekostigd	GGD en OJZ

Programma's en initiatieven

Programma: Gezonde School VO, thema Seksualiteit

Beschrijving	Binnen het programma Gezonde School Amsterdam-Amstelland biedt de GGD scholen ondersteuning aan voor het thema Seksualiteit. Binnen de pijler Educatie wordt het lesprogramma 'Lang Leve de Liefde' aangeboden. Hierin wordt aandacht besteed aan sexting. Scholen kunnen daarnaast ook nog kiezen voor een extra module over sexting: 'Love online'.
Initiatiefnemer	GGD Amsterdam, afdeling EGZ
Doelgroep	VO
Type (eenmalig, terugkerend, website)	Terugkerend.
Datum/sinds	2010
Doelstelling/resultaat	Scholen kiezen hun eigen thema uit 7 thema's van de Gezonde School. Andere thema's zijn bijvoorbeeld Preventie Genotmiddelen of |Gezonde Voeding. Nadat een school een thema gekozen heeft wordt in principe in twee leerjaren een structurele en integrale aanpak.
Bereik (mensen/scholen)	42 VO scholen werken met het lesprogramma Lang Leve de Liefde, enkele daarvan maken bovendien gebruik van de extra module over sexting.
Hoe is het bekostigd	GGD en OJZ

Programma's en initiatieven

Programma: Gezonde School, praktijkonderwijs, thema seksualiteit.

Beschrijving	Binnen het programma Gezonde School Amsterdam-Amstelland biedt de GGD scholen voor Praktijkonderwijs een extra programma aan ter preventie van seksueel grensoverschrijdend gedrag. Het programma heet 'Je Lijf, je Lief'. Binnen dit programma is aandacht voor seksueel grensoverschrijdend gedrag via sociale media bij online flirten en sexting.
Initiatiefnemer	GGD Amsterdam, afdeling EGZ
Doelgroep	Leerlingen van in het Praktijkonderwijs
Type (eenmalig, terugkerend, website)	Terugkerend.
Datum/sinds	2017
Doelstelling/resultaat	Docenten worden getraind om met het programma te werken. Het lesprogramma bestaat uit 5 lessen.
Bereik (mensen/scholen)	6 van de 7 Amsterdamse scholen voor praktijkonderwijs doen mee.
Hoe is het bekostigd	GGD en OJZ

Programma's en initiatieven

Programma: Gezonde School PO, thema Seksualiteit

Beschrijving	De GGD ondersteund scholen bij het inzetten van het lesprogramma 'Kriebels in je Buik'. Dit is een breed programma voor seksuele vorming voor het Primair Onderwijs. In de onderdelen voor groep 7 en 8 is aandacht voor het bewaren van je privacy online, het relativeren van beelden in de media en is aandacht voor sexting.
Initiatiefnemer	GGD Amsterdam, afdeling EGZ
Doelgroep	PO
Type (eenmalig, terugkerend, website)	Terugkerend.
Datum/sinds	2009. Het programma heeft zich sindsdien steeds verder ontwikkeld.
Doelstelling/resultaat	Docenten worden getraind om met het programma te werken. Er is lesmateriaal voor onder- midden- en bovenbouw.
Bereik (mensen/scholen)	In Amsterdam worden ongeveer 60 scholen voor PO bereikt.
Hoe is het bekostigd	GGD en OJZ

Programma's en initiatieven
Conferentie: (v)mbo mediawijs

Beschrijving	Digitale middelen en sociale media zijn niet meer weg te denken uit ons leven. Maar ook niet meer uit de klas. Dat stelt docenten voor uitdagingen. Hoe zet je digitale didactiek in? Thema's o.a. nepnieuws, cyberpesten en cybersecurity.
Initiatiefnemer	Gemeente Amsterdam, afdeling Onderwijs
Doelgroep	Docenten (v)mbo
Type (eenmalig, terugkerend, website)	Jaarlijks terugkerend met een verschillend thema, in 2019 was dat thema (v)mbo mediawijs
Datum/sinds	Februari 2019
Doelstelling/resultaat	…
Bereik (mensen/scholen)	Doelstelling bereiken van 250 docenten
Hoe is het bekostigd	…

Programma's en initiatieven
Campagne: Het Gesprek

Beschrijving	Campagne om sexting bespreekbaar te maken
Initiatiefnemer	QPido in samenwerking met gemeente Amsterdam
Doelgroep	Ouders
Type (eenmalig, terugkerend, website)	Tijdelijke campagne
Datum/sinds	December 2017
Doelstelling/resultaat	Bewustwording bij ouders over online risico's op seksueel grensoverschrijdend gedrag rondom jeugd
Bereik (mensen/scholen)	Aantal unieke personen: 123.323, waarvan: Nederlandstalig: 79.976, Arabisch: 6.103, Turks: 13.024, Engels: 34.913
Hoe is het bekostigd	Begroting Jeugd

Programma's en initiatieven
Website: Helpwanted.nl

Beschrijving	Site voor (ouders van) kinderen en jongeren die geconfronteerd worden met sexting, grooming en kinderporno
Initiatiefnemer	Gemeente Amsterdam, afdeling Onderwijs
Doelgroep	Ouders, kinderen, jongeren
Type (eenmalig, terugkerend, website)	Website
Datum/sinds	
Doelstelling/resultaat	
Bereik (mensen/scholen)	
Hoe is het bekostigd	

Programma's en initiatieven
Centrum voor Criminaliteitspreventie en Veiligheid (CCV)

Het CCV is een onafhankelijke stichting die in samenwerking met de VNG partijen helpt om Nederland veiliger en leefbaarder te maken. Het CCV heeft verschillende programma's tegen cybercrime die voor de gemeente Amsterdam interessant zouden kunnen zijn ter inspiratie.

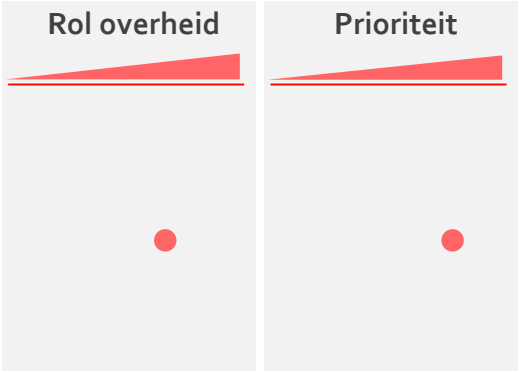
Cyber24	Cyber24 is een korte training voor jongeren die gemeenten - samen met scholen - kunnen inzetten om bewustwording bij jongeren te creëren wat de gevolgen zijn van bewust of onbewust onwenselijk online gedrag. De training wordt gestart met serious gaming waarin jongeren geconfronteerd worden met ID-fraude, digitaal pesten of bedreiging. Na de interactieve game volgt een gesprek met een begeleider over het vertoonde gedrag en de consequenties hiervan.
CCV-barrièremodel sexting	In het barrièremodel sexting wordt inzichtelijk wat de rollen, verantwoordelijkheden en mogelijke interventies van de verschillende professionals zijn waar het gaat om normoverschrijdend gedrag door jongeren in de (digitale) sociale context. Het barrièremodel sexting komt in 2019 beschikbaar.

Vooral cyberpesten moet serieuze aandacht krijgen

AANVULLINGEN UIT VALIDATIE EXPERTTAFEL

Conclusies en aanbeveling(en)

- Scope van dit thema zou gerichter kunnen door doelgroepen specifieker te maken
- Rol van de ouder(s) cruciaal: "omgangsvormen in de digitale wereld hebben een impact in de fysieke ruimte"
- Cyberpesten moet serieuze aandacht krijgen. Cijfers zeggen niet zoveel en pesten met digitale middelen wordt steeds makkelijker
- Zoek samenwerking met private initiatieven in de stad (bijv. aansluiten op de Stichting Cyber School van de DNB)



Gestarte acties voor 2019/2020

- Mede op basis van output experttafel wordt een monitor overzicht opgesteld (door OI&S) voor kwantitatieve gegevens op dreigingen/kenmerken digitalisering:
  - Cyberpesten
  - Identiteitsfraude
  - Koop- en verkoopfraude (incl. online)
  - Hacken
  - Beschikbaarheid laptop, tablet, personal computer per huishouden
  - Gebruik social media
  - Vertrouwen in de overheid

Bron: Experttafel (27-5-2019)

Thema: Private en maatschappelijke organisaties

Managementsamenvatting

Inleiding

Thema
Eigen huis op orde

Thema
Het individueel welzijn van burgers

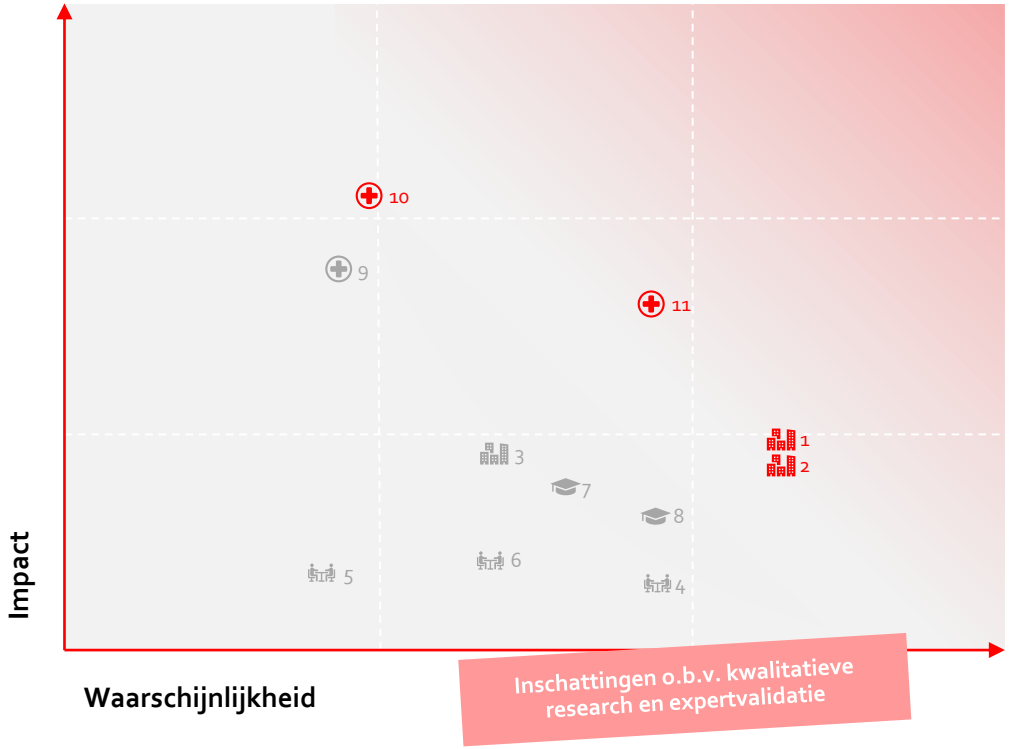
Thema
Private en maatschappelijke organisaties

Thema
Vitale infrastructuur

Thema
Democratie en bestuurlijke stabiliteit

Thema
De openbare orde en veiligheid

Digitaal Veiligheidsbeeld A'dam - Private en maatschappelijke organisaties



Grote bedrijven

1. Mal- of ransomware aanval op groot bedrijf, voornamelijk financiële sector
2. Ontvreemding van data van grote bedrijven
3. Datalek bij groot bedrijf

MKB

4. Aanval op systemen MKB
5. Hacken van bedrijfsprocessen in MKB
6. Ontvreemden van data in MKB

Onderwijsinstelling

7. Ontvreemden van data in onderwijsinstellingen
8. Datalek in onderwijsinstelling

Zorginstellingen

9. Aanval op zorginstelling
10. Hacken en verstoren van apparaten/systemen binnen zorginstellingen
11. Datalek bij zorginstellingen

Waarschijnlijkheid dreigingen

Laag | Medium | Hoog

Nr	Dreiging	Waarschijnlijkheid
1	Aanval op groot bedrijf, voornamelijk financiële sector	
2	Ontvreemding van data van grote bedrijven	
3	Datalek bij groot bedrijf	
4	Aanval op systemen MKB	
5	Hacken van bedrijfsprocessen in MKB	
6	Ontvreemden van data in MKB	
7	Ontvreemden van data in onderwijsinstellingen	
8	Datalek in onderwijsinstelling	
9	Aanval op zorginstelling	
10	Hacken en overnemen van apparaten / systemen binnen zorginstellingen	
11	Datalek bij zorginstellingen	

Bron: Expert interviews, Analyse projectteam

Mogelijke impact dreigingen

Beperkt | Medium | Significant

Nr	Dreiging	Territoriaal	Fysiek	Economisch	Ecologisch	Sociaal en politiek
1	Aanval op groot bedrijf, voornamelijk financiële sector			*Directe schade door diefstal, indirecte financiële schade door herstel- en beveiligingswerkzaamheden*		
2	Ontvreemding van data van grote bedrijven			*Indirecte financiële schade door claims en chantage, herstel- en beveiligingswerkzaamheden*		*Grote schade in betrouwbaarheid van bedrijf*
3	Datalek bij groot bedrijf			*Mogelijke indirecte financiële schade door claims, herstel- en beveiligings-werkzaamheden*		*Grote schade in betrouwbaarheid van bedrijf*
4	Aanval op systemen MKB			*Financiële schade door herstelwerkzaamheden en stilliggen bedrijfsprocessen*		
5	Hacken van bedrijfsprocessen in MKB			*Financiële schade door herstelwerkzaamheden en stilliggen bedrijfsprocessen*		
6	Ontvreemden van data in MKB			*Mogelijke financiële schade door diefstal intellectueel eigendom, claims en chantage*		
7	Ontvreemden van data in onderwijsinstellingen					*Schade in betrouwbaarheid van organisatie*
8	Datalek in onderwijsinstelling					*Schade in betrouwbaarheid van organisatie*
9	Aanval op zorginstelling		*Uitvallen van apparaten / systemen binnen zorginstelling*	*Schade door herstelwerkzaamheden*		
10	Hacken en overnemen van apparaten / systemen binnen zorginstellingen		*Fysieke schade patiënten door hacken van apparaten*	*Schade door herstelwerkzaamheden*		
11	Datalek bij zorginstellingen		*Mogelijkheid tot zware privacy schending*	*Mogelijke schade door claims en chantage*		*Grote schade in betrouwbaarheid van bedrijf*

Bron: Expert interviews, Analyse projectteam

Private en maatschappelijke organisaties
Verdieping

Speelveld private en maatschappelijke organisaties in Amsterdam

Private organisaties

Grote bedrijven
- Banken
- Supermarkten

MKB

Maatschappelijke organisaties

Onderwijsinstellingen
- Basisscholen
- Middelbare scholen
- Universiteiten/hogescholen

Zorginstellingen
- Ziekenhuizen
- Thuiszorg

Culturele instellingen
- Musea
- Debatcentra

Gemeente Amsterdam buiten scope in dit thema (zie thema Eigen huis op orde)

Digitale dreigingen - Private en maatschappelijke organisaties

	Type dreiging	Grote bedrijven	MKB	Onderwijsinstelling	Culturele instelling	Zorginstelling
Moedwillig	Verstoring	1	4		9	9
	Sabotage					
	Systeem- en Informatiemanipulatie		5			10
	Diefstal/spionage	2	6	7		
Onopzettelijk	Storing/uitval					
	Datalek	3		8		11

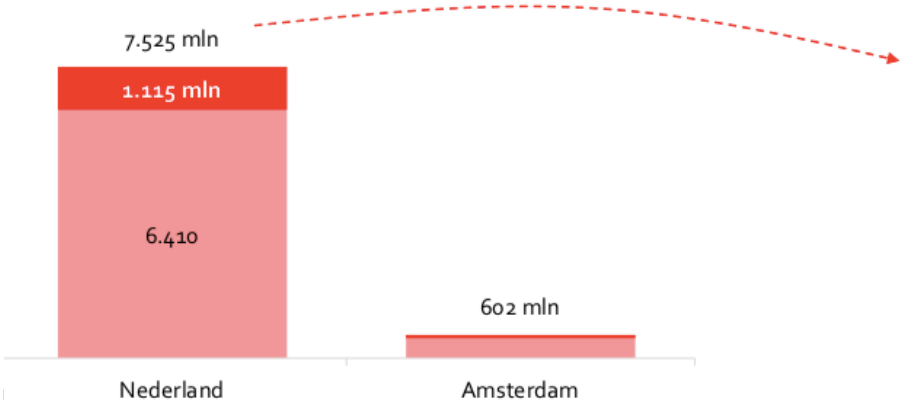
Belangrijkste dreigingen

1. Aanval op groot bedrijf, voornamelijk financiële sector
2. Ontvreemding van data van grote bedrijven
3. Datalek bij groot bedrijf
4. Aanval op systemen MKB
5. Hacken van bedrijfsprocessen in MKB
6. Ontvreemden van data in MKB
7. Ontvreemden van data in onderwijsinstellingen
8. Datalek in onderwijsinstelling
9. Aanval op zorginstelling
10. Hacken en verstoren van apparaten/systemen binnen zorginstellingen
11. Datalek bij zorginstellingen

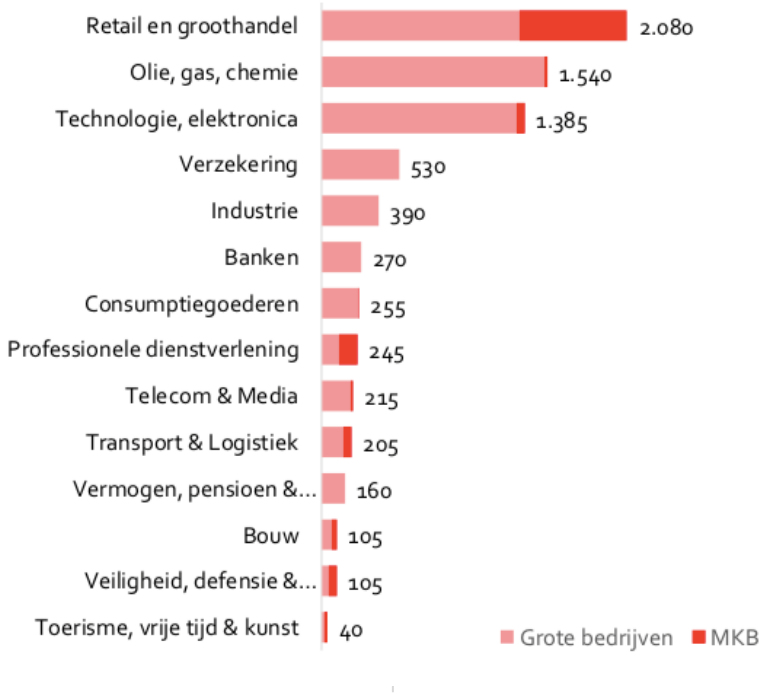
Bron: Expert interviews, Analyse projectteam

Jaarlijkse kosten cybercrime worden op ~€7,5 mld ingeschat voor NL, afgeleide kosten ~€0,6 mld voor Amsterdam

Totaal kosten 2017 grote bedrijven en MKB in mln, Amsterdam en landelijk



Kosten 2017 grote bedrijven en MKB per sector in mln, landelijk



Toelichting

- Cijfers uit onderzoek van Deloitte over 2017. In 2012 kwam TNO tot een inschatting van vergelijkbare grootte
- Amsterdamse kosten op basis van het aantal bedrijven in Nederland vs het aantal bedrijven in Amsterdam, kosten en verdeling naar rato afgeleid

Bron: Deloitte: Dealing efficiently with cybercrime; Cyber Value at Risk in The Netherlands 2017

Grote bedrijven zijn landelijk vaker doelwit dan MKB, met name financiële sector is slachtoffer

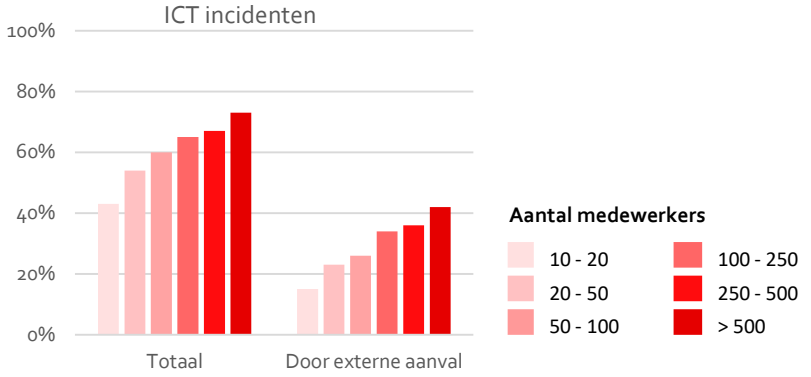
Grote bedrijven regelmatig getroffen

Uit cijfers van het CBS blijkt dat grotere bedrijven vaker digitale dreigingen ondervinden dan kleinere bedrijven. Een deel van die dreigingen zijn intern, een groot deel ook extern. Belangrijkste oorzaken zijn vaak onbewuste interne datalekken en bewuste externe aanvallen:

- Interne datalekken: vaak door fouten van medewerkers komen soms grote hoeveelheden data op straat te liggen.
- Externe aanvallen: het is steeds makkelijk om grootschalige aanvallen uit te voeren. Uit voorbeelden blijkt dat je al voor EUR 40 een aanval kan uitvoeren die grote gevolgen heeft voor slachtoffers.

Financiële sector relatief vaak slachtoffer

- Het Financieel Stabiliteitscomité waarschuwt in februari 2018 voor toenemende digitale dreiging voor de financiële sector. Aanvalstechnieken worden steeds geavanceerder en meerdere instellingen kunnen tegelijkertijd worden geraakt. De concentratie van financiële instellingen in Amsterdam maakt dat dit een voornamelijk Amsterdamse dreiging is.
- Volgens de Autoriteit Persoonsgegevens is de financiële sector de sector met de tweede grootste aantal datalekken in 2017 (26% van de gemelde datalekken)



In januari 2018 kreeg Nederland te maken met DDoS-aanvallen op verschillende overheids- en financiële instellingen [...]. Op 1 februari 2018 werd een man [...] gearresteerd op verdenking van het uitvoeren van de DDoS-aanvallen. Volgens zijn verklaring kon hij de aanvallen uitvoeren door 40 euro te betalen voor een zogenoemde stresser, een dienst die ingeschakeld kan worden om systemen te testen op de belastbaarheid.

- CSBN 2018

Bronnen: CBS (bestand Nathalie), https://www.financieelstabiliteitscomite.nl/, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarrapportage_meldplicht_datalekken_2018.pdf

Aandacht voor digitale dreigingen binnen MKB richt zich op bewustwordingscampagnes, onderwerp heeft weinig prioriteit

Bewustwording digitale veiligheid grootste aandachtspunt MKB

40% van het MKB landelijk heeft al eens een poging van cybercrime ondervonden. 20% is daadwerkelijk slachtoffer geworden. Bewustzijn van cybercrime is zeer laag onder MKB'ers en wordt vaak pas gestimuleerd na een poging.

Voor MKB Amsterdam en Platform Veilig Ondernemen Amsterdam-Amstelland gaat de aandacht voor digitale veiligheid voornamelijk uit naar bewustwordingscampagnes en trainingen in digitale veiligheid. Voor geen van de betrokken partijen heeft het onderwerp echter hoge prioriteit.

'Cybercriminelen maken misbruik van het gebrek aan kennis'

Vooral het mkb is gebaat bij meer bewustwording op het gebied van cybersecurityrisico's, blijkt uit het onderzoek van Interpolis en Capgemini. Risicodeskundige Johan Feenstra weet wat er moet veranderen.

Bij grote ondernemingen als verzekeraa
die bewustwording er wel, maar in het r
Het mkb is natuurlijk heel groot, zo'n on
om ondernemers te helpen. Vaak ligt in
directeur, of heeft iemand het in takenp

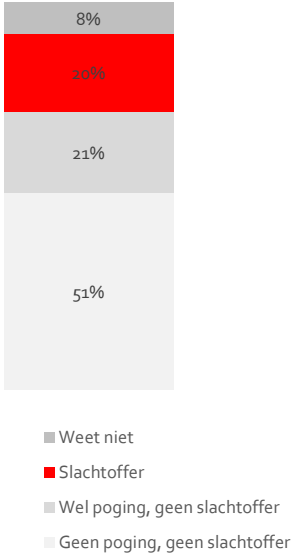
'BEWUSTZIJN DIGITALE VEILIGHEID MKB DAALT'

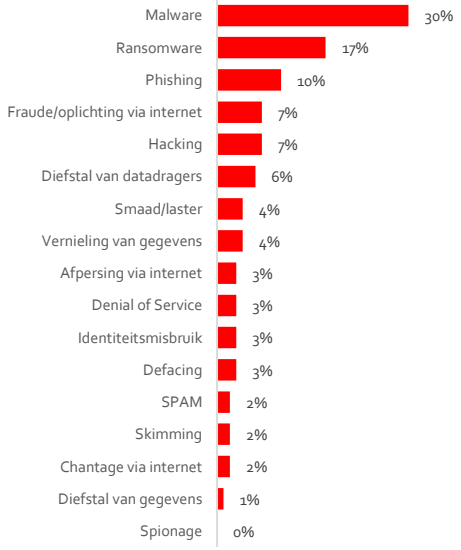
BNR webredactie / maandag 8 oktober 2018, 12:24

Bedrijven in het mkb worden steeds vaker slachtoffer van internetcriminelen. Reden genoeg tot zorgen, zou je zeggen. Maar uit onderzoek van Alert Online blijkt dat juist steeds minder mkb-bedrijven zich zorgen maken over hun digitale veiligheid. 'Als bij je buurman wordt ingebroken, zie je dat. Bij cyberaanvallen zie je dat niet, totdat het je overkomt', zegt Rutger Leukfeldt, lector cybersecurity in het mkb aan de Haagse Hogeschool.

Slachtoffers cybercrime MKB landelijk

Van de aanvallen die MKB'ers ondervinden is het grootste deel erop gericht om klant- en betaalgegevens te bemachtigen om daar geld mee te verdienen. Amsterdamse cijfers zijn niet bekend.





Bron: "Hoe cybersecure is het MKB?" De Haagse Hogeschool, https://www.alertonline.nl/nieuws/2018/cybersecurity-bewustzijnsonderzoek-2018-kleine-bedrijven-meest-geconfronteerd-met-phishing-en-acquisitiefraude

Binnen maatschappelijke organisaties vooral ziekenhuizen doelwit van digitale dreigingen door menselijke fouten en externe aanvallen

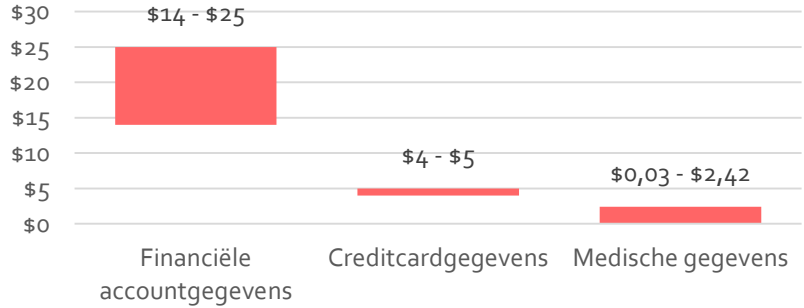
Cyberdreigingen bij ziekenhuizen

De digitale beveiliging van ziekenhuizen is beperkt, ziekenhuizen zijn regelmatig slachtoffer van digitale dreigingen. De meest voorkomende zijn:

- Datalekken: sector zorg heeft volgens de autoriteit persoonsgegevens de meeste datalekken. Van de bijna 21.000 datalekken die in 2018 gemeld zijn bij de Autoriteit Persoonsgegevens kwam bijna een derde uit de zorg[1].
- Data-ontvreemding: medewerkers in de zorg zijn wat betreft digitale veiligheid de zwakste schakel in de organisatie. Mede door wachtwoordgedrag en trucs om in en uit te loggen vormen ze een risico en spelen ze het ontvreemden van data in de hand.
- Ransomware: bestanden worden gegijzeld in ruil voor losgeld. Omdat ziekenhuizen elke dag backups maken hoeft er vrijwel nooit losgeld betaald te worden, maar de mogelijkheid tot hacken is zorgelijk.
- Hacken van IoT: hoewel een algemene dreiging, groeit IoT het hardst in de zorg (30% per jaar)[2] en kan het fysieke schade aanbrengen aan patiënten.

Dreigingen bij onderwijsinstellingen komen voor, maar minder frequent. Binnen de culturele sector zijn weinig meldingen van digitale dreigingen

De waarde van gestolen data per record



De marktwaarde van patiëntgegevens zijn lager dan bijv financiële gegevens omdat er meer handelingen uitgevoerd moeten worden voordat ze geld opleveren (zoals het koppelen aan andere databronnen). Daartegenover staat dat de waarde lang behouden zal blijven omdat de data niet te vervangen is, zoals creditcardgegevens dat wel zijn. Financiële gegevens zijn daarom populairder, maar ook medische gegevens zijn in trek.

Bron: https://www.dutchcowboys.nl/cybercrime/nederlandse-ziekenhuizen-lopen-vaak-achter-met-digitale-beveiliging, https://www.ictmagazine.nl/onderzoek-iot-koelkasten-bedrijven-en-ziekenhuizen-eenvoudig-te-hacken/, Health Warning, McAffee, https://nos.nl/artikel/2179941-zeker-vijftien-ziekenhuizen-geinfecteerd-met-ransomware.html,
1) https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarrapportage_meldplicht_datalekken_2018.pdf 2) https://www.dutchcowboys.nl/online/internet-of-things-gebruik-neemt-flink-toe-in-2021

Programma's en initiatieven

Platform Veilig Ondernemen (PVO)

PVO faciliteert zes gemeenten in Noord-Holland en heeft als belangrijkste speerpunten cybercrime, ondermijning, overvallen en de aanpak van winkeldiefstal

- De focus van het PVO ligt dit jaar bij MKB, omdat deze doelgroep het meest kwetsbaar is. MKB'ers lopen vaak achter op grote bedrijven in digitale veiligheid. Probleem is dat de mogelijke risico's van digitale onveiligheid minder leven dan fysieke veiligheid onder het MKB, en men vaak pas in actie komt als er een incident is geweest
- PVO is opdrachtgever voor een informatiebox veilig ondernemen die momenteel wordt ontwikkeld door de veiligheidscoördinatoren van de verschillende stadsdelen. Deze informatiebox is een map/doos met informatie over veilig ondernemen voor (nieuwe) ondernemers
- Daarnaast is bestaat er al een toolbox van het PVO. Deze toolbox is een digitaal overzicht van alle trainingen, workshops en tools die er beschikbaar zijn voor ondernemers in het kader van veilig ondernemen. Binnenkort zal deze toolbox te vinden zijn op de site van het PVO.

Team High Tech Crime, Politie

THTC is een speciaal team tegen de meest geavanceerde vorm van cybercrime

- THTC is bezig om te bekijken hoe zij meer de link naar de dagelijkse praktijk kunnen leggen om meer inzicht te krijgen in cybercrime. Daarvoor hebben ze o.a. contact met ondernemers

Programma's en initiatieven
Centrum voor Criminaliteitspreventie en Veiligheid (CCV)

Het CCV is een onafhankelijke stichting die in samenwerking met de VNG partijen helpt om Nederland veiliger en leefbaarder te maken. Het CCV heeft verschillende programma's tegen cybercrime die voor de gemeente Amsterdam interessant zouden kunnen zijn ter inspiratie.

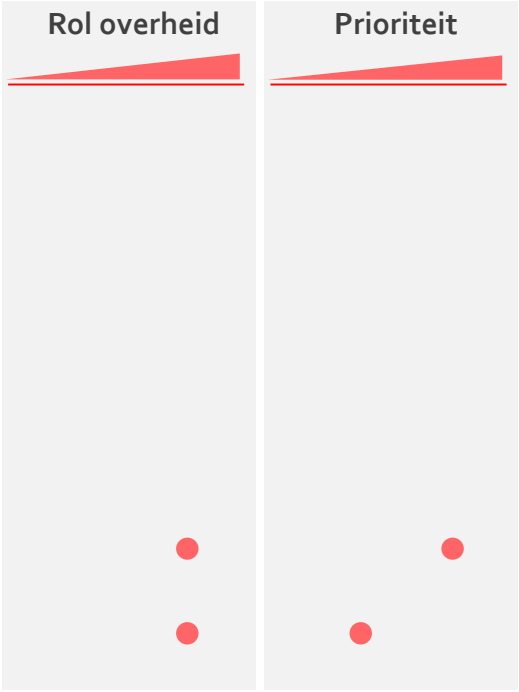
Cybercrime Digitaal Veilig	▪ In de training 'Cybercrime Digitaal Veilig' van het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV) leren mkb-ondernemers en hun medewerkers hoe zij het risico om slachtoffer te worden van cybercrime zoveel mogelijk kunnen verkleinen. Het is een praktijkgerichte training die met name ingaat op eenvoudig te nemen maatregelen en het eigen gedrag om de digitale veiligheid te verbeteren. Na afloop ontvangen de deelnemers een handige Kryptonizer die helpt om sterke wachtwoorden te maken.
Risicomodel en Keurmerk Cybersecurity voor ondernemers	▪ In het project Vertrouwd Digitaal Ondernemen ontwikkelt het CCV een risicomodel en een keurmerk voor het bedrijfsleven om cybercrime tegen te gaan. Dit doen ze samen met het Verbond van Verzekeraars, VNO-NCW MKB-Nederland, CIO Platform Nederland, Nederland ICT, Cyberveilig Nederland en Partnering Trust. Het CCV en de samenwerkingspartners hebben zich verenigd in de Commissie van Belanghebbenden Cybersecurity, waaruit twee werkgroepen zijn voortgekomen. ▪ De werkgroep Risicomodel buigt zich over de ontwikkeling van een risicomodel waarmee onder andere ondernemers de kans op een cyberincident beter kunnen inschatten. De werkgroep Keurmerk Cybersecurity onderzoekt de behoefte in de markt aan een keurmerk om cybercrime te weren en bepaalt de scope van dit mogelijke keurmerk. Het streven is om eind 2019 een eerste versie op te leveren van het risicomodel en het keurmerk.

Samenwerking overheid en private organisaties kan verder versterkt worden (1/2)

AANVULLINGEN UIT VALIDATIE EXPERTTAFEL

Conclusies en aanbeveling(en)

- Aanval en dreigingen zullen binnen dit thema volgens experts voornamelijk plaatsvinden in financiële sector. Deze sector loopt voor op andere sectoren en werken reeds op (inter)nationaal niveau met elkaar samen. Deze bedrijven hebben dan ook vaak hun eigen huis redelijk op orde qua informatiebeveiliging
- Andere vermoedelijke doelen zijn mediabedrijven, verenigingsleven en bedrijven die biometrische data van burgers/personen opslaan
- Meldingen bij (lokale) incidenten worden niet doorgegeven aan de gemeente, maar zouden evt. doorgegeven kunnen worden via ondernemingsorganisatie VNO-NCW
- Belangrijk om te bepalen wat het Amsterdamse perspectief is op scope impact. Geldt het pas bij verstoring van de openbare orde of ook wanneer het slechts economische schade betreft van een lokale organisatie?
- Opzetten en borgen van het proces van informatieberichtgeving voor grote private organisaties
- Opzetten van een stedelijke campagne rondom het vergroten van de weerbaarheid van (bewoners en) ondernemers. Mogelijke aansluiting bij huidige campagne genaamd 'Eerst checken, dan klikken'



Bron: Experttafel (27-5-2019)

Samenwerking overheid en private organisaties kan verder versterkt worden (2/2)

AANVULLINGEN UIT VALIDATIE EXPERTTAFEL

Gestarte acties voor 2019/2020

- Bevorderen kennisontwikkeling lokale professionals en vergroten bewustzijn
- Gebiedsgerichte benadering van ondernemers met een campagneteam
- Toolbox Platform Veilig Ondernemen (PVO)
- Informatiebox Veilig Ondernemen
- Onderzoek phishing: de MKB phishing test
- Verbeteren proces aangifte na cyberincident

Bron: Experttafel (27-5-2019)

Thema: Vitale infrastructuur

Managementsamenvatting

Inleiding

Thema
Eigen huis op orde

Thema
Het individueel welzijn van burgers

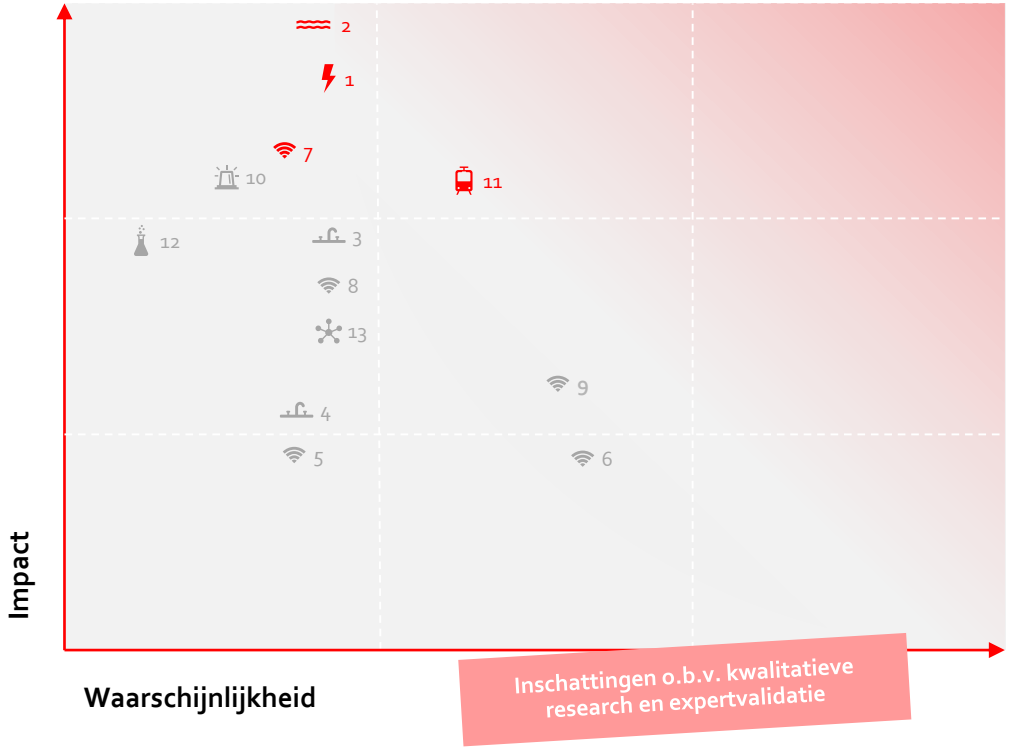
Thema
Private en maatschappelijke organisaties

Thema
Vitale infrastructuur

Thema
Democratie en bestuurlijke stabiliteit

Thema
De openbare orde en veiligheid

Digitaal Veiligheidsbeeld A'dam - Vitale infrastructuur



Energie

1. **Langdurige (ver)storing elektriciteit/gas in geheel A'dam**

Oppervlaktewater

2. **Uitzetten gemalen en openzetten waterkeringen**

Drinkwater

3. Moedwillig vervuilen A'dams drinkwater
4. Langdurige (ver)storing water/rioolafvoer in geheel A'dam

Communicatie

5. Sabotage van input (bijv. GPS) op vitale systemen
6. Grootschalige diefstal/spionage datacommunicatie in stad
7. **Langdurig verstoord telefoon- / dataverkeer in geheel A'dam**
8. Langdurige (ver)storing datacenters (met impact buiten A'dam)
9. Groot datalek bij telecombedrijf/ISP

OOV

10. Langdurig verstoorde communicatie van (alle) hulpdiensten

Transport

11. **Langdurig platleggen / saboteren:**
    a) **A'damse haven/sluizen**
    b) **Verkeerssignalering/data-netwerk**
    c) **Bruggen**
    d) **GVB**

Chemie

12. Opzettelijk destructief gebruik gevaarlijke stoffen (hack beveiliging opslag/transport)

Smart city

13. Hack/sabotage van een of meerdere systemen (zelfrijdende auto's, crowd, IoT, etc.)

Schiphol niet opgenomen omdat het binnen andere gemeente en veiligheidsregio valt

Bron: Expert interviews, Analyse projectteam

Waarschijnlijkheid dreigingen

Laag | Medium | Hoog

Nr	Dreiging	Waarschijnlijkheid
1	Langdurige (ver)storing elektriciteit/gas in geheel A'dam	
2	Uitzetten gemalen en openzetten waterkeringen	
3	Moedwillig vervuilen A'dams drinkwater	
4	Langdurige (ver)storing water/rioolafvoer in geheel A'dam	
5	Sabotage van input (bijv. GPS) op vitale systemen	
6	Grootschalige diefstal/spionage datacommunicatie in stad	
7	Langdurige verstoord telefoon- / dataverkeer in geheel A'dam	
8	Langdurige (ver)storing datacenters (met impact buiten A'dam)	
9	Groot datalek bij telecombedrijf/ISP	
10	Langdurig verstoorde communicatie van (alle) hulpdiensten	
11	Langdurig platleggen / saboteren:	
	▪ A'damse haven/sluizen	
	▪ Verkeerssignalering	
	▪ Bruggen	
	▪ GVB	
12	Opzettelijk destructief gebruik gevaarlijke stoffen (hack beveiliging opslag/transport)	
13	Hack/sabotage van een of meerdere systemen (zelfrijdende auto's, crowd, IoT, etc.)	

Bron: Expert interviews, Analyse projectteam

Mogelijke impact dreigingen

Beperkt | Medium | Significant

Nr	Dreiging	Territoriaal	Fysiek	Economisch	Ecologisch	Soc./politiek
1	Langdurige (ver)storing elektriciteit/gas in geheel A'dam					
2	Uitzetten gemalen en openzetten waterkeringen					
3	Moedwillig vervuilen A'dams drinkwater					
4	Langdurige (ver)storing water/rioolafvoer in geheel A'dam					
5	Sabotage van input (bijv. GPS) op vitale systemen					
6	Grootschalige diefstal/spionage datacommunicatie in stad					
7	Langdurige verstoord telefoon- / dataverkeer in geheel A'dam					
8	Langdurige (ver)storing datacenters (met impact buiten A'dam)					
9	Groot datalek bij telecombedrijf/ISP					
10	Langdurig verstoorde communicatie van (alle) hulpdiensten					
11	Langdurig platleggen / saboteren:					
	▪ A'damse haven/sluizen					
	▪ Verkeerssignalering					
	▪ Bruggen					
	▪ GVB					
12	Opzettelijk destructief gebruik gevaarlijke stoffen (hack beveiliging opslag/transport)					
13	Hack/sabotage van een of meerdere systemen (zelfrijdende auto's, crowd, IoT, etc.)					

Bron: Expert interviews, Analyse projectteam

Primaat ligt vaak niet bij gemeente

Gemeente | Gerelateerd aan Gemeente | Extern

Dreiging	Primair verantwoordelijke
Langdurige (ver)storing elektriciteit in geheel A'dam	Netwerkbeheerders en elektriciteitsproducenten
Langdurige (ver)storing gas in geheel A'dam	Netwerkbeheerders en gasproducenten
Uitzetten gemalen en openzetten waterkeringen	Waternet
Moedwillig vervuilen A'dams drinkwater	Waternet
Langdurige (ver)storing water in geheel A'dam	Waternet
Langdurige (ver)storing rioolafvoer in geheel A'dam	Waternet
Sabotage van belangrijke input (bijv. GPS) op vitale systemen	Vele verschillende partijen (w.o. alle in deze tabel)
Grootschalige diefstal/spionage datacommunicatie in stad	Telecomaanbieders, ISPs, AMS-IX
Langdurige (ver)storing telefoon- / dataverkeer (internet, GPS, etc.) in geheel A'dam	Telecomaanbieders, ISPs, AMS-IX
Langdurige (ver)storing datacenters (met impact buiten A'dam)	AMS-IX, commerciële eigenaren datacenters
Groot datalek bij vitale infrastructuur	Alle partijen in deze tabel
Langdurig verstoorde communicatie van (alle) hulpdiensten	Hulpdiensten (politie, brandweer, ambulance), communicatieleveranciers
Langdurig platleggen / saboteren:	
• A'damse haven/sluizen	Port of Amsterdam, Rijkswaterstaat, Waternet
• Verkeers-signalering	Gemeente Amsterdam
• Bruggen	Waternet
• GVB	GVB
Opzettelijk destructief gebruik gevaarlijke stoffen (hack beveiliging opslag/transport)	Verschillende commerciële partijen, Port of Amsterdam
Hack van een of meerdere systemen (zelfrijdende auto's, crowd, IoT, etc.)	Verschillende commerciële partijen, Gemeente Amsterdam (crowd)

Bron: Expert interviews, Analyse projectteam

Vitale infrastructuur
Verdieping

Nationale vitale infrastructuur is door NCTV vastgesteld door 25 vitale processen te identificeren

Bepaalde processen zijn zo belangrijk voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de nationale veiligheid. Deze processen vormen de Nederlandse vitale infrastructuur

Vitaal proces	Categorie *	Sector	Indeling verkenning
Landelijk transport en distributie elektriciteit	A	Energie	*Landelijk*
Regionale distributie elektriciteit	B		
Gasproductie, landelijk transport en distributie gas	A		*Landelijk*
Regionale distributie gas	B		
Olievoorziening	A		*Landelijk*
Internet en datadiensten	B	ICT/Telecom	
Internettoegang en dataverkeer	B		
Spraakdienst en SMS2	B		
Plaats- en tijdsbepaling middels GPS	B		
Drinkwatervoorziening	A	Drinkwater	
Keren en beheren waterkwantiteit	A	Water	
Vlucht- en vliegtuigafhandeling	B	Transport	
Scheepvaartafwikkeling	B		
Inzet defensie	B	Defensie	*Landelijk*

Vitaal proces	Categorie *	Sector	Indeling verkenning
Grootschalige productie/verwerking en/of opslag (petro)chemische stoffen	B	Chemie	
Opslag, productie en verwerking nucleair materiaal	A	Nucleair	*Landelijk*
Toonbankbetalingsverkeer	B	Financieel	*Landelijk*
Massaal giraal betalingsverkeer	B		*Landelijk*
Hoogwaardig betalingsverkeer tussen banken	B		
Effectenverkeer	B		
Communicatie met en tussen hulpdiensten middels 112 en C2000	B	OOV	
Inzet politie	B		
Basisregistraties personen en organisaties	B	Digitale overheidsprocessen	*Thema 5a*
Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties)	B		*Thema 5a*
Elektronisch berichtenverkeer en informatieverschaffing aan burgers	B		*Thema 5a*
Identificatie en authenticatie van burgers en bedrijven	B		*Thema 5a*

* A = meest vitaal, B = vitaal
Bron: "Weerbare vitale infrastructuur" (NCTV, 2017)

Beeld van de vitale infrastructuur in Amsterdam wordt bepaald door 17 vitale processen

Bepaalde processen zijn zo belangrijk voor de Amsterdamse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt en een bedreiging vormt voor de lokale veiligheid. Deze processen vormen de Amsterdamse vitale infrastructuur

A: *Meest vitale* [1]

Energie
- Elektriciteitsproductie & distributie
- Gasproductie & distributie

Oppervlaktewater
- Keren en beheren water-kwantiteit

Drinkwater
- Drinkwaterproductie, distributie & afvoer

B: *Vitaal*

Communicatie
- Internet & dataverkeer
- Spraakdienst & SMS
- Plaats- & tijdsbepaling (GPS, satellieten)
- Dataopslag & rekenkracht
- Alarmsysteem, radio

Transport
- Scheepvaartafhandeling
- Wegverkeer (incl. verbindingen en sturingssystemen)
- Openbaar vervoer (incl. datanetwerk)

Smart city
- Facilitatie van innovatieve informatiesystemen die fysieke elementen aansturen (IoT, zelfrijdende auto's, drones, crowd management, etc.)

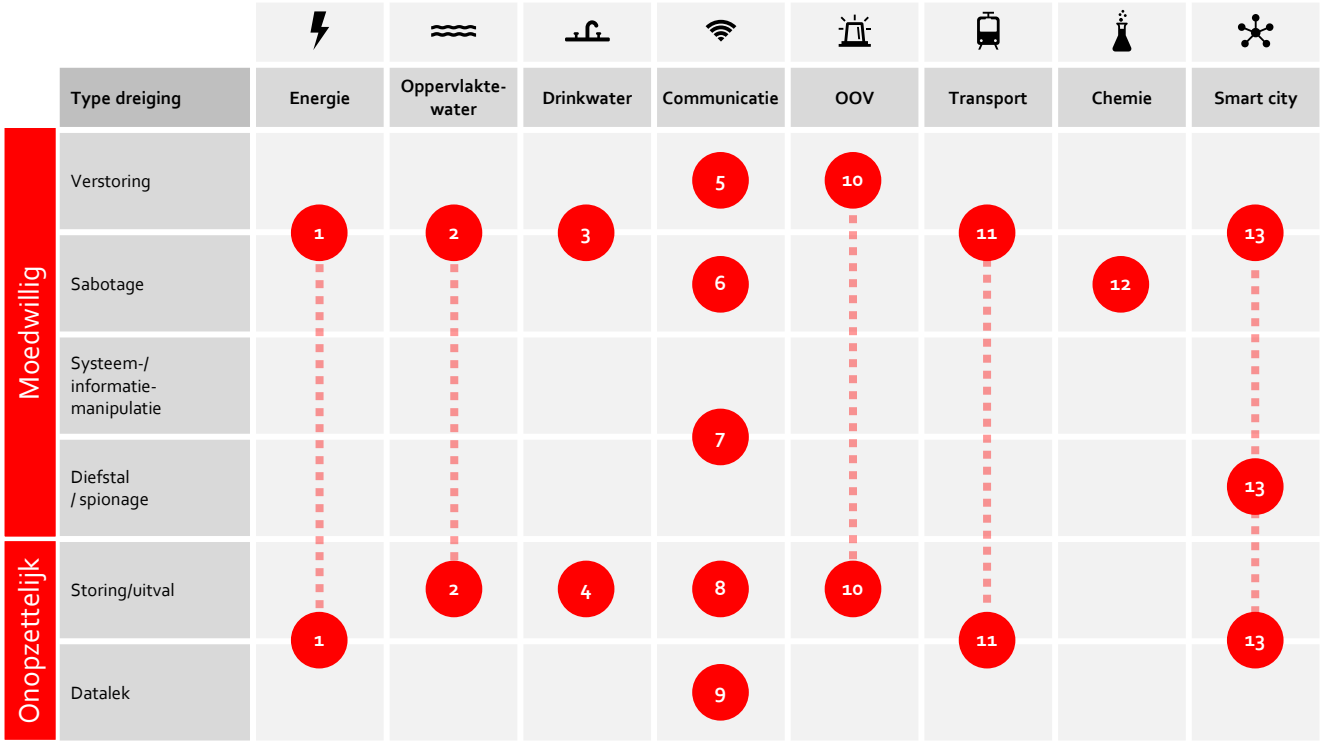
OOV
- Communicatie met en tussen hulpdiensten middels 112 en C2000
- Inzet politie

Chemie
- Productie & verwerking van chemische stoffen

Schiphol niet opgenomen omdat het binnen andere gemeente en veiligheidsregio valt

1 De vitaliteitsbeoordeling wordt gemaakt op basis van de opgestelde impactcriteria, zoals economische schade en fysieke gevolgen. Uitval van A-vitale processen heeft grotere potentiële gevolgen dan van B-vitale processen, Bron: Voornamelijk o.b.v. nationale indeling in "Weerbare vitale infrastructuur" (NCTV, 2017); TNO (2003): Bescherming Vitale infrastructuur; Bewerkt naar A'damse context

Digitale dreigingen – Vitale infrastructuur



Belangrijkste dreigingen

1. Langdurige (ver)storing elektriciteit/gas in geheel A'dam
2. Uitzetten gemalen en openzetten waterkeringen
3. Moedwillig vervuilen A'dams drinkwater
4. Langdurige (ver)storing water/rioolafvoer in geheel A'dam
5. Sabotage van input (bijv. GPS) op vitale systemen
6. Grootschalige diefstal/spionage datacommunicatie in stad
7. Langdurig verstoord telefoon- / dataverkeer in geheel A'dam
8. Langdurige (ver)storing datacenters (met impact buiten A'dam)
9. Groot datalek bij telecombedrijf/ISP
10. Langdurig verstoorde communicatie van (alle) hulpdiensten
11. Langdurig platleggen / saboteren:
    a) A'damse haven/sluizen
    b) Verkeerssignalering/datanetwerk
    c) Bruggen
    d) GVB
12. Opzettelijk destructief gebruik gevaarlijke stoffen (hack beveiliging opslag/transport)
13. Hack/sabotage van een of meerdere systemen (zelfrijdende auto's, crowd, IoT, etc.)

* Bij alle (ver)storingen gaat het om een langdurige storing (zo lang dat deze significante gevolgen heeft in Amsterdam)

Bron: Expert interviews, Analyse projectteam

Energiesector is een veelvoorkomend doelwit van hackers die elektriciteitsnetwerken direct aanvallen…

Digitale aanval energienet Oekraïne (Dec. 2016)

- *Een digitale aanval leidde tot het uitvallen van zo'n vijfde van het totale stroomnet in Oekraïne*
- *In juni 2017 kwam beveiligingsbedrijf ESET met een onderzoeksrapport naar buiten over de malware die hier mogelijk voor is ingezet*
- *De gebruikte malware, door de onderzoekers Industroyer genoemd, is in staat te communiceren met industriële controlesystemen (ICS) die (onder andere) worden gebruikt voor de aansturing van energienetwerken*
- *De malware is echter ook toepasbaar op andere organisaties in andere industrieën en andere landen, mogelijk ook in Nederland*
- *Een belangrijke voorwaarde om de malware in te kunnen zetten, is dat de aanvaller toegang moet hebben tot het netwerk van het doelwit*

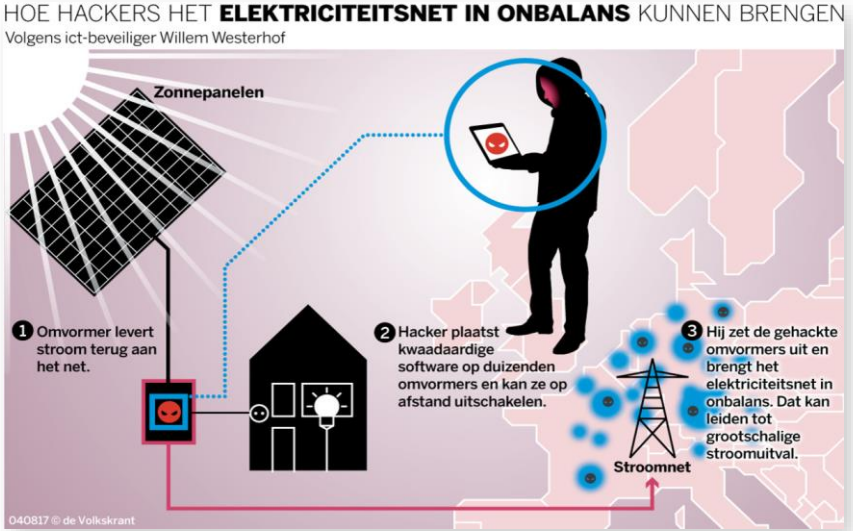
Dragonfly (okt. 2017)

- *In oktober 2017 meldt het Amerikaanse US-CERT aanvallen van geavanceerde actoren op vitale infrastructuur, waarbij een link wordt gelegd met de Dragonfly-campagne. Om binnen te komen in de netwerken van grote organisaties binnen de energiesector, richten de aanvallers zich op zwak beveiligde punten en kleine netwerken*
- *Er is sprake van twee soorten doelwitten. De initiële doelwitten zijn organisaties aan de buitenkant, zoals vertrouwde leveranciers met minder goed beveiligde netwerken. De aanvaller gebruikt de netwerken van de vertrouwde leveranciers als uitvalsbasis om hun uiteindelijke doelwitten aan te vallen*

Bron: https://www.deingenieur.nl/artikel/gevaarlijke-malware-legt-stroomnet-plat, CSBN (2018)

...maar ook via aangesloten apparatuur het netwerk lam zouden kunnen leggen

- *Grootschalig misbruik van een kwetsbaarheid in één apparaat kan bijvoorbeeld grote gevolgen hebben voor het functioneren van vitale processen*
- *De in 2017 in de media bekend geworden kwetsbaarheid in omvormers van zonnepanelen van een marktleider kan dienen als illustratie. Via de kwetsbaarheid zou het volgens de onderzoeker mogelijk zijn om een groot aantal omvormers tegelijkertijd op afstand uit te schakelen*
- *Een dergelijke grootschalige uitschakeling zou kunnen leiden tot een verstoring in de stroomvoorziening in grote delen van Europa. De Raad voor de leefomgeving en infrastructuur wijst er dan ook op dat de stabiliteit van het totale elektriciteitssysteem vooral wordt ondergraven vanuit onderdelen die niet in publiek eigendom zijn*



Bron: https://www.volkskrant.nl/nieuws-achtergrond/ict-lek-zonnepanelen-mogelijk-bedreigend-voor-europese-stroomvoorziening~bef49c64/

Volgens moderne maatstaven van digitale veiligheid zijn vitale waterwerken kwetsbaar

- *De minister heeft een aantal waterwerken die Rijkswaterstaat beheert als vitaal aangewezen. Een aanval op IT van deze waterwerken kan grote gevolgen hebben voor Nederland. Uit het onderzoek blijkt dat nog niet alle vitale waterwerken rechtstreeks zijn aangesloten op het Security Operations Center (SOC) van Rijkswaterstaat. De ambitie om eind 2017 bij alle vitale waterwerken digitale aanvallen direct te kunnen detecteren was in het najaar van 2018 daarmee nog niet gerealiseerd. Hierdoor bestaat het risico dat RWS een digitale aanval niet of te laat detecteert*
- *Gedurende het onderzoek is in samenwerking met Rijkswaterstaat een kwetsbaarheidstest uitgevoerd bij een van de vitale waterwerken. Daarbij wisten de ingehuurde ethische hackers het object fysiek binnen te dringen en zich toegang tot de controlekamer te verschaffen. De aanvallers werden echter direct opgemerkt door het SOC toen ze vanaf het terrein een laptop aansloten op het IT-netwerk van Rijkswaterstaat*

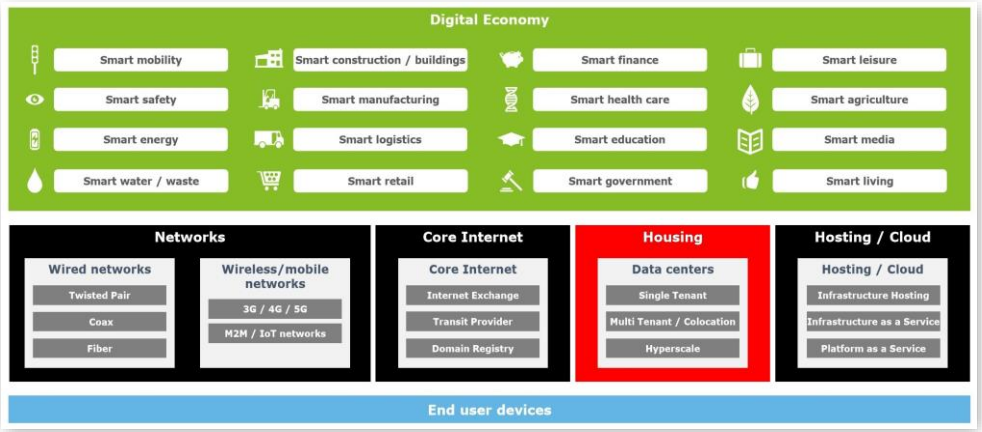
Bron: https://www.rekenkamer.nl/publicaties/rapporten/2019/03/28/digitale-dijkverzwaring-cybersecurity-en-vitale-waterwerken

Datacenters *enabler* digitale economie: een verstoring/uitval zal daarom steeds grotere economische impact hebben

Datacenters nemen een belangrijke rol in de digitale economie van Amsterdam. Ze faciliteren zowel consumenten, bedrijven, overheid als onderwijsinstellingen in hun behoefte aan ICT-services. Concreet zien we datacenters drie functies vervullen:

Webhosting	Digitalisering van producten en diensten ▪ Online shopping ▪ Dropbox, Google Drive
Infrastructuur hosting	IT, outsourcing ▪ AI, deeplearning, machinelearning ▪ Internet-of-things
Applicatie hosting	Everything-as-a-service ▪ Netflix, Spotify, Blendle ▪ Microsoft Office 365, Google Apps

Niet voor al deze functies is het noodzakelijk om datacenters in of nabij steden te plaatsen. Deze behoefte zit met name binnen infrastructuur hosting. Daar zien we dat ontwikkelingen als AI, deep learning, machine learning en IoT drastisch toe nemen. Om deze processen goed te kunnen uitvoeren is het belangrijk om de latency (wachttijd) zo laag mogelijk te houden. Dit vereist rekenkracht en opslag dichtbij de gebruiker.



Het in Amsterdam gevestigde AMS-IX is een van de grootste internetknooppunten ter wereld en heeft haar infrastructuur verdeeld over o.a. Amsterdamse datacenters. Zijn al aangemerkt als vitale infrastructuur door NCSC. Mocht AMS-IX uitvallen dan zal dit echter voornamelijk economische impact hebben vanwege vertraging en lagere efficiëntie. Het internetverkeer verplaatst zich dan simpelweg naar andere (langzamere) knooppunten

Bron: Onderzoek "Benutten van restwarmte uit datacenters in Amsterdam" (Gemeente Amsterdam 2018); Interview AMS-IX

Gevolgen digitale aanval zijn voelbaar in de transportsector

- *Rotterdamse haven getroffen door de neveneffecten van de geavanceerde sabotage-aanval 'NotPetya' – aanzienlijke economische schade (AIVD). Met name de schaalgrootte en geavanceerdheid van deze aanval wijzen naar een statelijke actor*
- *De gevolgen van een grootschalige digitale aanval werden duidelijk tijdens de hack op APM-terminals. De twee terminals van de dochteronderneming van het Deense Maersk lagen vanaf 27 juni 2017 stil door een ransomware aanval. Het probleem duurde meerdere dagen en had grote gevolgen voor de doorvoer vanuit desbetreffende terminals. Het Havenbedrijf Rotterdam werd niet geraakt bij de hack, de impact voor ons was beperkt*

"Dit virus kan in gemuteerde vorm terugkomen. Er zullen vaker computersystemen worden gehackt."

- Rotterdamse havenmeester René de Vries

Bron: https://jaarverslag2017.portofrotterdam.com/strategie-en-resultaten/veilige-en-effici%C3%ABnte-afhandeling/cybersecurity, https://www.ad.nl/rotterdam/cyberaanval-ontwrichtte-haven-het-blijft-niet-bij-deze-hack~a9df8631/

Ook het openbaar vervoer is veelvoudig slachtoffer van digitale aanvallen

- *Een ransomware aanval op het openbaar vervoer systeem in San Francisco geeft iedereen een gratis rit. Hackers waren in staat om meer dan 2.000 computers te hacken. Deze computers zorgden voor het operationele gedeelte om de toegangspoortjes open en dicht te houden. Hierdoor konden mensen gratis door de toegangspoortjes lopen. De hackers hebben 100 bitcoins gevraagd om de toegang weer terug aan het openbaar vervoers bedrijf terug te geven*
- *Volgens het Canadese Metrolinx zijn zij in 2018 het doelwit geweest van een cyberaanval. Daarbij wijzen zij naar Noord-Korea als schuldige*
- *Op informatieschermen en vertrekborden stond groot en duidelijk de tekst 'Ekber was here'. Rond 9u lokale tijd kon de hack weer worden teruggedraaid.Ook mensen die de Turkse OV-app gebruikten zagen het zelfde. Alle bestemmingen en haltes waren veranderd in 'Ekber was here'*

"UKrail network is in 2016 slachtoffer geweest van vier grote cyberaanvallen."

- Darktrace (IT-beveiligingsbedrijf)

Bron: Theguardian(2016), Thestart(2018), Turks(2016), Independent (2016)

Port of Amsterdam heeft actieprogramma Cybersecurity gelanceerd om zichzelf weerbaarder te maken

- Eind 2017 is het eindrapport "Inventarisatie Cybersecurity" opgesteld en op basis daarvan is in 2018 het Cybersecurity programma van Port of Amsterdam gelanceerd. Geïnspireerd op de programma's van Havenbedrijf Rotterdam en Schiphol
- Amsterdamse haven niet aangemerkt als nationale vitale infrastructuur (in tegenstelling tot bijv. Rotterdamse haven v.w.b. scheepvaartverkeersbegeleiding en Schiphol). Daarom geen wettelijke basis voor ondersteuning door NCSC maar wel erkenning voor Cybersecurity programma van Havenbedrijf Amsterdam door Digital Trust Center onderdeel Ministerie EZK voor niet-vitale infrastructuur/bedrijven en nauw contact met ministerie J&V
- Cybersecurity programma bestaat uit drie onderdelen:
  - Eigen Huis op Orde – interne digitale veiligheid
  - Port Security – De directeur CNB geeft invulling aan de ISPS wetgeving zowel op fysiek als op digitaal gebied
  - Awarenessprogramma - Op het thema Cybersecurity wordt invulling gegeven aan goed huisvaderschap door het creëren van awareness en het bijdragen aan de digitale weerbaarheid en veerkracht in het Noordzeekanaalgebied

NZKG ISAC is een van de cyberweerbaarheids-netwerken zoals erkend door Digital Trust Center

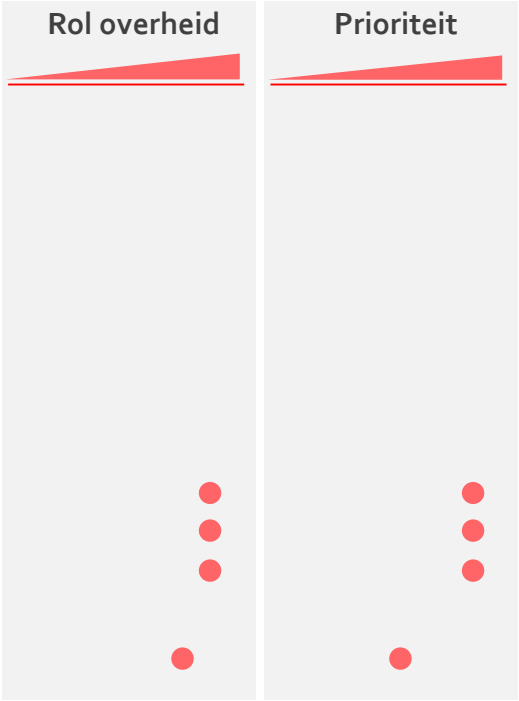
Bron: Interview en website Port of Amsterdam; Digital Trust Center website

Identificeren, beschermen en samenwerken essentieel voor vitale digitale infrastructuur (1/2)

AANVULLINGEN UIT VALIDATIE EXPERTTAFEL

Conclusies en aanbeveling(en)

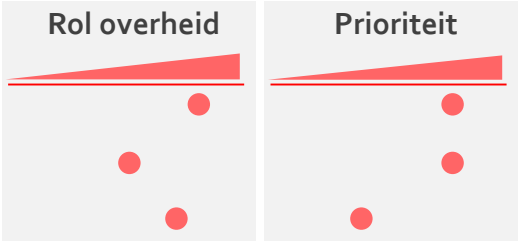
- De meest belangrijke conclusie binnen dit thema is dat het primaat vaak niet bij de gemeente ligt. Echter deels wel bij lokale instanties gerelateerd aan de gemeente
- Dreigingen zijn kort samen te vatten: "stroom loopt dwars door alles heen"
- Systeem voor Basisregistratie Personen: wat gebeurt er in geval van buitenlandse overnames en aandacht voor redundantie van gedigitaliseerde stad Amsterdam?
- Thema legt de focus (alleen) op systemen; "mens blijft nog altijd zwakste schakel"
- Zoek samenwerking met partijen in vitale infrastructuur (bijv. versterk relatie met het actieprogramma cybersecurity van Port of Amsterdam)
- Gezamenlijk opzetten van event ten behoeve van de bewustwording en weerbaarheid van de bedrijven in de keten Noordzeekanaal
- Voer een risicoanalyse uit voor vitale lokale processen
- Maak een netwerkanalyse (bijv.: wat/wie is lokaal nodig als 112 onbereikbaar is?)
- Oefen op de belangrijkste kroonjuwelen en maak hier scenario's voor
- Stel minimale eisen op voor apparatuur in de vitale digitale infrastructuur
- Zet in op voorlichting en creëer bewustwording voor de noodzaak om aan continuïteitsplanning te doen



Bron: Experttafel (27-5-2019)

Identificeren, beschermen en samenwerken essentieel voor vitale digitale infrastructuur (2/2)

AANVULLINGEN UIT VALIDATIE EXPERTTAFEL



Conclusies en aanbevelingen (cont'd)

- Pas de scenario's uit de Veiligheidsregio Amsterdam-Amstelland aan voor digitaal
- Zorg voor nood-energievoorziening op cruciale plaatsen (bijv. bij radiomasten van mobiele netwerken)
- Maak gebruik van de speciale subsidies t.b.v. digitale veiligheid

Gestarte acties voor 2019/2020

- Mede op basis van output experttafel wordt een monitor overzicht opgesteld (door OI&S) voor kwantitatieve gegevens op dreigingen/kenmerken digitalisering:
  - Elektriciteit/gas
  - Amsterdams drinkwater, water/rioolafvoer, haven/sluizen en waterkeringen
  - Schiphol en het openbaar vervoer
  - Verkeerssignalering en bruggen

Bron: Experttafel (27-5-2019)

Thema: Democratie en bestuurlijke stabiliteit

Managementsamenvatting

Inleiding

Thema
Eigen huis op orde

Thema
Het individueel welzijn van burgers

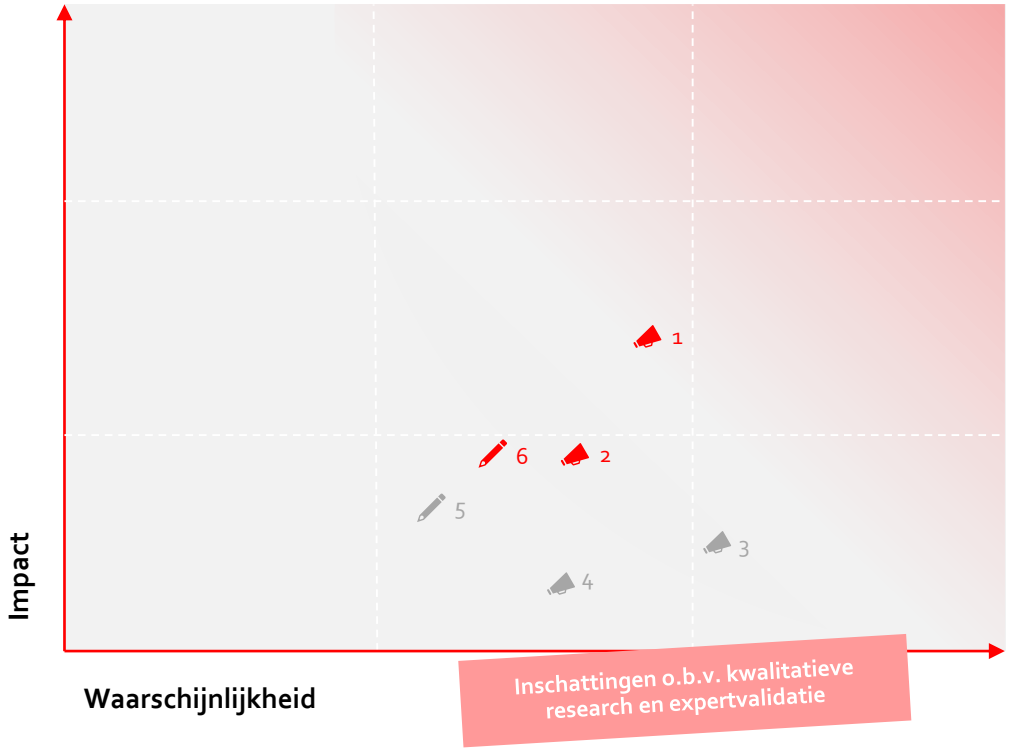
Thema
Private en maatschappelijke organisaties

Thema
Vitale infrastructuur

Thema
Democratie en bestuurlijke stabiliteit

Thema
De openbare orde en veiligheid

Digitaal Veiligheidsbeeld A'dam - Democratie en bestuurlijke stabiliteit



Media

1. **Staten en belangengroepen beïnvloeden Amsterdammers met nepnieuws**
2. **Staten en belangengroepen beïnvloeden d.m.v. trollen maatschappelijk sentiment**
3. De nieuwsfeeds van Amsterdammers worden al meer vervuild door pulpnieuws
4. Personificatie/filterbubbel zorgt voor versnippering/ polarisatie van Amsterdammers

Verkiezingen

5. Lokale participatietools worden misbruikt/gemanipuleerd
6. **Hacks bij politieke partijen**

Bron: Expert interviews, Analyse projectteam

Waarschijnlijkheid dreigingen

Laag | Medium | Hoog

Type aanval	Type dreiging	Dader	Motief	Waarschijnlijkheid
Nepnieuws				
Staten of belangengroepen beïnvloeden Amsterdammers met nepnieuws	Informatiemanipulatie	Buitenlandse staat, belangengroepering	Beïnvloeden van verkiezingsuitslag, beïnvloeden van maatschappelijk sentiment	*Beïnvloeding op andere thema's (bijv. MH17) wordt gemeld door AIVD, bij Amsterdamse thema's minder duidelijk*
Staten of belangengroepen beïnvloeden d.m.v. trollen het maatschappelijk sentiment	Informatiemanipulatie	Buitenlandse staat, belangengroepering	Beïnvloeden van maatschappelijk sentiment	*Beïnvloeding op andere thema's (bijv. MH17) wordt gemeld door AIVD, bij Amsterdamse thema's minder duidelijk*
De nieuwsfeeds van Amsterdammers worden al meer vervuild door pulpnieuws	Informatiemanipulatie	Individuen (binnen- of buitenlands)	Economische winst door reclameopbrengsten	*Pulpnieuws is alom tegenwoordig op internet. Impact is beperkt*
Personificatie/filterbubbel zorgt ervoor dat Amsterdammers alleen nog maar bevestigd worden in hun opvattingen	Informatiemanipulatie	D.m.v. (sociale) media, internetgiganten	Winstmaximalisatie	*Aantal Amsterdamse media met breed bereik is zeer beperkt*
Verkiezingen				
Lokale participatietools worden misbruikt/gemanipuleerd	Informatie/systeem-manipulatie	Hackers, indieners van voorstellen	Door een online stemming te manipuleren kan een andere uitkomst verkregen worden	*Er zijn al aantal keer valse stemmen gesignaleerd (en verwijderd)*
Hacks bij politieke partijen	Informatiediefstal	Buitenlandse staat, belangengroepering	Verkrijgen compromitterende inhoud	*In het buitenland is dit gebeurd. Er is geen aanleiding om te denken dat de beveiliging in Nederland beter is*

Bron: Expert interviews, Analyse projectteam

Mogelijke impact dreigingen

Beperkt | Medium | Significant

Type aanval	Territoriaal	Fysiek	Economisch	Ecologisch	Sociaal en politiek
Nepniews					
Staten of belangengroepen beïnvloeden Amsterdammers met nepnieuws	*Onafhankelijkheid Amsterdam in het geding*				*Democratische rechtsstaat onder druk*
Staten of belangengroepen beïnvloeden d.m.v. trollen het maatschappelijk sentiment					*Meningsvorming Amsterdammers wordt bewust gemanipuleerd*
De nieuwsfeeds van Amsterdammers worden al meer vervuild door pulpnieuws					*Vertrouwen in media neemt af*
Personificatie/filterbubbel zorgt ervoor dat Amsterdammers alleen nog maar bevestigd worden in hun opvattingen					*Samenleven van verschillende groepen komt in gevaar door versplintering en vervreemding*
Verkiezingen					
Lokale participatietools worden misbruikt/gemanipuleerd	*De stad wordt anders ingericht dan de inwoners eigenlijk zouden willen*				*Democratische rechtsstaat onder druk*
Hacks bij politieke partijen					*Verkiezingsthema's (en –uitkomsten) kunnen door hackers worden beïnvloed*

Bron: Expert interviews, Analyse projectteam

Gemeente zou kunnen overwegen om grotere rol in te nemen om mogelijke effecten van dreigingen te verminderen

Dreiging	Preventie	Crisis
Nepnieuws		
Staten of belangengroepen beïnvloeden Amsterdammers met nepnieuws	Gemeente: aanbod aan scholen voor lessen mediawijsheid Rijk: online bewustwordingscampagne nepnieuws	Gemeente en Rijk: via eigen communicatiekanalen en media betrouwbare en neutrale informatie verspreiden
Staten of belangengroepen beïnvloeden d.m.v. trollen het maatschappelijk sentiment	Rijk: monitoren inmenging van (buitenlandse) actoren	
De nieuwsfeeds van Amsterdammers worden al meer vervuild door pulpnieuws		
Personificatie/filterbubbel zorgt ervoor dat Amsterdammers alleen nog maar bevestigd worden in hun opvattingen	Gemeente: proberen om ook moeilijk te benaderen / in zichzelf gekeerde inwoners en subculturen te bereiken	
Verkiezingen		
Lokale participatietools worden misbruikt/gemanipuleerd	Gemeente: hack & pentests voor online gaan tools, volgen stemverloop	Gemeente: valse stemmen verwijderen, bron stemmen onderzoeken
Hacks bij politieke partijen		

Bron: Expert interviews, Analyse projectteam

Democratie en bestuurlijke stabiliteit

Verdieping

Deel van de kenmerken van een democratie onder vuur van digitale dreigingen

ProDemos, huis voor democratie en rechtsstaat, onderscheidt 8 kenmerken van een democratie. In de tabel is aangegeven welke kenmerken onder druk kunnen komen te staan door digitale criminaliteit.

Kenmerk	Raakvlakken met Digitaal Veilige Stad
Er is een volksvertegenwoordiging	
Er zijn vrije, eerlijke en geheime verkiezingen	De verwerking van de stemmen bevat digitale stappen die gemanipuleerd kunnen worden
Er is sprake van machtenscheiding	
Er wordt gestreefd naar politieke gelijkheid voor iedereen	
Er is een grondwet	
De vrijheid van burgers wordt beschermd	
Er is een maatschappelijk middenveld	
Er zijn vrije media	Vrije media kunnen bedreigd worden door online concurrentie, die bewust of onbewust onjuistheden verspreidt, waardoor de mogelijkheden voor burgers om zich over politieke en maatschappelijke thema's te informeren afneemt

Bron: prodemos.nl

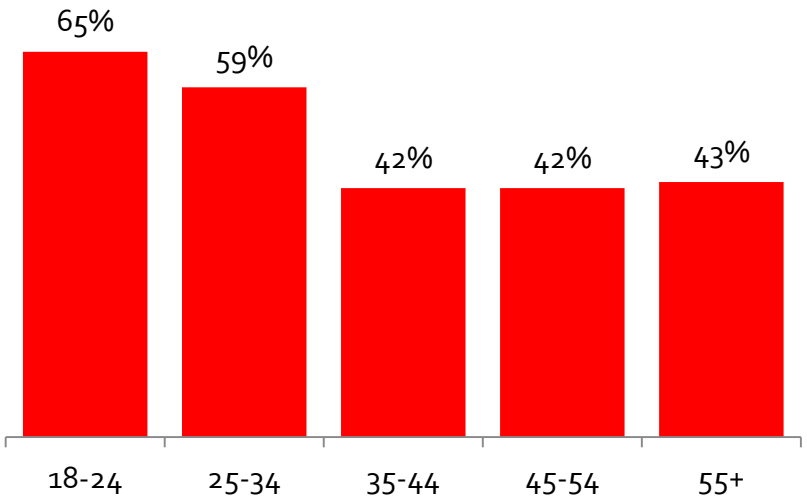
Digitale dreigingen – Democratie en bestuurlijke stabiliteit

Type aanval	Type dreiging	Dader	Motief
Nepnieuws			
Staten of belangengroepen beïnvloeden Amsterdammers met nepnieuws	Informatiemanipulatie	Buitenlandse staat, belangengroepering	Beïnvloeden van verkiezingsuitslag, beïnvloeden van maatschappelijk sentiment
Staten of belangengroepen beïnvloeden d.m.v. trollen het maatschappelijk sentiment	Informatiemanipulatie	Buitenlandse staat, belangengroepering	Beïnvloeden van maatschappelijk sentiment
De nieuwsfeeds van Amsterdammers worden al meer vervuild door pulpnieuws	Informatiemanipulatie	Individuen (binnen- of buitenlands)	Economische winst door reclameopbrengsten
Personificatie/filterbubbel zorgt ervoor dat Amsterdammers alleen nog maar bevestigd worden in hun opvattingen	Informatiemanipulatie	D.m.v. (sociale) media, internetgiganten	Winstmaximalisatie
Verkiezingen			
Lokale participatietools worden misbruikt/gemanipuleerd	Informatie/systeem-manipulatie	Hackers, indieners van voorstellen	Door een online stemming te manipuleren kan een andere uitkomst verkregen worden
Politieke partijen worden door gebrekkige beveiligingsdiscipline gehackt	Informatiediefstal	Buitenlandse staat, belangengroepering	Verkrijgen compromitterende inhoud

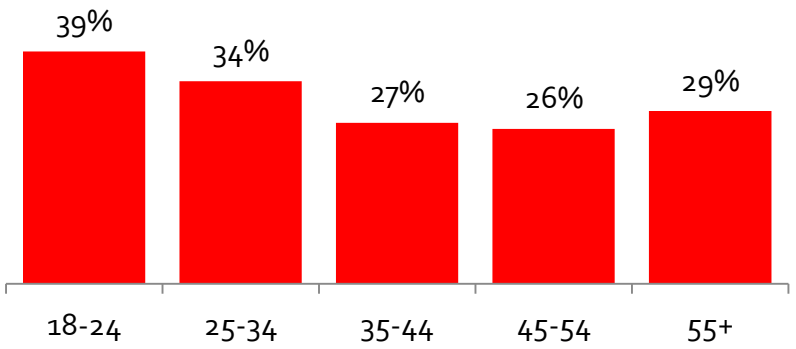
Bron: Expert interviews, Analyse projectteam

Vooral jongeren hebben wekelijks te maken met nepnieuws, en maken zich zorgen

Percentage Nederlanders dat afgelopen week nepnieuws tegenkwam



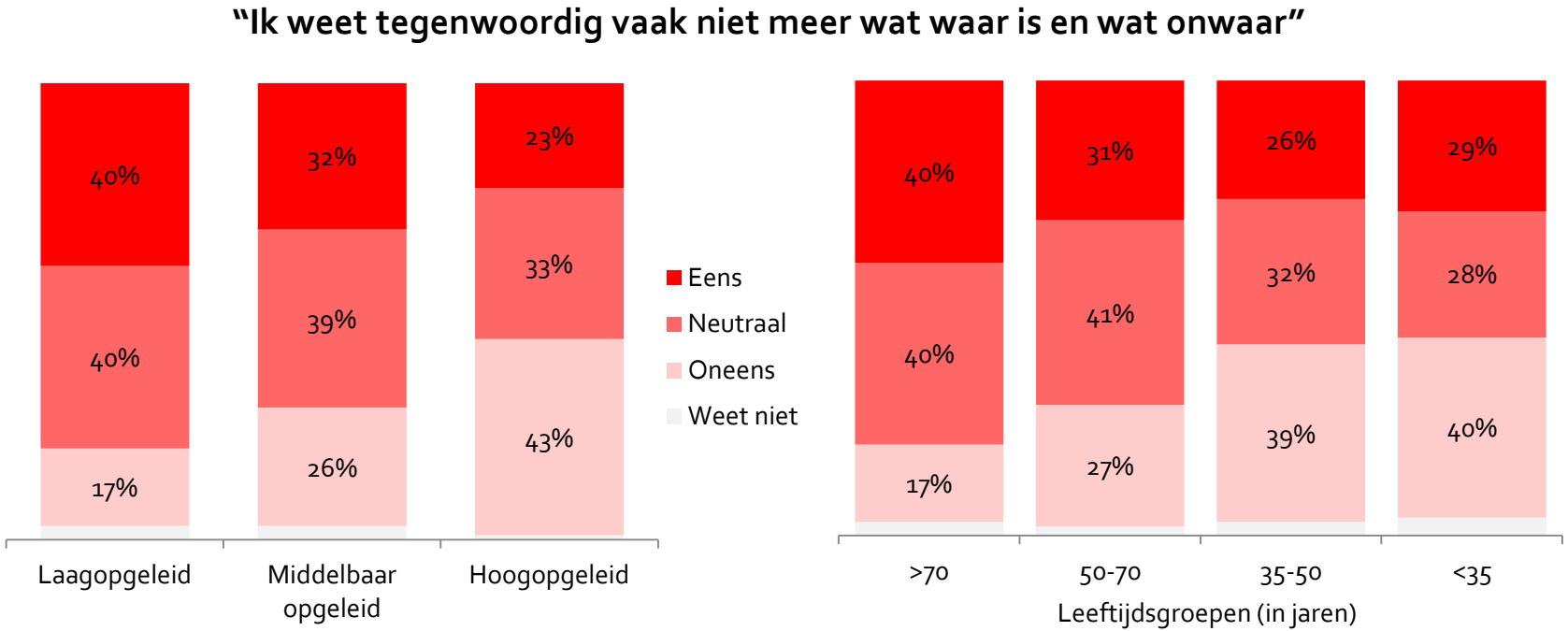
Percentage Nederlanders dat zich zorgen maakt over nepnieuws



Leeftijdsgroepen (in jaren)

Bron: Mediamonitor 2018 (Commissariaat voor de Media); Reuters

Vooral lager opgeleiden en senioren hebben moeite met het herkennen van nepnieuws



Bron:" Desinformatie leidt tot verwarring bij nieuwsconsument" (I&O Research, december 2017)

Buitenlandse groepen die het sentiment proberen te beïnvloeden lijken ook actief te zijn in Nederland

Russia 'meddled in all big social media' around US election

Russian trolls sent thousands of pro-Leave messages on day of Brexit referendum, Twitter data reveals

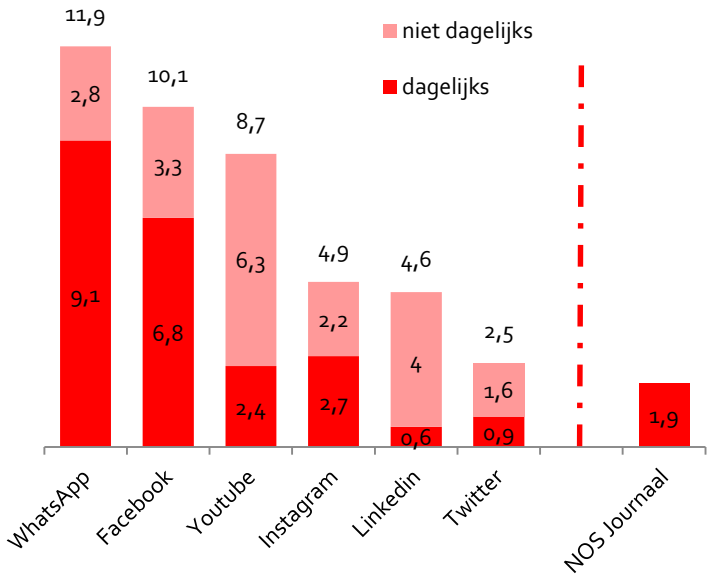
Russisch trollenleger ook actief in Nederland

Wees niet zo naïef over Kremlintrollen

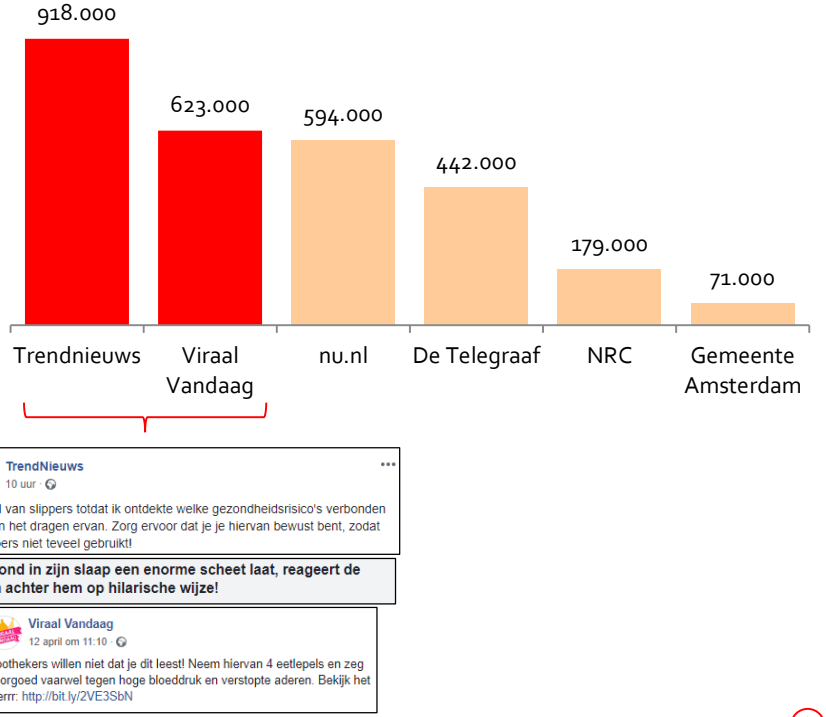
https://www.bbc.com/news/technology-46590890, https://www.telegraph.co.uk/technology/2018/10/17/russian-iranian-twitter-trolls-sent-10-million-tweets-fake-news/, https://www.theguardian.com/commentisfree/2018/jun/17/why-isnt-there-greater-outrage-about-russian-involvement-in-brexit, https://www.nrc.nl/nieuws/2018/12/20/de-eeuwige-oorlog-op-de-sociale-media-a3126615, https://www.nrc.nl/nieuws/2018/07/15/de-russische-trollen-zijn-anti-islam-en-voor-wilders-a1610155?_sp=eef8fd49-9f36-49b1-8ebb-a24d4ec52a7.1532516484195

Gebruik en bereik sociale media is groot in Nederland, en pulpnieuws heeft daar groot bereik

Aantal gebruikers social media in 2019
(in miljoenen)



Aantal likes op Facebook



Bron: Newcom Social Media Onderzoek 2019; Data van Facebook (per 1 april 2019)

Verkiezingsproces Amsterdam – Verouderde software is een landelijk probleem

- Bij de landelijke verkiezingen (Tweede Kamer, Provinciale Staten, Europees Parlement, Waterschappen) is de procedure in Amsterdam gelijk aan die in de rest van Nederland

- OSV, de software die gebruikt wordt om de stemmen van de verschillende stembureaus bij elkaar op te tellen, is oud en bevat technische kwetsbaarheden. Hierdoor bestaat de kans dat het aantal verkregen stemmen veranderd kan worden en hierdoor de verkiezingsuitslag kan worden gemanipuleerd. Door de Kiesraad is aangegeven dat deze software op korte termijn wordt vervangen. Dit zal landelijk gaan gebeuren. In de tussentijd worden er wel maatregelen genomen om de kans op misbruik zo klein mogelijk te maken. Waarschijnlijk zullen de Europese Verkiezingen de laatste verkiezingen zijn die nog van deze kwetsbare versie van OSV gebruik zullen maken

- In Amsterdam is een beveiligde omgeving ingericht om deze software veilig te kunnen gebruiken, waarvoor maar een beperkt aantal accounts is uitgegeven. Dit is een grote vooruitgang ten opzichte van de oude situatie waarin resultaten met een USB-stick van laptop naar laptop overgezet moesten worden

- Vanaf de Provinciale Statenverkiezingen moeten processen verbaal van de stembureaus openbaar gemaakt worden, zodat de berekeningen door iedereen gecontroleerd kunnen worden. Dit werd bij de Provinciale Statenverkiezingen nog niet door alle gemeenten gedaan

Bron: Brief Kiesraad aan Tweede Kamer, Aanbieding beveiligingsonderzoek OSV, 12 maart 2019; https://pointer.kro-ncrv.nl/artikelen/zo-verzamelden-wij-de-verkiezingsdata-van-bijna-alle-gemeenten

Verkiezingsproces Amsterdam – Bij nieuwe vormen van stemmen hangt robuustheid af van zwaarte stemming

- Naast de landelijke verkiezingen worden er in A'dam ook online stemmingen gehouden waarbij bewoners mogen meebeslissen over verschillende zaken, zoals de besteding van buurtbudgetten of de inrichting van de openbare ruimte. Streven is om stemmingen laagdrempelig te houden, bij lichte vormen van stemmen (over welke onderwerpen er geagendeerd wordt in de stadsdeelcommissie) hoeven kiezers alleen hun postcode in te voeren
- Bij ontwerpwedstrijden wordt postcode + emailverificatie gebruikt. Bij zwaardere verkiezingen worden stemcodes per post verstuurd en kan er digitaal of in persoon gestemd worden
- De veiligheid van de stemomgeving wordt getest door hack & pentesten uit te voeren. Bij eerdere stemmingen zijn stemmen van IP-adressen aan de andere kant van de wereld verwijderd. Bij plotselinge grote stemmentoename wordt gekeken of het om legitieme stemmen gaat en worden ze zonodig ongeldig verklaard. Structureel misbruik is tot nu toe niet waargenomen
- Er zijn op dit moment geen rigide regels welke onderwerpen zich wel en niet lenen voor een digitale stemming. Belangrijk is wel dat de stemming over Amsterdam gaat en dat de consequenties ook uitgevoerd kunnen worden. Daarnaast leent de vorm van uitvragen zich niet voor heel complexe onderwerpen
- Het is van belang om de veiligheid van deze stemmingen te waarborgen. Eventuele manipulatie bij door de overheid geïnitieerde verkiezingen brengt ook voor andere verkiezingen een afbreukrisico met zich mee
- Amsterdam gaat aan de slag met digitale identiteiten voor burgers, samen met Nijmegen (IRMA) en VNG. Dat stelt zware eisen aan het beveiligen hiervan maar zal nog niet op korte termijn beschikbaar komen

Bron: CTO Innovatieteam, CISO office

Politieke partijen kunnen een kwetsbare schakel zijn in het verkiezingsproces

- Het organiseren van veilige verkiezingen is een kerntaak van de overheid, veilige communicatie binnen een politieke partij is dat niet
- Zeker rond verkiezingstjjd wordt er binnen politieke partijen volop informatie uitgewisseld, zowel per mail als via appgroepen. De inhoud van deze communicatie is vaak vertrouwelijk en kan in handen van kwaadwillenden veel invloed hebben
- Toch kan er niet van uit gegaan worden dat de beveiligingsmaatregelen bij deze partijen op orde zijn
- Voorbeeld zijn de hacks van het bestuur van de Democratische Partij in de Verenigde Staten in 2016, waarbij vermoedelijk russische hackers mailaccounts hackten en de inhoud konden inzien. Een deel van de mails werd via Wikileaks ook openbaar gemaakt

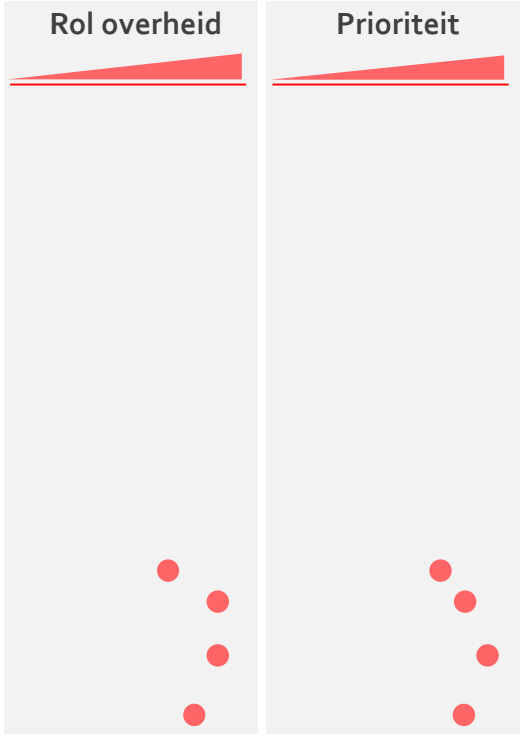
Bron: https://www.sutori.com/story/zo-onderzocht-argos-de-russische-hack-op-de-democratrische-partij; Expert interviews

Verder onderzoek en gesprekken nodig om tot oplossingen voor verhogen weerbaarheid te komen (1/2)

AANVULLINGEN UIT VALIDATIE EXPERTTAFEL

Conclusies en aanbeveling(en)

- Een kwalitatieve en volledige informatievoorziening met een groot bereik en toegang tot de Amsterdamse gemeenschappen is van groot belang
- In het kader van openbare orde en veiligheid is het van belang om naar een structurele informatievoorziening te kijken
- Verkennen van de monitoring- en mitigatie capaciteiten van de (lokale) overheid
- Typisch Amsterdams thema omdat grote tech-bedrijven hier gevestigd zijn en een veel grotere stem hebben dan elders in NL. Is hun fysieke aanwezigheid in de stad een (extra) dreiging?
- Welke bijzondere rol ligt er lokaal gezien dat Den Haag bovenaan staat in het nationaal dreigingsbeeld, immers daar de (inter)nationale politieke instellingen?
- Publieke anonimiteit in de stad wordt een trend (signature-spoofing: wie is wie online?)
- Verdiep onderzoek met toelichtingen en onderbouwing
- Ga in gesprek met de rijksoverheid en diverse platforms
- Ga in gesprek met gemeenschappen over informatie-ecosystemen (Turks, Marokkaans, Zuidoost, expats)
- Bedenk ontwerp van netwerk (technologisch & conceptueel) en redactie-structuur



Bron: Experttafel (27-5-2019)

Verder onderzoek en gesprekken nodig om tot oplossingen voor verhogen weerbaarheid te komen (2/2)

AANVULLINGEN UIT VALIDATIE EXPERTTAFEL

Conclusies en aanbeveling(en)

- Geïdentificeerde dreigingen ten aanzien van dit thema:
  - Beïnvloeding door staten en belangengroepen (kort/lang)
  - Vervuiling informatievoorziening door 'pulp nieuws'
  - Bubbels, uitholling gemeenschappelijkheid en polarisatie
  - Buitensluiting en afzondering digitale achterhoede
  - Bedreiging/intimidatie van publieke functionarissen

Bron: Experttafel (27-5-2019)

Thema: De openbare orde en veiligheid

Managementsamenvatting

Inleiding

Thema
Eigen huis op orde

Thema
Het individueel welzijn van burgers

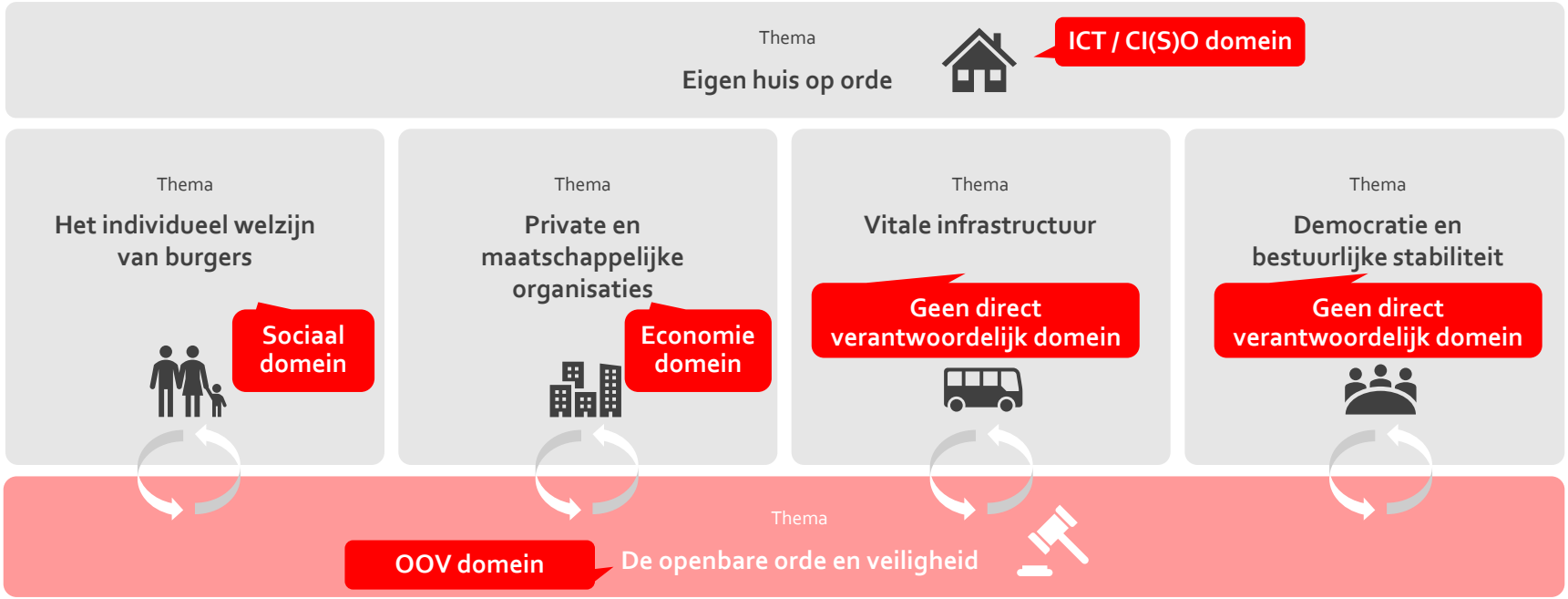
Thema
Private en maatschappelijke organisaties

Thema
Vitale infrastructuur

Thema
Democratie en bestuurlijke stabiliteit

Thema
De openbare orde en veiligheid

Dreiging ontpopt zich in thema, komt bij realisatie in OOV-domein terecht, waarna preventie weer in themadomein opgepakt wordt



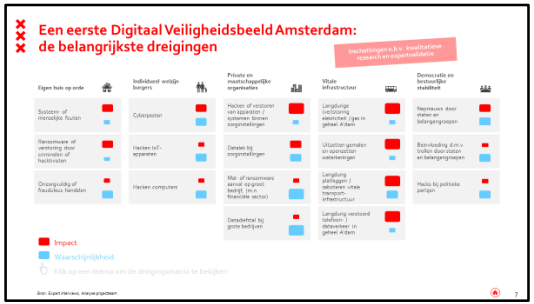
Wanneer significante (inter)nationale en/of A'damse digitale dreiging zich manifesteert kan de A'damse openbare orde in het geding komen

Realisatie van een digitale dreiging…

(Inter)nationale dreigingsmatrix (CSBN 2018)

	Overheid	Vitaal	Privaat	Burgers
Staten/ staatsgelieerd	Spionage Informatiemanipulatie	Sabotage Verstoring Spionage	Spionage Systeemmanipulatie	Spionage
Criminelen	Verstoring Systeemmanipulatie Informatiediefstal	Verstoring Systeemmanipulatie	Informatiediefstal Informatiemanipulatie Verstoring Systeemmanipulatie	Informatiemanipulatie Verstoring Systeemmanipulatie Informatiediefstal
Terroristen Hacktivisten	Sabotage Verstoring Informatiemanipulatie	Sabotage Verstoring Informatiemanipulatie	Verstoring Informatiediefstal Informatiemanipulatie	
Cybervandalen en scriptkiddies Insiders	Verstoring Informatiediefstal Informatiediefstal Verstoring	Verstoring Informatiediefstal Informatiediefstal Verstoring	Verstoring Informatiediefstal Informatiediefstal Verstoring	Informatiediefstal
Niet opzettelijk handelen	Storing/uitval Lek	Storing/uitval Lek	Storing/uitval Lek	Lek

Digitaal Veiligheidsbeeld Amsterdam



…met gevolgen voor A'damse openbare orde

Als effecten van een digitale dreiging voldoende schaal hebben kan deze grote gevolgen hebben voor openbare orde

Bij realisatie van zo'n dreiging dient gemeente daarom deze te herkennen / ingelicht te worden en te beschikken over juiste middelen

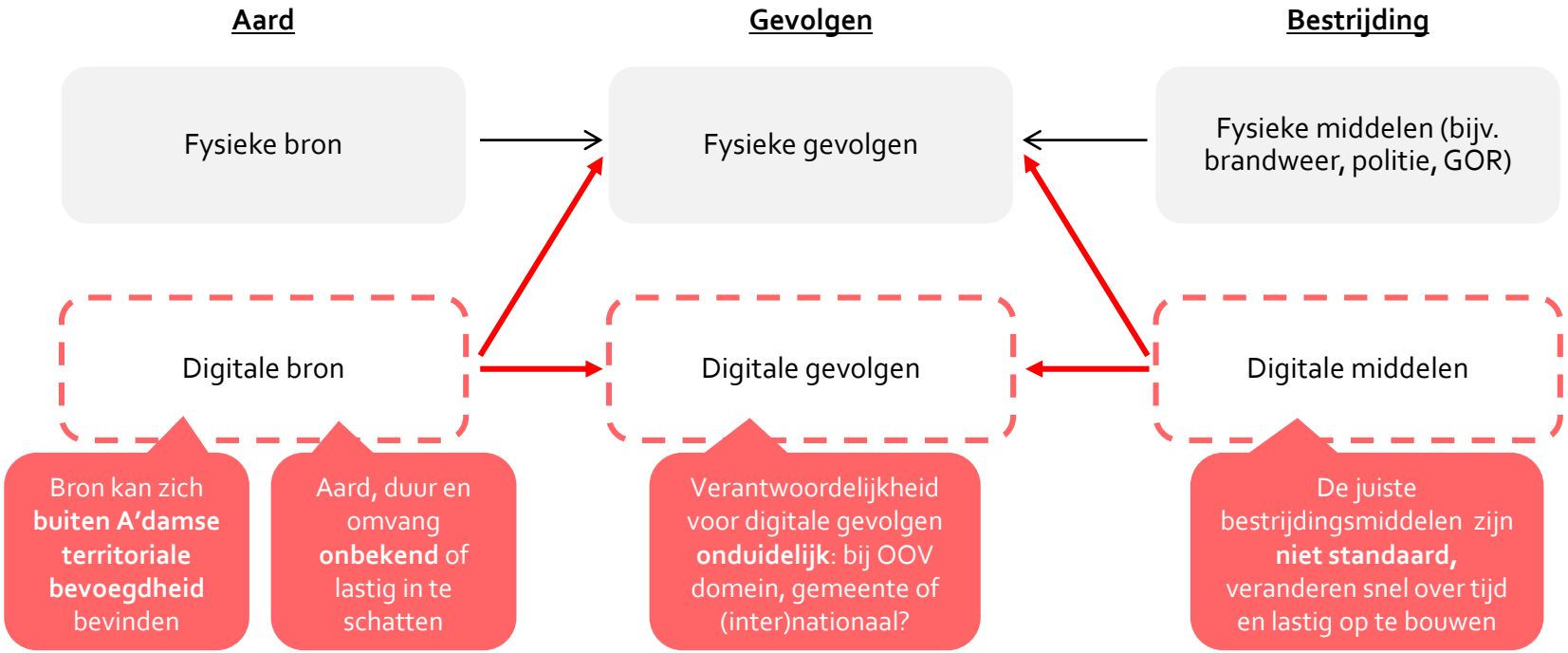
'Resilience' is het vermogen van een organisatie (in dit geval de stad en/of de gemeente zelf) om het functioneren aan te passen voorafgaand, tijdens of na verstoringen. Hierdoor kan het functioneren op peil blijven onder verwachte en onverwachte condities. Er zijn vier stadia in de cyclus:

1. **Voorbereiden**: het anticiperen op (on)voorziene dreigingen
2. **Monitoren**: het vermogen om incidenten te herkennen
3. **Absorberen**: snel en adequaat reageren op het incident, het continueren van de bedrijfsvoering tijdens een incident en het herstellen van verstoringen
4. **Aanpassen** aan bekende en onbekende dreigingen: het lerend vermogen staat voorop; kennis die is opgedaan tijdens het incident kan worden gebruikt om systemen, protocollen en mensen veerkrachtiger te maken

Bron: o.b.v. Hollnagel e.a. (2010)

OOV domein dient zich voor te bereiden om ook crises met een of meerdere digitale componenten te beheersen

Structuur van een crisis



Bron: OOV domein, Expert interviews, Analyse projectteam

Bij een nationale ICT-crisis levert NCSC vier functies die vertaald zouden kunnen worden naar de Amsterdamse situatie

INDICATIEVE VERTALING NAAR A'DAMSE CONTEXT

Functies	**Nationaal Cyber Security Centrum (NCSC)**	**Amsterdam**
Vormen crisisorganisatie	Wanneer tijdens een crisis verschillende ministeries zijn betrokken bij de aanpak daarvan, treedt de nationale crisisstructuur in werking. Bij een ICT-crisis is het NCSC onderdeel van de nationale crisisstructuur	Bij een ICT-crisis (met significante gevolgen voor de openbare orde) zou primaat en verantwoordelijkheden binnen gemeente/driehoek duidelijk moeten zijn. Cruciaal is dat verantwoordelijkheden en communicatielijnen uitgetekend zijn en er regelmatig wordt geoefend
Faciliteren van de ICT Response Board	Het NCSC faciliteert de ICT Response Board (IRB), het publiek-private adviesorgaan voor de nationale crisisbesluitvormingsstructuur bij een ICT-crisis. Tijdens een grootschalige ICT-crisis of dreiging maakt de IRB een analyse van de situatie. Dit gebeurt op basis van informatie-uitwisseling. Deelnemers van de IRB zijn ICT-experts uit een aantal vitale sectoren (onder andere telecom/ICT, energie, financieel en drinkwater) en uit betrokken overheidsorganisaties	Amsterdam zou een soortgelijk adviesorgaan kunnen opzetten dat een analyse van de situatie kan leveren in een ICT-crisis. Hierin zitten ICT-experts uit de Amsterdamse vitale sectoren en betrokken overheidsorganisaties. Vraag hierbij is of dit van voldoende toegevoegde waarde is of dat Amsterdam goed aangesloten kan worden op de nationale IRB
Nationale samenwerking tijdens crisis	Cruciaal in de versterking van ICT-crisisbeheersing is het inrichten van een stelsel van samenwerkingsverbanden op nationaal niveau. Daarom maakt het NCSC met publieke en private partners afspraken op welke wijze wordt samengewerkt tijdens een crisissituatie	Cruciaal is dat Amsterdam afspraken maakt met NCSC over samenwerking tijdens een ICT-crisis; o.a. het vastleggen van procedures en communicatielijnen. Essentieel is om de (communicatie)procedures in geval van een digitale dreiging uit te tekenen en meermaals te oefenen
Internationale samenwerking tijdens crisis	Binnen de EU werkt het NCSC aan de uitwerking van het EU-beleid op het gebied van ICT-crisis, dat is vastgelegd in de Europese Cybersecurity Strategie. Dit betreft deelname aan de tweejaarlijkse oefencyclus onder de naam Cyber Europe en het verbeteren van de samenwerking tussen de nationale CERTs via onder meer de opstelling van Standard Operating Procedures (SOP). Daarnaast neemt het NCSC deel aan het International Watch and Warning Network (IWWN)	Voor Amsterdam voldoet waarschijnlijk samenwerking met NCSC, omdat deze op haar beurt de internationale samenwerking coördineert

Bron: NCSC, Expert interviews, Analyse projectteam

Als opmaat naar een gemeentebreed actieplan is Directie OOV al begonnen met inventarisatie en acties m.b.t. digitale veiligheid

SCHETS VAN EERSTE ACTIES / PLAN VAN AANPAK

	Toelichting	*Status*
Voorbereiden op cybercrisissituaties	Er zijn al stappen gezet om beter voorbereid te zijn op crisissituaties die gerelateerd zijn aan digitale veiligheid. Binnen G4-verband wordt op dit moment gewerkt aan een Cybergevolgbestrijding Handreiking (na de zomer een eerste versie)	Work-in-progress
Initiëren / vergroten inzet op preventie	Er is nog weinig aandacht voor het niet-crisis deel van digitale veiligheid bij ambtenaren en burgers. Interne kennisdeling, themamiddagen en meetings met organisaties als Team High Tech Crime voor collega's van OOV kunnen helpen bij het doorvertalen van digitale veiligheid naar de werkzaamheden van de directie. OOV kan voorlichting en preventiecampagnes voor burgers en ondernemers in beeld brengen en waar nodig zelf initiëren, waarmee de weerbaarheid van kwetsbare groepen vergroot wordt	In voorbereiding
Onderzoeken of bevoegheden BM toereikend zijn	In rapport "Burgemeesters in Cyberspace" wordt geconstateerd dat de openbare orde bevoegdheden van de burgemeester in de gemeentewet zijn geschreven met de offline wereld in gedachten. Er wordt volgens hen nog veel vanuit het fysieke domein georiënteerd, waardoor de gemeentewet en burgemeesters niet goed voorbereid lijken op digitale veiligheid vraagstukken. Ook op lokaal niveau is het goed om te bespreken of de bevoegdheden van de burgemeester toereikend zijn op het gebied van digitale veiligheid	Onderzoek te starten
Onderzoeken beleid OOV m.b.t. cyberveiligheid	Belangrijk om vanuit het perspectief van digitale veiligheid staand of nieuw beleid op alle terreinen van OOV tegen het licht te houden. Vragen hierbij zijn bijv. hoe groot het fenomeen cybercrime is in Amsterdam. Wat voor delicten vinden er plaats? Maar ook: stellen we aanvullende vergunningsvoorwaarden aan horecagelegenheden op het gebied van digitale veiligheid? Moet een spy webshop een vergunning aanvragen? Moeten we een datacenter sluiten dat illegale servers host binnen de gemeente Amsterdam en daarmee ondermijnende impact heeft op de openbare orde? Ook liggen er bestuurlijke vraagstukken die door de politiek beantwoord moeten worden, zowel lokaal als landelijk. Is het gewenst dat allerlei sensoren en andere IoT apparaten in de openbare ruimte metingen verrichten (HCSS, 2017)? Gaan we de APV toepassen op soortgelijke digitale criminaliteit: is er een digitale APV nodig?	Onderzoek te starten
Starten periodiek ambtelijk overleg sub-driehoek	Periodiek ambtelijk overleg met het OM en politie in de vorm van een sub-driehoek kan helpen bij het versterken van de aanpak van cybercrime	In voorbereiding

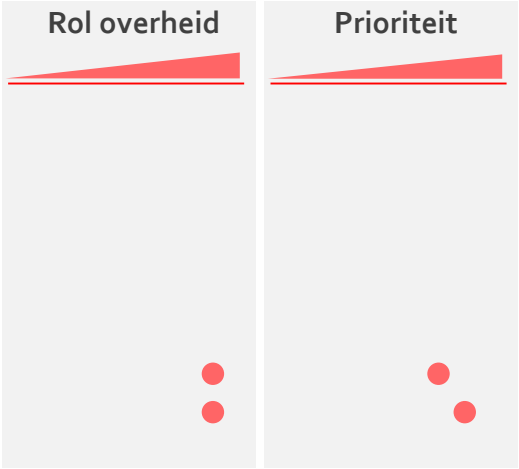
Bron: OOV (Notitie cyberveiligheid), Interpretatie door projectteam

Essentieel om digitale veiligheid te integreren in huidige veiligheidsaanpak en -beleid (1/2)

AANVULLINGEN UIT VALIDATIE EXPERTTAFEL

Conclusies en aanbeveling(en)

- In de koude fase (vóór een incident) moet je al weten hoe de keten van bepaalde processen in je organisatie in elkaar zit, zodat je in de warme fase (na een incident) weet waar de focus en actie moet liggen
- Werven van technische mensen met digitale skills
- Creëren van een overkoepelende veiligheidscultuur; "mensen denken vaak dat digitale veiligheid vooral lastig is", maar een goede zaak dat gemeente Amsterdam het nu ziet als iets essentieels
- Kijk naar de toepasbaarheid van het bestuurlijk instrumentarium op cyberveiligheid
- Houdt het huidige en toekomstige beleid vanaf heden langs deze spelregels voor digitale veiligheid



Bron: Experttafel (27-5-2019)

Essentieel om digitale veiligheid te integreren in huidige veiligheidsaanpak en -beleid (2/2)

AANVULLINGEN UIT VALIDATIE EXPERTTAFEL

Gestarte acties voor 2019/2020

- Team gevormd dat zich binnen OOV bezig houdt met digitale veiligheid
- OOV bereidt notitie voor over hoe digitale veiligheid zich verhoudt tot de dossiers van de directie
- Periodieke sub-driehoek geïnitieerd voor cyberveiligheid
- Het cyberteam van OOV voert gesprekken met alle teams binnen OOV en externe partners van OOV over invloed van digitale veiligheid op dossiers
- Inventariseren van preventieproducten en bewustzijnsmethodieken
- Notitie Cyberveiligheid en OOV
- Whitepaper Cyberveiligheid en OOV
- Scan invloed digitalisering op lopende dossiers OOV
- Awareness campagne OOV en veiligheidsafdelingen gemeente
- Aanbesteding handreiking cybergevolgbestrijding: opdracht gegund aan Berenschot op basis van uitvraag en subsidie namens Ministerie VenJ samen met de G4

Bron: Experttafel (27-5-2019)

Einde Digitaal Veiligheidsbeeld Amsterdam

Managementsamenvatting

Inleiding

Thema
Eigen huis op orde

Thema
Het individueel welzijn van burgers

Thema
Private en maatschappelijke organisaties

Thema
Vitale infrastructuur

Thema
Democratie en bestuurlijke stabiliteit

Thema
De openbare orde en veiligheid

Klik op de hoofdstukken om er naar toe te bewegen. Je kunt overal in het document via de Home-button terug naar deze slide!