Gemeente Amsterdam



Agenda Digitale Veiligheid

Juni 2020

Inhoud

Agenda Digitale Veiligheid Amsterdam	2
Zes doelen	7
Het welzijn van de burger	9
Veiligheid voor bedrijven en instellingen	12
De vitale infrastructuur	13
Crisis- en incidentenbeheersing	16
Democratie en bestuurlijke stabiliteit	18
Eigen huis van de gemeente op orde	20
Nawoord	23
Uitgave	24

A1Vrije_36905-180416-westerpark-bloesem_AN-8709.jpg

Agenda Digitale Veiligheid Amsterdam

Uit en thuis: altijd online

We doen steeds meer online, de hele dag door. Zowel als individuen in het dagelijkse leven, maar ook met z'n allen in het groot. In onze huidige samenleving wordt veel door computers geregeld. Neem alleen al het verkeer in en rond de stad: stoplichten, bruggen en spoorbomen werken automatisch. Tram, bus en metro rijden allang niet meer alleen door mensenhanden. Kijk naar andere soorten verkeer, zoals het betalingsverkeer. We vinden het heel gewoon om contactloos af te rekenen of geld uit een automaat te trekken. Maar er zit wel een enorm digitaal netwerk achter, zoals bij al het moderne verkeer het geval is. Of het nu om persoonsgegevens, televisie, telefoon of elektriciteit gaat: (on)zichtbare kabels, signalen en computerverbindingen leiden alles in goede banen.

Een digitale samenleving heeft veel te bieden

De toenemende digitalisering biedt zowel het individu als de samenleving grote voordelen. Bijna alles gaat sneller en makkelijker. Werken, contact onderhouden met vrienden, met instanties, geldzaken regelen, shoppen etc. – het kan allemaal online. Daardoor besparen we veel tijd en geld.

Dit geldt ook voor bedrijven. Doordat computers nu veel van het werk doen (en dat sneller doen) worden kosten bespaard. Bedrijven maken meer winst en blijven gezond, waardoor de economie een boost krijgt. Ook komen er steeds meer digitale diensten in de stad die gebruikmaken van handige apps of websites, zoals taxibedrijf Uber, verhuurder AirBnB en maaltijdkoerier Thuisbezorgd.nl. Het wordt de Amsterdammer makkelijker gemaakt.

Ook andere organisaties kunnen door automatisering zaken sneller en goedkoper afwikkelen. Neem de overheid. Via het internet kun je een vergunning of andere documenten aanvragen bij het stadsloket. Dat is voor jou als burger en voor de gemeente gemakkelijker. Daarnaast heeft digitalisering ook sociale voordelen. Mensen die, om wat voor reden dan ook, moeilijk de deur uitkomen, kunnen via social media contacten onderhouden, via de online webshop kleren kopen of boodschappen bestellen. Ze moeten dan wel over de juiste apparatuur en vaardigheden beschikken. Dit is een belangrijk aandachtspunt voor de samenleving in een digitale stad.

De schaduwkant van digitalisering

Naast alle voordelen brengt een gedigitaliseerde samenleving ook nieuwe risico's met zich mee. Digitale technologie kan het namelijk ook weleens laten afweten, wat ons kwetsbaar maakt. Wat moeten we doen als belangrijke systemen in de stad een storing krijgen en daardoor tijdelijk of niet beschikbaar zijn? Of dat nu per ongeluk gebeurt of met opzet, elke Amsterdammer kan er grote last van ondervinden.

Een ander bekend voorbeeld is dat de stroom uitvalt. Dan sta je er weer even bij stil hoe sterk we zijn aangewezen op elektriciteit. Je zit in het donker, de verwarming valt uit, de douche is ijskoud, terwijl de vriezer juist ontdooit. De Tv doet het niet en je kunt geen koffie meer zetten. Een vervelend gevolg hiervan is ook dat we geen gebruik meer kunnen maken van smartphones, tablets of pc's. Want als er geen stroom is, vallen WiFi-verbindingen en de grote telecom-masten ook uit. Een kleine ramp als je bedenkt wat we allemaal online doen en zelfs levensgevaarlijk als je dan net dringend hulp nodig hebt.

We zijn met z'n allen erg afhankelijk geworden van technologie. Dat brengt risico's met zich mee, waar we ons van bewust moeten zijn. Als netwerken, verkeer en energietoevoer niet goed functioneren, ligt het openbare leven in de stad al gauw plat. Daarmee komt ook de openbare orde in gevaar, net als de economische bedrijvigheid. Dit staat nog los van het feit dat bedrijven kwetsbaar zijn voor internetfraude en hacking: jaarlijks lijdt het Amsterdamse bedrijfsleven door die cybercriminaliteit ruim 600 miljoen euro schade.

Op persoonlijk vlak brengt digitalisering ook risico's met zich mee. Veel mensen hebben plezier van social media, maar deze open media kunnen ook misbruikt worden, met mogelijke psychische schade tot gevolg. Neem het cyberpesten, waar vooral jongeren het slachtoffer van worden. Soms gaat dat zelfs samen met chantage, waarbij gedreigd wordt met het online zetten van eerder gedeelde naaktfoto's of andere persoonlijke informatie. Deze jongeren zien soms geen uitweg meer omdat zij zich te erg schamen.

Andere risico's voor internetgebruikers zijn oplichting, via online platformen zoals bijvoorbeeld Marktplaats of Vinted en het zogenaamde phishing. Praktijken die je heel wat geld kunnen kosten. Naast je portemonnee loopt soms ook je privacy gevaar, bijvoorbeeld als je wachtwoord en of creditcard gestolen wordt via een datalek. Soms geven mensen ook zelf gegevens weg, vaak onbewust. Zo verzamelen apps van sommige digitale diensten meer data dan nodig is voor het gebruik. Als laatste noemen we hier het verspreiden van nepnieuws op online media. Dat kan mensen in verwarring brengen: wat is nu wél waar en wat níet? Bovendien willen we geen buitenlandse inmenging in onze verkiezingen. Ook het vertrouwen in bestuur, journalistiek of rechtspraak kan erdoor afbrokkelen.

Hoe digitaal veilig is Amsterdam?

Vergeleken met andere steden in de wereld staat Amsterdam er redelijk goed op. Het gerenommeerde blad The Economist beoordeelt elk jaar de veiligheid van zestig wereldsteden. Dat gebeurt op vier onderdelen, waarvan er één digitale veiligheid is. Het gaat om vragen als: wat doet een stad om de privacy van mensen te verzekeren? Werkt de gemeente samen met bedrijven aan méér veiligheid? Hier staat Amsterdam met 89 van de 100 punten op plaats 14, na steden als Tokio, Chicago, New York, Londen en Toronto. Toch is er geen reden om achterover te leunen. Als het even kan, moeten die 89 punten richting de 100. De ontwikkelingen in de digitale wereld gaan razendsnel. Amsterdam is in een rap tempo gedigitaliseerd en daarmee is ook onze digitale afhankelijkheid steeds groter aan het worden. Digitale verstoringen kunnen enorme impact hebben. Ook cybercriminaliteit lijkt steeds meer voor criminelen op te leveren, waardoor zij vaker via het internet hun geld verdienen.

De digitale ambities van Amsterdam

Amsterdam wil een digitaal veilige stad zijn. We moeten ervoor zorgen dat burgers, bedrijven en systemen beter bestand zijn tegen mogelijke bedreigingen. Kinderen en jongeren moeten veilig op het internet kunnen surfen. De zorg voor ouderen mag niet in gevaar komen door stokkende systemen. Alle Amsterdammers moeten kunnen vertrouwen op een goede energietoevoer, op storingsvrij transport van digitale data en signalen, op goed functionerend openbaar vervoer, op waarheidsgetrouwe informatie en op een veilige opslag van hun persoonlijke gegevens. De hele digitale infrastructuur moet op orde zijn.

Werken aan digitale veiligheid is noodzakelijk voor de hele Amsterdamse samenleving. We voorkomen daarmee dat bewoners, ondernemers en bezoekers last krijgen van verstoringen en hacking. Tegelijkertijd kunnen Amsterdammers nog meer profiteren van de kansen en voordelen. Digitalisering heeft economisch en maatschappelijk heel veel goeds te bieden. Om die ambities waar te maken, heeft de gemeente de Agenda Digitale Veiligheid opgesteld. Daarin staat hoe we willen bereiken dat de stad digitaal veiliger wordt.

Zes doelen

Amsterdam richt zich bij het vergroten van de digitale veiligheid op zes hoofdpunten:

1. **Het welzijn van de burger**
2. **Veiligheid voor bedrijven en instellingen**
3. **De vitale infrastructuur**
4. **Crisis- en incidentmanagement**
5. **Democratie en bestuurlijke stabiliteit**
6. **Eigen huis van de gemeente op orde**

Op elk punt heeft de gemeente onderzocht welke kansen en risico's er zijn. Welke gevolgen heeft dat en hoe kunnen we het voorkomen? In de Agenda Digitale Veiligheid staan acties en aanbevelingen. Wat gaat Amsterdam doen tegen digitale bedreigingen en wat zou er nog moeten gebeuren?



Foto: Angelo Abear

Het welzijn van de burger

Beter bestand zijn tegen cyberpesten, chantage, oplichting en schending van privacy

Inbraak: Informeren, verbinden, stimuleren

Jaarlijks is ongeveer 11% van de Amsterdammers slachtoffer van cybercriminaliteit. Vaak gaat het om online pesten, hacking, phishing of koop- en verkoopfraude. Ook WhatsApp-fraude komt steeds vaker voor, waar berichten met malafide betaling linkjes worden gedeeld. Wij willen deze nieuwe vormen van criminaliteit de kop in drukken. Hierbij zullen we nauw moeten samenwerken met het nieuwe Cyber Task Force van de Politie Eenheid Amsterdam-Amstelland, het Openbaar Ministerie en betrokken internetbedrijven. Uit het Cyber Intelbeeld van de politie komen een aantal vormen van digitale criminaliteit sterk naar voren. Dat worden dan ook onze speerpunten.

Pesten en chantage: onderzoek en initiatieven

Cyberpesten komt vooral onder jongeren (15-25 jaar) voor. Het gaat vaak om laster en chantage. Iemand deelt bijvoorbeeld naaktfoto's van een ander op social media, of dreigt die online te plaatsen. Dat kan heel erg schadelijk zijn voor het geestelijk welzijn van deze jongeren. Veel jongeren maken via internet kennis met seksualiteit. Dit maakt hen ook kwetsbaarder voor mogelijk misbruik. Ook volwassenen maken zich schuldig aan onlinemisbruik door te proberen via social media kinderen tot seksueel gedrag te verlokken door zich voor te doen als een leeftijdsgenoot.
De gemeente onderzoekt hoe weerbaar jongeren zijn tegen cyberpesten, zoals shame sexting. Dat is het zonder toestemming online zetten van naaktfoto's of filmpjes. Wat weten jongeren hier al over en wat nog niet? Daarbij is er extra aandacht voor mogelijk kwetsbare groepen. De gemeente vindt het belangrijk dat jonge Amsterdammers beter bedacht zijn op digitale bedreigingen en verkent samenwerkingen met initiatieven zoals bijvoorbeeld Stichting Cyberschool. Zij ontwikkelt op dit onderwerp een landelijk leerprogramma. Dit nieuwe programma richt zich voornamelijk op leerlingen, maar ook op ouders en leraren. Het is een levendig lespakket

dat van de praktijk uitgaat. Jongeren praten met elkaar over werkelijke situaties en doen oefeningen. Ook worden populaire apps en websites onderzocht op kwetsbaarheden zodat gebruikers en ontwikkelaars hier proactief op ingelicht kunnen worden. Ze leren risico's te herkennen en er beter mee om te gaan.

Hacking: bewustmaken en monitoren

Zo'n 5% van de Amsterdammers heeft weleens met hacking te maken gehad. Hacken is bijvoorbeeld het inbreken op een computer, op e-mailaccounts of op websites en profielen. Het aantal slachtoffers daalt licht. Dat niet wil zeggen dat de risico's afnemen, integendeel. Dit komt doordat steeds meer apparaten op het internet worden aangesloten, bijvoorbeeld een smart-tv of een koelkast met WiFi. Die apparaten zijn helaas vaak niet voldoende beveiligd en de instructies om ze na aanschaf uit de doos beter te beveiligen zijn voor de meeste gebruikers te hoog gegrepen. Daarnaast wordt ICT steeds ingewikkelder, waardoor gebruikers steeds kwetsbaarder zijn. Ook zijn gebruikers zich vaak niet bewust van hun digitale (on)veiligheid. Mensen hebben het soms zelf niet door als dat slachtoffer zijn geworden van hacking of phishing.

Voorbeelden van acties:

Het is van belang dat burgers beter weten waarop ze moeten letten en wat ze wel of juist niet moeten doen. Om een beeld te krijgen van de situatie, wil de gemeente in de veiligheidsmonitor (die ieder jaar onder Amsterdammers plaatsvindt) naast de reguliere veiligheid ook de digitale veiligheid van Amsterdammers weergeven. Dat kan door een koppeling te maken met andere enquêtes, waarin bijvoorbeeld wordt gevraagd: hoe vaak zit u op sociale media? En hoe vaak koopt u dingen op internet? Maar ook: hebt u weleens te maken met hacking, cyberpesten, misbruik van uw e-mailaccount, wachtwoorden of oplichting op verkoopsites? Daarnaast zullen meldingen en aangiftes bij politie van digitale delicten in de veiligheidsmonitor worden opgenomen. Hierdoor krijgen we zowel een gevoeld als een feitelijk beeld van digitale veiligheid en welzijn in de stad. Door gevoelde en feitelijke digitale veiligheid in kaart te brengen kan de gemeente beter inspelen op de behoeften van haar burgers.

- De gemeente Amsterdam wil de geleerde lessen van andere gemeenten onderzoeken om zo zelf tot een eigen Amsterdams model te komen. In Haarlem worden kinderen opgeleid tot cyberagent en in Breda worden burgers opgeleid tot digitaal ambassadeur. Voor zowel burgers als ondernemers is dit een model waarbij de gemeente in samenwerking met cyberexperts en politie anderen opleidt tot expert.

- Het leren van herkennen van online risico's en ook de juiste hulpmiddelen en kennis bieden bij een cyberincident blijkt aan de hand van het experiment in andere gemeenten succesvol te zijn.

- De gemeente wil bestaande educatieve projecten ondersteunen. Een voorbeeld hiervan is de Stichting Cyberschool.

- Beschermen van kwetsbare Amsterdamse meisjes die het slachtoffer worden van digitale afpersing, bijvoorbeeld met seksueel getinte foto's of video's (sextortion).

- Aanpakken van digitale kanalen en plekken waar internetcriminelen actief zijn en met elkaar communiceren, zoals marktplaatsen (op o.a. darkweb) voor drugshandel en ondermijning.

ambitie

Veiligheid voor bedrijven en instellingen

Beter bestand tegen datadiefstal, inbreuk op privacy en economische schade

De schade voor bedrijven door cybercriminaliteit bedraagt in Amsterdam ruim 600 miljoen euro per jaar (cijfer uit 2019). Daarnaast komt door hacking de privacy van mensen in gevaar.

Inbraak: Informeren, verbinden, stimuleren

Digitale aanvallen komen voor bij alle organisaties, bijvoorbeeld met ransomware, ook wel gijzelsoftware genoemd. Hiermee worden computers afgesloten van gebruik en toegang en als het ware gegijzeld. Het slachtoffer krijgt pas weer toegang tot alle gegevens als er losgeld wordt betaalt. Naast financiële schade heeft diefstal van data gevolgen voor privacy. Het geeft maatschappelijke onrust en onzekerheid.

De weerbaarheid tegen cybercrime is vooral laag bij het midden- en kleinbedrijf (MKB): men is zich in deze sector vaak niet genoeg bewust van de risico's. Ook ziekenhuizen zijn kwetsbaar, onder meer omdat zij werken met digitale patiëntendossiers. Het is zaak om (kleinere) bedrijven en maatschappelijke instellingen weerbaarder te maken. Dat gebeurt onder meer door middel van informatiecampagnes, bijeenkomsten en het opzetten van netwerken. In Amsterdam en de regio zijn hiervoor de volgende acties gepland.

Voorbeelden van acties:

- Beschermen van ondernemers die slachtoffer kunnen worden van hacking, afpersing via ransomware of fraude met digitale middelen.
- Nauw samenwerken met het Digital Trust Center (DTC) van het Ministerie voor Economische Zaken en Klimaat. Het DTC biedt de MKB'r nuttige informatie, adviezen en tools om de cyberweerbaarheid

bij ondernemers te vergroten. Zij werken aan een landelijk dekkend stelsel van samenwerkingen op het gebied van cyberweerbaarheid, waar de gemeente Amsterdam uiteraard deel van zal uitmaken. Waar het Nationaal Cyber Security Centrum (NCSC) vooral gericht is op de vitale sectoren, biedt het DTC ondersteuning aan de niet-vitale sectoren.

- Het Platform Veilig Ondernemen (PVO) organiseert bijeenkomsten om ondernemers digitale kennis bij te brengen en het bewustzijn over cybercrime te vergroten.
- Een campagneteam bezoekt ondernemers in digitaal minder veilige gebieden (binnen stadsdelen en Amstelland-gemeenten).
- In de digitale PVO-toolbox 'Veilig Ondernemen' zitten nu ook trainingen en workshops over cybercrime en komt ook beschikbaar op de nieuwe PVO-website.
- Er komt een phishingtest beschikbaar voor bij het MKB. Wie de test laat uitvoeren, krijgt een rapportage: hoe weerbaar de onderneming is tegen een phishing-aanval?
- We werken aan een handige flyer met 10 tips voor ondernemers: "Wat te doen na een cyberincident?". De Amsterdamse politie maakt het doen van aangifte nu makkelijker met een digitaal aangifteformulier.

ambitie

De vitale infrastructuur

Beter bestand tegen uitval processen

Steeds meer diensten in Amsterdam maken gebruik van digitale technologie. Dat vergroot het gemak voor de bewoner, de ondernemer en de bezoeker (afgekort 'BOB') van de stad. Maar ook hiervoor geldt dat systemen van informatie en communicatie kunnen uitvallen. Dan worden processen waar we als samenleving afhankelijk van zijn lamgelegd, met alle gevolgen van dien.

Eerst de belangrijkste processen

Uitval van belangrijke systemen heeft altijd gevolgen voor de gehele stad als het gaat om veiligheid en bereikbaarheid en soms zelfs de eerste levensbehoeften. Daarom is het noodzakelijk dat we werken aan een degelijke digitale infrastructuur. De hele digitale basisorganisatie moet op orde zijn en alles moet het veilig blijven doen.



Foto: Serhat Beyazkaya

Niet alles kan tegelijk. Daarom is het logisch te beginnen met de infrastructuur voor de vitale processen. Dat zijn de processen die de belangrijkste diensten leveren voor de Amsterdamse bevolking. Onder andere het verleden leert ons dat bedrijven en of diensten die niet perse aangemerkt zijn als vitaal wel bij uitval een vitale rol kunnen spelen in een digitale samenleving. We zullen nog beter in kaart moeten brengen welke instanties en diensten vitaal zijn voor de Amsterdammer. Welke voorzieningen zijn voor deze diensten vereist? Vervolgens gaan we na wat de risico's en wat de gevolgen van uitval zijn en hoe deze infrastructuur zo goed mogelijk te beveiligen is. Een aantal voorbeeldscenario's zijn:

- Langdurige verstoring van elektriciteit of gas
- Uitzetten van gemalen en openzetten van waterkeringen
- Langdurig verstoord telefoon- en dataverkeer
- Langdurig platleggen en of sabotage van onderdelen binnen de:
  - Amsterdamse haven en sluizen
  - Verkeerssignalering (netwerk van o.a. stoplichten)
  - Bruggen
  - Openbaar vervoer

Samenwerken is belangrijk

De gemeente kan het allemaal niet in haar eentje. We moeten samenwerken met de betrokken publieksdiensten, met kennisorganisaties en andere private partners. Het is zaak om kennis te delen over technologie en cybersecurity, landelijk maar ook internationaal. In de belangrijkste processen voor Amsterdam zijn we allemaal van elkaar afhankelijk. Samen met de vitale dienstverleners en kennisinstituten zullen we continue het risico- en veiligheidsbeeld moeten bepalen en de situatie blijven volgen.

Voorbeelden van acties:

De gemeente zal verder gaan uitzoeken:

- Wie de cyberdeskundigen zijn in de stad bij organisaties die samen willen werken aan het ontwikkelen van kennis en het voorkomen en bestrijden van digitale calamiteiten.
- Welke mogelijkheden er zijn om de vitale digitale infrastructuur te beschermen.
- Wat we moeten doen en met wie om de vitale digitale infrastructuur in de openbare ruimte zo veilig mogelijk te krijgen en te houden. Onderdeel daarvan is de nationale digitale vertrouwensinfrastructuur (DVI), een programma dat samen met andere overheidsinstanties (o.a. VNG, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Nationale Politie en de Veiligheidsregio) gerealiseerd wordt.
- Welke activiteiten er lopen, landelijk en in EU, om standaarden te ontwikkelen op het gebied van beveiliging van de vitale digitale infrastructuur en de bijhorende digitale diensten. Op basis daarvan wordt gekozen waarop Amsterdam kan aansluiten.
- Wat verder nog instanties of bedrijven zijn die nu niet als vitale infrastructuur zijn aangeduid door de NCTV, maar die mogelijk wel van vitaal belang zijn voor de Amsterdamse samenleving. De recente verstoringen bij de netwerkapplicatie Citrix tonen aan dat we door digitalisering van nieuwe soorten bedrijven afhankelijk zijn geworden. We zullen als gemeente zijnde goed in kaart moeten brengen welke nieuwe afhankelijkheden zijn ontstaan door digitalisering.

ambitie

Crisis- en incidentenbeheersing

Beter voorbereid op plotselinge verstoringen en digitale aanvallen

Digitale veiligheid heeft veel te maken met het werk van de directie Openbare Orde en Veiligheid in de stad (OOV). Een digitale aanval op vitale infrastructuur kan potentieel leiden tot een ernstige verstoring van de openbare orde en veiligheid in Amsterdam.

Digitale incidenten

Crisis- en incidentbeheersing door OOV is nodig om te voorkomen dat de openbare orde in Amsterdam wordt verstoord wanneer een digitale dreiging optreedt. Maar ook dient de directie mee te helpen om prioriteiten te stellen. Waar moeten we ons allereerst op richten? Waar en voor wie kunnen digitale bedreigingen ernstige gevolgen hebben? Voor welke personen of kwetsbare groepen, op welke gebieden, in welke branches?

Voorbeelden van acties:

1. Zorgen dat de belangrijkste digitale infrastructuur tegen een stootje kan. Voorbereiden op digitale bedreigingen voor de openbare orde in Amsterdam. Bijvoorbeeld: een cyberaanval op de transportnetwerken, het uitvallen van de energievoorziening of een verstoring van de pinautomaten in de stad.

2. Opstellen en uitwerken crisisplan. Uiteraard worden vitale processen gemonitord door landelijke instanties, maar het crisis- en incidentmanagement wordt decentraal geregeld. Daarom zal de gemeente vanuit OOV, samen met de vitale infrastructuur tot een gecoördineerd crisisplan moeten komen.



Foto: Jonas Denil

ambitie

Democratie en bestuurlijke prioriteit

Beter bestand tegen verstoring van verkiezingen, desinformatie, bedreiging van journalisten

Onze democratie is steeds meer afhankelijk van wat er in de digitale wereld gebeurt. Zo wordt er in sommige gevallen online gestemd. Dat is handig, maar het vergroot ook de kans op fraude. Stemsystemen kunnen gemanipuleerd worden. Verder baseren bewoners hun mening steeds meer (alleen) op online bronnen – en die zijn lang niet altijd zo betrouwbaar.

Informatievoorziening: goed blijven opletten

In Nederland hebben we een breed aanbod aan traditionele en 'nieuwe' media, zowel landelijk als regionaal. En die laten verschillende kanten van het nieuws zien. Echter, door sociale media is het mogelijk geworden om alleen media te volgen die jij als gebruiker hebt geliket. Het nadeel hiervan is dat dit kan leiden tot een tijdlijn die erg verschilt van een andere gebruiker. Ook kan de online nieuwsvoorziening niet altijd goed gecontroleerd worden op authenticiteit. Internet geeft ook de kans om allerlei meningen te verkondigen. Bijna iedereen kan die informatie op elk gewenst tijdstip en op elke plek tot zich nemen. Dit is een groot goed. Maar, mensen kunnen daarbij ook, opzettelijk of niet, onjuiste informatie op het internet zetten. Een stap verder gaat het plaatsen van nieuwsberichten die niet gecontroleerd zijn en die mogelijk schadelijk zijn voor anderen.

Vanuit de gemeente willen we meer samenwerken met journalisten en andere experts, om burgers beter te kunnen informeren over hoe nieuws tot stand komt, welke verificatiemethodes mogelijk zijn en wat de gevolgen kunnen zijn van de digitalisering van het publieke debat.

Daarbij stellen we de volgende vragen:

- Welke bronnen gebruiken Amsterdammers voor hun nieuwsvoorziening?
- Hebben Amsterdammers toegang tot digitaal nieuws (internet, social media)? En vinden ze daarin veilig hun weg?



Foto: Tycho Atsma

- Zijn zij wel eens in aanraking gekomen met wat zij zelf zouden bestempelen als desinformatie?
- Raadplegen de Amsterdammers overheids- of gemeentelijke communicatie in het geval van een verstoring van de openbare orde?

Voorbeelden van acties:

1. Samen met grote platforms en mogelijk ook veiligheidsdiensten beter toezicht houden (monitoren) op online-informatie die rondgaat binnen Amsterdamse gemeenschappen.
2. Een betere verspreiding van informatie door de gemeente zelf, waardoor meer mensen in de stad worden bereikt. Dit gaat via eigen kanalen van de gemeente, maar ook via andere afzenders (sociale en traditionele media).
3. Gemeentelijke stukken dienen in begrijpelijke taal geschreven te worden, zodat het voor alle burgers begrijpelijk is.
4. Samenwerking bevorderen met grote online platformen zoals Google, Facebook, veiligheidsdiensten en mediabedrijven.

Eigen huis van de gemeente op orde

Beter bestand zijn tegen diefstal van persoonsgegevens en inbreuk op privacy

ambitie

Wie orde op zaken wil stellen in de hele stad, doet er goed aan eerst in eigen huis rond te kijken. Is bij de gemeenteorganisatie zelf alles wel veilig? Wij blijven dat nauwgezet volgen.

Informatiebeveiliging: een continu proces

De gemeente Amsterdam is een grote en complexe organisatie die veel informatie verwerkt, waaronder veel gevoelige informatie over haar burgers.

Daardoor kan de gemeente een doelwit zijn voor hackers die op zoek gaan naar een datalek. Wij moeten dus ook zelf onze zaakjes goed op orde hebben.
Beveiliging van informatie is binnen de gemeente Amsterdam een continu proces. Voortdurend brengen we (nieuwe) dreigingen en risico's in kaart. Waar nodig nemen we gepaste maatregelen. Daar wordt met het personeel ook op geoefend, waarna we kijken of de maatregelen goed genoeg zijn. Steeds blijft het doel om de informatie nog beter te beveiligen. Dit is nodig, want uit diverse rapporten blijkt dat de digitale dreigingen steeds groter worden en dat we risico's verminderen door gegevens (dataverkeer) optimaal te beschermen en af te schermen voor onbevoegden.

Voorbeelden van acties:

1. Implementatie van de Baseline Informatiebeveiliging Overheid (BIO), één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele landelijke en lokale overheid.
2. Versterken en uitbreiden het Security Operations Center voor alle ICT- en informatiesystemen van de gemeente Amsterdam.
3. Intensiveren van de informatie-uitwisseling met Informatiebeveiligingsdienst (IBD) en het Nationaal Cyber Security Centrum (NCSC).
4. Ervoor zorgen dat er aandacht en monitoring is op de veiligheid van gemeentelijke websites en webapplicaties en deze regelmatig van veiligheidstests te voorzien.
5. Invoeren van een nieuw proces voor informatiebeveiligingsincidenten en datalekken, waarmee de gemeente incidenten met veel impact beter af kan handelen.
6. Uitwerken en invoeren van 'Business Continuity Management'. Dit gaat over het vaststellen van vitale processen binnen informatiesystemen en het invoeren van ontbrekende maatregelen.
7. Uitvoeren van verbeteracties naar aanleiding van de ICT-uitval bij de gemeente Amsterdam die begin 2019 plaatsvond.
8. Verder versterken van het beveiligingsbewustzijn van ambtenaren door het organiseren van een bewustwordingscampagne.



Foto: Frank Holleman

Nawoord

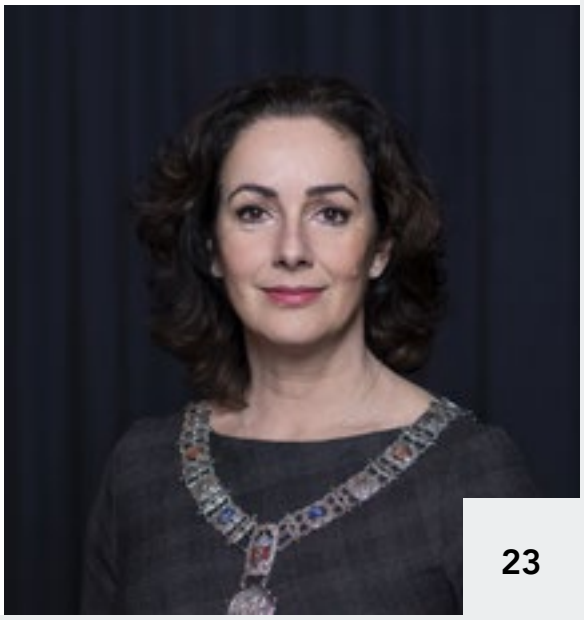
Amsterdam spreekt de ambitie uit om digitaal één van de veiligste steden te worden. Onderzoek toont aan dat 50% van de grote wereldsteden zich matig tot slecht voorbereiden om de stad en haar inwoners te beschermen op digitale veiligheid. Waar je ziet dat er landelijk jaarlijks gerapporteerd wordt over digitale dreigingen en risico's door de NCTV toont Amsterdam nu ook haar verantwoordelijk door een vertaling te hebben gemaakt van het nationale veiligheidsbeeld in de vorm van een Agenda Digitale Veiligheid.

Het is van belang dat de gemeente naast alle kansen ook de risico's van digitalisering bespreekbaar maakt. De stad zal weerbaarder moeten worden om haar bewoners, ondernemers en bezoekers te beschermen tegen digitale risico's. We kunnen dit niet alleen en zullen nauw samenwerken met private- en maatschappelijke partijen om Amsterdam digitaal bewuster en weerbaarder te maken.

De gemeente Amsterdam gaat zich inzetten op preventie van digitale verstoringen en cybercriminaliteit, alsmede de nazorg kant van eventuele crisissen en incidenten (in samenwerking met Directie Openbare Orde en Veiligheid. We zullen meer kennis en middelen moeten vergaren om eventuele digitale verstoringen van de openbare orde en veiligheid te voorkomen. Het digitale Veiligheidsbeeld zal jaarlijks bij worden gewerkt om de situatie te blijven monitoren.

Naast de fysieke veiligheid zal de gemeente Amsterdam zich ook hard moeten gaan maken voor het waarborgen van de digitale veiligheid van de stad en de burgers. Dit is een onomkeerbaar proces.

Femke Halsema
Burgemeester van Amsterdam



burgemeester_halsema2_231118.jpg

Uitgave

De Agenda Digitale Veiligheid is tot stand gekomenin opdracht van burgemeester Femke Halsema en in uitvoering door de gemeente Amsterdam in samenwerking met de Politie Eenheid Amsterdam en het Openbaar Ministerie Parket Amsterdam.

Gemeente Amsterdam
Postbus 2602
1000 CP Amsterdam

Datum Juni 2020

Versie 1.0 Definitieve publieksversie

Rubricering Niet vertrouwelijk

Vormgeving Marieke van Dijk &
Leonore Snoek, idiotēs

© Geen copyright maar 'right to copy' met bronvermelding: **Agenda Digitale Veiligheid, gemeente Amsterdam.**

Voor vragen en opmerkingen:
digitaleveiligheid@amsterdam.nl


Weteringschans 137