Agenda Digitale Veiligheid

Gemeente Amsterdam

Inhoudsopgave

Voorwoord

De stad Amsterdam behoort tot één van de grootste internetknooppunten ter wereld. Als stad werken we samen met partijen om de kansen die digitalisering biedt aan te grijpen om daar in de toekomst de vruchten van te kunnen plukken. Dat betekent dat we de stad ook gebruiken als test lab. Bijvoorbeeld met een proefopstelling van 5G technologie in samenwerking met de Johan Cruijff ArenA. Daar testen we hoe nieuwe technologie toepasbaar is binnen een Smart City context, maar ook in de wijken en buurten voor bewoners en bezoekers. Met de komst van 5G verwachten we per 2025 in Nederland ruim één miljoen verbindingen per vierkante kilometer van mobiele apparaten, uiteenlopend van een smartphone tot aan de elektrische deelfiets.

Als burgemeester van deze stad ben ik verantwoordelijk voor de openbare orde en veiligheid, waaronder ook de virtuele openbare ruimte. Een recente benchmark in The Economist stemt positief wanneer de positie van Amsterdam wordt vergeleken met andere Europese steden (positie 2), maar daalt zodra steden buiten Europa worden betrokken (positie 14). We hebben derhalve nog veel werk te verrichten en zien bijvoorbeeld dat 11% van de Amsterdammers jaarlijks te maken heeft met digitale onveiligheid. Dat loopt uiteen van cyberpesten onder de jeugd tot cybercrime bij ondernemers. Dat laatste heeft een geschatte economische schade van ruim 600 miljoen euro per jaar. De helft van de Amsterdammers komt wekelijks in contact met onjuiste data, die informatie wordt veelal verspreid via social media platformen als Facebook, Twitter en Instagram.

Digitale veiligheid is naast fysieke en infrastructurele veiligheid een aandachtsgebied geworden. Ik heb daarom het vergroten van de digitale weerbaarheid tot prioriteit gemaakt en een stedelijke agenda voor digitale veiligheid opgesteld. Samen met de steden Den Haag, Rotterdam, Utrecht, Almere en Eindhoven werken we eraan om onszelf weerbaar te maken tegen dreigingen via de digitale infrastructuur. Binnen Amsterdam werken we nauw samen met de Politie, het Openbaar Ministerie en private- en kennisinstellingen.

Ik nodig u van harte uit om mijn eerste opzet van de Amsterdamse agenda Digitale Veiligheid te lezen. We stellen suggesties of hulp zeer op prijs.

Femke Halsema
Burgemeester van Amsterdam

Uitdagingen in een digitale stad als Amsterdam

De Nederlandse samenleving digitaliseert in hoog tempo. De impact van digitalisering bij de *Smart City*, *Smart Office*, *Smart Home* en *Smart Citizen* is deels bekend en continue in beweging. Hierbij komt dat rollen, taken en bevoegdheden van private en publieke instanties, voor zo ver reeds duidelijk binnen het digitale domein, wijzigen en verschuiven. Er is behoefte aan multidisciplinaire samenwerking en er is noodzaak tot versterking op het gebied van onder andere infrastructuur, processen en middelen.

Er is naast bestaande documenten zoals de Amsterdamse I-Visie ook behoefte aan een dienst- en sector overstijgend gedragen visie op het gebied van digitalisering en publieke waarden waar het de digitale veiligheid betreft. Een visie biedt aan burgers, bedrijven, organisaties en overheid houvast hoe zich in de preventie weerbaar te maken en hoe te handelen wanneer men onverhoopt getroffen is binnen het digitale domein. Waar Nederland vaak voor- of koploper is binnen beleid in het fysieke domein kunnen we als Nederland en Amsterdam in het bijzonder ook koploper worden binnen het digitale domein. Daar waar Amsterdam bekend staat om zijn openheid, vrijheid, diversiteit en inclusiviteit is ook nadrukkelijk aandacht voor een veilige en open digitale samenleving in Amsterdam.

Coalitieakkoord
Er is een agenda Digitale Stad, onder leiding van wethouder Touria Meliani, waarin concepten worden uitgewerkt voor digitale dienstverlening en participatie (moderne, open overheid), cybersecurity, een veilige digitale infrastructuur en data-soevereiniteit. We blijven aandacht houden voor mensen die moeite hebben met digitalisering. Bewust omgaan met de mogelijkheden en bedreigingen van digitale technologieën, voor het beschermen van burgerrechten en voor eerlijke toegang tot en met het eerlijk verdelen van de opbrengsten van digitale technologieën.

Van coalitieakkoord naar beleidsdoelen
Amsterdam zet samen met zijn partners in op een veilig en open digitaal domein, waarin de kansen die digitalisering onze stad en samenleving bieden, volop worden benut, waarin aan dreigingen het hoofd wordt geboden en waarin fundamentele rechten en waarden worden beschermd.

- Amsterdam is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en in de preventie een handvat te bieden om de weerbaarheid en daar waar het binnen de verantwoordelijkheid en beheer van de gemeente ligt, samen met partners, ook de veiligheid en publieke waarden in het digitale domein te beschermen;
- Amsterdam richt zich op het voorkomen van schade door uitval, verstoring en misbruik van ICT.

Beleidsthema's
Deze thema's geven op hoofdlijnen invulling aan onderwerpen die het bestuur belangrijk acht bij het realiseren van een veilige digitale stad.

Rol burgemeester
Vanuit de portefeuille Openbare Orde en Veiligheid is de burgemeester verantwoordelijk voor deze zaken binnen de fysieke samenleving maar dit geldt net zo goed voor deze onderwerpen binnen de digitale samenleving, de digitale openbare ruimte. Een aanpak slechts gericht vanuit één portefeuille of directie binnen de gemeente Amsterdam is ongewenst. Digitalisering strekt zich uit over alle domeinen zoals wij deze kennen binnen onze stad, waaronder openbaar bestuur, openbare ruimte, economie, verkeer, welzijn, onderwijs, zorg, jeugd, digitale stad en natuurlijk openbare orde en veiligheid. Alle domeinen hebben ermee te maken dat de fysieke samenleving digitaliseert en er inmiddels een parallelle digitale samenleving is ontstaan doordat organisaties steeds meer informatie elektronisch uitwisselen en samenwerken in (digitale) netwerken. Voor deze beide paralellen dient de vraag gesteld te worden wat de impact van digitalisering is op de onderlinge samenhang en verhoudingen.

Digitaal veiligheidsbeeld Amsterdam

Door de snelle digitalisering en nieuwe technologie is digitale veiligheid steeds belangrijker. De gemeente wil Amsterdam zo digitaal veilig mogelijk maken voor haar burgers, ondernemers en bezoekers. Zoals eerder gezegd weerbaar zijn tegen 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 in termen van cybercrime slechts 1.4% van de aangiften tot vervolging.

Het Amsterdamse veiligheidsbeeld beslaat de volgende thema's:

Eigen huis op orde
Uit diverse rapporten (o.a. het Cyber Security Beeld Nederland 2019 van het NCTV) blijkt dat de digitale dreigingen steeds groter worden en dat het vergroten van de (digitale) weerbaarheid het belangrijkste instrument is voor overheden om risico's te verminderen. Gemeente Amsterdam is een grote en complexe organisatie die veel en ook gevoelige informatie verwerkt, ondersteund door informatievoorziening.
Dreigingen worden veroorzaakt door menselijke fouten, maar er moet ook rekening gehouden worden met hacking, verstoring, ransomware en sabotage/diefstal van data of geld door criminelen of hacktivisten.
Het gemeentelijke informatiebeveiligingsbeleid is gebaseerd op de VNG-standaarden, met daarbinnen toepassingsbeveiliging op basis van risico-inschatting. Periodiek worden beveiligingstests en audits uitgevoerd om te toetsen of de beveiliging op orde is. Het college rapporteert hier jaarlijks over aan de gemeenteraad en aan externe toezichthouders. Aan de hand van het veiligheidsbeeld kan het gemeentebestuur, door het stellen van prioriteiten, bepalen op welke risico's te focussen.

Burgers
Vooral jongeren hebben last van cyberpesten. Hacking, koop- en verkoopfraude zijn voorbeelden van cybercrimes waar in totaal jaarlijks circa 11% van de Amsterdammers slachtoffer van worden. Met name cyberpesten kan significante welzijnsschade tot gevolg hebben. Vanuit de overheid en op scholen is hier dan ook al veel aandacht voor door het stimuleren van digitale bewustwording (en ontwikkelen van digitale vaardigheden). Een ander veelgenoemd risico voor de burger is de lage weerbaarheid van (individuele) Internet of Things apparaten. Er ligt een kans voor Amsterdam om als stad hierin voorop te lopen door minimale veiligheidseisen te gaan stellen aan dergelijke apparaten, met als stip op de horizon om dit landelijk dan wel Europees te agenderen en te borgen.

Private & maatschappelijke organisaties
Verstoringsaanvallen komen voor bij alle organisaties (bijvoorbeeld met ransomware), datadiefstal en datalekken hebben een grote privacy-impact bij onder meer financiële instellingen en ziekenhuizen. Dit zorgt ook voor financiële schade: in Amsterdam kost cybercrime bedrijven, naast maatschappelijke onrust bij data-ontvreemding, naar schatting €600 miljoen per jaar. De weerbaarheid is vooral laag bij het MKB door het magere bewustzijn van risico's en bij ziekenhuizen door de relatief lage digitale vaardigheden van medewerkers. Overheden en gemeentelijke instellingen proberen de weerbaarheid te verhogen door bewustwordingscampagnes te houden.

Vitale infrastructuur van de stad
Binnen de stad beslaat dit 17 vitale processen. De grootste digitale dreigingen zijn langdurige verstoring van elektriciteit, sabotage van waterkeringen, scheepvaart of het verkeer. De huidige schaal en het aantal incidenten is vooralsnog niet beschikbaar maar iedere betrokkene geeft aan regelmatig digitale aanvallen te ondervinden. De primaire verantwoordelijkheid voor deze vitale processen ligt vaak buiten de gemeente maar samenwerking en goede (crisis)communicatie is essentieel om weerbaarheid in preventie te vergroten.

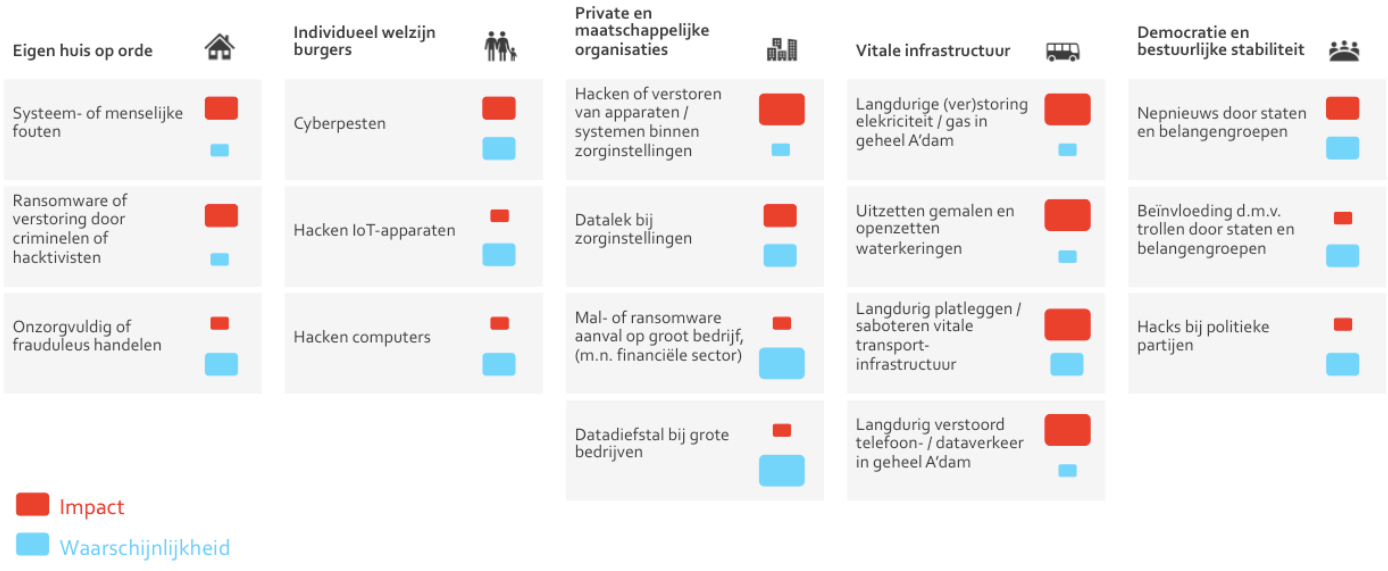
Crisis- en incidentmanagement (Openbare Orde & Veiligheid)
Wanneer een digitale dreiging zich manifesteert kan de Amsterdamse openbare orde in het geding komen. Daarom dient de gemeente direct ingelicht te worden, in staat te zijn een significant cyberincident te herkennen, goed voorbereid te zijn en te beschikken over de juiste middelen en communicatielijnen om (de gevolgen van) een cybercrisis te beheersen.
Het is cruciaal dat de gemeente met belangrijke partijen intern en in het Amsterdamse speelveld en met NCSC[1] duidelijke afspraken maakt over de verantwoordelijkheid en communicatielijnen en deze regelmatig oefent. Hiervoor en voor een hogere inzet op de preventie en aanpak van cybercrime is de directie Openbare Orde & Veiligheid van de gemeente Amsterdam reeds gestart met het opzetten van een plan van aanpak. Daarnaast is zij samen met onder meer nationale politie, veiligheidsregio, VNG en BZK mede initiatiefnemer van het project Digitale Vertrouwensinfrastructuur om een verantwoorde uitwisseling van gegevens te faciliteren bij onder meer incidenten en crisis.

Democratie & bestuurlijke stabiliteit
Circa 50% van de burgers komt wekelijks in contact met vormen van nepnieuws. Verdergaande digitalisering (bijvoorbeeld door middel van het gebruik van algoritmes) brengt risico's op maatschappelijke verkokering en polarisatie met zich mee. Een belangrijk dilemma behelst de vraag welke rol de overheid en daarbinnen de gemeente zouden moeten spelen om de weerbaarheid te vergroten. In het voorbeeld van digitaal stemmen is landelijke verkiezingssoftware kwetsbaar, dus ook bij lokale verkiezingen in Amsterdam. Bij het implementeren van nieuwe vormen van stemmen zal het stemresultaat direct in relatie staan tot de robuustheid en beveiliging van de digitale software.

Digitaal Veiligheidsbeeld Amsterdam
De hierboven benoemde thema's hebben op basis van een enquête, gehouden onder de cross-sectorale partijen en personen in de stad, geleid tot een verkenning. De belangrijkste dreigingen uit de verkenning zijn inhoudelijk getoetst met circa 60 domeinexperts tijdens een georganiseerde experttafel en verwerkt tot een lokaal veiligheidsbeeld voor 2019.

Het veiligheidsbeeld bevat de opgehaalde inzichten en informatie over de geïdentificeerde risico's, waarschijnlijkheden, impact en kansen in de stad. Dit document beschrijft aan de hand van de vastgestelde scope de vertaling naar concrete acties en aanbevelingen op hoofdlijnen. Echter zoals de openingszin van dit document aangeeft is er geen wetenschap over wat we niet weten.

Afbeelding 1: Een eerste digitaal veiligheidsbeeld A'dam: de belangrijkste risico's.



[1] NSCS: het Nationaal Cyber Security Center

Ambities

Amsterdam wil digitaal een veilige digitale stad zijn
Digitaal veilig zijn betekent weerbaar zijn tegen 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 digitaal opgeslagen informatie of schade aan de integriteit van die informatie. Digitale veiligheid is relevant voor de hele Amsterdamse samenleving.

Bijvoorbeeld; 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 aangeboden. Door de toenemende digitalisering en nieuwe technologie wordt digitale veiligheid steeds belangrijker voor Amsterdamse burgers, ondernemers en bezoekers.

Aansluiting op de Nederlandse Cybersecurity Agenda
In het huidige regeerakkoord is een structurele investering van 95 miljoen euro in cybersecurity vastgelegd. Het ministerie van Justitie en Veiligheid heeft vanuit de Nationaal Coördinator Terrorismebestrijding en Veiligheid een landelijke agenda voor digitale veiligheid opgesteld. Deze valt uiteen in de onderstaande zeven ambities waarin men de doelstelling heeft om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en daarmee de veiligheid in het digitale domein te beschermen:

1. Nederland heeft zijn digitale slagkracht op orde;
2. Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein;
3. Nederland loopt voorop in het bevorderen van digitaal veilige hard- en software;
4. Nederland beschikt over weerbare digitale processen en een robuuste infrastructuur;
5. Nederland werpt door middel van cybersecurity succesvol barrières op tegen cybercrime;
6. Nederland is toonaangevend op het gebied van cybersecurity kennisontwikkeling;
7. Nederland beschikt over een integrale, publiek-private aanpak van cybersecurity.

De vertaling van deze ambities van landelijk naar lokaal niveau betekent dat er elementen uit de landelijke agenda en onderliggende publiek en private samenwerkingen, kennis, expertise en structuren tot informatiedeling/posities hergebruikt kunnen worden.

Hoe veilig zijn we op de Safe Cities Index?
In de veiligheidsindex[2] van The Economist, waar 60 wereldsteden op een 4-tal veiligheidsonderdelen worden beoordeeld, scoort Amsterdam op de benchmark digitale veiligheid zeer hoog. Met maar liefst 89,0 punten volgt Amsterdam steden als Tokio, Chicago, New York, Londen en Toronto vanaf positie 14. De totale veiligheidsindex vergelijkt de waarden op de volgende veiligheidsdomeinen:

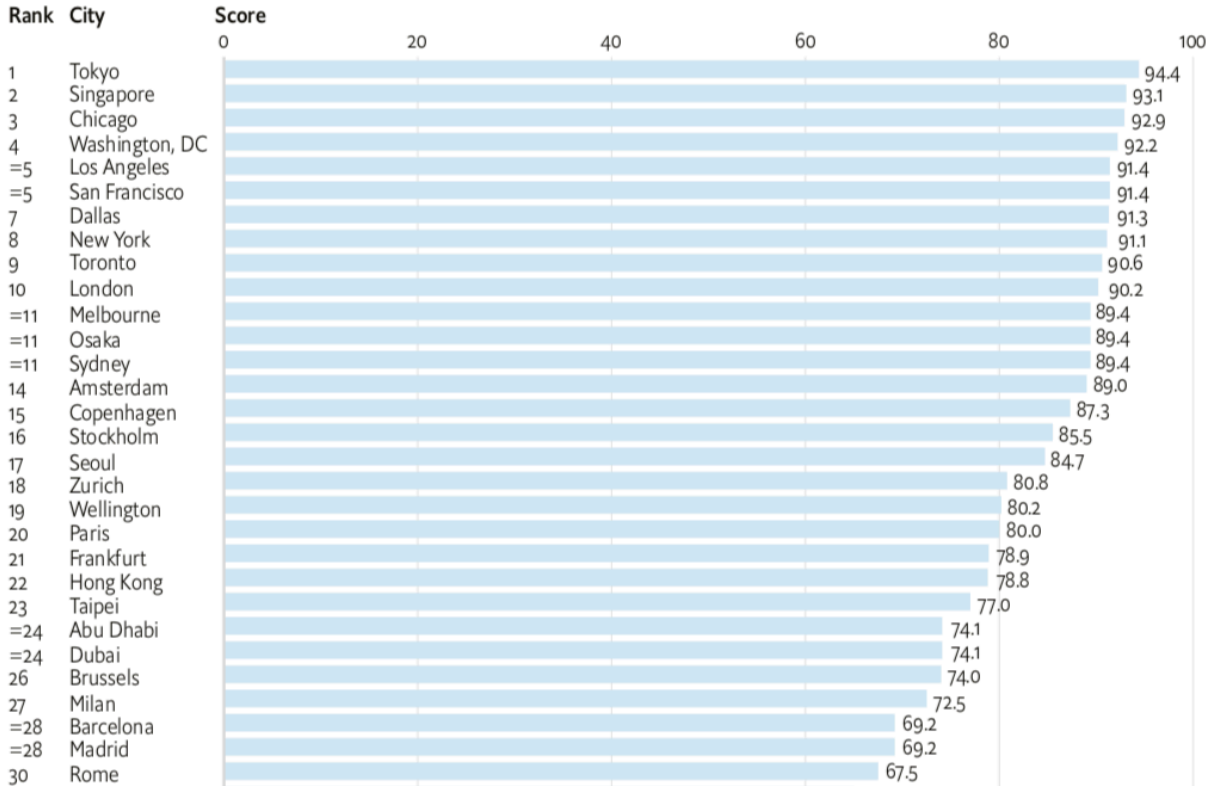
1. **Digitaal** (o.a. aanwezigheid van beleid op privacy, ethiek en publiek- en private samenwerking);
2. **Infrastructureel** (o.a. voetgangersvriendelijkheid, veiligheid voor transport en ook aanwezigheid van crisis- en incidentmanagement);
3. **Zorg** (o.a. aanwezigheid van beleid op duurzaamheid, toegang tot de zorg en de aanwezigheid van ziekenhuizen en doctoren);
4. **Individueel, de burger** (o.a. datagedreven werken, sociale controle, aanwezigheid van politie, publiek- en private samenwerking).

[2] Safe Cities Index 2019: *'Urban security and resilience in an interconnected world'*. Onderzoek door The Economist en NEC naar de integrale veiligheid van 60 wereldsteden op het gebied van veiligheid: persoonlijke, gezondheidszorg, infrastructurele en digitale veiligheid. Download voor meer informatie het complete rapport via de website https://safecities.economist.com.

Berekend over het totale gemiddelde van de 4 domeinen staat Amsterdam vanuit Europa gezien op positie 2. Deze positie daalt echter zodra steden buiten Europa worden betrokken naar positie 14. Het feit dat meer dan 50% van de onderzochte steden matig tot zeer slecht scoort geeft aan dat Amsterdam een voorbeeld is voor andere steden. Dit komt mede doordat wij als stad goed gebruik maken van wet- en regelgeving, de inzet van middelen en digitalisering goed onderzoeken evenals publiek private samenwerking op elkaar afstemmen.

Wanneer je steden rangschikt op een maximaal aantal inwoners per stad dan scoort Amsterdam de eerste plek. In steden tot 5 miljoen inwoners met een gemiddelde index van 75,9 staat Amsterdam bovenaan met 88,0. Echter is dit in een digitaal tijdperk met razendsnelle ontwikkelingen geen reden tot achterover leunen en de ruimte bieden dat kwetsbaarheden worden benut tot verstoring van de digitale stad.

Afbeelding 2: Safe Cities Index, getoond 30 van de 60 steden op algehele veiligheid met een gemiddelde van 67,2.



Hoewel dit een index is, creëert dit een referentiekader waaruit je kunt opmaken dat meer dan de helft van de onderzochte steden matig tot slecht scoort op digitale veiligheid. De urgentie om juist vanwege de snelle ontwikkelingen in het digitale domein te werken aan de weerbaarheid op lange termijn wordt in de veiligheidsindex ook omschreven als het lopen van een marathon en niet als een sprint. Overwogen acties om plannen, processen en middelen in te zetten op digitale veiligheid zal leiden tot een duurzame weerbaarheid van de digitale stad in tegenstelling tot snelle reparatie van digitale kwetsbaarheden.

Door elkaar scherp te houden, kennis te blijven ontwikkelen, te testen en te delen met andere steden werken we middels deze agenda toe aan de ambitie om de koplopers functie in digitale veiligheid te behouden.

Amsterdam werkt samen met andere steden
Amsterdam werkt samen met andere (grote) steden op digitale veiligheid en hierin middels het delen van kennis, expertise en innovatieve proeflabs van elkaar te leren. Een greep uit de ambities, acties en programma's op het gebied van digitale veiligheid bij de overige grote gemeenten in Nederland.

Gemeente Den Haag
- Ambieert voortrekkersrol op cybersecurity met organisaties zoals de HSD (the Hague Security Delta);
- Amsterdam gaat partnership aan met de HSD per 2020;
- 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 het tegengaan van grootschalige cybercrime niet als een taak voor de gemeente;
- Wil crisisorganisatie optimaal voorbereid hebben op cyberaanvallen op vitale infrastructuur.

Gemeente Rotterdam
- 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 cyberveiligheidsbeeld.

Gemeente 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 handelingsperspectief worden opgesteld;
- Meer inzicht verkrijgen in wie daders en slachtoffers van cybercriminaliteit zijn en meldingsbereidheid verhogen;
- Vergroten van de bewustwording over digitale risico's;
- Optimaal voorbereiden op cybercrises.

Gemeente Eindhoven
- Werkt aan digitale veiligheid middels een nota 'Digitalisering van de stad';
- Is aangesloten bij een landelijk samenwerkingsinitiatief genaamd City Deal. Bundeling van kennis en expertise met het Rijk en kennisinstellingen op het gebied van digitalisering en cybersecurity;
- Recente lancering van een cyberweerbaarheidscentrum op de Brainport Industries Campus door staatssecretaris Mona Keijzer.

Gemeente Almere
- Werkt onder het mom van 'digitaliseren met verstand' aan verbeteren digitale dienstverlening aan inwoners en ondernemers. Gebruikt data voor efficiënter werken, zet in op goede beveiligen gegevens die de gemeente heeft. Daar waar nodig wordt informatie gekoppeld, ook met partners. Voldoen aan privacyrichtlijnen is hierbij de grote opgave;
- Samen met Amsterdam, Politie en anderen trekker van een digitale vertrouwensinfrastructuur voor het veilig en verantwoord (privacy, security) uitwisselen van (persoonlijke) gegevens.

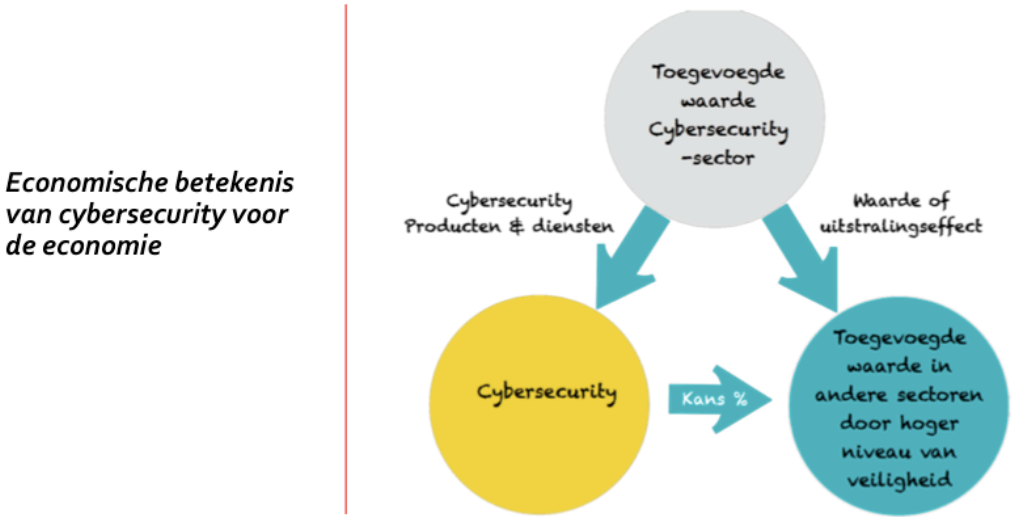
Koppositie in digitale veiligheid
Een opportuniteit en stimulans voor de technische en cybersecurity sector in Nederland als geheel. Nederland staat op veel ranglijsten al hoog, als het gaat om de mate van digitalisering van de economie.

Onderzoek door een bureau[3] onder 4.000 Nederlandse bedrijven wijst uit dat cyberscecurity als sector ook veel sneller groeit dan de IT-sector zelf. Inherent aan de digitaliseringsslag creëert men op hetzelfde moment een grote afhankelijkheid van een betrouwbare en veilige technologische infrastructuur. Uit het onderzoek komt ook de volgende analyse gemaakt van de sterkten, zwakten, kansen en bedreigingen van de Nederlandse cybersecurity-sector.

Sterkten	***Zwakten***
• Verregaande digitalisering geeft relatief sterke/volwassen (systeem van bedrijven) in cybersecurity-sector • Goede reputatie • Politiek, neutrale wet- en regelgeving, toezicht • Goede samenwerking binnen ISAC's en met NCSC • Goed informaticaonderzoek • Ligging, cultuur en ondernemersklimaat • Ligging, cultuur en ondernemersklimaat	• Onvoldoende specialisten/beschikbaarheid goed gekwalificeerde mensen • Investeringen en toegang tot (durf) kapitaal • Uitwisseling en samenwerking wetenschap, bedrijfsleven en overheid • Beperkt georganiseerde sector • Nederland vooral diensten en groothandel minder schaalbaar
Kansen	***Bedreigingen***
• Doorontwikkeling van de Nederlandse cybersecurity aanpak • Wetgeving • Betere uitwisseling bedrijfsleven-wetenschap • Groei awareness • Ontwikkeling domeinen	• Beschikbaarheid goed gekwalificeerde mensen • De thuismarkt is klein • Wetgeving • Kosten van beveiliging worden te hoog waardoor deze niet meer opwegen tegen de voordelen van gebruik digitale middelen. Met name voor MKB • Daling awareness • Kennis bij afnemers • Concurrentie van buitenlandse partijen en/of overnames

Met een omzet van 7,5 miljard euro hebben bedrijven die cyberactiviteiten uitvoeren met ongeveer 0,4 procent bijgedragen aan het Nederlandse Bruto Binnenlands Product. De benaderde bedrijven in het onderzoek verwachten een jaarlijkse groei van omzet (uit cybersecurity-activiteiten) van ongeveer 7%.

Afbeelding 3: Economische betekenis van cybersecurity voor de economie



[3] Economische kansen Nederlandse Cybersecurity-sector. Een verkenning. (Verdonck, Klooster & Associates, 2016)

Scope van de agenda

De gemeente Amsterdam staat voor de waarden en rechten in onze samenleving. Amsterdam neemt verantwoordelijkheid voor kwetsbare groepen en individuen in onze samenleving. Naast de fysieke omgeving bestaat er ook een digitale omgeving die van invloed is op de gemeentelijke werkelijkheid. De digitale wereld plaatst de samenleving, waaronder de gemeente Amsterdam, voor uitdagingen waarbij het van belang is om de waarden en rechten te garanderen en kwetsbaren (groepen) te beschermen.

Het beschermen van waarden en grondrechten in het digitale domein is belangrijk. Burgers moeten er op kunnen rekenen dat hun grondrechten zowel online als offline gewaarborgd zijn en dat hun privacy ook in het digitale domein gegarandeerd is. Amsterdammers moeten vertrouwen kunnen hebben in de digitale samenleving. Hiervoor hebben zij voldoende digitale vaardigheden nodig. Wat voldoende is zal mogelijk per persoon verschillen, van jong tot oud, van laag tot hoog opgeleid etc. Niet iedereen zal in gelijke mate de digitale wereld gaan begrijpen en of er direct in kunnen participeren. Vertrouwen in de digitalisering, de digitale componenten van de samenleving, is dan ook een belangrijke voorwaarde. Dit raakt ook aan het belang van het genereren en behouden van vertrouwen in de overheid. Helderheid krijgen ten aanzien van de overheid is binnen deze digitale context van de samenleving een strategische vraag uit het programma. Uit onderzoek blijkt dat afgerond 97% van de Nederlandse bevolking inmiddels online is. Nederland behoort daarmee tot de digitale voorhoede binnen Europa inclusief bijkomende economische en maatschappelijke kansen. Bij het efficiënter en effectiever benutten van deze kansen is meer aandacht voor cyber-security inherent. Zoals gezegd zal de Amsterdammer vertrouwen moeten hebben in onze informatie en informatiesystemen, waarbij men in de toekomst ook kan terugvallen op een overheid die voor jouw digitale identiteit klaarstaat.

Om dit vertrouwen te kunnen behouden werken we middels dit programma aan de ambitie om de stad Amsterdam digitaal een van de meest veilige steden te laten zijn. Dit doen we door de 6 thema's in de scope van het programma te plaatsen. De afbakening op onderwerpen en focus ligt daar *waar het digitaal blijft*. Hiermee wordt middels een voorbeeld gedoeld op dat bijvoorbeeld 'het verhandelen op (illegale) online markplaatsen' als ondermijnend gedrag buiten scope valt, maar dat 'online pesten' binnen scope en het digitaal weerbaar maken van burgers valt. Per thema kan de aanpak en kunnen de benoemde acties om tot realisatie te komen van elkaar verschillen.

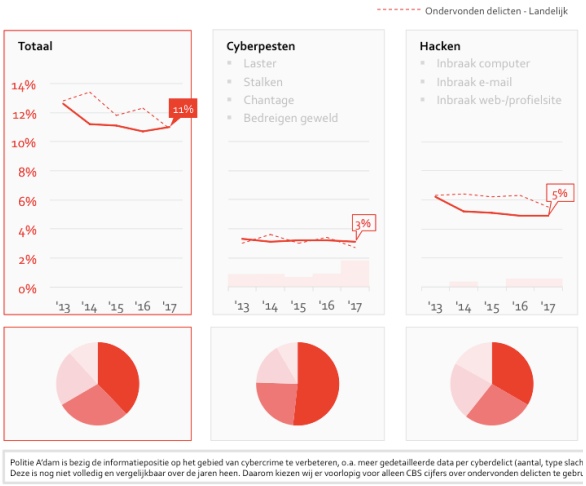
Afbeelding 4: Schematisch overzicht van de scope van de agenda Digitale Veiligheid

In de volgende hoofdstukken staan de uitwerkingen per thema nader beschreven, waarbij thematisch aangegeven is en naarmate het programma vordert, ondervonden zal moeten worden hoe en tot waar de rol van de (lokale) overheid reikt.

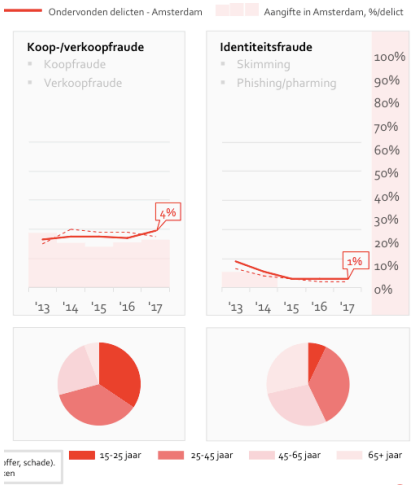
Individueel welzijn van de burger

Jaarlijks is ongeveer 11% van de Amsterdammers slachtoffer van cybercriminaliteit. Over de jaren 2013 tot en met 2017 is er een lichte daling waar te nemen in het percentage slachtoffers van cybercrime. Dit kan te maken hebben met de toenemende weerbaarheid als gevolg van voorlichtingscampagnes maar ook de lagere bereidheid tot melden.

Cyberpesten is één van de vier geïnventariseerde dreigingen en onderdeel van cybercriminaliteit, wat voornamelijk onder jongeren voorkomt. Laster en chantage vormen de grootste dreigingen binnen cyberpesten. Hoewel cyberpesten in het algemeen licht afneemt in de afgelopen jaren, neemt slachtofferschap op chantage juist toe. Samen met laster zijn dit de grootste twee dreigingen. Voornamelijk onder jongeren tussen de 15 en 25 jaar. Veel van de kennismaking met seksualiteit speelt zich online af. Hierdoor is er een toename van misbruik in onder andere het delen van naaktfoto's en –filmpjes.



Het aantal slachtoffers van hacken is de afgelopen jaren dus licht gedaald, uit cijfers van het CBS blijkt dat dit percentage rond de 5% ligt. Onder hacken wordt onder andere verstaan 'het inbreken op een computer, e-mailaccounts en web- en profielsites'. Er is echter wel een toenemend risico op hacken door de toename van (slecht beveiligde) Internet of Things verbindingen: er worden steeds meer apparaten gebruikt die op het internet zijn aangesloten.



De digitale weerbaarheid van burgers staat onder druk door een toenemende complexiteit en connectiviteit van het ICT-landschap, weinig aandacht voor digitale veiligheid en het feit dat slachtofferschap vaak niet opgemerkt wordt als het bijvoorbeeld gaat om hacken en phishing. Daarnaast kan cyberpesten significante welzijnsschade tot gevolg hebben. Vanuit overheid en op scholen is hier al veel aandacht voor, door het stimuleren van digitale bewustwording en het opbouwen van digitale vaardigheden. Cybercriminaliteit is lastig aan te pakken, doordat er weinig melding wordt gemaakt en aangifte gedaan. Ook vervolging is lastig: slechts 1,4% van de politieregistraties leidt uiteindelijk tot strafvervolging. Burgers worden niet of nauwelijks gestimuleerd om incidenten te melden. Men heeft het gevoel dat dit geen zin heeft.

Jeugd weerbaar maken

Omdat digitale veiligheid en de online weerbaarheid een gemeenschappelijke verantwoordelijkheid betreft, zal de gemeente ruimte en een platform moeten bieden voor initiatieven waarbij de jonge Amsterdammer handvatten geboden worden om de bewustwording van de digitale dreiging te verhogen. De stichting Cyberschool, opgericht door cyberspecialisten in samenwerking met de DNB en het Ministerie van Defensie, ontwikkelt een landelijk leerprogramma. Dit programma richt zich middels vrijwilligers op leerlingen, ouders en docenten. Op basis van een interactief lespakket, gebaseerd op praktijkervaringen van ethische hackers en cybersecurityspecialisten, maken zij als stichting de jeugd weerbaar tegen de digitale dreigingen.

Vanuit de agenda zal in nauwe samenwerking met de diensten binnen het cluster Sociaal gekeken moeten worden naar de mogelijkheden om lokaal nog meer samenwerkingen en initiatieven te stimuleren om de voornaamste dreigingen te proberen te verweren. Onder andere het initiatief van de Johan Cruijff Arena en stadsdeel Zuidoost om een smart city school op te richten past hierin.

Onderzoek, Informatie & Statistiek (OI&S)
Namens de gemeente Amsterdam kan IOS als directie een eenduidige informatiepositie innemen door publicaties over digitale veiligheid te verzorgen op basis van de volgende elementen:

- Veiligheidsmonitor (vragenlijst aan bewoners): opnemen vragen slachtofferschap cybercriminaliteit monitoren (hacken, cyberpesten, koop- en verkoopfraude en identiteitsfraude);
- Data Politie, OM en OOV over cybercriminaliteit;
- Index m.b.t. cybercriminaliteit naar relevante dimensies (bijv. leeftijdsgroepen, SES, opleiding);
- Criminaliteitsbeeld (rapportage met statistieken criminaliteit): toevoegen cybercriminaliteit;
- Veiligheidsbeeld Amsterdam: kwalitatief maar zoveel mogelijk onderbouwd met statistieken en eventueel externe databronnen;
- Opzetten van een panel waarin ontwikkelingen/impact van interventies op digitale veiligheid gemeten kan worden.

Informatiepositie op basis van bestaande bronnen
Om het veiligheidsbeeld cijfermatig te staven zal Onderzoek Informatie & Statistiek (OIS) de Veiligheidsmonitor als instrument inzetten. Hierin wordt naast de fysieke veiligheid in de stad ook de digitale veiligheid van Amsterdammers weergegeven. Dit betreft cijfers van de stand van zaken hoe het er op dit moment voor staat. Aan deze monitor worden cijfers gekoppeld uit landelijke beelden zoals het *CSBN (2019) van de NCTV*[4] of het *CBS onderzoek Digitale Veiligheid, Criminaliteit (2019)* en het *cyber intelbeeld van de Politie*. De (Amsterdamse) monitor kan vervolgens elk jaar opnieuw worden uitgebracht, met aanvulling van de meest recente cijfers en inzichten.

Subjectief
OIS kan voor deze nieuwe digitale monitor gebruik maken van de resultaten uit vier bestaande monitoren van OIS: Veiligheidsmonitor Amsterdam-Amstelland, Staat van de Stad, Burgermonitor en de Monitor Detailhandel. De Veiligheidsmonitor Amsterdam-Amstelland wordt drie keer per jaar uitgevoerd, de andere monitoren worden één keer in de twee jaar uitgevoerd. In de monitoren wordt aan de ene kant gevraagd naar middelen en toepassingen (in hoeverre gebruiken Amsterdammers sociale media, doen zijn aankopen via het web) en aan de andere kant naar online slachtofferschap (cyberpesten, identiteitsfraude, koop- en verkoopfraude en hacken). Ook wordt er gevraagd naar digitale veiligheid en het vertrouwen in de overheid.

Objectief
Daarnaast zal OIS (net als in de Cybersecurity monitor van het CBS) registraties, meldingen en aangiftes van de politie toevoegen aan de monitor. Het gaat hierbij om delicten die een digitale component in zich hebben. Hierdoor ontstaat in de monitor zowel een subjectieve als objectief beeld van digitale veiligheid en het welzijn van burgers.

Eenmalig uitgevoerd onderzoek
In 2017 is een onderzoek gedaan naar de veiligheidsperceptie van inwoners van de veiligheidsregio Amsterdam-Amstelland. Het ging hierbij niet alleen om digitale veiligheid, maar ook om fysieke vormen van veiligheid. De resultaten zullen daar waar relevant gebruikt worden in de (eerste uitgave van) de monitor. Indien gewenst kan, als vervolg op de eerste monitor, dit onderzoek herhaald worden.

[4] CSBN: Cyber Securitybeeld Nederland van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)

Informatiepositie op basis van nieuwe bronnen
Ten slotte kan OIS een vragenlijst opstellen over de digitale vaardigheden van burgers en deze één keer per jaar uitsturen in het Stadspanel, eventueel aangevuld met schriftelijke enquêtes. Voor het onderzoek kan inspiratie worden gehaald uit het landelijk onderzoek van het CBS over ICT-gebruik van huishoudens. Daarin wordt gevraagd naar ICT-voorzieningen, internetgebruik, activiteiten op het internet, ICT-vaardigheden en het wel of niet gebruiken van beveiligingssoftware. Dit zou aangevuld kunnen worden met vragen over de aanwezigheid van verbonden Internet of Things apparaten in het huishouden, zoals slimme televisies en koelkasten met WiFi.
Daarnaast is het goed te vermelden dat OIS op dit moment bezig is met een verkenning van digitale weerbaarheid van jongeren op het gebied van *'shame sexting'* en online pesten (waaronder bedreiging en intimidatie). Het doel van dit onderzoek is in kaart te brengen wat er al over deze onderwerpen bekend is en welke kennis eventueel nog ontbreekt, met specifieke aandacht voor mogelijk kwetsbare groepen.

Gegevens uit (externe) databronnen
Daar waar het wet- en regelgeving technisch mogelijk is kan OIS op basis van databestanden het gebruik van digitale applicaties/diensten (zoals *Mijn Amsterdam* en *DigiD*) meenemen in de monitor.

Rapportage
Daar waar mogelijk worden de gegevens van meerdere jaren vergeleken en wordt gekeken naar de trends als het gaat om de subjectieve beleving van digitale veiligheid. Daarnaast zullen er uitsplitsingen worden gemaakt op bepaalde achtergrondkenmerken. Te denken valt aan leeftijd, geslacht en opleidingsniveau. Ook kan hierbij slachtofferschap van cybercriminaliteit worden afgezet tegen slachtofferschap op vormen van traditionele criminaliteit.

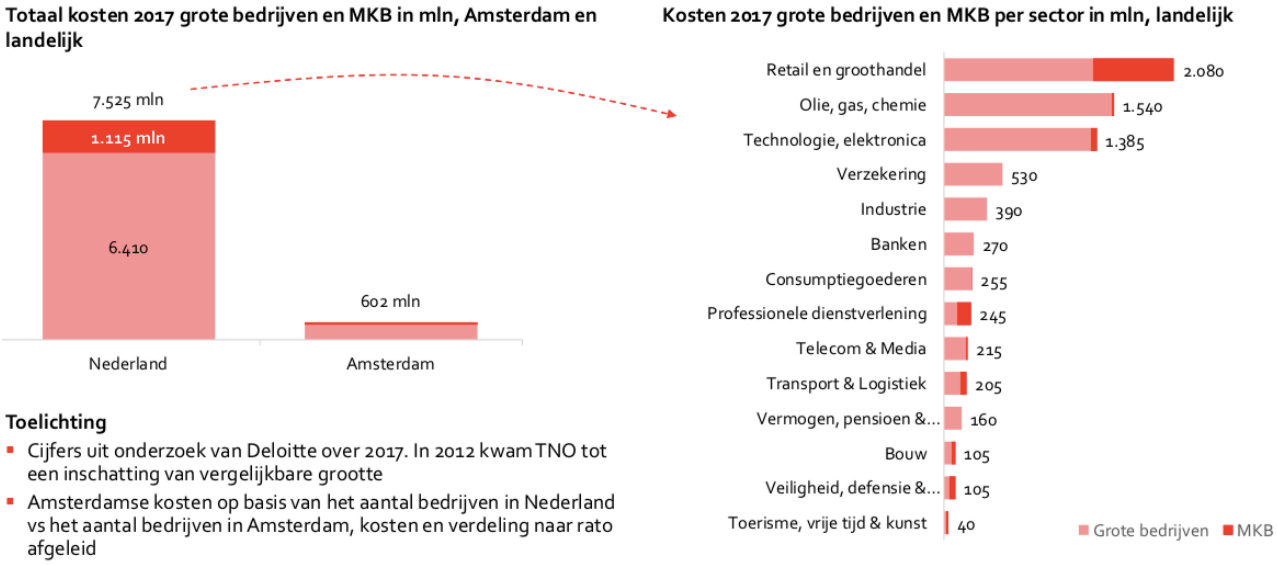
Private organisaties en maatschappelijke instellingen

In relatie tot het opgestelde veiligheidsbeeld voor Amsterdam zien we op dit thema dat cyberaanvallen vooral op (de grote) private organisaties binnen de financiële sector gericht zijn.
Per branche zijn CERT's[5] en ISAC's[6] ingericht. Hierin wordt informatie gedeeld over risico's, kwetsbaarheden en of aanvallen. De financiële sector heeft zijn digitale beveiliging over het algemeen beter geregeld dan andere sectoren. Landelijk speelt er de ontwikkeling dat zogeheten Digitale Trust Centers (DTC's[7]) worden opgericht, een informatievoorzienig waar het MKB zich voor aan kan melden.

Via gemeentelijke netwerkpartners zoals VNO-NCW en de ORAM zou de gemeente signalen en meldingen (over aanvallen, datalekken etc.) door kunnen krijgen vanuit de private organisaties en maatschappelijke instellingen, maar in de praktijk gebeurt dit nu nog niet. Ditzelfde geldt bij aanvallen waarbij ontvreemding van data van grote bedrijven heeft plaatsgevonden. Het wordt conform de wet wel gemeld (meldplicht datalekken), maar bedrijven doen nog niet in alle gevallen aangifte bij de politie en of gemeente.

Met betrekking tot het midden en kleinbedrijf zal er op basis van het lokaal veiligheidsbeeld (zie onderstaande afbeelding) met name gewerkt moeten worden aan de bewustwording over de risico's en mogelijke vormen van cybercrime en digitale veiligheid. De economische schade bedraagt voor Amsterdam ruim 602 miljoen euro op jaarbasis.

Afbeelding 5: Overzicht economische schade in het bedrijfsleven door cybercrime



De onderstaande 8 acties worden lokaal gepland om private organisaties en maatschappelijke instellingen meer weerbaar te maken op digitale veiligheid. Dit betreft acties tot het bijvoorbeeld informeren, verbinden, stimuleren en opzetten van netwerkstructuren:

[5] CERT: Computer Emergency Response Team zijn functiegerichte organisaties binnen (grote) bedrijven of rijksoverheid waarin deskundigen op het gebied van computer- en netwerkbeveiliging de afhandeling van (ernstige) beveiligingsincidenten coördineert en bewaakt.
[6] ISAC: Information Sharing and Analysis Centre. Een sectoraal overleg tussen organisaties uit dezelfde sector om gevoelige en vertrouwelijke informatie over incidenten, dreigingen, kwetsbaarheden, maatregelen en leerpunten op het gebied van cybersecurity te delen.
[7] DTC: Digital Trust Center. Het knooppunt voor informatievoorziening van het MKB (met circa 1.6 miljoen leden) eenduidige en herkenbare informatie krijgen over digitale weerbaarheid.

1. Bevorderen kennisontwikkeling lokale professionals en vergroten awareness
Door het Platform Veilig Ondernemen worden evenementen georganiseerd, zoals in de *Week van de Veiligheid* gericht op het bevorderen van kennisontwikkeling en het vergroten van bewustzijn, o.a. over cybercrime.

2. Gebiedsgerichte benadering van ondernemers met een campagneteam
Gedurende het najaar en de winter (gewenste start in oktober) worden in de stadsdelen en de Amstelland gemeenten gebieden bezocht waar de onveiligheid hoog is door een campagneteam in samenwerking met lokale professionals. Hierbij wordt gewerkt met een individuele benadering van ondernemers. De thema's waarover de ondernemers worden benaderd, worden vastgesteld op basis van de veiligheidscijfers en de input vanuit het lokale netwerk. Waar relevant, zal er ook informatie worden verstrekt over digitale veiligheid.

3. Toolbox Platform Veilig Ondernemen (PVO)
Een toolbox met een overzicht aan trainingen, workshops en tools om veilig ondernemen te bevorderen. In deze toolbox staat ook een aantal trainingen en workshops opgenomen i.h.k.v. cybercrime. De toolbox is een digitaal document met links dat vanuit de lokale professionals verspreid kan worden aan ondernemers. Het aanbod van de toolbox komt ook op de website van het PVO te staan (website is in ontwikkeling).

4. Informatiebox veilig ondernemen
Er wordt een informatiebox ontwikkeld die door de lokale professionals kan worden tijdens bijeenkomsten met en bezoeken aan ondernemers. In deze box zit informatie over veilig ondernemen, waaronder een webcam cover en een flyer of sticker over tegengaan cybercrime.

5. Onderzoek phishing: de MKB phishing test
Op initiatief van het Regionaal Platform Criminaliteitsbeheersing (RPC) Noord-Holland (zoals aangegeven zijn zij eigenlijk ook een PVO alleen zij wilden de naam RPC behouden) wordt een phishing test uitgevoerd bij het MKB. Wij ondersteunen dit initiatief van het RPC NH door de informatie over de phishing test uit te laten delen tijdens contactmomenten met lokale ondernemers. De ondernemer die de test heeft laten uitvoeren, krijgt een rapportage die inzicht geeft in de weerbaarheid van de onderneming tegen een phishing aanval en de medewerkers leren phishing e-mails beter te herkennen.

6. Verbeteren proces aangifte na cyber incident
Er lijkt nog maar weinig aangifte te worden gedaan over cyber incidenten. Mogelijk heeft dit er mee te maken dat men zich schaamt er 'toch in te zijn getrapt', men niet weet welke stappen er moeten worden ondernomen om aangifte te doen en/of men niet de juiste informatie kan verstrekken om aangifte te doen. We werken aan een handige flyer of een sticker (nog te bepalen) om ondernemers informatie te verstrekken met 10 tips wat men moet doen na een cyber incident. Dit wordt meegenomen in acties 2 t/m 4. Ook is er tegenwoordig in de politie eenheid Amsterdam een digitaal aangifteformulier beschikbaar dat het doen van aangifte makkelijker maakt. Dit formulier wordt echter nog niet op landelijk niveau door de politie eenheden gebruikt.

7. Digital Trust Center
Eén van de speerpunten welke voortkomen uit de prioriteiten van de landelijke Cybersecurity Agenda (CSA) waarin het MKB op dit platform terecht kan voor eenduidige informatie over digitale veiligheid. Op dit moment telt het DTC zo'n circa 1.6 miljoen leden. Vanuit het DTC worden diverse samenwerkingsverbanden en producten ontwikkeld om het MKB weerbaarder te maken tegen cybercrime. Onder meer wordt met de politie gebouwd aan een voorziening voor actuele en eenduidige informatie over cyberdreigingen voor burgers en MKB.

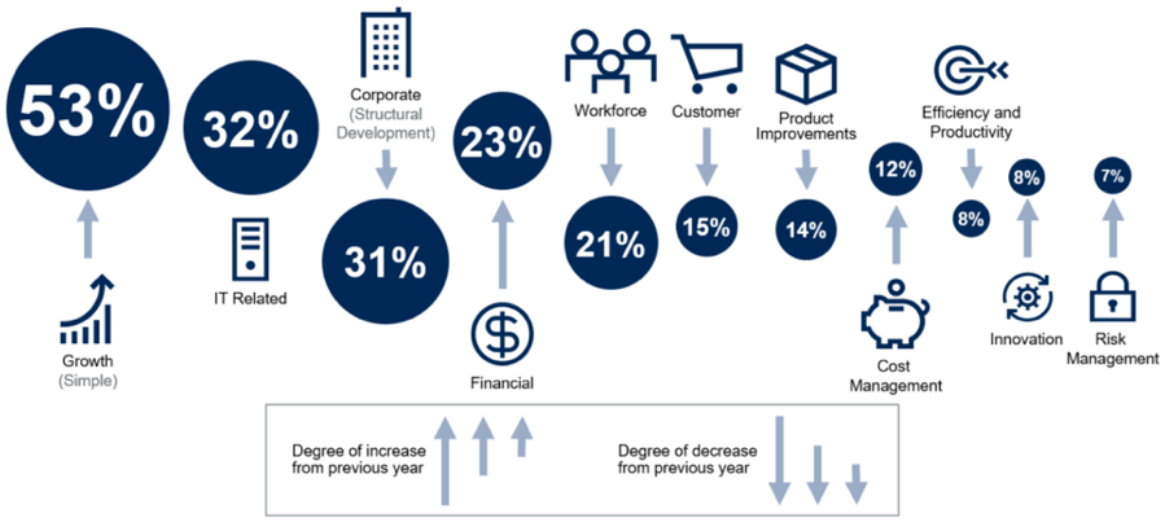
Vitale infrastructuur

De context
De toepassing van digitale technologie in een groeiend aantal diensten, verhoogt het comfort en gemak voor de *bewoner*, *ondernemer* en de *bezoeker* ('B.O.B.') van de stad. Dank zij de technologie ontstaan nieuwe mogelijkheden, bijvoorbeeld 'Mobility As A Service', waarmee de verkeersdrukte in de stad kan afnemen en er openbare ruimte vrijkomt voor ander gebruik. Technologie kan bijdragen aan een grotere veiligheid in en leefbaarheid van de stad. Dit kan tegen een lagere kostprijs en een hogere kwaliteit van de diensten die publieksdiensten en gemeente bieden. Voor het verzamelen en transporteren van data voor digitale diensten is een goed beschikbare, veilige en robuuste digitale infrastructuur nodig van digitale apparaten, frequenties, kabels, zenders en ontvangers. Deze infrastructuur is verweven met allerlei processen in organisaties, de privé omgeving, de overheidsdiensten en de openbare ruimte.

Met robuuste digitale diensten die de veiligheid, leefbaarheid en het comfort en gemak vergroten voor de BOB zijn we als stad een economisch aantrekkelijke vestigingsplaats voor allerlei organisaties. De technologische ontwikkelingen versnellen in een hoog tempo. Dat bijhouden is noodzaak. Technologie kan het leven en verblijven in de stad veraangenamen. Het geeft Amsterdam internationaal een extra 'competitive edge'. Het heeft echter ook een keerzijde.

Uitval van de digitale infrastructuur en de bijhorende digitale diensten en processen kan leiden tot ernstige ongeregeldheden en tot economische- en politieke schade. Daar zijn diverse kleine en grotere voorbeelden van in Nederland en daarbuiten. Neem recente voorbeelden zoals het ongemak voor burgers en veiligheidsdiensten bij het uitvallen van 112, de Albert Heijns die niet opengingen doordat de kassa's niet werkten. Maar ook grootschalige datalekken zoals de gegevens van 500 miljoen gasten van de Marriot Hotel Group[8] die 'op straat lagen' en de 'ransomware', waarmee criminelen de digitale omgeving in bezit nemen en pas prijs geven na betaling. Zoals bijvoorbeeld bij de gemeente River Beach in Florida die ruim een half miljoen betaalde voor de sleutel om alle bestanden van de gemeente weer toegankelijk te maken[9]. Dat gebeurt bij de overheid, personen (bijvoorbeeld artsen), kleine en grote organisaties. Ook steden en landen worden aangevallen.

Afbeelding 6: Business Priorities, percentage of the top 11 respondents (Gartner mei 2019)



[8] https://www.volkskrant.nl/nieuws-achtergrond/op-een-na-grootste-datalek-ooit-treft-500-miljoen-gasten-van-marriott-hotel-group-ook-creditcardnummers-buitgemaakt~b20fb2e3/
[9] https://www.ad.nl/tech/amerikaanse-stad-betaalt-ruim-half-miljoen-euro-losgeld-na-aanval-met-gijzelsoftware~a68d83ea/

Internationaal is de veiligheid van de digitale infrastructuur een belangrijk issue. In veel enquêtes bij managers, CTO's en CIO's komt cybersecurity terug in de top 3[10]. In Gartner's survey van 2019 komt naar voren dat innovation en riskmanagement issues zijn waar CEO's steeds meer geld aan besteden.

Conclusie
Door de toenemende afhankelijkheid van de digitale diensten hebben we te maken met een nieuwe kwetsbaarheid. Of de uitval van de infrastructuur die kritieke processen ondersteunen nu bedoeld of onbedoeld is, als deze infrastructuur uitvalt heeft dat gevolgen voor iedereen in de stad. Mogelijk voor de basis levensbehoeften, de bereikbaarheid en veiligheid van de stad. Het is daarom noodzakelijk te werken aan een robuuste digitale infrastructuur met robuuste digitale diensten en de bijhorende data, waarvan de continuïteit en de veiligheid zo goed mogelijk geregeld is, in organisaties en in de openbare ruimte. Dit is van economisch, maatschappelijk en politiek belang.

Wat er nodig is?
100% veiligheid bestaat niet; in de complexe digitale wereld al helemaal niet. De technologie ontwikkelt zich razendsnel; de risico's en de criminaliteit groeien mee. Het maatschappelijk belang van een veilige digitale omgeving is enorm. De veiligheid betreft het voorkomen van uitval van de vitale digitale infrastructuur en/of inbraak daarop. Nodig is een tijdige signalering van risico's en inbraakpogingen en het aanpakken van bedreigingen en calamiteiten. Dat vereist maatregelen, zowel technologisch als organisatorisch.
Omdat niet alles tegelijk kan, is het zaak te beginnen bij een waarborg voor de continuïteit en beschikbaarheid van de infrastructuur die noodzakelijk is voor de vitale processen, bijvoorbeeld de voorzieningen voor elektriciteit, water, gezondheid, voedsel en mobiliteit. Vraag is wat de vitale processen voor Amsterdam zijn en welke digitale infrastructuur voor deze diensten noodzakelijk is. Dan volgen de vragen welke risico's er zijn, wat de impact bij uitval kan zijn en hoe deze infrastructuur zo goed mogelijk te beveiligen is en te blijven beveiligen bij de zich verder ontwikkelende technologie. Daarbij is een continu actueel beeld van de risico's op uitval noodzakelijk om tijdige en effectieve besluiten te kunnen nemen ter voorkoming van calamiteiten.

Samenwerking is cruciaal
De invulling van die vragen kan de gemeente Amsterdam niet alleen. Samenwerken met organisaties voor de vitale diensten in de stad, de publieksdiensten, kennisorganisaties en eventuele andere organisaties, het delen van schaarse kennis op het gebied van technologie in het algemeen en van cybersecurity in het bijzonder, is noodzakelijk. Ook landelijk en internationaal. Daarnaast is het wenselijk de digitale weerbaarheid van Amsterdammers te vergroten. Immers, uitval gaat gebeuren. De technologie op zich is daarbij niet het enige noch het grootste risico. Ook de mens is een risicofactor door gebrek aan kennis, vaardigheid of attentie (bijv. slordigheid). Het is de vraag of iedereen zich bewust is van de grotere afhankelijkheid en de daarmee gepaard gaande grotere risico's voor de maatschappij.

Daarom gaan we binnen dit thema bepalen wat vitale processen zijn, welke digitale infrastructuur bij de vitale processen op lokaal niveau hoort en welke maatregelen we moeten treffen om de kans op uitval te verkleinen. De middelen die we in gaan zetten en nog gaan ontwikkelen, kunnen ambulance, politie en brandweer in onze stad helpen bij hun werkzaamheden. We kijken daarbij naar alle processen die we maatschappelijk vitaal achten voor Amsterdam. Gezien de onderlinge afhankelijkheid zetten we een samenwerking op met de vitale dienstverleners en kennisinstituten om het actuele risicobeeld te kunnen bepalen en te monitoren. Van andere steden welke net als wij ook zeer actief bezig zijn op dit onderwerp, gaan we leren. Een zeer belangrijk onderdeel, ter ondersteuning van een van de andere thema's binnen de scope is het weerbaarder maken van de bewoners en ondernemers. Dat er uitval en digitale criminaliteit is en zal blijven is een gegeven. We weten alleen niet wat, hoe, door wie en wanneer het zal gebeuren, wie het raakt en welke omvang en gevolgen het heeft.

[10] Cyber is een belangrijk investeringspunt in diverse landen, als gebleken tijdens Digital Government Exchange Singapore 2018 & DGX2019 (o.a. Estonia, Israël, Japan, Finland, Oostenrijk, Singapore, UK); GovConnect in Edinburg, 2019 (o.a. Maleisië, Schotland, UK, Vietnam).

Doelen thema Vitale Infrastructuur
Doelstellingen bij dit thema, de *Lokale Vitale Digitale Infrastructuur* (L-VDI):

1. Borgen van de beschikbaarheid en continuïteit van een veilige robuuste infrastructuur voor de vitale processen in de stad, inclusief een monitorsysteem voor een actueel risicobeeld en de mogelijkheid om aangepaste en nieuwe scenario's te simuleren in een digitale versie van Amsterdam (digitale twin);
2. Het realiseren van een menselijk netwerk en ondersteunende faciliteiten voor het delen en ontwikkelen van kennis in kleine kring van deskundigen op het gebied van digitale veiligheid, zodat deze elkaar kunnen helpen bij het voorkomen of bestrijden van digitale calamiteiten. Extra aandacht moet er zijn voor de vertrouwelijkheid zodat vitale dienstverleners bereid en in staat zijn gevoelige informatie uit te wisselen (in een kleine, bekende, vertrouwde groep);
3. Het verhogen van de cyberweerbaarheid (voorbereid zijn op een uitval van vitale systemen) van Amsterdam om cyber incidenten te voorkomen, te herkennen en er adequaat op te kunnen reageren zodat fysieke en economische schade voor burgers, ondernemers, bezoekers beperkt wordt. Dit kan in de fase van nazorg ook bijdragen aan het herstel van de burger in de politieke betrouwbaarheid.

Wij doen dit door preventie, detectie, response en recovery van digitale dreigingen procesmatig in te richten, samen te werken en een stadsbreed detectie netwerk te ontwikkelen. Een goede en goed blijvende cyberweerbaarheid vereist een structurele en langdurige samenwerking en gecoördineerde kennisuitwisseling in de gemeente tussen de diverse organisatie onderdelen (o.a. CIO, CTO, JZ, OOV) en met lokale, nationale en internationale partners zoals Alliander, Metro &Tram, politie (Amsterdam en landelijk), Port of Amsterdam, Schiphol, Waternet, KPN, Philips en kennisinstellingen als bijvoorbeeld AMS, HvA, UvA en de VU.

Voor de korte termijn gaan we:

1. binnen 6-12 maanden concretiseren:
   a) 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. Op basis van een convenant leggen we de samenwerking vast waarmee de kring waarin de vertrouwelijkheid geborgd is van de informatie die wordt gedeeld;
   b) wat de vitale digitale infrastructuur is en met welke methode of werkwijze die (te blijven) bepalen, wat de criteria zijn en wat de impact van uitval is;
   c) welke mogelijkheden er zijn om de vitale digitale infrastructuur te beschermen;
   d) wat we moeten doen en met wie om de vitale digitale infrastructuur in de openbare ruimte binnen een jaar zo veilig mogelijk te krijgen en daarna te houden. Onderdeel daarvan is de nationale digitale vertrouwensinfrastructuur (DVI) die samen met andere steden, VNG, BZK, politie, Veiligheidsregio en (kennis)organisaties gerealiseerd wordt;
   e) welke standaarden er zijn en welke activiteiten er lopen, landelijk en in EU-verband, 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 aan te sluiten.

2. Zorgen dat er uiterlijk 1 januari 2021:
   a) een crisisplan is waarin o.a.: wat te doen, door wie, waarmee in geval van een digitale calamiteit door uitval of criminaliteit. Dat plan is dan bij voorkeur tenminste één keer geoefend. Het bestaat uit onder meer noodscenario's en communicatie strategieën en middelen;
   b) een voorstel is voor de opzet en realisatie van een 'Joint Cyber Threat Detectie Network', bij voorkeur bewezen door een demonstratiemodel, en een 'Cyber Resilience Organisatie' (CRO)' (zie hierna, punt 2 en 4), dat wordt voorgelegd ter besluitvorming;
   c) een programma ontwikkeld is om de weerbaarheid van BOB te vergroten bij een calamiteit.

3. Zorgen dat er medio 2021:
   a) De vitale digitale infrastructuur bekend is, evenals de inrichting van de basis voorwaarden voor continuïteit en veiligheid. Dat doen we samen met de partners, veiligheids- en publieksdiensten en kennisinstellingen, nationaal en internationaal.

Crisis- en incidentmanagement (Openbare Orde & Veiligheid)

Digitale onveiligheid raakt het werkveld van het lokale veiligheidsdomein op vele fronten. De directie Openbare Orde en Veiligheid draagt daarbij zorg voor een integrale advisering binnen het kader van het programma Digitale Veiligheid. Enerzijds vanuit de crisis- en incidentbeheersing wanneer een digitale dreiging zich manifesteert waarbij de Amsterdamse openbare orde in het geding komt. Anderzijds vanuit het perspectief van enkele bestuurlijke prioriteiten waar digitale onveiligheid een grote impact kan hebben op personen, gebieden, branches etc.

Op basis van het Cyber Intelbeeld van de politie en een inventarisatie bij ketenpartners komen een aantal vormen van digitale criminaliteit sterk naar voren. We verkennen de komende tijd de mogelijke aanpak van de volgende vier speerpunten op het gebied van digitale veiligheid:

1) Amsterdammers, kwetsbare meiden, die het slachtoffer worden van digitale afpersing, bijvoorbeeld met seksueel getinte foto's of video's van jongeren (zogeheten 'sextortion');
2) Kwetsbare ondernemers die slachtoffer worden van hackers, ransomware, CEO fraude of andere vormen van social engineering met digitale middelen;
3) De aanpak van de digitale infrastructuur die ondermijnende activiteiten ondersteunt. Denk aan bijvoorbeeld *darkweb* marktplaatsen of online communicatieplatformen waarmee drugshandel wordt bedreven;
4) Resilient maken van de vitale digitale stedelijke infrastructuur. Voorbereiden op digitale dreigingen ten aanzien van de openbare orde die zich kunnen manifesteren in Amsterdam, bijvoorbeeld een gerichte cyberaanval op de transportinfrastructuur of het uitvallen van de energievoorziening of pinautomaten in de stad waardoor er geen transacties meer kunnen plaatsvinden in supermarkten.

Cybergevolgbestrijding (CGB)
In een memo van de VNG, Veiligheidsberaad en Regioburgemeesters[11] aan de lokale overheden, waar men onderzoek heeft gedaan naar de bestuurlijke aspecten ten aanzien van orde en veiligheid in het digitale domein kwam onder andere ter sprake dat veiligheidsregio's zoekende zijn naar hun rol bij digitale verstoringen. Binnen de veiligheidsregio's neemt de bewustwording toe dat de ontwikkelingen in het digitale domein (zoals digitale verstoringen en afhankelijkheid) om een bredere en wellicht aangepaste benadering van de risicoanalyse en vervolgprocessen vraagt.

Bij crisisbeheersing en incidentmanagement vraagt een cyberverstoring om de inrichting van een proces dat zich richt op het voorkomen van nieuwe risico (gevolgen) en het treffen van adequate maatregelen bij het optreden daarvan. De huidige processen richten zich echter meer op de fysieke risico's en aanleidingen tot verstoring(en).

Samen met de G4 en het Ministerie VenJ is er opdracht verstrekt aan adviesbureau Berenschot om een cybergevolgbestrijding (CGB) op te stellen. Hieronder worden alle activiteiten verstaan die worden ontplooid om de situatie te normaliseren nadat een digitale verstoring heeft plaatsgevonden. De focus ligt hierbij op de gevolgen van een digitale verstoring in het fysieke domein. Daarbij zal vrijwel altijd behoefte zijn aan een gedeeld beeld van de situatie en aan prioritering van de (capaciteits)inzet van de hulpdiensten en omringende gemeenten.

Om een rol hierin te kunnen spelen is informatie van groot belang voor veiligheidsregio's. Op basis hiervan kan de veiligheidsregio adequaat handelen, de bestuurder(s) kunnen adviseren en een handelingsperspectief richting de burgers communiceren. Hierin treden we in nauw overleg en samenwerking met landelijke partners alsmede lokale partners zoals de Amsterdamse eenheid van de politie alsmede het lokaal parket van het openbaar ministerie.

[11] Memo Samenwerking landelijke overleggen veiligheid Bestuurlijke aspecten digitale domein. Geschreven door de VNG, Regioburgemeesters en het Veiligheidsberaad (oktober 2018).

Democratie en bestuurlijke stabiliteit

Democratie is steeds afhankelijker van dat wat er in de digitale wereld gebeurt. Stemmen gebeurt steeds vaker online (denk in Amsterdam nu al aan het programma OpenStad, online participatietools) en bewoners baseren hun mening steeds meer op (alleen) online bronnen.

Digitalisering biedt een enorme kans om meer mensen op het juiste moment bij het democratische proces te betrekken. Het internet biedt de mogelijkheid om allerhande meningen en standpunten te verkondigen en bijna iedereen kan die informatie ongeacht het tijdstip of de locatie tot zich nemen.

Landelijk en Europees zien we allerhande overheidsinitiatieven die zogenoemd "Fake News" willen bestrijden. In Amsterdam gaan we niet bepalen wat goed en fout is. Wel willen we monitoren in hoeverre:

1. Er structureel door partijen bewust het nieuws wordt beïnvloed met propaganda of pulpnieuws;
2. Sommige Amsterdammers in hun eigen bubbels zitten en eenzijdig geïnformeerd worden;
3. Amsterdammers toegang hebben tot digitaal nieuws en hun weg daarin kunnen vinden.

In de analyse alsmede door de validatie met de experts komen we tot de volgende (onderliggende) uitdagingen en uitgangspunten:

- Een kwalitatieve en volledige informatievoorziening met een groot bereik en toegang tot de (verschillende) 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;
- In de Amsterdamse context omdat de grote Tech-bedrijven hier gevestigd zijn en een veel grotere stem hebben dan elders. Is hun fysieke aanwezigheid in de stad een (extra) dreiging?
- Publieke anonimiteit in de stad wordt een trend (signature-spoofing: 'wie is wie online?').

Daarnaast zien we dat via diverse (online) media mensen werkzaam in publieke organisaties steeds vaker worden bedreigd. Onderzoekers Brenninkmeijer en Odekerken schrijven hier onder andere over in een factsheet[12] over dreigingen binnen het journalistiek beroep met als cijfer dat 61% van de journalisten te maken met bedreigingen waarbij:

- 22% maandelijks te maken met (online) dreigingen;
- 43% jaarlijks te maken met (online) dreigingen;
- De consequenties hiervan is dat in 16% van de gevallen de journalist de berichtgeving aanpast uit angst voor de bedreigingen;
- 15% publiceert als gevolg van de dreiging helemaal niet;
- In totaal is 23% van de ondervraagde journalisten angstig om nieuws überhaupt naar buiten te brengen.

[12] Factsheet Een Dreigend Klimaat. Geschreven door M.W.A. Odekerken en prof. dr. A.F.M. Brenninkmeijer in opdracht van Nederlandse Vereniging van Journalisten, Stichting Persvrijheidsfonds, Stichting Democratie & Media, Stimulerings- fonds voor de Journalistiek en KIM Forum voor reflectie op journalistiek.

Samen met de rijksoverheid en media willen we gaan zorgen voor:

- Een kwalitatieve en volledige informatievoorziening met een groot bereik en toegang in de Amsterdamse gemeenschappen;
- Structurele informatievoorziening in het kader van veiligheid alsook op de korte termijn, in geval van een incident;
- Actief monitoren, mitigatie (reactie) en versterken van de weerbaarheid van Amsterdamse gemeenschappen ten opzichte van de genoemde dreigingen.

Aanpak
De aanpak moet gericht zijn in het versterken van de monitoring en mitigatie capaciteit van de gemeente door het aanleggen van een informatie-infrastructuur die dieper in de vezels van de Amsterdamse (sub)gemeenschappen doordringt. Dit om beter te kunnen monitoren, effectiever informatie te verspreiden en beter te kunnen reageren. Die versterking bestaat uit het inzetten van bredere media-typen (social, bijvoorbeeld via de app Telegram), aanleggen van een netwerk van sleutelpersonen in de Amsterdamse gemeenschappen en het actiever monitoren en actiever en effectiever verspreiden en beschikbaar maken van informatie.

Voorgestelde activiteiten
Het opzetten van een klein team met de volgende activiteiten

a. Monitoring (in samenwerking met grote platforms en mogelijk veiligheidsdiensten);
b. Opzetten effectieve infrastructuur van (voornamelijk sociale) media die dieper in de haarvaten van de stad komt (o.a. *Telegram*, *Instagram*, *WhatsApp*, *Google News* en reguliere media). Hierbij kunnen eigen kanalen van de gemeente worden ingezet maar ook andere labels en kanalen;
c. Gerichte (her-) disseminatie van informatie;
d. Herschrijven van gemeentelijke stukken voor bredere doelgroepen;
e. Opzetten acute response functie bij calamiteiten;
f. Samenwerking organiseren met grote platformen (Google, Facebook), veiligheidsdiensten en reguliere media.

Eigen huis op orde

Informatiebeveiliging is binnen de gemeente Amsterdam ingericht als continu proces. Verantwoordelijkheden zijn formeel belegd in het stedelijke informatiebeveiligingsbeleid. Er is een cyclus waarbij de volgende stappen zijn vastgelegd:

1. Inrichting van de governance;
2. Voortdurend (nieuwe) dreigingen en risico's in kaart brengen;
3. Doorvoeren van geschikte (mitigerende) maatregelen;
4. Bewustwording van het personeel;
5. Oefenen inclusief toetsing of de maatregelen voldoende blijken zijn;
6. Eventuele verbeteringen opstellen in het jaarplan, beleidskaders en of d.m.v. campagnes.

Jaarlijks wordt aan het college BenW en de gemeenteraad gerapporteerd over de status van de informatiebeveiliging en eventuele risico's. Sturing op de informatiebeveiliging van de gemeente Amsterdam vindt plaats via de in het beleid vastgestelde governance. Doelstelling is om de informatieveiligheid van de gemeente Amsterdam verder te versterken en te borgen op basis van risico's. Het door het College vastgestelde informatiebeveiligingsbeleid is het uitgangspunt daarbij. Kerndoel is de implementatie van de Baseline informatiebeveiliging Overheid (BIO) die in 2019 is vastgesteld. Implementatie van de BIO is een meerjarige opgave die in 2020 van start gaat.

Uit diverse rapporten (o.a. het Cyber Security Beeld Nederland 2019 van het NCTV) blijkt dat de digitale dreigingen steeds groter worden en dat het vergroten van de (digitale) weerbaarheid het belangrijkste instrument is voor overheden om risico's te verminderen. Gemeente Amsterdam is een grote en complexe organisatie die veel en ook gevoelige informatie verwerkt en daardoor een mogelijk doelwit is voor aanvallers. De in dit programma beschreven maatregelen hebben als doel om de weerbaarheid te vergroten. Daarbij worden preventieve, detectieve en correctieve maatregelen getroffen. Het Security Operations Center (SoC) vervult daarin een centrale rol.

In de agenda Digitale Veiligheid is ervoor gekozen om specifiek te focussen op de relatie tussen de binnenwereld en de buitenwereld. Hierin worden acties benoemd die effect kunnen hebben op de Amsterdammer. Daarnaast is het onderwerp beveiligingsbewustzijn opgenomen. Concrete acties die in het kader van "eigen huis op orde" worden voorgesteld zijn:

Gestarte acties voor 2019/2020	Wie	Kosten
• Implementatie van de Baseline Informatiebeveiliging Overheid (BIO), via o een afzonderlijk implementatieplan BIO met een eigen sturingslijn o periodieke dashboards over informatieveiligheid.	Wethouder Informatieveiligheid Gemeentelijk Management Team, CISO	Voorjaarsnota 2020
❑ Versterken en uitbreiden Security Operations Center ICT (generieke voorziening).	ICT	Kosten worden begroot via de Bestuursopdracht I-domein
❑ Intensiveren van de informatie-uitwisseling met IBD en NCSC, onderzoek aansluiting op het Nationaal Detectie Netwerk.	CISO	Bestaand budget
❑ 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.	CISO (coördinatie), Directie Communicatie, IV-eenheden, Directies	Bestaand budget

Gestarte acties voor 2019/2020	Wie	Kosten
❑ 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	CISO, IVE's, ICT	Bestaand budget
❑ Uitwerken en implementeren van '*Business Continuity Management'*: vaststellen vitale processen informatiesystemen en inregelen eventuele ontbrekende continuïteitsmaatregelen. Onderzoek Risico en audit comité is als start hiervoor geplandin2019. ❑ Uitvoeren verbeteracties n.a.v. ICT-uitval begin 2019	Business directeuren, ICT, IVE's, CISO	NOTK
❑ Verder versterken van het beveiligingsbewustzijn van medewerkers door het uitvoeren van een nieuwe bewustwordingscampagne, gebaseerd op de uitkomsten van een onlangs uitgevoerde meting . Campagne richt zich niet alleen op informatiebeveiliging maar ook op privacy, integriteit en heeft een relatie met antifraude-acties spoor 2.	CISO, samen met Functionaris gegevens-bescherming, Bureau Integriteit etc.	Budget CIO

Link met bestuurlijke prioriteiten

In het collegeakkoord is opgenomen dat er een Agenda Digitale Stad komt waarin concepten worden uitgewerkt voor digitale dienstverlening en participatie (moderne, open overheid), cybersecurity en veilige digitale infrastructuur en data-soevereiniteit. Bewust omgaan met de mogelijkheden en bedreigingen van digitale technologieën, voor het beschermen van burgerrechten en voor eerlijke toegang tot en het eerlijk verdelen van de opbrengsten van digitale technologieën.

Amsterdam wil in staat zijn een adequate respons te bieden op digitale dreigingen en aanvallen. Hiervoor moeten de benodigde (preventieve) maatregelen genomen worden en moet de basis op orde zijn. Hierbij is het van belang om zo goed als mogelijk te anticiperen op mogelijk risico's, het zo goed mogelijk helpen van getroffenen, het beperken van (im-)materiële schade en een zo spoedig mogelijke terugkeer naar een normale situatie. Om inzicht te hebben in de risico's, de aard en omvang van de lokale dreiging, is er naast het nationale veiligheidsbeeld (Cyber Security Beeld Nederland) en het veiligheidsbeeld informatiebeveiliging Nederlandse gemeenten een lokaal (Amsterdams) veiligheidsbeeld[13] opgesteld onder de naam 'Verkenning Digitaal Veilige Stad'. Hiermee kunnen bestuurders en burgers zich bewust worden van lokale risico's binnen het digitale domein voor Amsterdam.

De Amsterdamse verkenning dient inzicht te bieden in de dreigingen, belangen en weerbaarheid op het gebied van cybersecurity in relatie tot de digitale veiligheid in Amsterdam.

De hoofdvragen van de verkenning Digitaal Veilige Stad zijn:
1) Welke dreigingen kunnen de beschikbaarheid, vertrouwelijkheid en integriteit van informatie, informatiesystemen of -diensten aantasten, of hebben deze aangetast in de rapportageperiode?
2) Welke dreigingen vormen het grootste risico voor de Amsterdamse veiligheid?
3) Wat zijn de potentiële gevolgen voor de Amsterdamse veiligheid indien geïdentificeerde dreigingen zich manifesteren?
4) Welke combinaties van kwetsbaarheden en middelen hebben zich binnen de rapportageperiode in Amsterdam gemanifesteerd en (kunnen) worden toegepast?
5) In welke mate is Amsterdam weerbaar tegen de ingezette of inzetbare middelen, te misbruiken kwetsbaarheden en het manifest worden van dreigingen?
6) In hoeverre zijn er onderliggende oorzaken of factoren te identificeren die ten grondslag liggen aan het veiligheidsbeeld?

Om adequaat beleid te kunnen voeren is het noodzakelijk om een helder inzicht te hebben in de daadwerkelijk aanwezige risico's. De verkenning gaat over "*Wat bedreigt ons?"* en "*Hoe erg is dat?"* en is voornamelijk een inventarisatie en analyse van risico's als gevolg van een al dan niet moedwillige verstoring in het digitale domein. De verkenning gaat over de specifieke risico's die Amsterdam zouden kunnen treffen inclusief een weging van deze risico's ten opzichte van elkaar.

De verkenning Digitaal Veilige Stad is een logische doorvertaling van de beelden op nationaal niveau en op gemeentelijke niveau. Deze beelden richten zich respectievelijk op de brede maatschappij enerzijds en de eigen ICT organisatie van de gemeente anderzijds. Een lokaal beeld combineert deze tot het beeld ten aanzien van het eigen huis van de gemeente Amsterdam en ten aanzien van Amsterdam als stad, maatschappij, economie en samenleving.

[13] DVS: Onder de naam 'Digitaal Veilige Stad is er begin 2019 een verkenning opgesteld waarbij de landelijke beelden vertaald zijn naar lokale dreigingen. De acties en thema's uit de verkenning lopen synchroon met dit document waarbij de agenda een concretisering is op basis van het opgestelde en met experts gevalideerde veiligheidsbeeld.

Voor het complete veiligheidsbeeld voor Amsterdam verwijzen we naar het document Digitaal Veiligheidsbeeld Amsterdam (versie 2019)

Het beeld vormt ook de basis voor het ontwikkelen van gemeentelijk beleid ten aanzien van digitalisering, de agenda digitale stad en de omgang met dreigingen en risico's gepaard gaande met deze digitalisering. In dit beleid kan vastgelegd worden welke opgave, taken en verantwoordelijkheden het college ziet ten aanzien van deze digitalisering. Op basis de verkenning en het beeld en het hierop volgend te ontwikkelen beleid kunnen besluiten genomen worden over de inzet van (schaarse) middelen en kan bepaald worden welke risico's geaccepteerd worden.

Het is belangrijk om bij het opstellen en uitvoeren van dit beleid om ook de link met bestaande bestuurlijke prioriteiten en agenda's te leggen. Een beknopte opsomming van actuele bestuurlijke prioriteiten zijn:

1. Agenda Digitale stad;
2. Amsterdamse Aanpak Ondermijning;
3. Bestuursopdracht I-domein;
4. Innovatieve Inkoop;
5. Lopende subsidietrajecten;
6. Smart Mobility;
7. Energietransitie.

In samenwerking met de verschillende beleidsafdelingen, staffuncties en directies zal de link met bestuurlijke prioriteiten nader ingevuld moeten worden. Hier zal in een later stadium op teruggekomen worden.

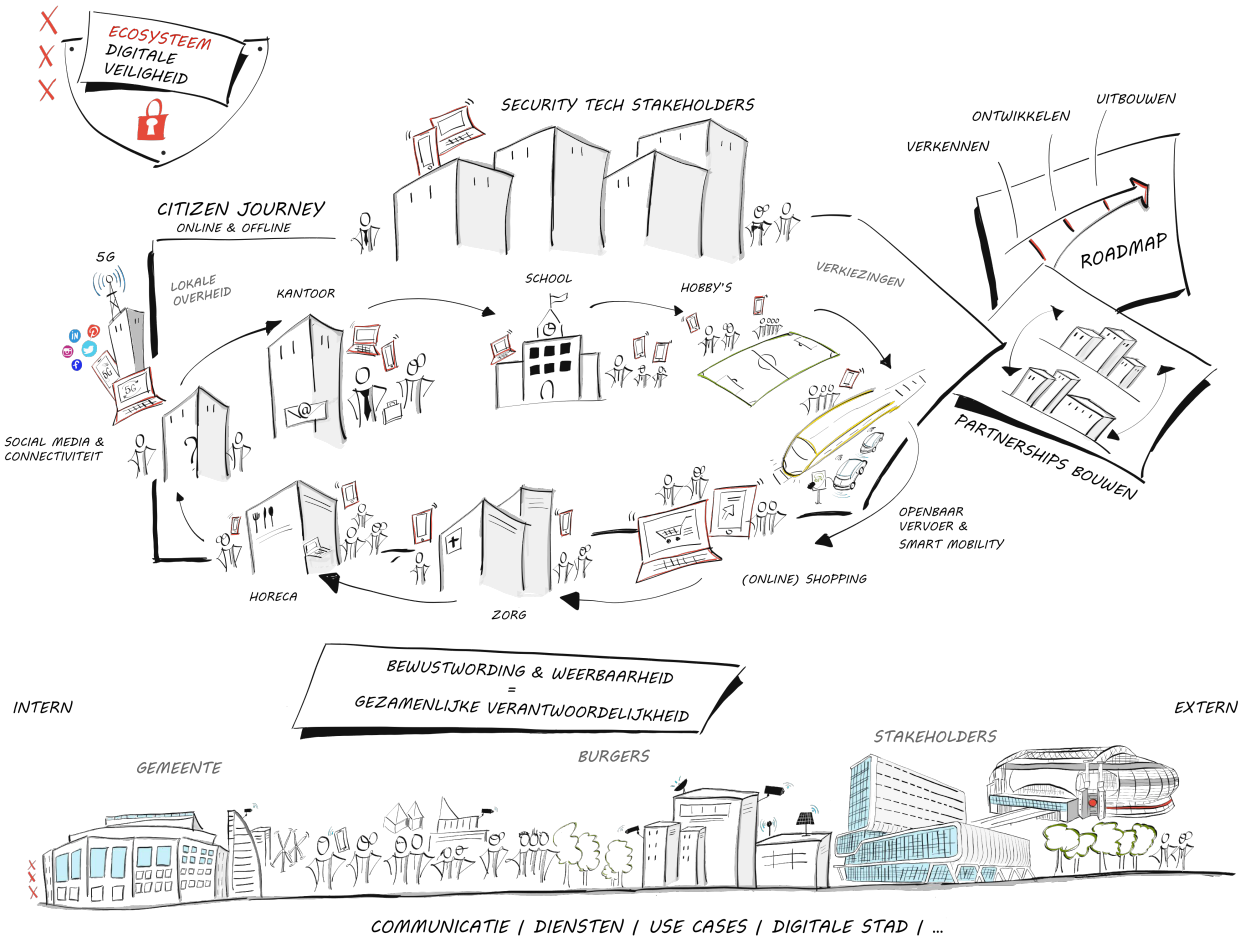
Werken in een ecosysteem

Het bewust kiezen om over de eigen grenzen van de gemeentelijke organisatie heen te werken maakt dat we netwerkend gaan werken in een ecosysteem. Dit heeft als doel om de gezamenlijke slagkracht te vergroten en de focus daar te leggen, waar die thuis hoort. Gemeente Amsterdam kent talloze partners welke mogelijk al lid zijn van interne of externe samenwerkingsverbanden. Binnen het innovatiedomein van de gemeente richt men zich op de 'smart city' concepten, waar publieke en private partijen via de technische toepassingen en data een bijdrage leveren om onze stad slimmer te maken. Daarmee loopt men vooruit in het werken in ecosystemen. Binnen het ecosysteem en de agenda digitale veiligheid staat de Amsterdammer centraal. Vanuit die perceptie is het ecosysteem (i.o.) ook opgesteld en visueel gemaakt in de onderstaande afbeelding.

Omdat de burger door zijn of haar dag heen zich, op bijna ieder moment en iedere locatie, ook begeeft in het digitale domein, zal door en om die 'citizen journey' heen ondersteuning geboden moeten worden om de weerbaarheid, daar waar nodig, te versterken. Dit is niet de verantwoordelijkheid van 1 partij, vandaar dat het hoofddoel is om bewustwording en weerbaarheid als gezamenlijke verantwoordelijkheid op te pakken door de technische stakeholders in de stad (bijv. domeindeskundigen als een Cisco, Atos, Deloitte, KPMG, Fox-IT etc.) uit te nodigen tot het sluiten van partnerships. Partnerships niet alleen met de gemeente, maar ook samen met andere bedrijven en instanties waar de Amsterdammer zich langs begeeft of die een (lokale) rol hebben in het publieke domein, zoals de politie.

Door samen, vanuit een ecosysteem, integraal te kijken naar de gemiddelde reis van een Amsterdammer kunnen we zorgdragen voor een hogere weerbaarheid. Dit geldt zowel voor de preventieve (koude) fase van de agenda Digitale Veiligheid alsmede ook de nazorg (warme) fase.

Afbeelding 7: Ecosysteem Digitale Veiligheid



De gemeente bereikt relatief minder Amsterdammers via de traditionele kanalen en zal via de communicatiekanalen van partners binnen het ecosysteem mogelijk een hoger bereik kunnen realiseren.

Een voorbeeld van acties en of producten die uit nieuwe partnerships ontstaan betreft de mobiel bankieren app die bijna iedereen tegenwoordig op de smartphone heeft. Door een simpele aanpassing in de mobiele app kan de bank gebruikers nu attenderen op het doen van transacties via een onbeveiligde en openbare WiFi. De suggestie om voor die handeling van de WiFi af te gaan en via het mobiele datanetwerk verder te gaan levert een hogere bewustwording op voor de gebruiker in tegenstelling tot een klassieke informatiecampagne via traditionele mediakanalen.

Dit is slechts een voorbeeld van een product en of dienst welke uit partnerships kan gaan ontstaan ter ondersteuning van de weerbaarheid van de Amsterdammer.

Programmastructuur

Om invulling te geven aan de gestelde ambities van de agenda zal er een actieprogramma moeten komen waarin de borging opgenomen zal worden. De uitvoering van het programma moet college breed, opgavegericht en multidisciplinair worden opgepakt. Om het college in staat te stellen invulling te geven aan de agenda en onderliggend actieprogramma wordt voorgesteld om te gaan werken met een stuurgroep en te starten met een taskforce.

De taskforce
De taskforce voert de centrale regie en informeert het bestuur over activiteiten in lijn met de gestelde ambities uit de agenda Digitale Veiligheid. Daarnaast werkt de taskforce aan de ontwikkeling en implementatie van producten en diensten op het gebied van digitale weerbaarheid in samenwerking met publiek- en private partners.

Voor de taskforce gelden de volgende uitgangspunten:
1. Adviseert naast de ambtelijke organisatie ook het college BenW over strategische digitale veiligheidsonderwerpen. Deze adviezen zijn richtinggevend en zetten aan tot handelen;
2. Opereert alleen initiërend en zal niet structureel de uitvoering van initiatieven ter hand nemen, maar proberen die onder te brengen binnen de lijnorganisatie;
3. Produceert niet alleen 'klassieke' adviezen, maar werkt ook met andere producten en activiteiten, zoals handreikingen, gesprekken en bijeenkomsten.

De taken van de taskforce bestaan uit:
Het gevraagd en ongevraagd verstrekken van strategisch advies over digitale veiligheid aan het college BenW.
1. Het volgen van trends en nieuwe technologische ontwikkelingen en deze waar nodig vertalen in strategische adviezen over mogelijke maatregelen om de risico's voor digitale veiligheid te verkleinen en de economische kansen te vergroten;
2. Het initiëren en/of versnellen van relevante initiatieven binnen de gemeente Amsterdam die een aantoonbare bijdrage leveren aan het verhogen van het weerbaarheidsniveau in Amsterdam.

Taskforce i.o.
De taskforce gaat uit van een gedistribueerd decentraal model waarin de expertise en acties binnen de lijnorganisatie zit, echter om regie en de bedrijfsvoering van het programma te bewaken zal de taskforce intern opgeschaald worden met de volgende functionele rollen:

- Inhoudelijke adviseur en expert op digitale veiligheid;
- Community manager (tbv ecosysteem);
- Programmamanagementondersteuning (secretaris, communicatie etc.);
- Deelprojectleiders tbv de 6 thema's in scope van de agenda.

Voor het moment gaan we uit van 3 fte voor de taskforce, plus de decentrale deelprojecteiders.

Stuurgroep
Een stuurgroep is samengesteld uit directeuren van de betrokken directies inclusief enkele externe inhoudelijk betrokken partners. De volgende functies zijn lid van de stuurgroep Digitale Veiligheid:

1. Chief Technology Officer (Gemeente Amsterdam, tevens voorzitter);
2. Stedelijk directeur Dienstverlening en Informatie (Gemeente Amsterdam);
3. Chief Information Officer (Gemeente Amsterdam);
4. Chief Information Security Officer (Gemeente Amsterdam);
5. Directeur Openbare Orde & Veiligheid (Gemeente Amsterdam);
6. Cyberfunctionaris (Politie Eenheid Amsterdam);
7. Cyberofficier (Openbaar Ministerie, parket Amsterdam).

Expert- en wetenschapstafel
Om invulling te geven aan de multidisciplinaire opgave en de publiek-private samenwerking is mede naar aanleiding van de experttafel (gehouden op 27 mei 2019) een externe focusgroep, community, opgezet bestaande uit cross-sectorale maatschappelijke en private organisaties, Amsterdamse kennisinstituten en burgers. Zij vertegenwoordigen de stad en klankborden voor ons op inhoud, focus en aanpak en geven hierbij (on)gevraagd advies.

Om de kennisontwikkeling te stimuleren en te borgen samen met de kennisinstellingen (zoals bijv. AMS Instituut, UvA, CWI en de VU) wordt voorgesteld om een wetenschapstafel in te richten. Binnen deze wetenschapstafel kan Amsterdam als platform van onderzoek en een field lab voor digitale veiligheid fungeren. Vraagstukken over de verhouding overheid, burger en samenleving kunnen hier besproken worden. Er kan discussie plaatsvinden op basis van (gepubliceerd) onderzoek en de vertaling van aanbevelingen en *'lessons learned'* naar richtinggevende adviezen en een agenda inclusief acties binnen Amsterdam. Per 2020 gaat Amsterdam, namens Economische Zaken, een partnership aan met de HSD (The Hague Security Delta) om zodoende meer kennisdeling, informatie uitwisseling en acties te bevorderen.

Capacity building, masterclass op digitale veiligheid
Als huidige werktitel naar aanleiding van een besluit uit de stuurgroep, is er gesproken over de opzet van een interne *masterclass weerbaarheid & digitale veiligheid*. In samenwerking met o.a. de Amsterdamse School is het streven om middels interne werving en selectie werknemers:

1. te kunnen opleiden en meer bewust maken op het onderwerp digitale veiligheid;
2. weerbaarder kunnen maken en daarmee een directe bijdrage leveren aan het thema 'Eigen Huis Op Orde';
3. kunnen werven van ambassadeurs in verband met de dienst overstijgende scope van de agenda Digitale Veiligheid; Feitelijk heb je als verlengstuk van je directe programmateam collega's met kennis en affiniteit nodig onder de verschillende RvE's en diensten van de gemeente. Middels dit traject zou je aan (indirecte) capaciteit kunnen bouwen zonder daar direct extern expertise voor te werven.

Externe samenwerking met bijv. het opleidingscurriculum zoals 'Integrale Veiligheidskunde' van de hoge scholen en of universiteiten in Amsterdam opzoeken behoort tot één van de punten welke nog nader uitgewerkt zal moeten worden.

Samenwerking tussen lokale overheden
Overkoepelend of per thema binnen de scope van de agenda Digitale Veiligheid is het zeker nuttig om bestaande samenwerkingsverbanden met bijv. de collega gemeenten ook in te zetten voor kennisdeling op het onderwerp. Per gemeente en regio zou men kunnen bekijken hoe resultaten in producten, kennis en of expertise deelbaar en of toepasbaar zijn op andere gemeenten. Zo is er reeds onder de naam *'Safety & Security'* een coalitie gevormd met de G5 steden om samen te werken op het dossier veiligheid.

Financiële paragraaf

Met het opstarten van dit traject (digitaal veiligheidsbeeld & agenda) zijn we uitgegaan van bestaande middelen, gedekt door de organisatieonderdelen CIO, CTO en OOV.

De taskforce zal per thema en actie binnen het nader op te stellen actieprogramma een begroting maken. De taskforce en het actieprogramma werkt naast de regie en coördinatie op bestaande en nieuw te ontwikkelen producten en diensten de komende maanden ook aan een verkenning tot een financiële constructie waarop de agenda Digitale Veiligheid de komende jaren gedekt zal worden.

Dit voorstel zal bij de voorjaarsnota 2020 ingediend worden op basis van de onderstaande template van een investeringstabel met daarin incidentele en of structurele kosten.

Afbeelding 8: Template van de jaarlijkse begroting aan lasten van de agenda Digitale Veiligheid.

Omschrijving	Jaar 0	Jaar 1	Jaar 2	Jaar 3
Individueel welzijn van de burger	-	-	-	-
Private organisatie en maatschappelijke instellingen	-	-	-	-
Vitale infrastructuur	-	-	-	-
Crisis- en incidentmanagement	-	-	-	-
Democratisering & bestuurlijke stabiliteit	-	-	-	-
Eigen huis op orde	-	-	-	-
Programmamanagement	-	-	-	-
PR & campagnes	-	-	-	-
Communicatie	-	-	-	-
Private samenwerkingen	-	-	-	-
Bestuurlijke prioriteiten	-	-	-	-
Veiligheidsbeeld (onderzoek)	-	-	-	-
Materieel	-	-	-	-
Indicatie totale kosten*	**0.00**	**0.00**	**0.00**	**0.00**
**bedragen x 1.000 euro*				

Planning en tijdlijn

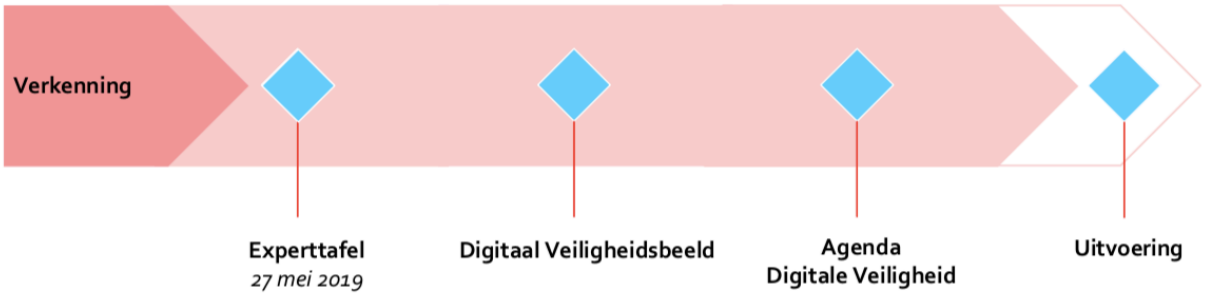
In afstemming met de betrokken diensten en directies zal er door de taskforce, programmateam i.o., een planning van activiteiten weggezet in de tijd worden opgesteld voor de jaren 2020/2021.

Onderdeel en inrichting van de planning zal tevens als blauwdruk dienen ten behoeve van de voortgangsrapportage aan o.a. de stuurgroep en stakeholders alsmede de themastaf Illegale Economie en Criminaliteit van burgemeester Halsema en de staf Digitale Stad van wethouder Meliani.

Vanuit de agenda Digitale Veiligheid zijn we nu beland bij de uitvoeringsfase. Vanaf begin 2019 is er middels een verkenning en validatie tijdens de experttafel gewerkt aan het tot stand brengen van het lokaal digitaal veiligheidsbeeld en de agenda zelf.

De volgende fase betreft de uitvoering onder leiding van de nader op te zetten taskforce en actieprogramma welke in de lijn van de agenda op detailniveau zal beschrijven hoe we zullen gaan werken aan de digitale weerbaarheid van de stad.

Afbeelding 9: Fasen van de agenda Digitale Veiligheid.



Nawoord

Amsterdam spreekt de ambitie uit om (ook) digitaal één van de veiligste steden te worden. Referentiekaders tonen aan dat ruim meer dan 50% van de onderzochte steden zich matig tot slecht equiperen om de stad en haar inwoners te beschermen op digitale veiligheid. Waar je ziet dat er landelijk jaarlijks gerapporteerd wordt op digitale dreigingen door de NCTV toont Amsterdam nu ook haar verantwoordelijk door lokaal een vertaling te hebben gemaakt van het nationale veiligheidsbeeld.

De stad kent zowel binnen het fysieke domein als digitaal risico's en kansen. De stad zal en moet weerbaarder worden om zichzelf, haar inwoners, bezoekers en ondernemers te beschermen tegen digitale risico's. We kunnen dit niet alleen en zullen in nauwe samenwerking met kennisinstellingen, publiek en private partijen moeten werken om bewustwording en ondersteuning te bieden op de weerbaarheid.

In de agenda Digitale Veiligheid leest u acties op korte termijn en plannen voor de lange termijn. Nadruk van de agenda en tevens de rol van de gemeente Amsterdam ligt meer op de preventieve kant en deels op de nazorg kant (thema Crisis- en Incidentmanagement) zodat wanneer een digitale dreiging zich manifesteert heeft, waarbij de Amsterdamse openbare orde in het geding komt, de juiste middelen beschikbaar zijn om de verstoring binnen het digitale domein te verhelpen. Aan de hand van het jaarlijks bijwerken van het veiligheidsbeeld zal ook inzichtelijk worden wat de impact is van de agenda.

Werken aan digitale veiligheid, een onomkeerbaar proces binnen de rol van de Gemeente Amsterdam.

Wanneer u nu na het lezen van de agenda Digitale Veiligheid mij een advies of anderszins wilt geven dan houd ik me daar van harte voor aanbevolen.

Colofon

De agenda Digitale Veiligheid is tot stand gekomen in opdracht van burgemeester Femke Halsema, onder verantwoordelijkheid van Ger Baron (Chief Technology Officer van de Gemeente Amsterdam) met bijdragen, medewerking, kritische reflectie en reacties van:

Tijs van Wijk
Joshua Serrao
Linda Goedhart
Nathalie Bosman
Marco van Beek
Mark de Smet
Eert Moonen
Steven Jonker
Daan Groenink
Tommie Leisink
Teun Gautier
Paul van Eeten
Mark Crooijmans
Maarten van Haasteren
Eric van Aart
Josca Boers
Hans Teengs Gerritsen
Theo Veltman
Jaap de Munnik
Hans Nouwens
Hester Diemer
Manon den Dunnen

Amsterdam, november 2019

Voor vragen en opmerkingen: cto@amsterdam.nl

Agenda Digitale Veiligheid
Gemeente Amsterdam