Uitvoeringsplan Digitale Veiligheid

Gemeente Lelystad



Inhoud

1. Achtergrond en aanleiding 3
2. Digitale Veiligheid, Veiligheidsrisico's en stand van zaken 5
2.1. Cijfers en achtergrond informatie? 5
2.2. Stand van zaken 7
3. Hoofdlijn van de aanpak 8
4. Financiën 9
Bijlage 1 planning behorende bij uitvoeringplan Digitale Veiligheid 10
Bijlage 2: Gebruikte documenten 13

1. Achtergrond en aanleiding

Cyberveiligheid of digitale veiligheid wordt steeds belangrijker als thema. Door de digitalisering wordt steeds meer online gedaan en er ontstaat steeds meer digitale data. Hierdoor is er ook steeds meer vraag naar digitale data en is het stelen van bijvoorbeeld persoonsgegevens eenvoudiger geworden. De coronamaatregelen leidden landelijk tot een verschuiving van criminaliteit in 2020. Het aantal geregistreerde woninginbraken daalde met 23 procent en de registraties van zakkenrollerij halveerde bijna. Daartegenover staat een forse toename van cybercrime, daarvan zijn in 2020 landelijk 127 procent meer gevallen geregistreerd.

Door de digitalisering is cyber(digitale)veiligheid een belangrijk onderdeel geworden van ons dagelijkse leven. Zeker in tijden van een pandemie zijn we als Nederland en ook als gemeente afhankelijk geworden van digitale diensten. Deze digitalisering biedt ons veel voordelen, maar over het algemeen wordt er onvoldoende nagedacht over de risico's en kwetsbaarheden en het nemen van beschermende maatregelen. Inwoners, bedrijven en instellingen weten tegenwoordig hun fysieke huis goed te beveiligen, maar de ramen en deuren van hun digitale huis staan veelal nog open. Om dit zoveel als mogelijk te voorkomen hebben we in het integraal Veiligheidsplan 2018-2022 een aantal acties benoemd en uitgevoerd. Gezien de huidige ontwikkelingen binnen de digitalisering, de stijging op landelijk en Lelystadsniveau blijkt dit niet afdoende. Vandaar dit uitvoeringsplan Digitale Veiligheid 2021-2023.

Digitale veiligheid gaat over het beschermen van mensen en organisaties tegen iedere dreiging die voorkomt uit een digitale omgeving. Dat kan de dreiging zijn die uitgaat van cybercrime/ digitale criminaliteit, maar ook van de dreiging die uitgaat van een ontoereikende beveiliging van genetwerkte systemen (hardware, software en data).

Cybercrime heeft vele gezichten. De gevolgen kunnen zeer ingrijpend zijn. Er zijn veel slachtoffers en het worden er niet minder. Zo zijn er veel verschillende risico's aan verbonden. De veiligheidsmonitor (landelijk onderzoek naar veiligheidsbeleving) beschrijft de belangrijkste en meest omvangrijke risico's in vier categorieën:
- Hacken;
- koop- of verkoopfraude;
- pesten;
- identiteitsfraude.

Daarnaast bestaan er grofweg drie typen cybercriminelen. Ten eerste zijn er de kwajongens die vanaf hun zolderkamer online kattenkwaad uithalen. De tweede groep, professionele hackers met kwaad in de zin, opereren individueel of maken deel uit van criminele organisaties. Zij gaan puur voor financieel gewin. Ten slotte zijn er de landen/staten met hun spionnen, die handelen vanuit geopolitieke of economische overwegingen. Dit uitvoeringsplan zal zich voornamelijk richten op het voorkomen van slachtofferschap. Het aanpakken van daders is aan de politie en het Openbaar Ministerie.

De aanpak van cybercriminaliteit is als prioriteit opgenomen in het Integraal Veiligheidsplan van de gemeente Lelystad. Ook in de Regionale Veiligheidsstrategie Midden-Nederland (2019-2022) wordt cyberveiligheid aangemerkt als een van de lokale en districtelijke prioriteiten. Binnen cyberveiligheid ligt in deze strategie de nadruk op:
- Preventie en bewustwording;
- samenwerking en kennisdeling;
- bestrijding cybercrime.

Volgens deskundigen wordt cybercriminaliteit qua omvang de fietsendiefstal van de toekomst. Het is een ontwikkelend fenomeen met constant veranderende vormen. Uit de Veiligheidsmonitor blijkt dat 13% van alle Nederlanders in 2019 slachtoffer is geweest van cybercrime. In Lelystad lag dat percentage nog hoger namelijk 18%.

Uit de laatst gehouden Veiligheidsmonitor (2019) onder Lelystedelingen blijkt dat van de cybercrimedelicten hacken het meest voor (6 procent). Dit werd gevolgd door koop- of verkoopfraude (5 procent), pesten via het internet (4 procent) en identiteitsfraude (1 procent).

In Lelystad zijn de slachtoffers verdeeld over 10% fraude via internet, 5% hacken en 7% pesten. In 2019 deed 8 procent van de slachtoffers van cybercrime in Lelystad, aangifte bij de politie. Verder waren er in 2019 in Lelystad 257 fraudedelicten via online handel bekend bij de politie. Een stijging van 32% ten opzichte van het jaar 2018.

2. Digitale Veiligheid, Veiligheidsrisico's en stand van zaken

In dit uitvoeringsplan beschrijven we hoe we de komende drie jaar om willen gaan met de nieuwe uitdagingen. We gaan de bestaande aanpak meer structureren, actualiseren en aanscherpen. Het doel van de aanpak is om eind 2023 en verder beter beschermd te zijn tegen digitale indringers en criminelen. Daarnaast willen we bewerkstellen dat de aanpak van digitale criminaliteit en onveiligheid net zo normaal is, als de aanpak van bijvoorbeeld woninginbraken en veelvoorkomende criminaliteit.

2.1. Cijfers en achtergrond informatie?

Cybercrime komt in veel verschillende vormen voor. Denk hierbij bijvoorbeeld aan:

- het inbreken in computers voor nieuwe vormen van diefstal;
- afpersing van burgers en bedrijven;
- het platleggen van websites;
- bedrijfsspionage;
- Oplichting via (valse) websites of het niet leveren van producten (koop/verkoop fraude)
- handel op het darkweb;
- het hacken van computers om geld naar criminele bankrekeningen over te schrijven;
- het ongemerkt aanzetten van camera's en microfoons om mensen in hun eigen omgeving te kunnen bespioneren;

De veiligheidsmonitor beschrijft de belangrijkste en meest omvangrijke risico's in vier categorieën: Hacken, koop- of verkoopfraude, online bedreiging & cyberpesten en identiteitsfraude.

Hacken
Van de cybercrimedelicten komt hacken in 2019 het meest voor (6 procent).

Wat is Hacken?:
Bij hacking probeert iemand binnen te dringen in andermans computer. Het is strafbaar als dit gebeurt zonder toestemming van de eigenaar van die gegevens. Doel van de criminele hacker is de computer overnemen of gegevens stelen of onbruikbaar maken t.b.v. afpersing.
Hackers proberen toegang tot computers te krijgen door:

- het raden of achterhalen van iemands inloggegevens
- iemand te dwingen zijn gegevens te vertellen (door bedreiging of chantage);
- phishing of social engineering
- gebruiken van inloggegevens die zijn buitgemaakt bij andere gehackte websites

Koop- of verkoopfraude
Van cybercrimedelicten komt in 2019 Koop- of verkoopfraude in 5 procent van de gevallen voor.

Wat is koop of verkoopfraude?:
Bij koop- en verkoopfraude gaat het om oplichting via internet bij het kopen of verkopen van goederen of diensten, bijvoorbeeld doordat gekochte goederen niet geleverd worden of niet betaald wordt voor geleverde diensten.

Online bedreiging & cyberpesten;
Tussen de 1% en 3% van de Nederlanders is slachtoffer (geweest) van online bedreiging & cyberpesten. Dit percentage geldt t/m 2018. Meer specifiek blijkt uit de veiligheidsmonitor 2019 dat cyberpesten is gestegen tot ruim 4% (CBS 2020). Onder jongeren ligt dit percentage vele malen hoger. Dit komt voornamelijk omdat jongeren het vaakst online zijn en daardoor het meeste risico

lopen en ook meer risico's nemen. De online wereld voelt voor jongeren anoniem en dit heeft impact op hun gedrag en de mate waarin zij de schade van hun acties overzien. Vooral bij cyberpesten en/of het zonder toestemming verspreiden van seksueel beeldmateriaal (sexting) zijn bekende fenomenen.

Wat is online bedreigen en cyberpesten?
Online pesten, cyberpesten, digitaal pesten: het zijn allemaal termen die we gebruiken voor pestgedrag via sociale media. Beschermd door anonimiteit gaat cyberpesten veel verder dan andere vormen van pesten.
Digitaal pesten kan op veel manieren. Online pesten mensen, vooral scholieren, elkaar door:

- Misbruik van privégegevens (zoals het stelen van wachtwoorden of het aanmaken van nep-accounts)
- Uitsluiting in WhatsApp-groepen
- Het verspreiden van beeldmateriaal (zoals intieme foto's (sexting) of filmpjes van mishandeling)
- Dreigtweets en haatposts

Sexting:
Bijna een kwart van de Nederlandse jongeren (23%) heeft wel eens een naaktfoto of foto in ondergoed ontvangen. Meisjes ontvangen vaker sexting (24,5%) dan jongens (21,6%). Zij doen zelf ook vaker aan sexting: 7,1% van de meisjes tussen de 12 en 17 jaar heeft wel eens een naaktfoto of foto in ondergoed naar iemand gestuurd, tegenover 5,5% van de jongens.

Wat is Sexting?
Sexting is een combinatie van de Engelse woorden sex en texting (texting betekent sms-en):
Het versturen van een eigen naaktfoto, spannende video en/ of erotisch tekstbericht via sms en ook via WhatsApp en andere sociale media. Het is belangrijk jongeren te waarschuwen en voor te lichten over sexting. Sexting kan leiden tot pesten, schaamte en ernstige psychische problemen. Het gebeurt regelmatig dat jongeren een erotisch bericht online zetten of doorsturen aan andere jongeren, docenten en/of ouders. De verspreiders van het bericht denken hier vaak niet over na en ook niet over de gevolgen die het voor henzelf kan hebben. Jongeren denken al snel 'eigen schuld' bij sexting en weten vaak niet dat het verspreiden van andermans foto strafbaar is. Als je een dergelijke berichten doorstuurt, is dit een strafbaar feit.

Identiteitsfraude:
Identiteitsfraude ongeveer 1% was hiervan in 2019 slachtoffer.

Wat is identiteitsfraude?
Bij identiteitsfraude maken criminelen misbruik van valse of gestolen identiteitsgegevens. Ze kopen bijvoorbeeld op naam van iemand anders spullen zonder te betalen.

2.2. Stand van zaken

Wat doen we al vanuit het Integraal Veiligheidsplan?

Versterken van de samenwerking:
We werken op digitale veiligheid samen met andere partijen. We werken samen op landelijk niveau , eenheidsbreed (politiegebied Midden Nederland, 39 gemeenten) en binnen Flevoland. Onze activiteiten zijn afgestemd op het programma Digitale Veiligheid en de Regionale Veiligheidsstrategie 2019-2022. Ook is er afstemming over de aanpak met de Taskforce Digitale Veiligheid. Daarin zijn politie, OM en alle districten vertegenwoordigd.

Diverse activiteiten:
We zetten al op diverse vlakken acties in voor cyberveiligheid. Denk aan preventie en bewustwording van onze inwoners. Samenwerking en kennisdeling tussen de veiligheidspartners, onder meer doordat er binnen Midden Nederland één gezamenlijke de regionale veiligheidsstrategie is opgesteld. Verder blijven we aansluiting houden bij landelijke initiatieven en campagnes.

Waarom dan een uitvoeringsplan Digitale Veiligheid?
Met dit uitvoeringsplan willen extra inzetten op de aanpak van cybercriminaliteit en snel kunnen inzetten op nieuwe ontwikkelingen. We gaan de bestaande aanpak meer structureren, actualiseren en aanscherpen. De effecten van het uitvoeringplan worden tussentijds meegenomen in de evaluatie van het Integraal Veiligheidsplan.

3. Hoofdlijn van de aanpak

Aan de hand van het programma Digitale Veiligheid, van de Regionale Veiligheidsstrategie Midden-Nederland, het Integraal Veiligheidsplan 2018-2022 gemeente Lelystad en brief van de Minister van Justitie en Veiligheid Ferd Grapperhaus over de integrale aanpak van cybercrime is dit uitvoeringsplan ontstaan.

1. **Er wordt geïnvesteerd in preventie, weerbaarheid en bewustwording.**

Preventie en bewustwording van onze inwoners en ondernemers, jong en oud met als inzet: weerbaarheid in cyberveiligheid. Doel is digitale privacy, weerbaarheid en veiligheid te vergroten. We willen doelgroep gericht concreet aan de slag met interventies om slachtofferschap maar ook daderschap (onder jongeren) te voorkomen.

2. **De opsporing wordt versterkt, criminele activiteiten worden verstoord en daders worden aangepakt.**

De anonimiteit en snelheid van de ontwikkelingen in de digitale wereld vormen voor de opsporing een bijzondere uitdaging. Contact leggen over het internet kan anoniem en versleuteld. De technologie om de privacy van gebruikers te beschermen wordt ook gebruikt door criminelen om hun identiteit beter af te schermen.
De nadruk zal liggen op het bestrijding van cybercriminaliteit door het samen met de veiligheidspartners vormgeven van preventie en repressie, waaronder opsporing en vervolging. Daarbij hoort tevens handelingsperspectief voor slachtoffers.

3. **De kennis en weerbaarheid binnen de gemeente vergroten.**

Het uitvoeringsplan digitale veiligheid richt zich in eerste instantie op jongeren, MKB-organisaties en inwoners van Lelystad. Maar ook op onze eigen organisatie. Informatie beveiliging en gegevensbescherming is intern binnen de gemeente Lelystad belegd bij de afdeling informatiemanagement en automatisering. We gaan in de samenwerking zorgen dat de infrastructurele informatiehuishouding op orde blijft, daarbij gaan we oefen en trainen in het kader van crisisbeheersing. Doel is helder te krijgen welke problemen we als gemeente hebben indien we te maken krijgen met cybercriminaliteit en te zorgen dat we beter zicht krijgen op de aard en omvang van deze problematiek, ervaring opdoen in hoe te handelen als het toch mis gaat. Concreet gaan we aan de slag met interventies om slachtofferschap binnen de gemeente te voorkomen.

4. **Integrale samenwerking vergroten**

Samenwerking en kennisdeling tussen de veiligheidspartners, maar ook publiek-privaat;
We zoeken nadrukkelijk aansluiting bij (komende) landelijke initiatieven.

4. Financiën

In de kadernota 2022 heeft de afdeling Veiligheid extra middelen gevraagd om Cybercrime aan te pakken. Deze middelen zijn niet toegekend. Dit betekent dat er weinig financiële ruimte is voor dit uitvoeringsplan en dat we genoodzaakt gebruikt te maken van het huidige veiligheidsbudget en reeds bestaande netwerken, partners en hun acties tegen cybercriminaliteit, Politie, gemeente, CCV, Veiligheidsmonitor, provincie, taskforce digitale veiligheid, inwoners, bedrijfsleven, Openbaar Ministerie, onderwijs, RIEC, Veiligheidsregio en andere betrokken partijen. Daarnaast gaan we op zoek naar eventuele subsidie mogelijkheden.

Bijlage 1 planning behorende bij uitvoeringplan Digitale Veiligheid

Doelgroep	Partners	Actie	Cybercrime vorm	wanneer	2021	2022	2023	kosten
Preventie, weerbaarheid en bewustwording								
Inwoners algemeen	gemeente, politie bedrijfsleven	Indien mogelijk inzet escaperoom aandacht Cybercrime in de week van de Veiligheid	Diverse vormen komen aan de orde	okt	okt-21	okt-22	okt-23	?
Ouderen	Zorgcentra/ buurtwatsappgroepen	Campagne voor ouderen over verschillende type digitale oplichtingsvormen	Type cybercrime: verschillende vormen, waaronder babbeltrucs, phishing en spoofing	Aansluiten bij de landelijke week van de ouderen		apr-22	?	€ 0,00
Kinderen (8-12jaar)	Politie, basisscholen, bibliotheek, Rabobank, Flavour, BSO, ed.	HackShield en Hackshield in de klas	Internet criminaliteit/ gevaar van cyberpesten tm hacken (heel breed)	Aansluit op de agenda HackShield en contentplanning Lelystad	jul-21	doorlopend	doorlopend	€ 4.000,00
Ondernemers	Politie, Rijk, De Veiligheidscoalitie Midden-Nederland, ondernemersverenigingen.	Voorlichtingsbijeenkomst	Hacken, Phising.	start 4e kwartaal 2021 in overleg	?	doorlopend	doorlopend	PM
Datingfraude	politie, gemeente, bibliotheek buurtwatsapp	Campagne voorlichting	Datingfraude	najaar richting feestdagen	okt-21	okt-22	okt-23	€ 0,00

Doelgroep	Partners	Actie	Cybercrime vorm	wanneer	2021	2022	2023	kosten
Jongeren	Het CCV, het ministerie van Justitie & Veiligheid en Scholieren.com, bibliotheek, Middelbare scholen en MBO	Campagne Geflasht	Ticketfraude, online oplichting nep webwinkels, online fraude, ID Fraude.	Doorlopend, ticketfraude vanaf evenementen weer los gaan in 2021	aug-21	mei-22	mei-23	€ 0,00
Inwoners algemeen	Buurtwatsapp groepen, Politie	Onderzoeken mogelijkheden tot Digitale buurt ambassadeurs	alle vormen Algemeen	na uitwerking hoe en wat.		jan-22	doorlopend	PM
Inwoners algemeen	Buurtwatsapp groepen, Politie	Bij de media kijken of we iets kunnen doen met een interview e.d. om de Podcastserie Digitaal beroofd onder de aandacht te brengen	Drie afleveringen De podcastserie Digitaal Beroofd bestaat uit 3 afleveringen over cyberdelicten die heel veel voorkomen: • Helpdeskfraude • Afpersing met DDOS (met name geschikt voor ondernemers/MKB) • Vriend-in-nood-fraude	afstemmen communicatie	dec-21	doorlopend	doorlopend	PM
Integrale samenwerking versterken								
Inwoners algemeen	Middelbaar onderwijs, Politie, gemeente, bibliotheek, basisonderwijs, ondernemersverenigingen, banken	Sturing op de integrale aanpak Cybercrime d.m.v. het Inrichten regiegroep Cybercriminaliteit Aansluiten bij digitaal district en RVS	alle vormen Algemeen	september	sep-21	doorlopend	doorlopend	PM

Doelgroep	Partners	Actie	Cybercrime vorm	wanneer	2021	2022	2023	kosten
De kennis en weerbaarheid binnen de gemeente vergroten.								
De doelgroep van de Overheidsbrede Cyberoefening en Webinars zijn professionals, managers en bestuurders van overheden en bedrijven	Rijk, Interne organisatie, privacy officer afdeling Informatie Management en Automatisering	onderzoeken deelname aan Overheidsbrede Cyberoefening	Hacken, Phising.	okt-21	nov-21	?	?	PM
Collega's gemeente	Interne organisatie, privacy officer afdeling Informatie Management en Automatisering	Actief informeren van collega's over cybercriminaliteit	Via intranet collega's informeren over cybercriminaliteit en de acties die je zelf kan nemen			doorlopend	doorlopend	PM

Bijlage 2: Gebruikte documenten

Inventarisatie Cyberveiligheid CCV en VNG
Cybersecuritybeeld Nederland CSBN 2019
Regionale veiligheidsstrategie Midden-Nederland 2019-2022
Programma digitale veiligheid 2020-2022 Veiligheid Coalitie Midden-Nederland
Tweede Kamer Aanpak Cybercrime 2018
Uitvoeringsplan 2021-2022 Integraal Veiligheidsplan gemeente Lelystad
www.veiliginternetten.nl