Onderwerp Agenda Digitale Veiligheid 2025-2028
ter informatie

De leden van de raad van de gemeente Groningen
te
GRONINGEN

Telefoon	14 050	Bijlage(n)		Ons kenmerk	344847-2024
Datum		Uw brief van		Uw kenmerk	

Geachte lezer,

Met deze brief informeren wij u over de inhoud en noodzaak van de Agenda Digitale Veiligheid 2025-2028. De agenda is een vervolg op de Agenda Digitale Veiligheid 2021-2024 en is gebaseerd op dezelfde landelijke richtlijnen en wettelijke regelgeving.

Aanleiding
Onze maatschappij wordt steeds meer digitaal en nieuwe technologieën ontwikkelen zich razendsnel. Dit geeft voordelen, maar deze afhankelijkheden brengen ook risico's met zich mee. Digitale onveiligheid in de vorm van online criminaliteit of cyberaanvallen kan grote impact hebben en raakt het werkveld van het lokale veiligheidsdomein op veel fronten. Inwoners, bedrijven en ook gemeentelijke organisaties worden regelmatig slachtoffer van cybercrime en gedigitaliseerde criminaliteit. Dit leidt niet alleen tot veel persoonlijke financiële schade en emotionele impact bij slachtoffers, maar kan ook tot maatschappelijke ontwrichting leiden wanneer (overheids-)organisaties en bedrijven geraakt worden. Om deze reden werd in 2021 de Agenda Digitale Veiligheid 2021-2024 door ons vastgesteld om aan de hand van drie deelprogramma's met bijbehorende actiepunten directie en afdeling overstijgend (Informatie & Services, Openbare Orde en Veiligheid en Economische Zaken) hieraan uitvoering te geven. Dit jaar loopt deze agenda ten einde, maar de urgentie van dit onderwerp blijft onverminderd hoog. Daarom is het nodig om deze agenda te hernieuwen en met de Agenda Digitale Veiligheid 2025-2028 ons te blijven inzetten voor een digitaal veilige(re) gemeente. Hiermee blijft de gemeente ook aangesloten bij landelijke richtlijnen van de Vereniging van Nederlandse Gemeenten (VNG) en het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en voldoet het aan wettelijke regelgeving.

Volgvel 1

Inhoud

De Agenda Digitale Veiligheid 2025-2028 bevat thema's, ambities en activiteiten om te komen tot een digitaal veilige(r) gemeente. Met de agenda bouwen we voort op de activiteiten uit de vorige editie. Hierbij onderscheiden we 3 deelprogramma's:

1. Eigen huis op orde

Gemeenten zijn zelf verantwoordelijk voor informatiebeveiliging en dus voor de digitale weerbaarheid van de eigen organisatie. Dit gebeurt aan de hand van de Baseline Informatiebeveiliging Overheid (BIO), een gezamenlijk normenkader voor alle overheidsorganisaties gebaseerd op de internationaal erkende en actuele ISO-normatiek. De BIO kent verschillende facetten: de mens, proceskant, techniek, monitoring, rapportage, evaluatie en bijstelling. Directie SSC-I&S is verantwoordelijk voor de coördinatie en technische implementatie van deze BIO-maatregelen (rapportage via ENSIA)[1]. Ter vergroting van de bewustwording heeft gemeente Groningen gemeente breed het Digitaal Rijbewijs ingevoerd met deelnameverplichting. Jaarlijks worden verschillende interne bijeenkomsten en een regionaal congres georganiseerd om collega's en externen digitaal weerbaarder te maken. In 2024 had het congres voor het eerst het thema Hack050, waarbij ethische hackers hebben geholpen om nog onbekende kwetsbaarheden in de ICT-infrastructuur van gemeente Groningen op te sporen zodat deze kunnen worden opgelost.

2. Voorbereiding op digitale ontwrichting, incidenten en crises

In dit deelprogramma bereiden wij ons voor op digitale ontwrichting, dit is een vorm van maatschappelijke ontwrichting waar een verstoring van een digitaal (ICT)-systeem aan te grondslag ligt. De rol van de gemeente is tweevoudig als het gaat om de voorbereiding op cyberincidenten en cybercrises. Net als elke andere organisatie is de gemeente verantwoordelijk voor de eigen informatiebeveiliging en dus voor de afhandeling van interne cyberincidenten om de interne bedrijfscontinuïteit te kunnen waarborgen. Een belangrijke interne actielijn is bijvoorbeeld het verdere aansluiten van het ICT-continuïteitsplan op het bedrijfscontinuïteitsplan waarbij rekening wordt gehouden met de mogelijkheid dat een intern incident gevolgen kan hebben in het fysieke domein of op de openbare orde en veiligheid.

Naast de interne rol van de gemeente in het geval van cyberincidenten is er nog de rol die de gemeente inneemt bij een cybercrisis. De gemeente is immers binnen het veiligheidsstelsel primair verantwoordelijk voor de openbare orde en veiligheid, de processen van bevolkingszorg en het herstellen van de maatschappelijke continuïteit. Een cybercrisis is een crisis die betrekking heeft op de beveiliging van netwerken en informatiesystemen met aanzienlijke maatschappelijke gevolgen met daaraan gerelateerde cascade- en gevolgeffecten in het fysieke domein. Hierdoor kan opschaling via de GRIP-structuur noodzakelijk zijn wanneer digitale ontwrichting (dreigt) door een organisatie of vitale sectoren buiten de gemeentelijke organisatie. Denk bijvoorbeeld aan digitale incidenten met cascade-gevolgeffecten bij (semi)publieke voorzieningen en instellingen, zoals: bruggen, sluizen, scholen, ziekenhuizen, culturele instellingen, verzorgingshuizen, etc. In de koude fase borgen wij in afstemming met onder andere de Veiligheidsregio de voorbereiding op digitale

[1] Eenduidige Normatiek Single Information Audit. https://vng.nl/projecten/ensia

ontwrichting naast de standaard crisisbestrijding in de vorm van een lokaal risicobeeld, maar ook door het organiseren van een relevante cybercrisisoefening.

3. Versterken cyberweerbaarheid inwoners en ondernemers

In dit deelprogramma werken wij aan het versterken van de cyberweerbaarheid van onze inwoners en ondernemers. Menselijk handelen is een belangrijke oorzaak van waarom mensen slachtoffer worden van online delicten. Wanneer mensen zich bewust zijn van de risico's van online criminaliteit, kennis hebben over hoe ze zichzelf kunnen beschermen en zich ook daadwerkelijk gaan beschermen verkleint de kans dat ze slachtoffer worden van cybercriminelen. Dit wordt ook wel cyberweerbaarheid genoemd en is het doel van preventieve interventies. Voor slachtoffer- maar ook daderpreventie wordt samengewerkt met maatschappelijke partners als de politie, het OM, WIJ, Bureau Halt, onderwijs, bibliotheken en nog vele anderen.

Hoewel iedereen wel eens te maken heeft of zal hebben met online criminaliteit in de vorm van bijvoorbeeld phishing, zijn er een aantal doelgroepen die als extra kwetsbaar worden gezien voor specifieke online delicten.

Jongeren
Jongeren zijn oververtegenwoordigd als daders en slachtoffers van online criminaliteit. Kenmerkend hierbij is de wisselwerking tussen dader- en slachtofferschap. Er is vaak onvoldoende zicht op wat online wel en niet mag in combinatie met weinig inzicht in lange termijn consequenties. Veelvoorkomende vormen van online criminaliteit waar jongeren mee te maken krijgen zijn onder andere sextortion, geldezelen, verschillende vormen van online fraude, online pesten, etc. Iedere jongere kan hiermee te maken krijgen, maar met name de doelgroep met kwetsbare omgevingsfactoren lopen groter risico om slachtoffer of dader te worden. Er worden grofweg twee dadertypes onderscheiden: jonge opportunisten met weinig technische kennis en de cyberbreinen met bovengemiddelde IT-kennis. Een groep die tussen dader en slachtoffer in vallen zijn de geldezels. Wij zetten samen met maatschappelijke partners in op interventies voor daderpreventie, slachtofferpreventie en tegen geldezelproblematiek.

Senioren en laaggeletterden
Hoewel iedereen slachtoffer kan worden van online criminaliteit is de doelgroep senioren en laaggeletterden extra kwetsbaar voor met name online oplichting zoals whatsappfraude (vriend-in-noodfraude) en bankhelpdeskfraude. Het is een groep die vaak minder digitaal vaardig is en daardoor vaker als doelwit wordt gekozen door criminelen. Dit zorgt voor grote financiële schade en gevoelens van onveiligheid en schaamte. Voor deze doelgroep worden informatiebijeenkomsten georganiseerd met diverse lokale samenwerkingspartners om de cyberweerbaarheid te verhogen. Hierbij wordt bijvoorbeeld gebruik gemaakt van de interactieve film 'Echt of Nep?'

Midden- en kleinbedrijf (MKB)
Zoals ook inwoners heeft vrijwel elk bedrijf tegenwoordig te maken met online criminaliteit. Waar grote bedrijven kunnen investeren in de eigen cybersecurity, heeft het MKB vaak niet de mensen, middelen of de tijd om de eigen informatiebeveiliging goed op orde te brengen waardoor ze meer risico lopen slachtoffer te worden van bijvoorbeeld ransomware. MKB-ondernemers zijn vaak sterk afhankelijk van hun toeleveranciers (ketenrisico) en hun IT-leverancier (software-beveiliging). Als ze

slachtoffer worden kunnen ondernemers enorme financiële schade oplopen die soms zelfs kan leiden tot faillissement. We zetten in op bewustwording bij ondernemers over digitale veiligheid in hun bedrijfsvoering.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd.