GEMEENTE WEERT

DUS Weert
t.a.v. Peter Weekers

Weert, 10 november 2022

Onderwerp: Beantwoording vragen 27-10-2022

Beste heer Weekers,

In beantwoording op uw vragen in de brief d.d. 27-10-2022 met als onderwerp “Structurele aandacht en financiering voor informatieveiligheid op lokaal niveau”, geef ik u middels dit schrijven antwoord hierop.

1. Kunt u aangeven hoe de gemeente/ICT-NML hun rol hebben gepakt in het versterken van de digitale weerbaarheid van burgers?

In het Integrale Veiligheidsplan (IVP) van 2019 – 2022 is het thema cybercrime voor de eerste keer opgenomen als prioriteit, zodat burgers bewust bekwaam worden gemaakt omtrent cybercrime en digitale criminaliteit. In deze periode is op provinciaal niveau een taskforce cybercrime opgericht om deze gemeentegrens overschrijdende vorm van criminaliteit gezamenlijk aan te pakken in samenwerking met o.a. de politie en het OM. Onderstaand beschrijven we een aantal acties die ten uitvoer zijn gebracht in deze periode. In het aankomende IVP van 2023 – 2026 is cybercrime wederom opgenomen als prioriteit.

De gemeente Weert zet HackShield in om de digitale weerbaarheid van kinderen te vergroten. Via het landelijk cyberprogramma HackShield spelen de kinderen een game waarin ze als Cyber Agent leren om online gevaar te herkennen en te voorkomen. Het idee is dat kinderen als Cyber Agents niet alleen zichzelf, maar ook hun omgeving (ouders, opa's, oma's, broertjes, zusjes, vriendjes, vriendinnetjes en andere familieleden en bekenden) beschermen tegen online criminaliteit.

Tevens is in samenwerking met Platform Veilig Ondernemen en Gilde Opleidingen de StuDesk opgericht. De IT-studenten van Gildeopleidingen bemensen deze helpdesk om vragen te beantwoorden om de digtale veiligheid van burgers te verbeteren.

Wilhelminasingel 101
Correspondentie: Postbus 950, 6000 AZ Weert
Telefoon: 14 0495 of (0495) 57 50 00 - E-mail: gemeente@weert.nl
Website: www.weert.nl – Twitter: www.twitter.com/gemeenteweert

Daarnaast heeft het Mobiele Media Lab van de politie twee keer Weert bezocht. Tijdens de aftrap van HackShield en op de open dag veiligheid die op zondag 29 mei werd georganiseerd. Op 21 november zal het Mobiele Media Lab wederom een bezoek brengen aan Weert, in de wijk Molenakker, waar zij burgers bewust maken van digitale veiligheid. Dit is een samenwerking tussen buurtpreventie, politie en gemeente.

Vanuit communicatief oogpunt gebruiken we de gemeentelijke sociale media kanalen, zoals Facebook, om berichten te delen over online veiligheid en gebruiken we het Weerter Magazine om te delen.

2. Kunt u aangeven hoe van overheidswege de structurele aandacht en financiering ten behoeve van de preventieve en repressieve aanpak van digitale onveiligheid op gemeentelijk/lokaal niveau is/zal worden gerealiseerd?

Op gemeentelijk niveau is structurele aandacht voor digitale veiligheid in 2022 vergroot door het inzetten van een security awareness programma, waarbij ambtenaren wekelijks een digitale vraag ontvangen in het kader van informatieveiligheid en privacy. Daarnaast wordt er per kwartaal een gespecificeerde leertaak uitgebracht om de aandacht op een specifiek onderwerp te richten. Daarnaast zijn er nieuwe technische maatregelen genomen door ICTNML om de digitale onveiligheid te verkleinen en wordt er doorlopend gekeken om verdere preventieve maatregelen te nemen zoals een Security Information and Event Managementsysteem (SIEM) en een Security Operation Center (SOC).

In het kader van de ALV van de VNG is in de begroting van 2023 - 2026 een structurele verhoging van het informatieveiligheidsbudget opgenomen van ca. 15% per jaar, waarmee de gemeente Weert de digitale weerbaarheid wilt vergroten.

3. Kunt u aangeven of de processen rondom BIO en ENSIA, zodanig zijn ingericht dat niet alleen getoetst wordt of het vereiste instrumentarium aanwezig is, maar ook getoetst wordt in hoeverre dit structureel bijdraagt aan informatieveiligheid voor inwoners, ondernemers en (gemeentelijke) processen?

De processen rondom BIO en ENSIA zijn zodanig ingericht dat er ook aandacht is voor de structurele bijdrage van informatieveiligheid voor inwoners, ondernemers en de gemeentelijke processen. Er worden op diverse manieren getoetst (IT-Audit, Interne controles, Risico-analyse, ENSIA-audits) of de genomen maatregelen conform de BIO en ENSIA niet alleen aanwezig zijn, maar ook effectief en efficiënt zijn middels de Plan-Do-Check-Act methodiek. Met nieuwe initiatieven van informatieveiligheid wordt rekening gehouden met de structurele bijdrage ervan.

4. Kunt u aangeven welk deel van het ICT-budget van ICT-NML wordt ingezet voor digitale veiligheid?

Digitale veiligheid is een integraal onderdeel van de dienstverlening van ICT NML. Wij kunnen met zekerheid stellen dat meer dan 10% van de kosten gerelateerd zijn aan digitale veiligheid, hetzij direct dan wel indirect. ICT NML volgt hierbij de mondiale ontwikkelingen en indien nodig zullen we hier ook aanvullende stappen in zetten.

Hopende u hiermee voldoende te hebben geïnformeerd, verblijf ik.

Hartelijke groet,

Ron Meerts

Afdelingshoofd Informatie