Memo

Aan
Commissie Maatschappij en Welzijn

Datum
2 mei 2025

Documentnummer
366005

Auteur
J. Bertrand

Domein/Team
Domein Samenleving - Team Beleid maatschappij

Openbaarheid

Ambtelijk opdrachtgever
Domein Maatschappij - Manager team Beleid Maatschappij

Doel van de memo
Informeren

Afschrift aan

Bijlage(n)
n.v.t.

Onderwerp
Informatie voorzorgsmaatregelen inzake informatietechnologie

Aanleiding
Op de agenda van de commissievergadering Maatschappij en Welzijn van 21 mei 2025 staat het punt 'Voorzorgsmaatregelen inzake informatietechnologie' ter bespreking. Toegezegd is de commissie op dit thema te informeren en hierbij relevante heldere en toegankelijke informatie aan te leveren. Voorliggende memo vat deze informatie samen, geeft een stand van zaken en verwijst waar mogelijk naar toegankelijke informatie. Er volgt eerst een schets van de bredere context van dit thema, daaropvolgend een toelichting hoe we ons vanuit en in de gemeentelijke organisatie (verder) voorbereiden op het scenario van een cyberaanval en tot slot geven we inzicht in onze inzet om de inwoners van Heerlen hierop voor te bereiden.

Context van weerbare informatietechnologie
Vanuit het Ministerie van Justitie en Veiligheid hebben de Nationaal Coördinator Terrorismebestrijding en Veiligheid en de waarnemend directeur-generaal van Defensie sinds eind 2024 actiever gecommuniceerd over onze veiligheid als gevolg van diverse omstandigheden in de wereld (o.a. de gewapende conflicten, zoals de Russische oorlog in Oekraïne). Dit had als doel een brede bewustwording te creëren, over het feit dat onze veiligheid en vrijheid kwetsbaar zijn en dat het nodig is om de weerbaarheid van onze samenleving te verhogen. Niet met de bedoeling om angst te zaaien, maar wel om goed geïnformeerde keuzes te maken en grip te geven/krijgen op onverwachte situaties. We begrijpen dus ook dat er in dit kader meer aandacht is voor de weerbaarheid van onze digitale systemen.

Vooropgesteld goed te vermelden: deze risico's zijn in de crisisbeheersing niet nieuw sinds 2024. Bekend is dat we in brede maatschappelijke zin al

geruime tijd steeds meer afhankelijk zijn van hard- en software systemen die onderling met elkaar verbonden zijn. Zo ook onze gemeentelijke organisatie. Deze onderlinge verbondenheid schept immers vele mogelijkheden om o.a. efficiënt te werken, in netwerken samen te werken en te communiceren. Deze afhankelijkheid van systemen leidt vanzelfsprekend ook tot nieuwe risico's, zoals uitval. Daarom is in eerdere (provinciale, regionale en lokale) risicoprofielen dit risico al een tijd in beeld en zijn we voortdurend aan de slag om ons hierop voor te bereiden. Wel is het zo dat we hier op dit moment extra stappen in zetten, omdat onze afhankelijkheid van digitale systemen groot is en het risico op een aanval op deze systemen ook toeneemt.

De WRR schrijft specifiek over cyberaanvallen bijvoorbeeld in een rapport[1] dat de internationale verhoudingen "complexer, grimmiger en turbulenter zijn geworden, waarbij we ons ook meer moeten voorbereiden op digitale ontwrichting". De WRR concludeerde dat we daar als hele samenleving eigenlijk nog onvoldoende op voorbereid zijn. Aanvullend stelde de Informatiebeveiligingsdienst (IBD) in het dreigingsbeeld van 2023/2024 afgelopen jaar ook dat cyberrisico's toenemen en gaf het advies aandacht te hebben en te houden voor deze weerbaarheid. Vanuit deze context zijn we daarom al langer volop aan de slag met dit thema.

Voorzorgsmaatregelen vanuit en in de organisatie

Binnen de Veiligheidsregio Zuid-Limburg (VRZL) werken we allereerst regionaal samen om ons voor te bereiden op de scenario's van digitale verstoringen en digitale ontwrichting[2]. Deze voorbereiding bestaat onder andere uit de nodige afspraken en planvorming (denk aan opschaling in de crisisorganisatie, afspraken over multidisciplinaire inzet, operationele voorbereiding en informatieposities). Waar mogelijk zijn we hierdoor vanuit de crisisorganistie voorbereid om met dit scenario in onze regio om te gaan. Crisisfunctionarissen zijn en worden ook getraind op dit scenario. Zo is duidelijk wie welke rol pakt en op welke wijze de hulpdiensten gecoördineerd op- en afschalen, net zoals bij een fysieke ramp of crisis zoals brand of overstroming.

Sinds vorig jaar zetten we ook in onze eigen organisatie nog een stap extra:

[1] https://www.wrr.nl/publicaties/rapporten/2024/07/01/nederland-in-een-fragmenterende-wereldorde

[2] Digitale ontwrichting is een vorm van maatschappelijke ontwrichting waar een verstoring van een digitaal (ICT)-systeem aan ten grondslag ligt.

Zo zijn medewerkers en bestuurders in samenwerking met de IBD door middel van oefeningen getraind op dit scenario en is er in de organisatie een doorlopende bewustwordingscampagne rondom cyberweerbaarheid. Op dit moment zijn we verder aan de slag met actualisatie van de planvorming om de bedrijfscontinuïteit van onze organisatie, om deze ook gericht op nieuwe risico's te kunnen waarborgen. Het is echter nog te vroeg om dit plan beschikbaar te stellen; dit wordt in 2025 verder ontwikkeld. Wij zullen de commissie en/of gemeenteraad over het vervolg op de hoogte houden.

Daarnaast is de burgemeester vanuit zijn verantwoordelijkheid voor de openbare orde en veiligheid al geruime tijd bezig met het verstevigen van de voorbereiding op de gevolgen die hierop kunnen ontstaan, door een cyberaanval op de gemeentelijke organisatie of in de stad. Dit doet hij in samenwerking met de partners van de Lokale Driehoek, Politie en Openbaar Ministerie. Met deze partners wordt ook geregeld geoefend om adequaat te kunnen handelen. Zo vindt op 3 december 2025 de tweede grote Limburgse cyberoefening plaats waarbij alle Limburgse burgemeesters, Politie en Openbaar Ministerie oefenen met reële scenario's.

Bewustwording en ondersteuning inwoners rondom cyberrisico's
Zoals bekend is burgemeester Wever vanuit zijn RIEC-portefeuille namens alle Limburgse gemeenten de Cyberburgemeester. Vanuit deze rol zorgt hij voor de bevordering van samenwerking omtrent dit thema en zijn er ook voortdurend preventieve interventies om inwoners weerbaarder te maken, variërend van gamen met de politie voor jongeren tot de Echt Niet film voor ouderen.

Daarnaast bestaat er vanuit onze regionale inzet onder andere op de website van de VRZL (www.zuidlimburgveilig.nl) ook een handelingsperspectief voor internetstoringen en digitale ontwrichting: 'Wat te doen bij Internetstoring en digitale ontwrichting'[3]. De website geeft onder het menu 'Wat te doen bij…' een compleet overzicht van praktische tips en handige weetjes waardoor mensen zich goed kunnen voorbereiden zijn op allerlei soorten incidenten (en de gevolgen daarvan), zoals bijvoorbeeld wateroverlast, (langdurige) stroomuitval en storm.

[3] https://www.zuidlimburgveilig.nl/wat-te-doen-bij/internetstoring-en-digitale-ontwrichting

Ook is in dossiers op de websites van de Rijksoverheid[4] en de NCTV[5] nog meer relevante en toegankelijke achtergrondinformatie te vinden over dit thema. Daarnaast is er ook de landelijke website beschikbaar voor alle inwoners: www.denkvooruit.nl. Op deze website is ook een scenario toegelicht over cyberveiligheid[6]. Daarop staat een heldere toelichting op hoe mensen zich zelf kunnen voorbereiden en wat de verschillende instanties in dit werkveld op dit moment (kunnen) betekenen.

Ten slotte ligt er in het kader van weerbaarheid in brede zin een solide basis waar we op aangehaakt zijn: de Veiligheidsstrategie voor het Koninkrijk der Nederlanden, de Landelijke Agenda Crisisbeheersing, maar ook de NAVO Weerbaarheidsdoelen. Om de lokale en regionale dimensie hierin goed te betrekken, is er overleg met de VRZL, van waaruit we ook betrokken zijn bij het Veiligheidsberaad en de VNG over dit thema, ieder vanuit de eigen rol. Zo werken we verder aan de weerbaarheid in brede en maatschappelijke zin. Vanuit een regionale aanpak werken we op dit moment aan de concrete vervolgstappen om de weerbaarheid nog verder te verhogen. Na het zomerreces zullen wij ook de gemeenteraad hierover verder informeren.

Concluderend

We werken landelijk, in onze regio en lokaal intensief samen om Heerlen zo veilig mogelijk te maken en te houden. Dat doen we vanuit risicoprofielen en -analyses, waar de voorbereiding en preparatie op het risico van cyberdreiging zeker onderdeel uitmaakt. Om de weerbaarheid nog verder te verhogen in onze gemeentelijke organisatie én in onze gemeente, zetten we op dit moment de nodige extra stappen. Daarover houden we de commissie en/of raad vanzelfsprekend op de hoogte; informatie wordt met u gedeeld, zodra deze definitief beschikbaar is en/of openbaar kan worden gesteld.

Hoogachtend,
burgemeester en wethouders van Heerlen,
namens dezen

drs. R. Wever

[4] https://www.rijksoverheid.nl/onderwerpen/dreiging-in-nederland
[5] https://www.nctv.nl/onderwerpen/weerbaarheid
[6] https://www.denkvooruit.nl/risicos/overzicht/cybercriminaliteit