

Vergaderjaar 2020–2021

**29 517**

**Veiligheidsregio's**

**26 643**

**Informatie- en communicatietechnologie (ICT)**

**Nr. 194**

**BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 7 oktober 2020

Veiligheidsregio's spelen een cruciale rol bij crisisbeheersing. Vanuit mijn verantwoordelijkheid voor dit stelsel en tevens mijn coördinerende rol op het gebied van digitale veiligheid vind ik het van belang om uw Kamer te informeren over een recente gijzelsoftware-aanval op de Veiligheidsregio Noord- en Oost Gelderland (VNOG). Op 12 september heeft het bestuur van de VNOG mij geïnformeerd dat zij is getroffen door gijzelsoftware. Door deze aanval zijn interne systemen geraakt en werden met name de kantoorprocessen ernstig verstoord. Kritische processen zoals C2000, meldkamerprocessen en inzetprocessen voor de brandweer hebben continue gefunctioneerd. Het bestuur van de VNOG heeft aangegeven dat de veiligheid van personeel en burgers in de genoemde veiligheidsregio dan ook niet in het geding is en is geweest. Dat geldt ook voor de rol van de Veiligheidsregio bij de bestrijding van het coronavirus.

In nauwe samenwerking met zowel publieke als private partners wordt gewerkt aan spoedig herstel. Systemen die operationele informatie bevatten zijn inmiddels weer werkzaam. Inmiddels hebben de medewerkers weer toegang tot hun werkomgeving. Belangrijke voorwaarde hiervoor was dat de beveiliging voor thuiswerken op orde is.

Het Nationaal Cyber Security Centrum heeft op verzoek van de VNOG initieel incident response geleverd en geholpen bij de start van het herstel. Met specialisten en deskundigen, van onder meer landelijke autoriteiten, waaronder de politie, is door de VNOG onderzocht of de aanvallers toegang tot data hebben gekregen en wat de gevolgen zijn. De conclusie is dat er geen data-exfiltratie heeft plaatsgevonden. De aanval is meteen gemeld bij de politie en er is aangifte gedaan.

De besturen van veiligheidsregio's zijn primair zelf verantwoordelijk om te zorgen voor weerbaarheid van de ict-systemen van de eigen regio's. Zij leggen hierover verantwoording af in de eigen regio. Het Veiligheidsberaad ziet digitale weerbaarheid als één van haar strategische aandachtspunten. In dit kader werken veiligheidsregio's onder meer actief mee aan

collegiale toetsing van informatieveiligheid. Veiligheidsregio's voeren die gezamenlijk uit en zij volgen eventuele aanbevelingen die hieruit voortkomen actief op. Hiertoe hebben zij zich ook georganiseerd in een Information Sharing and Analysis Centre (ISAC) waarin alle regio's deelnemen.

Naar aanleiding van de gijzelsoftware-aanval bij VNOG wordt er door de veiligheidsregio's geïnvesteerd in extra veiligheidsmaatregelen waaronder een actieve security monitoring via een extern SOC (Security Operations Center). Daarnaast is er veel aandacht voor het handelen en het gedrag van mensen.

Ik ben van mening dat het goed functioneren van veiligheidsregio's van essentieel belang is voor risico- en crisisbeheersing. Er wordt daarom alles aan gedaan om herhaling van een dergelijke aanval op veiligheidsregio's in den brede te voorkomen. Alle relevante partijen zijn en blijven alert en betrokken.

De Minister van Justitie en Veiligheid,  
F.B.J. Grapperhaus