Van	Carol van Eert
Aan	Algemeen Bestuur
Ingekomen stuk	2
Datum	03-04-2017
Onderwerp	Cybersecurity-veiligheidsregio's
Telefoon	
E-mailadres	

Memo

Vorig jaar is Marijke van Veen gevraagd door de Blomberg Society om in het kader van de Innovatie Challenge Veilige Samenleving/Don Berghuijs Award 2016, vraageigenaar te worden van het thema 'Vitale sectoren – maatschappelijke continuïteit'. Dit thema is vertaald in 'veiligheidsregio's en veiligheid digitale infrastructuur'.

Samen met een team, dat is samengesteld uit mensen van kennisinstellingen (zoals UvA, RU Leiden, Haagse Hogeschool), bedrijven (o.a. Stedin, Gasunie, Centric, Fox-IT, Antea), NCTV en veiligheidsregio's (Twente en Gelderland-Zuid) is gezocht naar een innovatieve oplossing voor de veiligheidsregio's.

Op 11 mei wordt bekend gemaakt wie de Don Berghuijs Award 2017 wint. In de jury zitten o.a. Ben Ale (voorzitter), Siebe Riedstra (S-G Min VenJ), Han Moraal, generaals Gino van der Voet en Nico van der Zee en Martin Sitalsing (Lentis).

Het vraagstuk waarvoor een oplossing gezocht wordt luidt:
"Hoe kunnen veiligheidsregio's de samenwerking met de stakeholders versterken zodat zij de fysieke en maatschappelijk effecten van cyberincidenten voor uiteindelijk de burger kunnen minimaliseren, ondanks de toenemende hoeveelheid cyberincidenten?"

<u>Context</u>
Cybersecurity: misschien niet het eerste onderwerp waar je aan denkt bij een veiligheidsregio. Toch is het niet zo ver gezocht. Veiligheidsregio's gaan in essentie over het voorkomen en beheersen van crises. Branden blussen, mensen evacueren, reanimeren en vervoeren naar ziekenhuizen. Steeds meer richten zij hun aandacht op het voorkomen van crises. Om dat te kunnen moet je wel weten welke risico's er zijn, want dan kun je gericht sturen op voorkomen. Wij noemen dat risicogerichtheid.

We zien in een relatief kort tijdsbestek nieuwe risico's ontstaan waarvan we de aard en de omvang nog niet goed kennen. Digitale risico's: cyberaanvallen en cybercriminaliteit. We weten dat deze kunnen leiden tot grote en onbekende effecten. Bedenk wat de gevolgen zijn van het openzetten van sluizen, het laten ontsnappen van gifwolken of het platleggen van de meldkamers. We weten dat

deze incidenten en crises vaker kunnen gebeuren, dat onze inwoners hierdoor vaker gevaar lopen en dat veiligheidsregio's dus vaker in actie moeten komen. Dat heeft ook bestuurlijke impact: er wordt bij crises door onze inwoners eerst naar de gemeenten en naar ons gekeken, ongeacht of we er wel of niet over gaan.

Risicogerichtheid past hier ook. Ons belang en het belang van (risicovolle) bedrijven is continuïteit van de samenleving en dus het voorkomen van crises ten gevolge van cyberaanvallen. Omdat we een gedeeld belang hebben, kunnen we komen tot een gezamenlijke aanpak.

Innovatieve oplossing

Het plan is om op het geografische niveau van de veiligheidsregio een kennisnetwerk te organiseren, waarin bedrijven, kennisinstellingen en veiligheidsregio's zitten. In een vertrouwelijke setting delen zij hun kennis en ervaringen, hun aanvals- en verdedigingsinformatie om van elkaar te leren wat werkt. Daardoor zijn zij zelf beter in staat cybersecurity te organiseren. Voor de veiligheidsregio's biedt dit platform ook een goede ingang om zich beter voor te kunnen bereiden op incidenten die het gevolg zijn van cyberattacks. Het voordeel van deze aanpak op regionaal niveau is dat veel partners elkaar vaker tegenkomen, alleen nog niet als het gaat om cyberveiligheid.

Mij lijkt het mooi als we dit als Algemeen Bestuur allemaal ondersteunen en het initiatief verder op weg helpen. Wij krijgen daarbij ook hulp o.a. vanuit het innovatieteam.