provincie Zuid-Holland

Antwoord van Gedeputeerde Staten op vragen van

E.W. Kegel
(d.d. 30 juni 2022)

Nummer
3870

Onderwerp
Cybersecurity provincie Zuid-Holland

Aan de leden van Provinciale Staten

Toelichting vragensteller

Deze schriftelijke vragen zijn naar aanleiding van de brief van gedeputeerde de Zoete (getiteld " Toezegging Statencommissie RWE inzake cybersecurity" van 29 april 2022. In de commissievergadering BMM van 29 juni 2022 is afgesroken dat deze vragen schriftelijk worden ingediend. De bedoelde brief geeft op hoofdlijnen zicht op de wijze waarop de provincie de cybersecurity heeft ingericht. Maar in de ogen van Forum van Democratie is deze brief te algemeen en gaat deze niet in op een aantal specifieke zaken die voor de provincie van toepassing zijn. We beseffen ons dat de gestelde vragen misschien niet in alle gevallen in openbaarheid zijn te beantwoorden. Wij verzoeken u dan een modus te vinden op basis waarvan we wel van deze informatie kennis kunnen nemen.

In talloze artikelen is in de afgelopen jaren stil gestaan bij het fenomeen cybersecurity en cyberaanvallen. Daarbij valt het op dat de aanvallers zich met name richten op organisaties en componenten die een belangrijke maatschappelijke spilfunctie vervullen, omdat daar de potentiële schade het grootst is en er door middel van het eisen van ransomware voor hun het meeste geld te verdienen valt[1][2].

1. *NCSC wordt gevolgd voor wat betreft de adviezen. Wat uit brief niet duidelijk blijkt of dat ook het door NCSC gepropageerde Zero Trust model wordt gevolgd bij de implementatie van veiligheidsmaatregelen. De essentie van het model komt er op neer dat niet alleen van buitenaf de infrastructuur verdedigd wordt, maar dat ook van binnenuit uitgebreide beveiligingsmaatregelen worden doorgevoerd (don't trust, but verify-principe). In hoeverre wordt dat model gevolgd binnen de provincie Zuid-Holland?*

Antwoord
Het Zero Trust model is een van de uitgangspunten die gehanteerd worden bij de implementatie van veiligheidsmaatregelen binnen provincie Zuid-Holland. Denk hierbij aan het aanbrengen van scheidingen in het netwerk (segmentering), het toepassen van multifactorauthenticatie en het uitbreiden van logging en monitoring. Veiligheidsmaatregelen worden continu heroverwogen en doorontwikkeld. De principes

[1] https://www.nctv.nl/themas/cybersecurity/nieuws/2020/06/29/nctv-cyberincidenten-kunnen-onze-maatschappij-verlammen

[2] Cobouw 8-9-2021: Ethische hackers luiden noodklok: infra kwetsbaar voor cyberaanvallen

van het Zero Trust model zullen daardoor de beveiliging van steeds meer in gebruik zijnde systemen en identiteiten gaan verbeteren.

2. *De brief geeft geen zicht op de sterk veranderde situatie met het thuiswerken sinds 2020 en de gevolgen daarvan voor de cybersecurity. In hoeverre is het risicoprofiel van de beveiliging van de provincie hierdoor verhoogd of veranderd?*
Welke maatregelen zijn genomen om (nieuwe) risico's te mitigeren?

Antwoord
Thuiswerken is een IT-voorziening die al lange tijd in gebruik is binnen de provincie. Deze voorziening wordt met regelmaat gecontroleerd of het voldoet aan de laatste beveiligingsstandaarden. Sinds het uitbreken van de Coronapandemie is het gebruik van thuiswerkfaciliteiten sterk toegenomen, waardoor het risicoprofiel van de voorziening voor de provincie is veranderd. De continuïteit van de provincie is er immers afhankelijker van geworden. Met name de capaciteit van de voorziening is uitgebreid, zoals de access gateway en de dataverbinding. Ook zijn gebruikers nadrukkelijker geïnformeerd over specifieke risico's rond thuiswerken en voorzien van richtlijnen (bijv. 'Thuiswerken? Zo doe je het veilig'). Provincie Zuid-Holland is zich ervan bewust dat het risicoprofiel continu verandert. Recent is wederom een onderzoek afgerond naar de toekomst van hybride werken en de thuiswerk-voorzieningen in het bijzonder. De aanbevelingen die hierin zijn gedaan worden op kort mogelijk termijn doorgevoerd, denk o.a. aan:

- Opnieuw beschouwen van de effectiviteit van PZH-laptops en smartphone.
- Verhogen van de monitoring van remote toegang.
- Opstellen en uitvoeren van strategie / visie op telewerken.

3. *Wat is de reikwijdte qua cyber security die met deze brief beoogd wordt: hebben we het hier over kantoorachtige systemen (DMS, zaaksystemen, tekstverwerking e.d.) die door de ambtenaren op (thuis-)lokatie gebruikt worden of wordt ook over systemen die processen besturen, zoals de bediening van bruggen, sluizen e.d..? Systemen die processen besturen zijn interessanter voor cyberaanvallers vanwege (maatschappelijke) impact en hebben daarom ook een hoger risicoprofiel (zie artikel FD[3]).*

Antwoord
De brief heeft betrekking op kantoorautomatisering.

4. *In hoeverre hebben de systemen die voor processen als bediening van bruggen en sluizen gebruikt worden afhankelijkheid van buitenlandse ondernemingen?*
Vormt eventuele afhankelijkheid een (in)directe bedreiging voor de continuïteit van deze processen?

Antwoord
Voor de bediening van onze bruggen en sluizen maken wij ook gebruik van buitenlandse systemen en ondernemingen. Dit vormt echter geen bedreiging of risico voor (de continuïteit van) de bedienprocessen. De afhankelijkheid van de betreffende buitenlandse ondernemingen wordt ook door het Nationaal Centrum voor Cyber Security niet als risico gezien. Overigens gaan we uiteraard bewust geen samenwerking aan met landen die een "offensief cyberprogramma" hebben tegen Nederland, zoals China, Iran en Rusland.

5. *In de brief wordt genoemd dat universiteiten en hogescholen worden bijgeschakeld bij ethical hacking van provinciale systemen. Nu zijn aan deze instituten buitenlandse studenten verbonden.*

[3] Financieel Dagblad 8-5-2021: Cyberaanval legt grote brandstof pijplijn in Amerika plat

Welke waarborgen zijn er dat deze hackers op een gegeven moment minder ethical optreden, informatie achterhouden en deze doorspelen naar mogelijk vijandige actoren en staten?

Antwoord
Uitvoering van securityassessments (pentest) en de samenwerking met universiteiten en hogescholen staan los van elkaar. We schakelen geen studenten in voor ethical hacking van provinciale systemen. Provincie Zuid-Holland werkt samen met een onafhankelijke en gecertificeerde ethical hackers (via een beveiligingsbedrijf). Met dit bedrijf is een driejarig contract overeengekomen. Onderdeel van het contract is een geheimhoudingsverklaring.
De samenwerking met universiteiten en hogescholen is gericht op het vergaren van kennis, bijvoorbeeld door onderzoek te doen naar de digitale veiligheid van Greenport West-Holland. Onderzoek is gedaan in samenwerking met de opdrachtgevers Greenport West-Holland en Security Delta (HSD) en is uitgevoerd door de Haagse Hogeschool (Kenniscentrum Cybersecurity). De financiering voor dit onderzoek is afkomstig van provincie Zuid-Holland.

Den Haag, 4 augustus 2022

Gedeputeerde Staten van Zuid-Holland,

secretaris,	loco-voorzitter,
drs. H.M.M. Koek	E.F.A. Zevenbergen