Vragen Commissie Bestuur 21 januari 2022

CU, Jan Henk Verburg, over Brief GS van 9 november 2021 over Voortgangsrapportages grote projecten en risicoparagraaf augustus, september en oktober 2021 - 104880, agendapunt 7

Vragen Commissie Bestuur	Antwoorden
1. In de risicoparagraaf is de volgorde ongewijzigd. Op plaats 6 staat cybersecurity. Na de citrix en Log4j komen steeds weer nieuwe kwetsbaarheden naar boven, dit jaar wordt een golf aan aanvallen door hackers verwacht. Waarbij sprake kan zijn van ontwrichting van de samenleving (Bron: NCSC). Betekent de relatieve stilstand van het risiconiveau dat Provincie Zeeland extra investeert in cyberweerbaarheid? Hoe heeft men de laatste grote kwetsbaarheid rond Apache Log4j kunnen verhelpen?	1. Het risiconiveau van cybersecurity is onverminderd groot en het dreigingsbeeld wordt continu gemonitord. Ook is er voor cybersecurity extra budget vrijgemaakt om aan te wenden voor bewustwording bij de medewerkers. Daarnaast wordt er door CISO en Senior adviseur Beveiliging continu op toe gezien dat alle systemen van de provincie zijn en worden voorzien van de laatste updates van de software. De Senior adviseur Beveiliging houdt ook voortdurend het darkweb in de gaten om dreigingen tijdig voor te zijn. De Log4J-kwetsbaarheid was daardoor al bij Provincie Zeeland in beeld én gemitigeerd voordat het NCSC met de melding kwam. Meteen op 7 december is opgeschaald naar een interprovinciaal crisisteam (alle CISO's van de provincies) en intern naar een crisisberaad. Ook zijn provinciesecretaris en gedeputeerde continu op de hoogte gehouden door de CISO. Al onze systemen zijn meteen diepgaand gescand en er waren geen sporen van besmetting. Uit voorzorg is wel de volledige backup van 1 december geïsoleerd om in het uiterste geval uitweg te bieden bij een ransomware aanval. Alle provincies hebben meteen verhoogde dijkbewaking ingesteld waarbij 24/7 de systemen in de gaten werden gehouden. Er zijn inderdaad meerdere aanvallen op onze systemen geweest maar die zijn effectief tegengehouden door de firewall. Alle leveranciers van onze systemen en software zijn benaderd en bevraagd op hun eigen kwetsbaarheid. Die systemen waar een kwetsbaarheid in zou kunnen zitten zijn tijdelijk uitgeschakeld en pas wanneer de leverancier kon aantonen dat een patch afdoende was weer ingeschakeld. Op 31 december zijn de genoemde crisisteams afgeschaald naar het niveau van normale waakzaamheid.