Onderwerp: Datalek bij uitvoeringsorganisatie BIJ12

Preambule van GS
U heeft deze vragen gesteld ter voorbereiding van de commissie van woensdag 17 februari. Wij hebben ons best gedaan ze zo goed mogelijk te beantwoorden. Vanwege het feit dat ICT-experts van de provincie Utrecht maar zijdelings betrokken zijn bij BIJ12 hebben we de antwoorden voor een groot deel buiten de organisatie moeten zoeken. Het blijven natuurlijk de antwoorden van GS. Wel vragen we vooraf uw begrip voor het feit dat ook woensdag dit gebrek aan kennis in de organisatie ons parten kan spelen. Op sommige vragen zullen wij schriftelijk terug moeten komen.

Graag wijzen wij u er ook op dat de reden voor geheimhouding voor de eerste brief, dat we hackers niet willen wijzen op de kwetsbaarheden, is weggevallen en dat die brief daarmee openbaar is geworden.

Vragen ingediend door de fracties van: JA21, VVD, PVV en SGP
Agendapunt 3.7 BEM 17 februari 2021

Achtergrond
In een brief van 26 januari kenmerk 2021BEM021 geeft u aan dat er op 25 januari een aantal ICT systemen bij uitvoeringsorganisatie BIJ12 tijdelijk offline zijn gezet als noodzakelijke voorzorgsmaatregel omdat er kwetsbaarheden zijn geconstateerd in de beveiliging van deze systemen. Wanneer deze kwetsbaarheden precies zijn geconstateerd, wordt niet duidelijk uit uw schrijven. Wel staat er dat er tot dit moment nog geen concrete sporen van inbreuk zijn geweest.

U heeft hier ook een geheime brief over gedeeld met uw Staten alleen zullen wij hier verder niet uit citeren omdat onze fracties graag willen dat de antwoorden op deze vragen openbaar zijn.

Tevens lezen wij in een artikel in het Noordhollands Dagblad van 29 januari over ditzelfde onderwerp, dat de kwetsbaarheden al maanden bekend waren, alleen dat de provincies tot dat moment amper hebben ingegrepen. Het artikel beschrijft dat er al maanden geleden een ICT rapport lag, dat de kwetsbaarheden bloot heeft gelegd. Pas nadat er een tweede rapport is verschenen, dat ongeveer hetzelfde constateerde is, actie ondernomen.

Vragen
Onze fracties hebben daarom de volgende schriftelijke vragen bij deze Statenbrief:

- Volgens de brief 2021BEM021 zijn er kwetsbaarheden geconstateerd. Op welke datum zijn deze kwetsbaarheden voor het eerst geconstateerd?
  Beveiliging is een continu proces. Dat een aantal applicaties geleidelijk aan het verouderen is, was bij BIJ12 al langer de situatie. Daarop zijn ook steeds maatregelen genomen, maar beperkt van scope. Als applicaties verouderen dan ontstaat het moment dat ze moeten worden vernieuwd. Een aantal applicaties stond al op de nominatie om een herbouw-beslissing over voor te leggen. In december 2019 zijn de kwetsbaarheden bij BIJ12 mondeling gedeeld in een overleg met de provinciale ICT security experts. Tijdens dit overleg leek het er op dat de kritische kwetsbaarheden

allemaal zeer snel opgelost konden worden en dat de overige kwetsbaarheden verholpen konden worden in 2020. BIJ12 is hier toen direct mee gestart.

Wat in het najaar 2020 nieuw was, is dat BIJ12 geconcludeerd heeft op basis van een rapportage van een ICT-dienstverlener dat het verouderingsproces van diverse applicaties geleidelijk aan zover gevorderd was dat het niet langer verantwoord was om maatregelen gefaseerd te plannen rond voorzieningen die open blijven.
Een belangrijke rol in die afweging was mede dat de risico's van de achterblijvende ICT-veiligheid de laatste jaren geleidelijk aan veel groter zijn geworden. Dit is door de provinciale security-experts ook nadrukkelijk naar voren gebracht bij BIJ12.
Bij de beslissing om nu offline te gaan is de doorslag uiteindelijk gegeven doordat er brede bekendheid van de kwetsbaarheden dreigde te ontstaan. Als zoiets in de publiciteit komt, dan is dat in de regel aanleiding voor verhoogde aandacht. In de huidige cyber-wereld verandert een kwetsbaarheid daardoor in een risico. Daarom wilde BIJ12 nu niet meer volstaan met de aanpak om de "winkel tijdens de verbouwing open te houden".

De recente maatregelen zijn dus een verschuiving van de aanpak. BIJ12 had de reparaties en herbouw liever gedaan terwijl de winkel open was gebleven. Eerder was het idee dat dit kon, mede omdat er nooit inbreuken waren gevonden. Maar in deze gewijzigde omstandigheden vond BIJ12 dat risico niet meer aanvaardbaar en heeft het IPO bestuur uit voorzorg besloten tot het offline halen van de applicaties.

Consequentie daarvan is uiteraard wel dat het proces van herstel en herbouw in een sterk versneld tempo moest worden aangepakt om de onderbroken dienstverlening weer zo snel mogelijk te herstellen. Dat is wat BIJ12 nu doet.

- Op welke manier zijn deze kwetsbaarheden geconstateerd? Is er een rapport opgesteld dat de kwetsbaarheden constateerde? En indien dit het geval is, wat was de trigger om dit rapport op te laten stellen?

  De kwetsbaarheden zijn geconstateerd naar aanleiding van een adviesrapport van een ICT-dienstverlener. Het advies is door de ICT-dienstverlener opgesteld in het kader van het reguliere beheer en onderhoud van de systemen. Nadat dit door BIJ12 is ingebracht in het interprovinciaal overleg van ICT-security-experts is er door een van de provincies een extra scan uitgevoerd op de netwerkvoorzieningen in beheer van BIJ12. Daar kwam uit naar voren dat de systemen verouderd zijn en daarmee kwetsbaar. Dat is aanleiding geweest voor het offline halen van systemen en voor BIJ12 om een gespecialiseerd bureau te laten onderzoeken over welke kwetsbaarheden we het hebben en of daar door kwaadwillende gebruik van is gemaakt. Dit onderzoek is nog niet afgerond.

- Als dit niet geval is, hoe zijn de kwetsbaarheden dan aan het licht gekomen?
  Zie bovenstaande antwoord.

- Kunt u specifieker zijn over wat voor kwetsbaarheden het gaat?

De kwetsbaarheden betreffen situaties waarbij het voor, eventuele, niet geautoriseerden en/of kwaadwillenden mogelijk is om ongeautoriseerd toegang te hebben tot een systeem en/of gegevens in te zien. Het kunnen kwetsbaarheden zijn zoals bijvoorbeeld achterstallige patches en updates, verouderde software, operating systems (OS) die niet meer actueel zijn (i.v.m. verouderde software (end-off-life).

- Als er een rapport is opgesteld, kunt u dan een kopie van dit rapport delen met de Staten?
  Zie eerder antwoord. Het betreffende advies is eigendom van BIJ12. De scan door een andere provincie is eigendom van die provincie. Het rapport van het gespecialiseerde bureau wordt bij oplevering eigendom van BIJ12. BIJ12 heeft aangegeven dat zij het IPO-bestuur hierover zal informeren. Daarna kunnen wij daarover aan u rapporteren.

- Wanneer verwacht u dat het onderzoek naar de inbreuken op de systemen wordt afgerond?
  BIJ12 verwacht het onderzoek in maart af te ronden.

- In de brief staat dat sommige applicaties zodanig lek zijn dat ze opnieuw moeten worden opgebouwd? Hoe kan het zijn dat deze kwetsbaarheden niet eerder zijn opgemerkt?
  Sommige applicaties zijn sterk verouderd. Er zijn door BIJ12 maatregelen genomen maar met de genomen maatregelen waren de kwetsbaarheden nog niet verholpen. Om de kwetsbaarheden structureel te verhelpen is de verwachting dat voor deze applicaties herbouw nodig is.

- Het lek is gemeld bij de AP, wanneer?
  BIJ12 heeft eind januari 2021 een pro forma melding gedaan bij de Autoriteit Persoonsgegevens. Hoewel er, voor zover tot op heden bekend, geen inbreuk of diefstal van (persoons)gegevens is geconstateerd, is wel tot een pro forma melding besloten omdat er door de kwetsbaarheden een data-beveiligingsrisico bestond.
  Er is dus voor zover tot nu toe bekend geen 'datalek' geweest en er is dus ook geen melding van een 'lek' gedaan, alleen een melding van een mogelijk risico.

- Valt dit binnen de wettelijke termijn van 72 uur, nu de problemen al maanden bekend lijken te zijn?
  De termijn van 72 uur die in de AVG wordt gesteld voor het melden van een datalek vangt aan bij ontdekking van het datalek. In de situatie van BIJ12 is geen sprake van het aantoonbaar plaatsvinden van een datalek. De gezamenlijke Functionarissen Gegevensbescherming vonden de geconstateerde kwetsbaarheid zo groot dat er voldoende aanleiding lag om het risico op een datalek te melden. Er is tot op heden geen aanwijzing dat er daadwerkelijk gegevens door derden zijn gezien. Mocht een datalek geconstateerd worden dan zal BIJ12 dat binnen de gestelde termijn melden van de AP.

- Zo ja, zijn de (mogelijke) getroffenen van het datalek geïnformeerd? Op welke wijze?
  De betrokkenen zijn hierover niet geïnformeerd omdat voor zover bekend geen datalek heeft plaatsgevonden. De AVG schrijft het informeren voor wanneer sprake is van een

hoog risico voor de privacy van betrokkenen. Nu (nog) niet is vastgesteld dat er toegang is geweest door onbevoegden (alleen de kans op) én het soort gegevens weinig gevoelig is (voornamelijk NAW-gegevens), is geen sprake van een hoog risico. Mocht uit onderzoek blijken dat dit risico hoger is dan nu wordt ingeschat, zullen de betrokkenen alsnog worden geïnformeerd door BIJ12.

- Kan GS meer in het algemeen reflecteren hoe dit heeft kunnen gebeuren?
  GS komt tot de conclusie dat het belangrijk is bij samenwerkingsverbanden en -partners te borgen dat de databeveiliging goed op orde is. Het college is geschrokken dat dit kennelijk en vooralsnog bij BIJ12 onvoldoende is gewaarborgd. Daar worden momenteel acties op ondernomen. Bij GS leeft het besef dat ook andere samenwerkingspartners namens de provincie Utrecht gegevens beheren. We willen daarom dat breed wordt gekeken of de afspraken die we hierover hebben gemaakt met partners afdoende zijn. GS zal daarnaast in de besturen van verbonden partijen aandacht vragen voor databeveiliging.

- Kan GS aangeven welke applicaties nu niet meer beschikbaar zijn? Wat betekent dit voor de dienstverlening van BIJ12?
  Het betreft onderstaande applicaties. Deze applicaties zijn in een beveiligde omgeving geplaatst en zijn nu vandaaruit beschikbaar gesteld aan provincies en andere overheden en ketenpartners. Daarnaast heeft BIJ12 een loket ingericht zodat vragen worden beantwoord van burgers en bedrijven die geen toegang tot de applicaties hebben.

PDBS	Provinciaal Depot Beheer Systeem/Archeodepot
CDS 2.0	Centrale Data- en Services (CDS)
IBIS	Integraal Bedrijventerreinen Informatie Systeem
LGR	Landelijk Grondwater Register (LGR)
LZR	Zwemwater portaal en register
Provisa	Provinciale Selectielijst Archieven
RK	Risicokaart NL
SNL 2.0	Applicatie Subsidiestelsel Natuur en Landschap
NDVH	Nationale Databank Vegetatie en Habitats

- Hoe worden inwoners en/ of bedrijven geraakt die afhankelijk zijn van de offline gehaalde informatie?
  Zover bekend betreft het geen informatie waar bij inwoners of bedrijven grote afhankelijkheid speelt omdat de meeste systemen vooral of zelfs alleen maar ambtelijke gebruikers kennen. We hebben de mogelijkheid om voor individuele accounts toegang te creëren voor inwoners of bedrijven.
  Het ook door BIJ12 verzorgde 'mijn.faunazaken' (waar veel agrarische bedrijven op inloggen om fauna-schade te melden) is opengebleven omdat kwetsbaarheden in dat systeem direct konden worden opgelost.

- Worden en zijn ze eventueel al gecompenseerd?
  Daar is geen aanleiding voor, zie bovenstaande antwoord.

- Is inmiddels geregeld dat zij op een andere manier toegang krijgen tot deze informatie?
  BIJ12 heeft een loket ingericht zodat vragen worden beantwoord van burgers en bedrijven die geen toegang tot de applicaties hebben.

- Kan GS een inschatting geven van de kosten die hiermee gemoeid zijn, met het repareren van deze data lekken?
  Op dit moment is er door het IPO nog geen becijfering van de kosten gemaakt voor het repareren van de kwetsbaarheden . Los van deze incidentele kosten kunnen er structurele kosten naar boven komen om dit soort risico's in de toekomst te voorkomen. Dat wordt momenteel in beeld gebracht en vervolgd via de reguliere P&C cyclus van het IPO en daarmee ook de Provincie Utrecht.

- Kan GS aangeven of dit binnen de bestaande begroting kan worden opgelost of dat hiervoor extra middelen voor nodig zijn? En zo ja? Als dat laatste het geval is, aan hoeveel extra middelen moeten we dan denken?
  Het is aannemelijk dat het oplossen van de betreffende kwetsbaarheden niet mogelijk is binnen de bestaande begroting van BIJ12. In de voorjaarsnota van het IPO zal er meer duidelijk worden over de kosten en de dekking daarvan. Datgene dat niet gevonden kan worden binnen de begroting van het IPO zal door de provincies moeten worden opgebracht. De provincie Utrecht zal hier dan ook een proportioneel deel van moeten dragen.

Verder hebben de fracties de volgende vragen met betrekking tot het stuk in het Noord Hollands dagblad

- Is GS bekend met het stuk in het Noord Hollands dagblad van 29 januari 2021 over dit onderwerp?
  Ja, GS heeft kennis genomen van het gepubliceerde artikel in het Noord Hollands dagblad van 29 januari 2021

- Klopt het wat het stuk schrijft dat er enkele maanden geleden een rapport van een ICT leverancier lag dat constateerde dat de systemen kwetsbaar waren?
  Ja, dit is correct.

- Indien ja, kunnen wij een afschrift hiervan krijgen?
  De betreffende rapportage bevat tot op detail niveau beschreven de gevonden kwetsbaarheden. Het openbaar maken van deze kwetsbaarheden is vanuit het oogpunt van informatiebeveiliging dan ook niet wenselijk. Zoals eerder aangegeven stellen wij u voor u eventueel het rapport het gespecialiseerde bureau op te sturen dat in opdracht van BIJ12 wordt opgesteld en naar verwachting in maart wordt opgeleverd. Het rapport wordt overigens opgesteld voor de ambtelijke staf en is minder gericht op leesbaarheid voor en door PS.

- Indien ja, wanneer was u van dit rapport op de hoogte?

Op 10 december 2020 kwamen de eerste signalen bij GS dat er problemen waren bij BIJ12 via een nieuwsbericht vanuit het IPO.

- Klopt het dat er in december opnieuw een rapport lag met een vrijwel identieke inhoud?
  Nee, het zogenaamde 'tweede rapport' zoals genoemd in het krantenartikel betreft niet een herhaling van de reguliere leveranciers-rapportage van september, maar uitkomsten van de extra uitgevoerde 'vulnerability-scan'. Die uitkomsten bevestigden wel dat er serieuze kwetsbaarheden waren. Dit was aanleiding voor de afweging die leidde tot het afsluiten van de betreffende applicaties.

- Indien ja, kunnen wij ook hiervan een afschrift krijgen?
  De betreffende rapportage bevat tot op detail niveau beschreven de gevonden kwetsbaarheden. Het openbaar maken van deze kwetsbaarheden is vanuit het oogpunt van informatiebeveiliging dan ook niet wenselijk. Zoals hierboven aangegeven stellen wij voor het rapport af te wachten dat in maart wordt opgeleverd in opdracht van BIJ12. Eventueel kunnen we verzoeken of dit rapport aan u kan worden verstrekt. Wel tekenen we daarbij aan dat het doel van het rapport is informatiespecialisten te informeren en het niet is geschreven voor GS-en of PS-en.

- Klopt het feit uit het krantenartikel dat er een vergadering van informatie beveiligers in december 2019 is geweest waar zij 'enorm geschrokken' zijn en het liefst de stekker er direct uit getrokken hadden zodat de applicaties niet meer beschikbaar waren?
  Volgens ons doelt u op een CIBO vergadering van december 2020 waarin door een aantal leden is aangegeven dat zij enorm geschrokken waren van de bevindingen en dat de betreffende personen het liefst de betreffende systemen onbereikbaar zouden maken voor de buitenwereld. In die vergadering is door een aantal leden echter ook al aangegeven dat er altijd een afweging is met het belang van de continuïteit in bepaalde voorzieningen. Sommige applicaties zoals de Risicokaart kunnen niet goed gemist worden.
  Hierboven is aangegeven hoe en waarom die afweging tussen het security-belang, behartigd door deze functionarissen, en het belang van de uitvoering van (wettelijke) taken, behartigd door inhoudelijk verantwoordelijken uiteindelijk is beslecht door de directie van IPO/ BIJ12 in een voorstel aan het IPO-bestuur.

- Kan GS een afschrift van dit gespreksverslag delen met de Staten?
  Dit zouden we moeten afstemmen met de andere provincies. Zoals hierboven aangegeven adviseren wij u te wachten op de reflectie op het rapport van het gespecialiseerde bureau dat momenteel plaatsvindt.

- Kan GS uitleggen waarom de applicaties niet werden stilgelegd 1) na verschijning van het eerste rapport, 2) na verschijning van het tweede rapport of 3) de genoemde vergadering. Graag een duidelijke toelichting bij elk van drie genoemde punten in de tijd.
  De afweging om systemen offline te halen is geen eenvoudige afweging. Dit besluit kan slechts genomen worden na beraadslaging in het IPO-bestuur. Zoals hierboven beschreven was de hoop de noodzakelijke beveiligingsslag te kunnen maken zonder

dat de dienstverlening geraakt zou worden. Toen de conclusie genomen moest worden dat dit niet meer mogelijk was, zijn de systemen in een beveiligde omgeving te plaatsen en slechts beperkt toegankelijk te maken.

- Kan GS uitleggen waarom er op 25 januari er wel voor is gekozen de applicaties stil te leggen, terwijl het onderzoek dat in december werd ingezet nog niet is afgerond en volgens de brief van GS tot nu toe geen ongerustmakende resultaten lijkt op te leveren?
  De kans op het openbaar worden van de kwestie en daarbij het toenemende risico op hacks op BIJ12, noopte BIJ12 om de applicaties in een beveiligde omgeving te plaatsen en zo de dienstverlening naar provincies en andere overheden te kunnen continueren. Dit was eerder niet gebeurd omdat de hoop was dat kwetsbaarheden konden worden opgelost terwijl de applicaties online bleven.

- Kan GS uitleggen, zoals het krantenartikel constateert, dat er grootschalig achterstallig onderhoud is op de ICT afdeling van BIJ 12.
  BIJ12 is een samenwerkingsverband tussen de verschillende provincies. BIJ12 beheert onder meer applicaties voor de provincies. Sommige applicaties kunnen na verloop van tijd niet meer worden beveiligd met updates. De afweging om al of niet tot herbouw over te gaan is achteraf gezien soms langer blijven liggen dan wenselijk was, mede omdat voor betrokkenen niet voldoende helder was wie daarover zou moeten beslissen. Duidelijk is dat daar door de opdrachtgevers van de applicaties ook te weinig gestuurd is op het onderhoud en de beveiliging en dat hier ook te weinig budget voor beschikbaar is gesteld. Op dit moment is de directie van IPO/BIJ12 de nodige stappen aan het zetten om dit voor de toekomst te voorkomen.

- Als er een rapport is van enkele maanden geleden, kan GS dan aangeven waarom er bestuurlijk niets mee is gebeurd. Waar en bij wie is dit rapport precies blijven hangen?
  Zoals aangegeven, BIJ12 heeft het CIBO op 14-09-2020 de betreffende rapportage verstrekt. Die hebben aan BIJ12 gevraagd actie te ondernemen. Daarop is ambtelijk overleg gevolgd over de aanpak. Begin december zijn de leden van het IPO-bestuur geïnformeerd. Op 25 januari 2021 is het eerder genoemde besluit voorgelegd aan het IPO bestuur toen bleek dat de problemen niet snel te verhelpen waren en de risico's op datalekken opliepen.

- Heeft GS van de provincie Utrecht als lid van het bestuur van BIJ 12 eerdere signalen ontvangen dat de ICT niet op orde was?
  GS is geen lid van het bestuur van BIJ12. BIJ12 is een uitvoeringsorganisatie van het IPO en GS is lid van het bestuur van het IPO. GS heeft als zodanig geen eerdere signalen ontvangen anders dan hiervoor aangegeven.

- Welke stappen gaat GS nemen om herhaling te voorkomen?
  Toen de signalen binnenkwamen bij het IPO bestuur is hier zo snel mogelijk op geacteerd. Dat was het eerste moment dat GS aan zet was. Nu de applicaties beveiligd zijn, is de directeur van IPO/BIJ12 aan het kijken hoe herhaling kan worden voorkomen. Gezamenlijk met de andere provincies zullen we hierover het gesprek voeren zodat we voor de toekomst meer zekerheid hebben dat de dienstverlening bij BIJ12 goed

beveiligd is. Hierbij is het goed om te weten dat BIJ12 zich, net als de provincie Utrecht, gecommitteerd heeft om in 2023 certificeerbaarheid te bereiken op de informatie-beveiligingsnorm ISO-27001. De processen die daarvoor moeten worden ingericht hebben als doel om dit soort problemen te voorkomen.

Driebergen, februari 2021