Uittreksel uit conceptverslag PS 1-2-2021 behandeling vragen PvdA inz. Datalekken

De VOORZITTER: Dan gaan we naar de derde vraag in het kader van het vragenuur. Die wordt gesteld door de PvdA en gaat over slecht beveiligde ICT.

De heer CARTON (PvdA): De Provincie Noord-Holland moet volgens de PvdA Noord-Holland zorgvuldig en veilig omgaan met de gegevens van haar inwoners. Na alle terechte commotie over datalekken en het verkopen van persoonsgegevens is de fractie enorm geschrokken van het bericht van vrijdag 29 januari jl. dat ook de ICT-systemen van de provincie al maanden lek zijn. De provincie verwerkt grote hoeveelheden en gevoelige informatie. Met de toenemende digitalisering neemt dat ook alleen maar toe. Informatiebeveiligers zeggen enorm geschrokken te zijn over de verouderde beveiliging van de systemen en het gebrek aan onderhoud, dat soms jaren teruggaat. Informatiebeveiligers geven aan dat we er misschien wel vanuit moeten gaan dat we gehackt zijn. De PvdA-fractie maakt zich dan ook ernstige zorgen over de staat van onze systemen. Inwoners moeten kunnen vertrouwen op een provincie die zorgvuldig omgaat met persoonlijke en gevoelige informatie. We roepen Gedeputeerde Staten dan ook op om direct actie te ondernemen en te zorgen dat de beveiliging goed op orde is. We hebben aanvullende vragen op de brief van vrijdag jl. Kunnen Gedeputeerde Staten de zekerheid geven dat de beveiliging van de ICT-systemen van Provincie Noord-Holland op dit moment op orde is en de gegevens onze inwoners goed beschermd worden? Welke actie neemt het college om potentiële beveiligingsrisico's te verhelpen? Hoe voorkomen Gedeputeerde Staten dat dergelijke beveiligingsrisico's in de toekomst optreden? Waarom is niet eerder ingegrepen na de signalen en conclusies van informatie beveiligers over de situatie bij BIJ12? Tot slot, dit is een ontzettend belangrijk onderwerp en ook erg complex, dus daarom vragen we ook om dit te agenderen in de commissie Economie, Financiën en Bestuur, zodat er op een later moment nog verder over doorgepraat kan worden, als er meer bekend is. Besproken kan worden hoe we dit in de toekomst beter kunnen gaan doen.

Gedeputeerde STIGTER: Om te beginnen met het laatste. Het is goed dat we vandaag stilstaan bij deze actualiteit. Het is ook goed om in de commissie Economie, Financiën en bestuur hierover nog eens verder van gedachte te wisselen, zodat we meer de diepte in kunnen en we meer nog dan vandaag weten over welke maatregelen er bij BIJ12 verder genomen worden. Ik heb ook toegezegd om voor de zomer met een datastrategie te komen, waarin we alle belangrijke aspecten rondom ICT-data de revue laten passeren. Ook daar zal informatieveiligheid een centrale rol spelen.
Even terug naar uw vragen. Provincie Noord-Holland verwerkt dagelijks ontzettend veel informatie. Burgers, bedrijven, organisaties en overheden mogen er ten alle tijden vanuit gaan dat het betrouwbare informatie is en dat wij zorgvuldig omgaan met de gegevens die daarbij aan de orde zijn. Daarom is informatieveiligheid van groot belang. Dat vraagt ook continu aandacht. Iets wat vandaag nog veilig is, is dat misschien over een maand niet meer. Dat vraagt dat we elke dag alert zijn en elke dag hard werken om dat voor elkaar te krijgen. Twee dingen wil ik noemen, die we daar in oppakken. Allereerst hebben de gezamenlijke overheden met elkaar een basisniveau afgesproken rondom informatiebeveiliging. Tot voor kort had iedere overheidslaag zijn eigen systeem. Dat was

niet handig. Alle overheden gaan nu uit van één basisniveau. De Baseline Informatiebeveiliging Overheid (BIO). Wij leggen al onze informatiesystemen, zoals we dat ook kennen bij onze bediencentrale, langs de maatlat van de BIO. Als blijkt dat we niet adequaat zijn dan zullen we gepaste maatregelen nemen. We werken in onze dienstverlening heel veel met externe partijen, die voor ons werken aan informatie. Ze moeten voldoen aan de strenge internationale veiligheidsnormen, vanuit NEN ISO.
Wat hebben we gedaan om de veiligheidsrisico's te verhelpen? Ik verbijzonder het even tot BIJ12. Dat was ook de aanleiding van de vragen. Op het moment dat de eerste signalen binnenkwamen, is daar een extern onderzoek opgezet en zijn er ook maatregelen genomen. Op basis van het onderzoek is gebleken dat die maatregelen niet voldoende waren. We hebben toen een vervolgstap gezet in de escalatie daarvan door een aantal applicaties stop te zetten. We hebben samen met de andere provincies gekeken hoe we de dienstverlening zo goed mogelijk gecontinueerd kan worden terwijl tegelijkertijd risico's worden beperkt. Na het stopzetten hebben we gekeken hoe we gebruik kunnen maken van de systemen van BIJ12, met een beperking van de veiligheidsrisico's. Dat is gebeurd door de systemen stand alone te laten werken, waardoor het publiek geen toegang meer heeft, maar er nog wel mee gewerkt kan worden. Dat is een tijdelijke situatie. Op dit moment wordt bekeken welke maatregelen genomen moeten worden om ervoor te zorgen dat in de toekomst veilig met de applicaties kan worden gewerkt. Dat is soms een kwestie van een aantal kleinere maatregelen op korte termijn. Voor sommige applicaties zullen we echt nog wel de diepte in moeten gaan. We kijken dus ook welke oplossingsrichtingen voor de langere termijn mogelijk zijn. We hebben dus niet het signaal afgewacht. We hebben direct maatregelen genomen. Stap voor stap zijn die maatregelen strenger geworden op dat vlak.

De **VOORZITTER**: De heer Carton heeft u in tweede termijn nog een vraag?

De heer **CARTON** (PvdA): Ja, een korte vraag. Ik dank de gedeputeerde voor de antwoorden. Het is goed het de volle aandacht heeft van Gedeputeerde Staten en ook dat we in een later stadium door kunnen praten met elkaar. Waarom kan het zo zijn dat informatiebeveiligers constateren dat het onderhoud zoveel jaar achterstand heeft en dat het in slechte staat is?

De heer **ZOON** ((PvdD): We hebben nog een paar vragen hierover. Ik kan me voorstellen dat de gedeputeerde nog met een brief komt, die we nog kunnen bespreken in de commissie. Ik zou graag iets van een tijdlijn willen hebben. Wanneer zijn deze kwetsbaarheden geconstateerd? Het offline zetten van een systeem is wel het laatste redmiddel. Hebben we wel op tijd gehandeld? Heeft dit alles financiële gevolgen? We hebben de begroting van BIJ12 laatst vastgesteld. Ik kan me voorstellen dat wanneer alles opnieuw ingericht moet worden dat wel wat geld kost.
Kwetsbaarheden ontstaan niet zomaar. BIJ12 heeft als kerntaak het verwerken van gegevens. Ik heb altijd vertrouwen in onze IT-organisatie, maar ik vraag me af of BIJ12 wel geschikt is. Kan de gedeputeerde daar een antwoord op geven? We worden nu eigenlijk achteraf geïnformeerd. Had de gedeputeerde ons niet eerder kunnen informeren?

Gedeputeerde STIGTER: Ik denk dat we over de vragen van de heer Zoon het beste van gedachte kunnen wisselen in de commissie. Vanaf 2019 zijn er signalen binnengekomen dat er rondom een aantal applicaties sprake was van onzorgvuldig onderhoud. Op basis daarvan zijn maatregelen genomen. Het is niet zo dat er niets is gedaan. Afgelopen najaar uitmondend in december bleek dat die maatregelen onvoldoende zijn geweest. In de applicaties van BIJ12 zitten systeemaspecten die ervoor zorgen dat de veiligheidsissues ook niet allemaal even snel oplosbaar zijn. Er is fundamenteel wat meer aan de hand. Op dat moment zijn we samen met andere provincies daarmee aan de slag gegaan. Dat leidde tot het stopzetten van applicaties. Die zijn op afstand gezet. Per applicatie wordt nu bekeken wat de situatie is en welke maatregelen voor de lange termijn genomen moeten worden.

De VOORZITTER: Meneer Stigter, u bent door uw spreektijd heen. Ik hoorde dat u dit onderwerp verder wilt bespreken in de commissie.

Gedeputeerde STIGTER: Dit zeg ik toe. Dan zal ik ook vragen die ik niet heb kunnen beantwoorden meenemen in mijn voorbereiding, zodat we er in de commissie uitgebreider bij stil kunnen staan.