Vragen van het lid Gerkens aan de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over **het bericht dat inloggen op DigiD niet waterdicht is**.

De **voorzitter**: D-i-g-i-D? Ik doe het altijd nog gewoon met de hand.

□

Mevrouw **Gerkens** (SP): Voorzitter. Het probleem is dat dat niet lang meer zal kunnen en dat ook u aan DigiD zal moeten. Zo is er een autohandelaar in Castricum die alles weet over een vrouw in Beneden-Leeuwen, niet omdat deze twee een relatie hebben of elkaar op de een of andere manier kennen. Nee, hij logde met zijn DigiD per ongeluk in op de ″spullen″ van zijn naamgenoot. Alles, van de donorregistratie tot de kinderbijslag, was toen voor hem openbaar. De reactie van het ministerie daarop is: tja, toeval bestaat. Maar hoe toevallig is dat? Nog geen maand geleden, op 17 maart, stelde ik de staatssecretaris vragen over iemand voor wie via DigiD huurtoeslag was aangevraagd. Die persoon woonde echter in een koophuis. Ook het rekeningnummer waarop de huurtoeslag moest worden gestort, klopte niet. Dat is een kinderlijk eenvoudige fraude, waarvan de staatssecretaris in haar antwoorden vertelde dat daar meer gevallen van zijn. Zij vertelde daarbij niet hoeveel gevallen dat zijn. Op 19 april 2006, bijna op de kop af vier jaar geleden, stelde ik aan de toenmalige minister Pechtold ook al vragen over de veiligheid van DigiD. Het antwoord was toen dat er uiteindelijk drie niveaus van veiligheid moesten komen. Wij zijn nu vier jaar later en wij hebben nog steeds geen goede beveiliging van DigiD. De banken kennen wel een goed systeem. De Belgen kennen bovendien een veel beter systeem, want in België gaat het met het ID-bewijs, met het paspoort dus. Waarom houden wij dan in Nederland nog steeds vast aan een onveilig systeem?

□

Staatssecretaris **Bijleveld-Schouten**: Voorzitter. Ik heb natuurlijk ook kennisgenomen van dit bericht. Mevrouw Gerkens zegt terecht dat ik op 17 maart al soortgelijke vragen heb beantwoord over een andere casus. De buitenwereld heeft de indruk dat er sprake is van een vorm van kraken van DigiD. Dat is echter niet aan de orde. Dat stel ik hier duidelijk. Het bericht gaat namelijk over een autohandelaar uit Castricum die de combinatie van gebruikersnaam en wachtwoord voor zijn DigiD vergeten is. Hij doet een aantal inlogpogingen en kiest toevalligerwijs de gebruikersnaam-wachtwoordcombinatie van een naamgenoot. Vervolgens kan de man met die combinatie gegevens inzien die toegankelijk zijn op het DigiD-basisniveau. Mevrouw Gerkens heeft gelijk daarin, want voor het DigiD-basisniveau is de combinatie van gebruikersnaam en wachtwoord voldoende.

In dit geval is het wachtwoord niet goed gekozen en daardoor is het verkeerd gegaan. Bij DigiD-basis veronderstellen wij namelijk dat je een goed wachtwoord kiest. Als je dat doet, kun je opzettelijk misbruik, maar ook toevallige inzage – want daarom gaat het hier – voorkomen. De DigiD-website geeft diverse tips voor de juiste keuze van een wachtwoord.

Mevrouw Gerkens stelde ook een specifiekere vraag over de veiligheid. DigiD-basis kan niet voor alle niveaus gebruikt worden. Je moet immers specifiek naar de doelen kijken. DigiD kent inderdaad meerdere niveaus van identificatie. Hier ging het om de gebruikersnaam en het wachtwoord. Voor diensten waarvoor dit niet goed genoeg is, is er echter een ander niveau van DigiD. Mevrouw Gerkens weet dat ongetwijfeld ook. Dan kun je namelijk gebruikmaken van sms-authenticatie. Dit is specifiek gericht op individuele mensen en is dus een hoger beveiligingsniveau. Wij werken bovendien naar een systeem toe dat ik zelf beter vind. Ik steun in dit kader dan ook wat mevrouw Gerkens naar voren brengt. Naast de twee niveaus die wij nu kennen, komt ook het EPD-DigiD-niveau, met excuses voor het jargon. Dit niveau is alleen te activeren door in persoon een brief met activeringscode op te halen. Dat is de volgende fase. Het hoogste niveau is de elektronische Nederlandse identiteitskaart. Dat is het systeem dat mevrouw Gerkens aanhaalt en dat in België en meerdere andere landen gebruikt wordt. Ik heb zelf ook daarnaar gekeken, want ik vind het inderdaad belangrijk dat wij de stap in die richting zetten. Daarover bestaat geen misverstand. Ik heb daarom de mogelijkheid tot realisatie van dat laatste, hoogste niveau opgenomen in de aanbestedingsvoorwaarden rondom de nationale identiteitskaart. Ik zal de Kamer dan ook zo snel mogelijk informeren wanneer dit ook operationeel kan zijn.

Mevrouw **Gerkens** (SP): Het is heel fijn dat de staatssecretaris toezegt dat wij nu eindelijk werken aan een eID-identificatie. Dat is heel erg goed. Waarvoor gaat de staatssecretaris die dan gebruiken? Zij spreekt namelijk over een basisniveau en zegt in die context dat het eigenlijk de schuld is van de gebruiker, omdat het wachtwoord niet goed was. Het gaat echter over zeer gevoelige gegevens en persoonlijke informatie. De staatssecretaris noemt dit misschien niet gevoelig, maar ik vind de informatie over donorregistratie, kinderbijslag en de huurtoeslag wel gevoelig. Het gaat over financiële gegevens. Het systeem van DigiD kan alleen werken als wij wel altijd een goede beveiliging hebben. Een wachtwoord is inderdaad niet genoeg. Wij moeten daarom werken met een ander systeem, een veel zwaarder systeem. De staatssecretaris kent de mening van de SP, want die wil hieraan ook nog het elektronisch patiëntendossier koppelen. Internetbankieren is immers zelfs geen 100% veilige methode, dus ook die kan gekraakt worden. Is de staatssecretaris daarom bereid om voor alle niveaus van DigiD over te gaan op het elektronische identiteitsbewijs?

Staatssecretaris **Bijleveld-Schouten**: Op die vraag moet ik ″nee″ zeggen. Ik ben daartoe niet bereid, want je moet echt kijken naar het doel dat gediend wordt. Ik vind het belangrijk dat je bij de beveiligingsniveaus goed kijkt naar het doel. Overigens zijn de overheidsinstanties die DigiD gebruiken er zelf verantwoordelijk voor dat zij goed informeren over het gebruik. Ik denk wel dat wij naar een steeds hoger niveau moeten. Bij het epd is het zeker zo dat er een hoger niveau moet wordt bereikt. Ik vind het echter niet nodig om dit hogere niveau in alle gevallen te gebruiken.

Het schiet mij nu overigens te binnen dat ik mevrouw Gerkens nog een antwoord verschuldigd ben. Zij vroeg in de eerste termijn: hoe vaak komt dit voor? Daarbij

moet ik zeggen: dit voorval is niet bij ons gemeld, maar komt uit de Metro. Daarom heb ik nog eens nagevraagd hoe vaak dit soort zaken gemeld worden. Dan blijkt dat dit circa zes keer per jaar voorkomt. Zo vaak wordt onze helpdesk benaderd met een dergelijk voorval. Op de vraag of dit vaak is – ik vind dat overigens een intrigerende vraag, want ik deel voor een deel haar zorgen – kan ik het volgende zeggen: er zijn 7,5 miljoen gebruikers van DigiD, onder wie overigens niet de Kamervoorzitter, die zelf hun gebruikersnaam en wachtwoord kiezen. DigiD wordt 25 miljoen keer gebruikt. Tegen dat aantal moeten die zes meldingen worden afgezet.

Mevrouw **Van der Burg** (VVD): Voorzitter. Je hebt een naam, je kiest een wachtwoord en dan kan het fout gaan. Er kunnen dus ook rekeningnummers worden veranderd, misschien zelfs ID-nummers. Voor de mensen die dit overkomt zijn de consequenties heel ernstig. Dat zien wij in bepaalde situaties ook bij de Ombudsman. Als de staatssecretaris niet de hoogste vorm wil, is het dan geen idee om sms-authentificatie toe te voegen om dit soort gevallen te voorkomen? Wat zou dat betekenen en is de staatssecretaris daartoe bereid? Is dat een grote stap, in financieel opzicht en qua veiligheid, en is zij bereid deze stap te zetten?

Staatssecretaris **Bijleveld-Schouten**: Ik kijk steeds naar de doelen waar het om gaat. Ik heb voor ogen dat wij daar met de Kamer steeds over gesproken hebben. Je hebt niet voor alles een hoger niveau van beveiliging nodig. Ik kan nog het volgende zeggen tegen mevrouw Gerkens en mevrouw Van der Burg. Stel er wordt er een huursubsidie aangevraagd, dan komt er ook een schriftelijke bevestiging van wat er gebeurt. Overheidsinstanties houden het natuurlijk zelf ook goed in de gaten. Ik weet niet uit mijn hoofd wat dat betekent. Daar moet ik het antwoord op schuldig blijven. Het is wel veel duurder als je naar het hogere beveiligingsniveau gaat. Het is bovendien niet in alle gevallen nodig. Ik vind belangrijk dat je het doel van het beveiligingsniveau goed voor ogen houdt. Daar moeten wij in de toekomst maar eens verder over spreken.

Mevrouw **Azough** (GroenLinks): Voorzitter. Ik ben waarschijnlijk een van de weinige Nederlanders zonder DigiD, samen met de voorzitter. Toch heb ik afgelopen jaren een en ander overleefd. Het kan dus. Desondanks heb ik een belangrijke vraag aan de staatssecretaris. Ik verbaas mij enigszins over het feit dat de staatssecretaris als argument gebruikt dat de veiligheid aan het doel moet worden gekoppeld. Als iemand – weliswaar door toeval, maar desondanks toch – de mogelijkheid heeft om inzage te krijgen in privégegevens van personen en daarin veranderingen kan aanbrengen die cruciaal zouden kunnen zijn, dan is er toch geen sprake van een basisniveau dat een beetje beveiligd moet worden? Dan moet er toch sprake zijn van een basisniveau dat zo goed is dat niemand dit kan doen?

Staatssecretaris **Bijleveld-Schouten**: Het basisniveau moet inderdaad goed genoeg zijn voor de doelen die ermee worden gediend. Wij hebben echt te maken met een incident, daarom heb ik ook de aantallen maar eens genoemd. Wij zullen nog eens bezien of wij wel goed genoeg waarschuwen voor de koppeling met het wachtwoord. Je moet het wachtwoord zo kiezen, dat het niet erg eenvoudig is. Het blijft altijd een afweging tussen het stimuleren van veilige wachtwoorden of het afdwingen ervan – want dat kan ook. Je kunt veiliger wachtwoorden afdwingen, maar dat doen wij nu niet. Het blijft echter iedere keer een afweging tussen aan de ene kant gebruiksvriendelijkheid met het voorkomen van allerlei heraanvragen. Dat zien wij namelijk ook bij DigiD. Ingewikkelde wachtwoorden worden immers vaker vergeten. Nogmaals, het gaat om de afweging tussen gebruiksvriendelijkheid en veiligheid.

Ik ben het eens met degenen die zeggen dat het systeem zo veilig mogelijk moet zijn. Een veiligheid van 100% is niet te garanderen, maar wel zo veilig mogelijk. Goed gekeken moet worden voor welk doel welk niveau van DigiD ingezet wordt. Dit gebeuren beschouw ik wel als een incident. Naar aanleiding hiervan ben ik bereid om met name de afdwingbaarheid van de wachtwoorden te bekijken. Ik denk dat dit al een verbetering zal kunnen zijn.

De heer **Van Raak** (SP): De staatssecretaris zegt: als je DigiD gebruikt bij het invullen van het belastingformulier is het eigenlijk altijd veilig, behalve als je een verkeerd soort wachtwoord gebruikt. Dat klinkt allemaal niet zo veilig. De staatssecretaris zegt ook dat het maar een incident is. Dat weten wij echter niet, want niet iedereen bij wie het mis gaat, zal dat zomaar melden. Bij internetbankieren weet je overigens altijd precies om wie het gaat. Dat systeem is volgens mij ook veel beter. Waarom zegt de staatssecretaris niet "dan gaan wij zo'n soort systeem maken", als wij weten dat een dergelijk systeem beter is? Waarom kan dat niet?

Staatssecretaris **Bijleveld-Schouten**: Overigens is het niet zo dat het systeem bij banken altijd beter is. U moet dat niet onderschatten; ook daar gaat wel eens wat mis. Ik heb overigens al in antwoord op de vragen van mevrouw Gerkens gezegd dat wij ook aan hogere veiligheidsniveaus werken; wij hebben dus DigiD met de sms-authenticatie. Daarnaast zijn soms face to face controles mogelijk; je kunt het dan ook uitgeven. Ik denk hierbij aan paspoorten; daarbij gebeurt dat ook. Nogmaals, dan geven wij iets uit. Dat zal ook gebeuren bij het EPD, elektronisch patiëntendossier, DigiD. Bij het elektronisch patiëntendossier zal dus ook een face tot face controle horen. Er wordt dus wel degelijk ook gekeken naar andere middelen die ingezet kunnen worden. Nogmaals, het is niet in alle gevallen nodig. Bij het elektronisch patiëntendossier achten wij het nodig, maar ik herhaal dat dit niet in alle gevallen nodig is. Wij kijken er dus naar. Daarnaast werken wij aan de elektronische identiteitskaart en die kan het altijd mogelijk maken.

De heer **Algra** (CDA): Het is vaak met het vragenuurtje dat het erop lijkt dat het om een incident gaat. De staatssecretaris zegt dat het om 6 gevallen op 25 miljoen gaat. Het CDA vindt dat vervelend; het is namelijk alsof het ons overkomt. Kan de staatssecretaris aangeven in hoeverre dit ingecalculeerd is? Wat was de berekening, toen wij begonnen met DigiD, van het aantal van dit soort fouten, dus als iemand inlogt op de code van iemand anders? Klopt dat aantal met de realiteit? Of is ons dit nu weer overkomen?

Staatssecretaris **Bijleveld-Schouten**: Het is geen geval

dat ons is overkomen. Vandaar dat ik zeg dat het steeds een weging is tussen gebruiksvriendelijkheid en veiligheid. Mevrouw Gerkens heeft al gerefereerd aan de hele invoeringsgeschiedenis van DigiD. Ik heb al gezegd dat een veiligheid van 100% niet bestaat. Bij de introductie van DigiD is een afweging gemaakt tussen de veiligheid en de klantvriendelijkheid. Het zijn allemaal overheidsorganisaties die met DigiD werken. Die organisaties zijn ook bekend met de werking van het uitgifteproces. Op basis daarvan bepalen zij of een dienst al dan niet met DigiD geleverd kan worden. Deze organisaties moeten dus zelf een afweging maken, mede met het oog op de beveiligingsniveaus. Als zij denken dat de beveiliging van DigiD-basis niet goed genoeg is, moeten zij dus voor een hoger veiligheidsniveau kiezen. Zo zit het systeem in elkaar. Dit is van het begin af aan wel duidelijk geweest. Ik doel op het feit dat DigiD als systeem zo werkt. Uiteindelijk is dit ook niet het ultieme middel voor gegevens die nooit ergens terecht mogen komen. Nogmaals, dat is bekend.

De heer **Heijnen** (PvdA): Het lijkt een overzichtelijk probleem, maar ik zou de voorzitter niet aanraden om als wachtwoord ″0000″, vier keer nul, te nemen, als zij op DigiD overgaat. Ik denk dat dit wel duidelijk is. Tegelijkertijd heeft dat een aspect waarop ik de aandacht wil vestigen. U zegt immers: het beveiligingsniveau hangt af van het doel waarvoor je het systeem gebruikt. Er is echter nog iets anders in het geding en dat is privacy, het gevoel dat andere mensen, mits zij jouw wachtwoord achterhalen, in jouw gegevens kunnen kijken. Dit staat los van de vraag hoe vaak het voorkomt en waarvoor het systeem gebruikt is. Bent u met mij van mening dat, tijdens de beslissing om zo snel mogelijk tot een hoger beveiligingsniveau te komen, ook privacy een rol moet spelen?

Staatssecretaris **Bijleveld-Schouten**: Dat ben ik inderdaad met de heer Heijnen van mening. Wat het EPD betreft, is om die reden al voor een ander beveiligingsniveau gekozen. Daarbij speelde de discussie over privacygevoelige gegevens een rol. De EPD-DigiD is alleen te activeren door een persoon die een brief heeft gekregen met een activeringscode die hij fysiek moet ophalen. De niveaukeuze wordt overigens niet altijd door ons gemaakt. Dat gebeurt meestal door de overheidsinstellingen die daarvan gebruikmaken. Zij moeten bij het maken van die keuze dus rekening houden met de privacy.