Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2008–2009

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2328

Vragen van het lid **Gerkens** (SP) aan de minister van Sociale Zaken en Werkgelegenheid over *de slechte beveiliging van UWV-servers.* (Ingezonden 20 maart 2009)

1
Wat is uw reactie op het bericht dat het UWV verzuimd heeft haar servers te vergrendelen?[1]

2
Hoe kan het dat de servers van het UWV in een voor meerdere partijen toegankelijke ruimte staan en dat van de mogelijkheid om de servers af te sluiten geen gebruik is gemaakt?

3
Bent u ervan op de hoogte dat in hetzelfde datacenter aparte voorzieningen zijn voor servers met gevoelige data? Kunt u uitleggen waarom het UWV geen gebruik gemaakt heeft van deze voorzieningen?

4
Welke data zijn door deze servers bereikbaar?

5
Zijn er op andere plekken ook servers van het UWV? Zo ja hoe zijn deze beveiligd?

6
Welk beveiligingsbeleid is er bij het UWV? Zijn er richtlijnen voor de beveiliging? Zo nee, bent u bereid deze te ontwikkelen? Zo ja zijn er controles op het fysieke vlak voorzien in richtlijnen?

7
Bent u bereid te inventariseren op welke wijze er bij andere (semi-)overheidsinstellingen om wordt gegaan met de beveiliging van servers? Zo nee waarom niet?

8
Welke maatregelen gaat u treffen om te voorkomen dat een dergelijke situatie opnieuw kan ontstaan?

[1] Webwereld, 17 maart 2009: «UWV en Achmea verzuimen servers te vergrendelen».

Antwoord

Antwoord van minister **Donner** (Sociale Zaken en Werkgelegenheid) (ontvangen 15 april 2009)

1
UWV heeft alle uitvoerende werkzaamheden op ICT gebied uitbesteed, en dat geldt ook voor het technische beheer van servers. In de betreffende contracten worden eisen gesteld aan de beveiliging. Er is dus sprake geweest van een ernstige inbreuk op deze eisen, waar in de eerste plaats een niet-bevoegde toegang heeft gekregen tot de ruimte waarin de servers zijn geplaatst, en in de tweede plaats een aantal serverskasten niet waren afgesloten. Een dergelijke ernstige inbreuk is onacceptabel.

2 en 3
Beveiliging van informatiesystemen vereist niet alleen goede afspraken over de beveiliging maar ook een consequente naleving van deze afspraken. In dit geval heeft het op een aantal punten aan dat laatste ontbroken. Ook bij een aparte ruimte is nog steeds goed beheer van de toegang tot die ruimte vereist om een adequaat niveau van beveiliging te bereiken. Het delen van rekencentra is algemeen gebruikelijk en draagt bij aan de economische basis en schaal om de beveiliging optimaal in te kunnen richten. Welk niveau van beveiliging gekozen wordt voor het beheer van een bepaalde server is afhankelijk van verschillende factoren, waaronder de risico's die optreden als kwaadwillenden fysieke toegang tot een server krijgen. UWV heeft destijds gemeend dat de beveiliging van de servers in de gedeelde ruimte – gelet op hun functie – voldoende was geborgd. UWV heeft echter een aantal servers met gevoelige functies, bij hetzelfde datacentrum wél in een aparte (niet gedeelde) ruimte ondergebracht. Het

KVR35875
2009Z05207
0809tkkvr2328
ISSN 0921 - 7398
Sdu Uitgevers
's-Gravenhage 2009

gebeurde is voor UWV aanleiding om in overleg met de leverancier dit nader te bezien, maar de belangrijkste factor blijft het goede beheer van de toegang tot de ruimte.

4
In principe betekent fysieke toegang tot deze servers niet dat toegang tot klantgegevens van UWV ontstaat. Toegang tot de betreffende systemen en data is beperkt tot geautoriseerde gebruikers. De gegevens zijn logisch beveiligd met inlogcodes en firewalls. Dit laat onverlet dat toegang van binnenuit tot het netwerk de kwetsbaarheid voor inbraken vergroot. Voorts is duidelijk dat de processen op de servers verstoord kunnen worden door eenvoudig kabels voor stroom of netwerkverkeer los te koppelen. Er is daarom geen enkele twijfel over het feit dat onbevoegde toegang tot de servers volstrekt onaanvaardbaar is.

5
Ja, alle partijen die technisch beheer uitvoeren voor het UWV of eventueel voor dienstverleners die diensten leveren aan UWV, beheren servers van het UWV in de zin dat de data en processen die op die servers verwerkt worden van het UWV zijn. Het UWV hoofdrekencentrum bevindt zich in Brussel, in een overigens gedeeld rekencentrum van IBM. Daarnaast staan er nog belangrijke servers in het rekencentrum van het voormalige GAK en SFB en wordt er voor kantoorautomatisering nog gebruik gemaakt van servers op UWV-locaties zelf. In alle gevallen gelden dezelfde kaders en normen voor de beveiliging en die zijn uitgangspunt bij het contracteren van de diensten.

6
Ten aanzien van het beveiligingsbeleid van het UWV geldt de algemene verplichting tot beveiliging op grond van artikel 13 Wet Bescherming Persoonsgegevens (WBP). Het CBP heeft voor de invulling hiervan een richtlijn vastgesteld[1].
De WBP vormt tevens de basis voor de bijlage I van de Regeling SUWI waarin voorgeschreven wordt dat de uitvoeringsorganisatie zich in het jaarverslag verantwoordt over de continuïteit en betrouwbaarheid van de gegevensverwerking respectievelijk de beveiliging van het Suwinet. Daarnaast is in artikel 76 van de Wet SUWI opgenomen dat het Uitvoeringsinstituut Werknemersverzekeringen en de Sociale verzekeringsbank op de voet van de ter zake voor de Rijksdienst geldende voorschriften zorg dragen voor de nodige technische en organisatorische voorzieningen ter beveiliging van hun gegevens tegen verlies of aantasting en tegen onbevoegde kennisneming, wijziging en verstrekking van die gegevens. Fysieke beveiliging is hier onderdeel van, evenals audits en verantwoording.
Voor het waarborgen van de verplichtingen die hieruit voorvloeien heeft UWV een Strategisch en Tactisch beleidskader Beveiliging en Privacy opgesteld. Deze kaders zijn tevens van toepassing op uitbestede dienstverlening.

7
Zoals door staatssecretaris Bijleveld-Schouten van Binnenlandse Zaken en Koninkrijksrelaties in antwoord op uw vragen over noodplannen (Kamerstuk 2080912470) is medegedeeld, zijn overheidsorganisaties binnen de Rijksdienst op grond van het Voorschrift Informatiebeveiliging Rijksdienst (VIR2007) verplicht tot een risicoanalyse en -afweging. Op basis van deze afweging nemen organisaties onder eigen verantwoordelijkheid voor hun systemen passende maatregelen. Jaarlijks worden de maatregelen in de mate waarin ze toereikend zijn naar opzet, bestaan en werking ge-audit. Een afzonderlijke inventarisatie vind ik derhalve niet noodzakelijk.
De mede-overheden blijven zelf verantwoordelijk voor het nemen van passende maatregelen. Zoals eerder geantwoord bevordert het kabinet het risicobewustzijn bij mede-overheden, ook via organisaties zoals GOVCERT.NL, het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) en tot en met 2009 ook via het programma Nationale Infrastructuur Cybercrime (NICC) en biedt daarmee ook overlegstructuren om informatie, kennis en ervaringen met elkaar te delen.

8
In lijn met het antwoord op de vraag 6 zal ik er op toezien dat het UWV zich verantwoordt over de maatregelen die genomen worden.

[1] Achtergronden en Verkenningen 23 (categorieën van beveiliging afhankelijk van soort gegevens).