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

1903

Vragen van het lid **Gerkens** (SP) aan de minister van Binnenlandse Zaken en Koninkrijksrelaties over *uitval ICT.* (Ingezonden 6 februari 2009)

1
Kent u het nieuwste ICT-barometer-onderzoek van Ernst & Young? Wat is uw reactie op de bevindingen uit dit onderzoek?[1]

2
Wat is de oorzaak dat slechts 23 procent van de organisaties uit de publieke sector een noodplan heeft? Wat gaat u er aan doen om dit percentage het komende jaar fors te verhogen?

3
Wat is uw reactie op het feit dat uit het onderzoek blijkt dat overheidsdienaren relatief weinig vertrouwen hebben in hun eigen ICT-systemen? Waar komt dit gebrek aan vertrouwen vandaan? Wat gaat u er het komende jaar aan doen om dit vertrouwen te verbeteren?

4
Wat gaat u doen aan de blinde vlekken van werknemers in de publieke sector voor de typische risico's van moderne technologie?

5
Zijn de softwarebeveiligingen op ICT-systemen bij de overheid en in de publieke sector up to date?[2] Zo nee, wat gaat u hier aan doen?

6
In welke mate zijn overheidsinstellingen en instellingen in de publieke sector het afgelopen jaar getroffen door virussen, digitale aanvallen en hackers? En in de jaren daarvoor? Is er sprake van een daling of een stijging? Kunt u dit toelichten?

[1] NU.nl, 28 januari 2009: «Overheid niet voorbereid op uitval ICT».
[2] http://www.ict-barometer.nl/, persbericht «Digitale generatiekloof remt investeringen in ICT-beveiliging».

Antwoord

Antwoord van staatssecretaris **Bijleveld-Schouten** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 12 maart 2009)

1
Ja. In de hieronder weergegeven antwoorden op de door u gestelde vragen is mijn reactie verwerkt.

2
Het kabinet is van mening dat de overheid een voorbeeldfunctie heeft als het gaat om veilige en betrouwbare omgang met en bescherming van informatie.
Zoals vorig jaar naar aanleiding van de ICT-Barometer 2008 al aan uw Kamer is gemeld (kamerstuk 2070811120), zijn op grond van het Voorschrift Informatiebeveiliging Rijksdienst (VIR2007) overheidsorganisaties binnen de Rijksdienst verplicht tot een risicoanalyse enafweging.
Op basis van deze afweging nemen organisaties onder eigen verantwoordelijkheid voor hun systemen passende maatregelen. Een noodplan kan hier onderdeel van uitmaken, maar dat hoeft niet. De mate waarin bedrijfsprocessen afhankelijk zijn van ICT en de mate waarin ze daarbij kwetsbaar zijn, speelt een belangrijke rol. Jaarlijks worden de maatregelen in de mate waarin ze toereikend zijn naar opzet, bestaan en werking ge-audit.
De mede-overheden zijn zelf verantwoordelijk voor het nemen van passende maatregelen. Het kabinet bevordert het risicobewustzijn, ook bij de mede-overheden, 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. Bovengenoemde organisaties hebben in de afgelopen jaren diverse activiteiten ontplooid/gestart om het bewustzijn te bevorderen en passende diensten aan te bieden/te implementeren. Zij blijven in de nabije toekomst hun diensten aanbieden.

KVR35401
2080912470
0809tkkvr1903
ISSN 0921 - 7398
Sdu Uitgevers
's-Gravenhage 2009

3
Uit het onderzoek blijkt dat het vertrouwen in de beveiliging van de eigen organisatie bij de meeste sectoren rond 54% ligt, met een piek naar 45% en 61%. Dat zijn weliswaar verschillen, maar zij zijn onderling niet heel groot. De illustratie in het onderzoeksrapport laat dit ook zien. Het onderzoek geeft helaas geen inzicht in de verdeling van de score binnen de overheid (Rijk, provincie, gemeenten etc.). Evenmin is bij ondervraagden doorgevraagd naar verdere motivering.
Er is een verschil tussen de perceptie van de beveiliging en de effectiviteit van de genomen maatregelen. Immers, veel maatregelen zijn onzichtbaar voor de gebruiker. Het kan echter wel zijn dat minder vertrouwen op zichzelf een negatief effect heeft op de beveiliging. Het is de verantwoordelijkheid van de verschillende organisaties te bezien in hoeverre hiervan sprake is en in dat geval gepaste maatregelen te nemen, bijvoorbeeld door op maat gesneden voorlichting.

4
In het ICT-Barometer-onderzoek constateert de schrijver dat er een verschil is in de risicoperceptie van jonge en die van oudere respondenten als het gaat om moderne technologie, maar rept niet over een blinde vlek. Of één van de percepties klopt met de werkelijkheid is moeilijk te zeggen. Over het algemeen is de ervaring dat mensen die langer in dit vak meelopen beter in staat zijn risico's in te schatten, ook van moderne technologie.
Op dit moment ondersteunt GOVCERT.NL de verantwoordelijken voor beveiliging bij de overheid door:
– Alerts met beveiligingsadviezen te sturen naar de mensen die de ICT-infrastructuur beveiligen bij deelnemende organisaties. Hierdoor worden zij in staat gesteld schade door incidenten te voorkomen.
– Achtergronden, factsheets en adviezen te leveren bij beveiligingsvraagstukken die (mogelijk) spelen bij organisaties in de publieke sector. Deze worden toegestuurd aan deelnemende organisaties of worden publiek beschikbaar gesteld op de website. Ook moderne technologie komt aan de orde, evenals reële actuele dreigingen. Tevens komen nieuwe dreigingen aan de orde tijdens het jaarlijkse symposium, waarbij alle deelnemers zijn uitgenodigd.
– Via het kanaal van de waarschuwingsdienst.nl tips en adviezen te geven over risico's die Nederlanders in het algemeen lopen door gebruik van informatietechnologie en internet.

5
Zie mijn beantwoording onder 2.

6
Er is geen meldingsplicht van incidenten aan een centrale (overheids)organisatie. Dit antwoord kan alleen gegeven worden door de instellingen zelf. Overigens verschijnt er jaarlijks een trendrapport van GOVCERT.NL waarin een indicatie wordt gegeven van de ontwikkeling van virussen en digitale aanvallen bij de overheid. Het monitoringssysteem detecteerde 99.911 malware-aanvallen, 2 keer meer dan het jaar ervoor. Hierbij werden 14.637 verschillende soorten malware gebruikt. Dit is 7,5 keer meer dan het jaar ervoor. De efficiëntie van de virusscanproducten die in het systeem gebruikt worden steeg van 85 procent herkenning van malware naar 89 procent. In het trendrapport kan niet worden ingegaan op de specifieke incidenten waarbij GOVCERT optrad. In meer algemene bewoordingen wordt wel de ontwikkeling van de bedreiging beschreven. Botnets zijn een serieuze dreiging, internetcriminelen werken professioneler en er is een markt ontstaan rond diensten/producten op het gebied van cybercrime. Verder valt er een toename te constateren in gerichte aanvallen, en een toename in aanvallen naar eindgebruikers. Deze ontwikkelingen worden meegenomen in de uitvoering van de gezamenlijke preventieagenda (TK 2006–2007, 30821, nr. 3) die eind 2007 aan uw Kamer is gestuurd.