2009Z18547

Vragen van het lid Gerkens (SP) aan de staatssecretarissen van Binnenlandse Zaken en Koninkrijksrelaties en van Economische Zaken over een meldplicht voor ICT-incidenten. (Ingezonden 9 oktober 2009)

1
Wat is voor u de aanleiding geweest om te pleiten voor verbetering van de beveiliging van informatiesystemen bij de overheid? 1)

De aanleiding voor mijn uitspraak zijn de conclusies van het in juli 2009 uitgebrachte Trendrapport Cybercrime, waarin GOVCERT.NL een analyse presenteerde van dreigingen en kwetsbaarheden van het internet en hoe daarvan in toenemende mate misbruik wordt gemaakt door criminelen. Een meer directe aanleiding werd gevormd door een aantal grote incidenten dat zich deze zomer voordeed, waarbij GOVCERT.NL werd ingeschakeld voor incident response. Een aantal hiervan is tevens in de media verschenen, zoals de malware-infectie van de (gehackte) website van de Raad van State en de virusuitbraak op het ICT-netwerk Rechterlijke Organisatie (ICTRO) van de Raad voor de Rechtspraak / Openbaar Ministerie.

2
Hoeveel incidenten zijn bij u bekend? Om wat voor incidenten ging het? Waar schortte het aan de beveiliging?

Bij GOVCERT.NL zijn in de afgelopen twaalf maanden (1-10-2008 tot 1-10-2009) door overheidsinstanties achtendertig incidenten gemeld, waarbij om ondersteuning van GOVCERT.NL is gevraagd.

Het gaat voornamelijk om incidenten die te maken hebben met virusinfecties, waardoor systemen niet meer naar behoren functioneren. Tevens gaat het om lekken in de beveiliging van websites, waardoor deze niet meer geraadpleegd kunnen worden of de bezoekers mogelijk infecteren met virussen op het moment dat ze deze websites bezoeken.
In de meeste gevallen blijkt dat de noodzakelijke processen rondom IT- beheer niet afdoende geborgd zijn, zoals een goed patchmanagement[1] proces om snel en gericht in te kunnen spelen op nieuwe kwetsbaarheden en de bijbehorende patches.

3
Welke informatie is hierdoor op straat komen liggen? Met welke gevolgen?

Incidenten waarbij informatie ongewenst op straat is komen te liggen zijn bij mij niet gemeld.

4
Zijn mogelijke problemen die hier uit voortvloeien voor mensen opgelost? Zo nee, waarom niet?

Zie antwoord op vraag 2 en 3. De incidenten die bij GOVCERT.NL zijn gemeld, zijn adequaat afgehandeld.

5
Deelt u de mening dat een meldplicht, zoals omschreven door u op het symposium, niet alleen zou moeten gelden voor de overheid, maar ook voor het bedrijfsleven? Zo nee, waarom niet?

6
Bent u bereid de meldplicht voor overheidsinstellingen te combineren met de meldplicht voor bedrijven bij verlies van persoonsgegevens uit datasystemen? 2) Zo nee, waarom niet?

---

[1] Het doel van patchmanagement is tweeledig. Ten eerste is het gericht op het inzichtelijk maken van de actuele stand van kwetsbaarheden en toegepaste patches binnen de beheerde infrastructuur. Het tweede doel is op een zo efficiënt mogelijk wijze met zo min mogelijk verstoringen een stabiel (veilig) systeem te creëren.

Gecombineerd antwoord op vragen 5 en 6
Tijdens het symposium heb ik aangegeven, dat ik nader wil onderzoeken of het mogelijk is om een meldplicht voor ICT-incidenten bij de (Rijks)overheid in te stellen.
Uiteraard is het van belang dat ICT-incidenten niet alleen binnen maar ook buiten de overheid worden voorkomen. Echter, vanuit mijn verantwoordelijkheid voor netwerk- en informatiebeveiliging binnen de overheid, richt ik mij op een meldplicht binnen de overheid.
Dit is een andere meldplicht dan de EU-meldplicht waaraan is gewerkt in het kader van de herziening van het EU-reguleringskader (richtlijnen) voor de elektronische communicatie. In deze Europese richtlijnen (w.o. voorstel tot wijziging van RL 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, de zgn. e-privacy richtlijn) wordt onder andere geregeld dat de beheerder of aanbieder van openbare elektronische communicatiediensten verplicht wordt de veiligheidsinbreuken onmiddellijk te melden aan de toezichthouder. Daarnaast zullen eveneens de betrokkenen worden geïnformeerd over de (veiligheids)inbreuk indien de inbreuk naar verwachting nadelige gevolgen kan hebben voor diens persoonlijke levenssfeer. Besluitvorming over de invoering van de meldplicht in geval van verlies van privacygevoelige gegevens voor de elektronische communicatie vindt binnen de EU plaats.

Koppeling met de door mij aangegeven meldplicht voor ICT-incidenten is in dit Europese traject dat de herziening van het EU-reguleringskader voor de elektronische communicatie behelst, niet mogelijk. Wel zal in het door mij aangekondigde onderzoek de relatie tussen de meldplicht voor ICT-incidenten en de EU-meldplicht worden meegenomen.

7
Zo ja, wanneer mogen wij een voorstel van de kant van het kabinet verwachten tot invoering van de meldplicht?

Verwijzend naar de door uw Kamer ontvangen brief, zal het kabinet na afronding van de besluitvorming op Europees niveau overgaan tot nationale invoering van de geharmoniseerde meldplicht in de sector elektronische communicatie.

Ik verwacht u in de loop van 2010 te kunnen informeren over een aanpak voor het melden van ICT- incidenten binnen de overheid.

8
Wanneer zal definitieve besluitvorming op Europees niveau over de invoering van een meldplicht plaatsvinden?

De meldplicht, waarover u eerder per brief bent geïnformeerd (TK, 2008–2009, 26 643, nr. 138), is een onderdeel van de herziening van het EU-reguleringskader voor de elektronische communicatie. De definitieve besluitvorming over de herziening van de Europese richtlijnen op het gebied van de elektronische communicatie zal nog dit jaar plaatsvinden.

9
Bent u bereid alvast stappen te ondernemen om een snelle invoering van een meldplicht voor zowel overheid als bedrijfsleven mogelijk te maken? Zo nee, waarom niet?

10
Bent u bereid, indien besluitvorming in Europa nog lang op zich laat wachten, op eigen initiatief een meldplicht in te stellen, zodat Nederland alvast werk kan maken van de beveiliging van persoonsgegevens in zowel de publieke als private sector? Zo nee, waarom niet?

Gecombineerd antwoord op vragen 9 en 10.De besluitvorming in Europa zal nog dit jaar plaatsvinden (zie ook de antwoorden op vraag 7 en 8).

1) Tweakers.net, 8 oktober 2009: "Staatssecretaris wil meldplicht voor ICT-incidenten bij overheid"