Voorstel tot wijziging van de Wet beveiliging netwerk- en informatiesystemen

Beantwoording vragen Integraal afwegingskader voor beleid en regelgeving (IAK)

1. Wat is de aanleiding?
De Minister van Justitie en Veiligheid kan beschikken over dreigings- en incidentinformatie over de netwerk- en informatiesystemen van aanbieders die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid (hierna: andere aanbieders). In sommige gevallen kan de minister deze informatie niet doen toekomen aan andere aanbieders of aan de schakelorganisatie waarvan zij tot de doelgroep behoren, omdat hiervoor een wettelijke grondslag ontbreekt in de Wet beveiliging netwerk- en informatiesystemen.

2. Wie zijn betrokken?
De Minister van Justitie en Veiligheid (in de praktijk: het Nationaal Cyber Security Centrum, NCSC), aanbieders die geen vitale aanbieder zijn en evenmin deel uitmaken van de rijksoverheid, en organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over digitale dreigingen en incidenten (OKTT's).

3. Wat is het probleem?
Zonder dreigings- en incidentinformatie over hun eigen netwerk- en informatiesystemen weten andere aanbieders bij dreigingen en incidenten niet dat hun systemen kwetsbaar zijn. Dit kan tot gevolg hebben dat één of meer van hun netwerk- en informatiesystemen kwetsbaar blijven. Hierdoor bestaat er een vergroot risico op bijvoorbeeld het door derden succesvol installeren van gijzelsoftware (*ransomware*) waarmee bestanden worden versleuteld. Een ander risico is bijvoorbeeld het door derden binnendringen van de systemen om kennis te nemen van de daarin aanwezige gegevens of om deze te wijzigen. Dit kan leiden tot de uitval van de beschikbaarheid of het verlies van de integriteit van netwerk- en informatiesystemen die aanbieders voor hun dienstverlening nodig hebben, met alle nadelige consequenties voor de continuïteit van hun dienstverlening van dien.

4. Wat is het doel?
Het doel van de voorgestelde wijziging van de Wet beveiliging netwerk- en informatiesystemen is dat andere aanbieders in ruimere mate de beschikking krijgen over dreigings- en incidentinformatie over hun eigen netwerk- en informatiesystemen. Op basis hiervan kunnen zij maatregelen nemen om incidenten te voorkomen of de gevolgen daarvan te beperken.

5. Wat rechtvaardigt overheidsinterventie?
Voor de gewenste informatiedeling met andere aanbieders of met de OKTT's die hun schakelorganisatie zijn is een wettelijke grondslag nodig en daarin voorziet dit voorstel.

6. Wat is het beste instrument?
Een wettelijke grondslag in de Wbni.

7. Wat zijn de gevolgen?
Het gevolg van de voorgestelde wijziging van de Wbni is dat andere aanbieders, al dan niet via OKTT's, de beschikking krijgen over dreigings- en incidentinformatie over hun eigen netwerk- en informatiesystemen. Het is aan andere aanbieders zelf om af te wegen of en welke maatregelen zij treffen naar aanleiding van de ontvangen dreigings- en incidentinformatie. Dit voorstel leidt dus niet tot verplichtingen, regeldruk(kosten), administratieve lasten en nalevingskosten voor burgers en bedrijven. Van toezicht op en handhaving van de naleving van verplichtingen is dan ook geen sprake.

Dit voorstel heeft financiële gevolgen voor het ministerie van JenV. Naar schatting is maximaal € 11.000,- per jaar nodig aan extra financiële middelen. Deze kunnen binnen de bestaande begroting van het ministerie van JenV worden opgevangen. Verder heeft dit voorstel uitvoeringsgevolgen voor het NCSC. Verwacht wordt dat werkprocessen aangepast moeten worden, maar dat de impact daarvan minimaal is. De technische aanpassing van ICT-systemen is niet noodzakelijk.