Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 808 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 december 2021

De Onderzoeksraad voor Veiligheid (OVV) heeft op 16 december 2021 het rapport «Kwetsbaar door software – Lessen naar aanleiding van beveiligingslekken door software van Citrix» gepubliceerd. Ik bied u hierbij het rapport[1] aan mede namens de Minister van Economische Zaken en Klimaat, en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties.

De beveiligingslekken in de software van Citrix werden in december 2019 bekend. Deze problematiek heeft breed zichtbaar gemaakt hoe afhankelijk we als samenleving zijn van digitale systemen en hoe uitval kan leiden tot maatschappelijke ontwrichting. Door de kwetsbaarheden in de software van Citrix hadden veel organisaties tijdelijk problemen met de externe toegang tot hun netwerk, waardoor problemen met thuiswerken en files op de weg ontstonden. De impact van dit incident zou nu, tijdens de COVID-19 pandemie waarin we massaal thuiswerken, veel groter zijn geweest.

Bovendien maakte de problematiek duidelijk dat een probleem in software van een enkele leverancier wereldwijd voor grote problemen kan zorgen bij vele organisaties die hier direct maar ook indirect van afhankelijk zijn. Dit zien we nu mogelijk ook met de Apache Log4j kwetsbaarheid.

Met het oog hierop dank ik de OVV voor het onderzoeksrapport en de daarin opgenomen aanbevelingen ter bevordering van de digitale veiligheid van Nederland. Het is belangrijk dat ook hier lessen uit worden getrokken.[2]

De OVV doet in zijn adviesrapport de volgende zeven aanbevelingen:

---

[1] Raadpleegbaar via www.tweedekamer.nl.

[2] Zie in dit kader ook de kabinetsreactie op het rapport «Voorbereiden op digitale ontwrichting» van de WRR en een overzicht van de geleerde lessen van de Citrix-problematiek (*Kamerstuk 26 643, nr. 658*

kst-26643-808
ISSN 0921 - 7371
's-Gravenhage 2021

Aan het Nederlandse kabinet en aan organisaties in Nederland die software gebruiken:

1. Zorg er op korte termijn voor dat alle potentiële slachtoffers van cyberaanvallen snel en doeltreffend – gevraagd en ongevraagd – worden gewaarschuwd, zodat zij maatregelen kunnen treffen voor hun digitale veiligheid. Breng daartoe private en publieke responscapaciteit samen en zorg daarbij voor voldoende mandaat en wettelijke waarborgen.

Aan de Eurocommissaris voor Interne Markt en de Eurocommissaris voor een Europa dat klaar is voor het digitale tijdperk:

2. Zorg dat uw initiatieven om te komen tot wetgeving voor veiligere software leiden tot een Europese verordening die de verantwoordelijkheid van fabrikanten vastlegt en afnemers inzicht geeft in hoe fabrikanten die verantwoordelijkheid invullen. Leg vast dat fabrikanten aansprakelijk zijn voor de gevolgen van softwarekwetsbaarheden.

Aan fabrikanten van software gezamenlijk:

3. Ontwikkel met andere fabrikanten good practices om software veiliger te maken. Neem in de overeenkomsten met uw afnemers op dat u zich hieraan committeert.
4. Waarschuw en help al uw afnemers zo snel en doeltreffend mogelijk wanneer kwetsbaarheden in software gesignaleerd worden. Schep de randvoorwaarden die noodzakelijk zijn om uw afnemers te kunnen waarschuwen.

Aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Economische Zaken en Klimaat (ten behoeve van alle organisaties en consumenten in Nederland):

5. Bevorder dat Nederlandse organisaties en consumenten gezamenlijk veiligheidseisen formuleren en afdwingen bij softwarefabrikanten. Zorg dat de overheid daarbij een voortrekkersrol speelt. Ga uit van het principe: collectieve samenwerking waar mogelijk; branche-specifiek waar noodzakelijk.

Aan het Nederlandse kabinet:

6. Creëer naar analogie van de Comptabiliteitswet een wettelijke basis voor de beheersing van digitale veiligheid door de overheid.
7. Verplicht alle organisaties om op eenduidige wijze verantwoording af te leggen over de wijze waarop zij digitale veiligheidsrisico's beheersen.

Het kabinet zal de aanbevelingen uit dit OVV-rapport zorgvuldig bestuderen en binnen de wettelijke reactietermijn van 6 maanden richting de OVV schriftelijk reageren. Uw Kamer zal daarover worden geïnformeerd. Ook zal uiteraard worden bezien op welke wijze het kabinet de aanbevelingen kan meenemen ten behoeve van de ontwikkeling van een integrale Nederlandse cybersecuritystrategie en het verder versterken van het cybersecuritystelsel in Nederland en Europa.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus