Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 **Informatie- en communicatietechnologie (ICT)**

36 084 **Wijziging van de Wet beveiliging netwerk- en informatiesystemen in verband met de uitbreiding van de bevoegdheid van de Minister van Justitie en Veiligheid om dreigings- en incidentinformatie over de netwerk- en informatiesystemen van niet-vitale aanbieders te verstrekken aan deze aanbieders en aan organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten ten behoeve van deze aanbieders**

Nr. 861 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 1 juni 2022

Tijdens het debat met de Commissie Digitale Zaken van uw Kamer op 25 mei jl. over de eventuele anticipatie op het wetsvoorstel tot wijziging van de Wet beveiliging netwerk- en informatiesystemen (Wbni) heb ik toegezegd om uw Kamer nader te informeren over het aantal gevallen waarin het Nationaal Cyber Security Centrum (NCSC) in de afgelopen periode genoodzaakt was informatie te delen met andere niet-vitale aanbieders of hun schakelorganisaties.

Aanleiding

Het NCSC ontvangt dagelijks informatie over meer dan 500.000 kwetsbare, misbruikte of gecompromitteerde Nederlandse computersystemen. Het is van belang dat het NCSC deze dreigings- en incidentinformatie kan analyseren en, indien nodig, zo snel mogelijk kan verspreiden, zodat aanbieders actie kunnen ondernemen tegen digitale aanvallen en de mogelijke impact hiervan kunnen beperken. Primair deelt het NCSC deze informatie direct met onderdelen van de rijksoverheid en vitale aanbieders. Daarnaast deelt het NCSC deze informatie waar mogelijk met andere schakelorganisaties binnen het Landelijk Dekkend Stelsel, zoals het Digital Trust Center.

Bij inwerkingtreding van de Wbni in 2019 is vrij snel een weeffout geconstateerd. Hierdoor is het voor het NCSC lang niet altijd mogelijk om informatie te delen met deze schakelorganisaties. Hierdoor weet het NCSC

kst-26643-861
ISSN 0921 - 7371
's-Gravenhage 2022

dat bepaalde aanbieders kwetsbaar zijn voor digitale aanvallen, maar mogen zij deze andere niet-vitale aanbieders of hun schakelorganisaties hier niet over informeren. Dit gaat bijvoorbeeld om schakelorganisaties in de hightech industrie en de Rotterdamse Haven of individuele organisaties zoals politieke partijen en distributeurs van voedselwaren. Over de belemmeringen die het NCSC ondervindt bij informatiedeling is eerder de nodige aandacht geweest, bijvoorbeeld in de aanbevelingen van de Cyber Security Raad en de Onderzoeksraad voor Veiligheid en in de media. Ook zijn hierover in het verleden diverse Kamervragen gesteld. Daarom is vorig jaar zomer het wetsvoorstel tot wijziging van de Wbni in procedure gebracht die vorige maand bij uw Kamer is ingediend. Met dit wetsvoorstel wordt het voor het NCSC mogelijk om in ruimere zin dreigings- en incidentinformatie te delen met schakelorganisaties of direct met andere niet-vitale aanbieders.

Vanwege de oorlog in Oekraïne is er op dit moment sprake van een reële digitale dreiging die mogelijk grote gevolgen voor andere niet-vitale aanbieders kan hebben én daarmee een grote impact voor de Nederlandse samenleving. Daarom heb ik uw Kamer op 13 mei jl. (Kamerstuk 36 084, nr. 5) een brief gezonden en hierin mijn dilemma uiteengezet om in zeer uitzonderlijke gevallen te anticiperen op het wetsvoorstel tot wijziging van de Wbni. In bovenbedoeld debat van 25 mei jl. over deze brief heb ik uw Kamer laten weten dat het NCSC eerder bij hoge uitzondering, vooruitlopend op de inwerkingtreding van het wetsvoorstel, in ruimere zin dreigings- of incidentinformatie heeft moeten delen met andere niet-vitale aanbieders of hun schakelorganisaties. Het overzicht van deze gevallen vindt u, zoals toegezegd, in de bijlage.

Toelichting overzicht

Het overzicht ziet op de periode vanaf 1 januari 2019, het moment dat de Wbni volledig in werking is getreden. Van de genoemde grote hoeveelheid informatie die het NCSC dagelijks ontvangt, zag het NCSC zich bij hoge uitzondering in achtentwintig gevallen genoodzaakt om deze dreigings- en incidentinformatie te delen met andere niet-vitale aanbieders of hun schakelorganisaties. Hierbij is alleen informatie gedeeld die noodzakelijk is, zoals bijvoorbeeld specifieke getroffen IP-adressen, gebruikersnamen en computernamen, om maatregelen te treffen. Het NCSC heeft hierbij geen bijzondere persoonsgegevens gedeeld. In deze gevallen heeft het NCSC telkens een zorgvuldige afweging gemaakt waarbij met name is gekeken naar de ernst van een dreiging en de impact daarvan voor belanghebbende aanbieders.

Door deze informatie te delen heeft het NCSC digitale aanvallen op de Nederlandse economie en samenleving kunnen afweren. Hiermee zijn onder meer grote ransomware-aanvallen voorkomen, hebben aanbieders de continuïteit van hun dienstverlening kunnen waarborgen en is kwaadwillenden de toegang tot grote hoeveelheden, mogelijk gevoelige informatie over bedrijfsprocessen, klanten of burgers verhinderd. Hierdoor zijn mogelijk ook verstorende keteneffecten richting vitale aanbieders of onderdelen van de rijksoverheid uitgebleven. Concreet betekent dit dat organisaties, zoals belangrijke commerciële dienstverleners, of publieke instellingen, zoals veiligheidsregio's, een provincie of een ambulancedienst, soms op het laatste moment grote potentiële schade hebben voorkomen.

De zorgvuldige afweging die hierbij is gemaakt in het kader van de digitale veiligheid heeft geleid tot een integraal en aangescherpt afwegingskader dat ik eerder met uw Kamer heb gedeeld. Eventuele toekomstige uitzonderlijke gevallen zullen aan de hand van dit vaste

afwegingskader worden beoordeeld. Zoals door mij voorgesteld in het commissiedebat van 25 mei jl. zal vanaf heden uw Kamer per geval, waar mogelijk open en indien nodig vertrouwelijk, zo spoedig mogelijk achteraf navolgbaar worden geïnformeerd.

Indien gewenst bied ik uw Kamer graag een vertrouwelijke briefing aan, waarin de casuïstiek in de bijlage nader kan worden toegelicht.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius