Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 864

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 27 juni 2022

In het debat over online veiligheid en cybersecurity van 7 april jl. (Kamerstuk 26 643, nr. 849) heeft het lid Bontenbal (CDA) gevraagd wat voor soort bedrijven bij het Digital Trust Center zijn aangesloten op de informatiedienst die bedrijven waarschuwt over ernstige digitale dreigingen en kwetsbaarheden en over het soort bedrijven dat ongevraagd is geïnformeerd. De Minister van Justitie en Veiligheid heeft in het debat toegezegd dat ik u hierover voor de zomer een brief zal sturen en over de voortgang van deze informatiedienst. Met deze brief wil ik de toezegging gestand doen.

Zomer 2021 – Informatiedienst Digital Trust Center van start gegaan

Het Digital Trust Center is in juni 2021 gestart met de informatiedienst, nadat zij de zogenaamde OKTT-status[1] van het Ministerie van JenV heeft ontvangen. Met deze OKKT-status kan het Digital Trust Center dreigingsinformatie ontvangen van het Nationaal Cybersecurity Centrum. Hierover is uw Kamer geïnformeerd op
2 juni 2021[2] en 7 februari 2022.[3] Sinds de zomer van 2021 worden individuele niet-vitale bedrijven actief geïnformeerd over bij de overheid bekende ernstige digitale dreigingen en kwetsbaarheden (hoge kans, hoge impact). De informatiedienst heeft twee aandachtsgebieden, namelijk het informeren van bedrijven waar het Digital Trust Center nog geen relatie mee heeft en het informeren van bedrijven die zich actief hebben aangemeld voor een pilot. De informatiedienst is nog in opbouw, dus informatie delen gebeurt op dit moment op beperkte schaal. De informa-

[1] OKTT: «organisatie met objectief kenbaar tot taak» (OKTT) om organisaties of het publiek te informeren over dreigingen en incidenten die voor hen relevant zijn. Dit kan een samenwerkingsverband zijn binnen een branche, een regio of een keten.
[2] Kamerstuk 26 643, nr. 760.
[3] Kamerstuk 26 643, nr. 817.

kst-26643-864
ISSN 0921 - 7371
's-Gravenhage 2022

tiedienst wordt de komende jaren op basis van opgedane kennis en ervaringen stapsgewijs uitgebreid.

Informatiedienst: notificeren van bedrijven waar het Digital Trust Center nog geen relatie mee heeft

Bij het notificeren van individuele bedrijven waar het Digital Trust Center nog geen relatie mee heeft, waarschuwt het Digital Trust Center, na het achterhalen van de contactgegevens van deze bedrijven, telefonisch of per mail over ernstige cyberdreigingen. Deze waarschuwing bevat ook relevant handelingsperspectief toegespitst op de betreffende dreiging. In de periode zomer 2021 tot en met eind 2021 zijn er 15 verschillende aanleidingen geweest om bedrijven direct te waarschuwen.

Hiertoe heeft het Digital Trust Center 361 bedrijven gewaarschuwd voor een ernstige cyberdreiging. Bij het inrichten van de Informatiedienst is uitgegaan van dataminimalisatie. Dat betekent dat het Digital Trust Center geen metadata verzamelt en vastlegt over het soort bedrijven, de omvang van de bedrijven of de branche waarin de bedrijven actief zijn. In 2022 zijn (peildatum 15 juni) 31 aanleidingen geweest om 1378 bedrijven te waarschuwen voor een ernstige cyberdreiging.

De dreigingen waarvoor gewaarschuwd wordt gaan met name over apparatuur en software waar een kwetsbaarheid is geconstateerd en die verbonden zijn met het internet. Ongeautoriseerden kunnen op deze wijze toegang krijgen tot bedrijfssystemen, met als gevolg dat het bedrijf slachtoffer kan worden van ransomware of diefstal van bedrijfsgegevens. Gewaarschuwde bedrijven reageren over het algemeen erg positief op het ontvangen van de waarschuwing.

Pilot notificeren van bedrijven aangemeld bij het Digital Trust Center

Om ook bij grootschalige cyberdreigingen, die duizenden individuele bedrijven kunnen raken, tijdig te kunnen waarschuwen, onderzoekt het Digital Trust Center de schaalbaarheid van de informatiedienst. Daarom loopt er parallel aan de uitrol van de informatiedienst zoals hierboven beschreven, een pilot met bedrijven die zich bij het Digital Trust Center hebben aangemeld. Met een testgroep van 57 bedrijven wordt in een pilot van 12 maanden onderzocht of de dienst geautomatiseerd kan worden.

De bedrijven die deelnemen aan de pilot vertegenwoordigen negen sectoren om zo een spreiding te hebben over het Nederlandse bedrijfsleven.[4] Deze bedrijven hebben hun contact- en technische gegevens, zoals IP-adressen of domeinnamen aangeleverd waardoor het Digital Trust Center, in samenwerking met het Nationaal Cyber Security Centrum, deze gegevens kan matchen met bij hen bekende cyberdreigingen. Het Digital Trust Center vult deze informatie aan met andere beschikbare (openbare) bronnen. Bij een match wordt vervolgens geautomatiseerd een waarschuwing verstuurd. Op 15 oktober 2021 is de eerste deelnemer genotificeerd over kwetsbaarheden die betrekking hadden op meerdere systemen van het desbetreffende bedrijf. Sinds de eerste melding in oktober 2021 tot de peildatum van 12 mei 2022 hebben 32 van de deelnemende partijen een notificatie ontvangen. In totaal gaat het hierbij om 182 notificaties over kwetsbaarheden en/of dreigingen, dit betekent

[4] Deelnemende bedrijven worden geclassificeerd onder sectoren: 1) gezondheidszorg en welzijn, 2) handel en dienstverlening, 3) ICT, 4) landbouw, natuur en visserij 5) media en communicatie 6) onderwijs, cultuur en wetenschap 7) techniek, productie en bouw 8) transport en logistiek 9) food&retail en scheepsbouw.

dat er een aantal deelnemende partijen meerdere notificaties heeft ontvangen.

Eerste beeld pilot

De pilot is opgezet om ervaring op te doen met het geautomatiseerd verwerken van dreigingsinformatie op basis van door bedrijven aangeleverde contact- en technische gegevens. Daarnaast moet de pilot inzicht geven in de snelheid en de schaalbaarheid van deze informatiedeling. Het eerste beeld is dat het beschikken over de contact- en technische gegevens de snelheid van informatiedeling kan bevorderen. Het verkrijgen en verwerken van de technische gegevens van deelnemers aan de pilot was daarentegen zeer arbeidsintensief. Voor het breder uitrollen van de pilot richting het overige Nederlandse bedrijfsleven is het nodig om te kijken naar mogelijk efficiëntere distributiemodellen.

Vervolg

Zoals hierboven aangegeven zijn snelheid van informatiedeling en schaalbaarheid voor het Digital Trust Center zeer belangrijke uitgangspunten voor een succesvolle dienstverlening. De komende maanden wordt nader onderzocht, hoe en op welke wijze de voorlopige beelden uit de pilot kunnen worden gebruikt om een toekomstbestendige, schaalbare dienstverlening op te zetten. Hierbij wordt niet alleen gekeken naar technische oplossingen, maar ook naar organisatorische oplossingen. Nauwere samenwerking met het Nationaal Cybersecurity Centrum en met publiek-private partijen kan een goede bijdrage leveren aan de schaalbaarheid. Het Nationaal Cybersecurity Centrum, het Digital Trust Center en het Cyber Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP) hebben de wens te komen tot verdergaande samenwerking in de uitvoering van informatiedeling en het verhogen van cyberweerbaarheid. De vorm van deze verdergaande samenwerking wordt momenteel nader verkend.

Parallel aan deze verkenning wil het Digital Trust Center blijven innoveren om het bedrijfsleven te bereiken met dreigingsinformatie. Zoals gezegd is uit de pilot gebleken dat het beschikken over contact- en technische gegevens de snelheid bevordert waarmee informatie kan worden gedeeld. Om deze informatie sneller ter beschikking te hebben zet het Digital Trust Center, onder andere in samenwerking met het Nationaal Cybersecurity Centrum, in op een nieuwe internetstandaard, namelijk security.txt. Deze standaard maakt het mogelijk dat een bedrijf via een eenvoudig tekstbestand op zijn server vinders van digitale dreigingen en kwetsbaarheden in de gelegenheid stelt om deze te melden op een vooraf opgegeven contactadres. Vervolgens heeft de ontvanger de mogelijkheid om actie te ondernemen op de dreiging of kwetsbaarheid.

Om deze werkwijze breed te kunnen uitrollen is het Digital Trust Center onder meer in gesprek met het Forum voor Standaardisatie en het Nationaal Cyber Security Centrum. Een brede adoptie van deze standaard kan leiden tot de gewenste snelle informatieoverdracht en de vergroting van het bereik van het Digital Trust Center.

Omdat niet alle bedrijven op korte termijn deze nieuwe internetstandaard gaat adopteren, blijft het Digital Trust Center ook bedrijven waar het Digital Trust Center geen relatie mee heeft, waarschuwen bij ernstige dreigingen.

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens