Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2008

Vragen van de leden **Van Dam**, **Van den Berg** en **Van der Molen** (allen CDA) aan de Minister van Justitie en Veiligheid over *het bericht «Exclusief: Interview Citrix CISO, Fermín Sera, waar ging het mis?»* (ingezonden 31 januari 2020).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid), mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 6 maart 2020). Zie ook Aanhangsel Handelingen, vergaderjaar 2019–2020, nr. 1816.

Vraag 1
Heeft u kennisgenomen van het bericht op Techzine.be van 27 januari 2020 «Exclusief: Interview Citrix CISO, Fermín Sera, waar ging het mis?»?[1]

Antwoord 1
Ja.

Vraag 2
Klopt het dat er op 17 december 2019 een tijdelijke oplossing van het beveiligingslek beschikbaar werd gesteld door Citrix en dat met deze oplossing, mits goed doorgevoerd, gebruikers van Citrix beschermd waren geweest tegen het beveiligingslek?

Antwoord 2
Citrix heeft op 17 december 2019 de kwetsbaarheid bekend gemaakt en tussentijdse mitigerende maatregelen beschikbaar gesteld voor de kwetsbare Citrix-producten. Of bij goed doorvoeren gebruikers beschermd waren tegen de kwetsbaarheid, hangt af van meer factoren dan alleen het al dan niet juist doorvoeren van deze maatregelen. Na de bekendmaking van de kwetsbaarheid door Citrix, heeft het Nationaal Cyber Security Centrum (NCSC) op 18 december 2019 in een beveiligingsadvies geadviseerd om de door Citrix beschikbaar gestelde tussentijdse mitigerende maatregelen door te voeren. In januari 2020, heeft het NCSC op basis van de toen beschikbare informatie geconcludeerd dat niet alleen als de tussentijdse mitigerende maatregelen niet of niet goed waren doorgevoerd, maar ook als deze niet vóór 9 januari 2020 op de juiste wijze waren doorgevoerd, organisaties ervan moesten uitgaan dat hun systemen niet beschermd waren. Daarnaast heeft Citrix

[1] Techzine, 27 januari 2020, https://www.techzine.be/blogs/security/52120/exclusief-interview-citrix-ciso-fermin-serna-waar-ging-het-mis/

ah-tk-20192020-2008
ISSN 0921 - 7398
's-Gravenhage 2020

16 januari 2020 aan het NCSC gemeld dat de tijdelijke beschikbaar gestelde oplossing bij één softwareversie mogelijk niet effectief is geweest. Dit was ten tijde van bekendmaking van de kwetsbaarheid door Citrix nog niet bekend. Het NCSC heeft steeds zijn adviezen afgestemd op de laatst beschikbare informatie. Voor een overzicht hiervan verwijs ik u naar de brieven aan uw Kamer over dit onderwerp van 20 en 23 januari 2020.[2]

Vraag 3, 4
Indien het klopt wat de CISO van Citrix beschrijft ten aanzien van de tijdelijke oplossing, waarom is deze oplossing dan niet doorgevoerd bij de overheidsdiensten die gebruik maken van Citrix?
Is er sprake geweest van overheidsdiensten of semipublieke organisaties die de tijdelijke patch die op 17 december 2019 werd gepubliceerd door Citrix onjuist hebben doorgevoerd? Doet u daar onderzoek naar?

Antwoord 3, 4
Het beveiligingsadvies van het NCSC van 18 december 2019 is op 24 december 2019 verhoogd naar het hoogste niveau (high/high: hoge kans op misbruik én hoge schade aan systemen bij misbruik). De overheid hanteert de Baseline Informatiebeveiliging Overheid (BIO) als basisnormenkader voor haar informatiebeveiliging. Ten aanzien van kwetsbaarheden met een hoge kans op misbruik en een hoge schade aan systemen bij misbruik (high/high) schrijft de BIO voor kwetsbaarheden binnen één week op te lossen en in de tussentijd mitigerende maatregelen te treffen op basis van een risicoafweging.
Er zijn bij het NCSC en CIO-Rijk geen aanwijzingen dat Rijksoverheidsdiensten de tussentijdse mitigerende maatregelen van Citrix van 17 december 2019 onjuist hebben doorgevoerd. Wel is bij het NCSC bekend dat er binnen de rijksoverheid nog organisaties waren die deze oplossing niet of niet tijdig hebben doorgevoerd. Informatie van semipublieke organisaties is niet beschikbaar.
Ten aanzien van medeoverheden (provincies, gemeenten en waterschappen) zijn er geen aanwijzingen bij het Ministerie van BZK dat de tussentijdse mitigerende maatregelen van Citrix van 17 december 2019 onjuist zijn doorgevoerd. Overheden zijn autonome bestuursorganen en zijn zelf verantwoordelijk voor hun informatieveiligheidsbeleid, inbegrepen de risicoafweging die zij maken en de maatregelen die zij treffen.
Deze casus wordt geëvalueerd in opdracht van de Minister van Justitie en Veiligheid. De daaruit geleerde lessen worden samen met de kabinetsreactie op het WRR-rapport «Voorbereiden op digitale ontwrichting» met uw Kamer gedeeld.

Vraag 5
Kunt u lering trekken uit de wijze waarop andere landen om zijn gegaan met dit beveiligingslek? Kunt u verklaren waarom met name in Nederland dit beveiligingslek tot grote problemen heeft geleid?

Antwoord 5
Elk land maakt eigen afwegingen met betrekking tot kwetsbaarheden in informatie- en netwerksystemen. Internationaal heeft Nederland snel, maar niet als enige gehandeld als het gaat om advisering over hoe om te gaan met deze kwetsbaarheid. Door het NCSC is meerdere malen contact en afstemming geweest met collega-organisaties in het buitenland.

Vraag 6
Hoe beoordeelt u de ongeschreven regel in de industrie die zegt dat er binnen 90 dagen nadat een beveiligingslek wordt gemeld, deze niet publiekelijk wordt gemaakt, zodat een bedrijf het lek kan dichten? Acht u het wenselijk dat een dergelijke periode formeel wordt vastgelegd, al dan niet op Europees niveau?

[2] Kamerstukken II 2019/20, 26 643, nr. 658/Kamerstukken II 2019/20, 26 643, nr. 660.

Antwoord 6
Zodra een kwetsbaarheid publiek bekend wordt gemaakt, stellen veel leveranciers in beginsel zo snel mogelijk een sluitende oplossing beschikbaar, zodat de kans op misbruik kan worden beperkt. In de Leidraad Coordinated Vulnerability Disclosure[3] van het NCSC zijn bouwstenen opgenomen die organisaties kunnen gebruiken voor het maken van een eigen beleid t.a.v. het verhelpen van kwetsbaarheden. In deze leidraad wordt een richtlijn meegegeven van 60 dagen voor het kunnen verhelpen van kwetsbaarheden in software voordat deze publiekelijk worden gemaakt, zodat de leverancier voldoende tijd heeft om bij bekendmaking ook een oplossing beschikbaar te hebben. In het geval van de Citrix kwetsbaarheid zijn er ten tijde van bekendmaking van de kwetsbaarheid alleen tussentijdse mitigerende maatregelen beschikbaar gesteld. Elke kwetsbaarheid is anders en elke leverancier kan eigen richtlijnen hanteren voor het tijdig verhelpen van een kwetsbaarheid. Per leverancier, maar ook rekening houdend met het type systemen, zal maatwerk nodig zijn. Ik hecht er wel waarde aan dat bedrijven omwille van veiligheid van ICT-systemen een duidelijk beleid hanteren voor het zo snel mogelijk verhelpen van kwetsbaarheden.

[3] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/cvd-leidraad