Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

Aanhangsel van de Handelingen

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

3477

Vragen van het lid **Verhoeven** (D66) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over *Europese dreiging van de Eternal Blue exploit* (ingezonden 4 juni 2019).

Antwoord van Staatssecretaris **Knops** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de Minister van Justitie en Veiligheid (ontvangen 16 juli 2019).

Vraag 1
Kent u het artikel «In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc»?[1]

Antwoord 1
Ja.

Vraag 2
Hoe beoordeelt u de cyberaanval op Baltimore door digitale «afpersers», waarbij e-mail, vastgoedtransacties, rekeningen van waterbedrijven, medische noodoproepen en vele andere diensten zijn geraakt?

Antwoord 2
Gelet op de samenhang in de vragen 2, 3 en 4 is ervoor gekozen de beantwoording van deze vragen samen te voegen.

Vraag 3
Hoe analyseert u de gevolgen voor het (openbare) leven in de stad? Kunt u daarbij in het bijzonder ingaan op de impact die het heeft gehad op de lokale overheid van Baltimore? Welke kosten heeft de lokale overheid van Baltimore hierdoor moeten maken?

Antwoord 3
Gelet op de samenhang in de vragen 2, 3 en 4 is ervoor gekozen de beantwoording van deze vragen samen te voegen.

[1] https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html

ah-tk-20182019-3477
ISSN 0921 - 7398
's-Gravenhage 2019

Vraag 4
Herkent u de toenemende dreiging van het misbruik van de Eternal Blue exploit voor Europa en Nederland door cybercriminelen? Zo nee, waarom niet? Zo ja, hoe bereidt u zich voor op dergelijke aanvallen?

Antwoord 4
Aanvallen als deze zijn zeer onwenselijk en het is uitermate vervelend dat burgers (tijdelijk) niet kunnen beschikken over overheidsdiensten waar ze normaal gesproken op moeten kunnen vertrouwen. De lokale overheid van Baltimore heeft gemeld dat alle diensten bereikbaar en leverbaar zijn, zij het soms via alternatieven als tijdelijke mailadressen. Over de kosten zijn geen mededelingen gedaan, anders dan dat de lokale overheid niet aan het verzoek tot betaling van het losgeld zal voldoen[2].
Het kabinet doet er alles aan om te voorkomen dat een dergelijke situatie zich in Nederland zal voordoen. Mogelijke dreigingen worden zeer serieus genomen en risico's worden, waar mogelijk, gemitigeerd. Ten aanzien van Eternal Blue kan gezegd worden dat het kabinet bekend is met deze exploit en de dreiging die daarvan uitgaat. In het Cyber Security Beeld Nederland (CSBN) 2018 is deze exploit al meerdere keren genoemd[3]. In het in 2017 gepubliceerde beveiligingsadvies (NCSC-2017–0229[4]) van het Nationaal Cyber Security Centrum (NCSC) werd de kans op misbruik van de kwetsbaarheid, door gebruik van deze exploit, als «hoog» geclassificeerd. Deze classificatie was vanwege actief misbruik van deze kwetsbaarheid, met een hoge kans op schade wanneer een organisatie getroffen wordt. Dit beveiligingsadvies is nog steeds van kracht. Het NCSC blijft de ontwikkelingen nauwlettend volgen en indien er reden toe is zal het beveiligingsadvies worden aangepast. Op dit moment is daar echter geen aanleiding voor.
Ten aanzien van het voorbereiden van organisaties op digitale aanvallen is het van belang te melden dat dit kabinet via de Nederlandse Cyber Security Agenda (NCSA) investeert in het versterken van de digitale weerbaarheid. Zo wordt met de uitvoering van verschillende maatregelen onder de NCSA het Nederlandse stelsel van samenwerkingsverbanden versterkt. Door dit stelsel wordt informatie over kwetsbaarheden bij zo veel mogelijk organisaties bekend en kunnen organisaties passende maatregelen treffen. Voor het bereiken van de organisaties die buiten de vitale infrastructuur en de rijksoverheid vallen, is in 2018 het Digital Trust Center (DTC) in het leven geroepen. Het DTC en het NCSC werken samen om, ter verhoging van de cyberweerbaarheid van de onderscheidenlijke doelgroepen (niet-vitale bedrijfsleven; rijksoverheid en vitale bedrijven), zo veel als mogelijk informatie te kunnen ontsluiten. Het uitgangspunt daarbij is dat organisaties binnen genoemde doelgroepen zelf het best in staat zijn om vanuit hun eigen verantwoordelijkheid en inzicht in de bedrijfsprocessen, te bepalen hoe zij patchmanagement voor hun organisatie hebben georganiseerd. Uitstel of afstel van updates en het nemen van alternatieve mitigerende maatregelen kan voor een organisatie soms een keuze zijn in verband met de continuïteit van processen. Wanneer het echter misgaat kan het wel grote gevolgen hebben. Daarom wordt bijvoorbeeld op de website van het NCSC ook informatie gedeeld over het inrichten van patchmanagement om organisaties daarbij te helpen. Daarnaast is er een actieve rol voor het DTC om het niet-vitale bedrijfsleven daarin goed te bereiken. Vanzelfsprekend wordt ook op de website van het Digital Trust Center informatie gedeeld over onder andere updates.

Vraag 5
Hoe beoordeelt u het feit dat Nederland op de achtste plaats staat als het gaat om machines die nog steeds gebruik maken van het SMBv1-protocol waar de Eternal Blue exploit gebruik van kan maken?[5]

---

[2] https://www.baltimorecity.gov/ransomware-faq
[3] Het CSBN wordt jaarlijks vastgesteld door de NCTV en biedt inzicht in de belangen, dreigingen, weerbaarheid en daarmee samenhangende ontwikkelingen op het gebied van cybersecurity.
[4] https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2017–0229+1.01+MS17–010+Microsoft+verhelpt+kwetsbaarheden+in+Windows+SMB+Server.html
[5] https://www.welivesecurity.com/2019/05/17/eternalblue-new-heights-wannacryptor/#single-post-fancybox-1

Antwoord 5
Uiteraard is het zorgelijk dat wordt gesignaleerd dat machines in Nederland mogelijk nog steeds kwetsbaar zijn voor misbruik doordat updates niet zijn gedraaid. Echter de hoge score in de lijst hangt samen met de hoge mate van digitale connectiviteit van Nederland. Nederland is immers één van de meest gedigitaliseerde landen ter wereld. Ondanks deze wetenschap is het belangrijk ervoor te zorgen dat machines in Nederland weerbaar zijn. Het NCSC adviseert met het oog hierop, net als bij alle andere bekende kwetsbaarheden, om systemen tijdig en volledig te updaten met de meest recente beveiligingsupdates of alternatieve mitigerende maatregelen te treffen. Hierover publiceert het NCSC zoals gezegd beveiligingsadviezen. Sinds de komst van het DTC is er ook een mogelijkheid om het niet-vitale bedrijfsleven actief te benaderen. Het NCSC en het DTC werken samen om beveiligingsadviezen zo breed mogelijk te delen.

Vraag 6
Welke maatregelen neemt u om het patchbeleid bij overheden te stimuleren? Ziet u naar aanleiding van de toenemende dreiging van de Eternal Blue exploit aanleiding aanvullende maatregelen te nemen? Zo nee, waarom niet?

Antwoord 6
Ik zie vanwege deze ene specifieke kwetsbaarheid geen reden het overheidsbrede patchbeleid aan te passen, zoals dat is opgesteld in de Baseline Informatiebeveiliging Overheid[6] (BIO). De BIO bevat ten aanzien van kwetsbaarheden en patches de volgende bepalingen:
Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken. (12.6.1)
Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen. (12.6.1.1)
Zoals gezegd wordt de kans op misbruik van deze kwetsbaarheid sinds 2017 door het NCSC als «hoog» geclassificeerd vanwege actief misbruik dat is waargenomen. In geval van een kwetsbaarheid met een hoge kans op misbruik en hoge vervolgschade neemt het NCSC actief contact op met organisaties in haar doelgroep (rijksoverheid, vitale bedrijven), met het advies direct actie te ondernemen. Het beveiligingsadvies van het NCSC omtrent deze kwetsbaarheid en de daarmee samengaande maatregelen zijn nog steeds van kracht.
Tot slot is het goed te vermelden dat in Baltimore de gemeente werd getroffen. In Nederland is in een dergelijk geval de Informatiebeveiligingsdienst (IBD) het sectorale computercrisisteam voor alle Nederlandse gemeenten. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en werkt daartoe onder meer samen met het NCSC.

Vraag 7
Kunt u elke vraag afzonderlijk beantwoorden?

Antwoord 7
Gelet op de samenhang in de vragen 2, 3 en 4 is ervoor gekozen de beantwoording van deze vragen samen te voegen.

[6] De Baseline Informatiebeveiliging Overheid is op 16 april 2019 gepubliceerd in de Staatscourant (Staatscourant 2019 nr. 26526)