Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1218

BRIEF VAN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 10 september 2024

Tijdens de regeling van werkzaamheden op 3 september verzocht mevrouw Kathmann (PvdA-GL) om een brief over recente digitale incidenten, namelijk het lekken van metadata bij Webex in juni, de updatefout van CrowdStrike in juli, en de softwarefout bij Defensie van eind augustus. In deze brief zal ik eerst een korte toelichting geven op hoe cybersecurity binnen het kabinet wordt opgepakt en u vervolgens informeren over de drie recente incidenten.

Nederlandse Cybersecurity Strategie

Binnen het kabinet is de Minister van Justitie en Veiligheid coördinerend bewindspersoon voor het cybersecuritybeleid. Het brede cybersecurity-beleid van het kabinet is uiteengezet in de Nederlandse Cybersecurity Strategie (NLCS) 2022–2028. De volgende NLCS-voortgangsrapportage wordt eind oktober met uw Kamer gedeeld. Hierin zal de Minister van Justitie en Veiligheid de voortgang op de verschillende acties uit de NLCS beschrijven en zal hij daarnaast overkoepelend ingaan op incidenten zoals CrowdStrike en NAFIN.

In deze brief beperk ik mij, als verantwoordelijk bewindspersoon voor digitalisering, daarom tot uitsluitend nieuwe informatie die aan het licht is gekomen en de impact hiervan op de (rijks)overheid.

kst-26643-1218
ISSN 0921 - 7371
's-Gravenhage 2024

Recente incidenten

Webex

Uw Kamer is reeds geïnformeerd over het incident bij de rijksvideovergadervoorziening Webex per Kamerbrief d.d. 5 juni jl.[1] en 7 juni jl.[2]

Naar aanleiding van de gevonden kwetsbaarheden is een beveiligingsonderzoek uitgevoerd door onafhankelijke onderzoekers. Uit dit onderzoek zijn nog een aantal kwetsbaarheden gevonden, die inmiddels ook zijn verholpen.

CrowdStrike

Uw Kamer is door de Minister van Justitie en Veiligheid reeds geïnformeerd over de computerstoring CrowdStrike per Kamerbrief d.d. 19 juli jl.[3]

Op 19 juli jl. waren er computerstoringen die in Nederland en wereldwijd hebben plaatsgevonden als gevolg van een software-update van het programma Falcon Sensor van het cybersecuritybedrijf CrowdStrike.

CrowdStrike heeft tevens op 19 juli een workaround, incl. later op de dag een geautomatiseerde versie van de workaround, beschikbaar gesteld. Microsoft heeft een recoverytool beschikbaar gesteld voor getroffen organisaties.

Defensie – NAFIN

Uw Kamer is geïnformeerd door de Minister van Defensie over de IT-storing bij Defensie en andere overheidsdiensten per Kamerbrief d.d. 28 augustus jl.[4] Conform deze Kamerbrief zal uw Kamer nader geïnformeerd worden zodra er meer bekend is.

Conclusie

Er is geen indicatie dat de incidenten van de afgelopen drie maanden op enigerlei wijze aan elkaar gerelateerd zijn. Wel maken de diverse incidenten de afhankelijkheid van de rijksoverheid van netwerk- en informatiesystemen zichtbaar en de impact op de dienstverlening van de (rijks)overheid wanneer deze systemen tijdelijk uitvallen. Deze afhankelijkheid is onvermijdelijk. Daarom is het van belang dat alle (rijks)overheidsorganisaties naast het nemen van maatregelen ook plannen maken voor wanneer systemen toch uitvallen. Overheidsorganisaties moeten voorbereid zijn op uitval en ook veel oefenen. Het kabinet blijft daarom inzetten op de Nederlandse Cybersecurity Strategie 2022–2028 (NLCS) en de acties uit het actieplan.

In de komende periode worden de afgelopen incidenten geëvalueerd en worden, waar nodig, acties uitgezet om de digitale weerbaarheid van de rijksoverheid verder te verbeteren.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
F.Z. Szabó

---

[1] Kamerstuk 26 643, nr. 1181
[2] Kamerstuk 26 643, nr. 1182
[3] Kamerstuk 26 643, nr. 1212
[4] Kamerstuk 26 643, nr. 1214