Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1212

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 19 juli 2024

Met deze brief informeer ik uw Kamer over de computerstoringen die in Nederland en wereldwijd hebben plaatsgevonden als gevolg van een softwareupdate van het programma Falcon Sensor van het cybersecurity-bedrijf Crowdstrike. Deze software wordt gebruikt voor het beveiligen van servers en computers. De update heeft geleid tot verstoringen in de dienstverlening van organisaties die gebruik maken van deze software. De NCTV en het Nationaal Cybersecurity Centrum (NCSC) hebben op dit moment geen indicaties dat deze verstoringen moedwillig tot stand zijn gekomen. Daarnaast informeer ik uw Kamer over de tot op heden genomen acties door het NCSC.

Impact van de computerstoring

Veel organisaties in Nederland en wereldwijd maken gebruik van de diensten van Crowdstrike, een cybersecuritybedrijf uit de Verenigde Staten. Sinds de update van 19 juli 2024 raken systemen waar deze software op draait verstoord tijdens het opstartproces, en kunnen daardoor niet meer goed worden gebruikt.

De NCTV heeft met interdepartementale partners een inventarisatie gemaakt van de impact van deze verstoring in Nederland binnen de verschillende sectoren waarvoor zij verantwoordelijk zijn. Uit deze inventarisatie, berichtgeving in de media en informatie van het NCSC blijkt dat de verstoring in Nederland impact heeft op organisaties binnen de (Rijks)overheid en in onder andere de zorg en de transportsector (luchtvaart, maritiem en openbaar vervoer). In sommige gevallen is de dienstverlening van deze organisaties verstoord of stilgelegd.

Als gevolg van de *workaround* die ter beschikking is gesteld door Crowdstrike, lijken de gevolgen van de storing gedurende de dag af te nemen en kan de getroffen dienstverlening weer worden opgestart.

kst-26643-1212
ISSN 0921 - 7371
's-Gravenhage 2024

Acties vanuit de leverancier

Er is op dit moment nog geen patch beschikbaar vanuit Crowdstrike om de verstoring te verhelpen, en het is ook nog niet bekend wanneer de leverancier dit zal doen. Wel heeft Crowdstrike op 19 juli 2024 een *workaround* beschikbaar gesteld, waarmee de verstoring kan worden opgelost bij getroffen systemen. Het uitvoeren van deze *workaround* is echter arbeidsintensief en kan (afhankelijk van de inrichting van de netwerken van een organisatie) veel tijd kosten.

Acties vanuit de Rijksoverheid

Door het NCSC is in de ochtend van 19 juli 2024 een doelgroepenbericht uitgestuurd. Hierin worden organisaties die gebruik maken van Falcon Sensor geadviseerd om de laatste update niet te installeren totdat er een geverifieerde oplossing beschikbaar is. Indien deze update toch is geïnstalleerd, wordt deze organisaties geadviseerd om de door Crowdstrike aangeboden *workaround* uit te voeren. Later op de dag op 19 juli 2024 is dit bericht aangevuld met aanvullend handelingsperspectief voor organisaties voor wie de oorspronkelijke *workaround* nog niet effectief was.

Dit bericht is door het NCSC verspreid onder de doelgroeporganisaties van het NCSC (de Rijksoverheid en vitale sectoren). Daarnaast is dit bericht ook verspreid onder schakelorganisaties binnen het Cyberweerbaarheidsnetwerk, zodat deze organisaties ook hun eigen achterban kunnen informeren. Binnen het Cyberweerbaarheidsnetwerk wordt in publiek-privaat verband samengewerkt om dreigingsinformatie snel onderling te kunnen delen.[1] Het bericht is ook openbaar beschikbaar via de website van het NCSC.

Zoals eerder aangegeven staat de NCTV in nauw contact met de verschillende betrokken overheidsorganisaties, inclusief de ministeries die verantwoordelijk zijn voor de verschillende getroffen (vitale) sectoren.

Vervolg

Het NCSC en de NCTV blijven de situatie nauwlettend monitoren en blijft in contact met haar doelgroepen en (internationale) partners. Bij relevante ontwikkelingen zal ik uw Kamer nader informeren.

Tot slot

Nederland is een sterk gedigitaliseerd land. Dat biedt veel kansen, maar brengt ook risico's met zich mee. Niet voor niets was een van de conclusies uit het Cybersecuritybeeld Nederland 2023 dat door verwevenheid van processen in het digitale ecosysteem iedereen gevolgen kan ervaren van een cyberincident.[2] Deze kwetsbaarheid laat dat goed zien. Zelfs als een organisatie alle cybermaatregelen op orde heeft, kan een organisatie toch getroffen worden. Daarom is het van belang om naast de basismaatregelen ook plannen te maken voor wanneer systemen toch uitvallen. Organisaties moeten voorbereid zijn op uitval en ook veel

[1] Kamerstukken II 2023/24, 26 643, nr. 1176
[2] Kamerstukken II 2022/23 26 643, nr. 1045.

oefenen. Het kabinet blijft daarom onder mijn coördinatie inzetten de Nederlandse Cybersecurity Strategie 2022–2028 en de acties uit het actieplan.[3]

De Minister van Justitie en Veiligheid,
D.M. van Weel

[3] Kamerstukken II 2022/23 26 643, nr. 925.