Ministerie van Volksgezondheid,
Welzijn en Sport

> Retouradres Postbus 20350 2500 EJ Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34
www.rijksoverheid.nl

Ons kenmerk
3512189-1043372-DICIO

Bijlagen
1

Datum document
02 februari 2023

Correspondentie uitsluitend richten aan het retouradres met vermelding van de datum en het kenmerk van deze brief.

Datum 16 maart 2023
Betreft Kamervragen

Geachte voorzitter,

Hierbij zenden wij u de antwoorden op de vragen van de leden Tielen en Rajkowski (beiden VVD) over het bericht 'Pro-Russische DDoS-aanvallers vallen Nederlandse ziekenhuizen aan' (2023Z01700).

Hoogachtend,

de minister van Volksgezondheid, Welzijn en Sport,

Ernst Kuipers

de minister van Justitie en Veiligheid,

Dilan Yeşilgöz-Zegerius

Antwoorden op Kamervragen van de leden Tielen en Rajkowski (beiden VVD) over het bericht 'Pro-Russische DDoS-aanvallers vallen Nederlandse ziekenhuizen aan' (2023Z01700, ingezonden 2 februari 2023).

Vraag 1.
Bent u bekend met het bericht 'Pro-Russische DDoS-aanvallers vallen Nederlandse ziekenhuizen aan'?

Antwoord op vraag 1.
Ja.

Vraag 2.
Is bekend of ook ziekenhuizen in andere landen te maken hebben (gehad) met DDoS-aanvallen? Is bekend of hierbij patiëntgegevens of continuïteit van zorg in gevaar is gebracht?

Antwoord op vraag 2.
Dat klopt. Andere landen hebben bevestigd dat ziekenhuizen getroffen zijn door DDoS-aanvallen. Wij hebben geen volledig beeld van de gevolgen in andere landen van deze DDoS-aanvallen.

Vraag 3.
Wat is de (potentiële) schade die Killnet, en mogelijk andere hackerscollectieven, aan hebben kunnen richten aan de zorginfrastructuur in Nederland? Hoe zien de effecten van dit soort veiligheidsrisico's eruit voor patiënten en zorginstellingen? Zijn zorgorganisaties of ziekenhuizen of websites onbereikbaar geweest? Kunt u meer vertellen over de modus operandi van de aanvallen? Welke lessen worden hieruit getrokken?

Antwoord op vraag 3.
De Russische groep Killnet gebruikt DDoS-aanvallen voornamelijk om de dagelijkse dienstverlening van de beoogde slachtoffers te frustreren. Deze aanvallen passen in het huidige digitale dreigingsbeeld. Tijdens de DDoS-aanvallen waar het artikel naar verwijst is de zorgcontinuïteit niet in het geding geweest. De aanvallen hebben vooral geleid tot het beperkt beschikbaar zijn van de websites van ziekenhuizen. Ziekenhuizen zijn via andere kanalen wel bereikbaar gebleven.

De geleerde les is in hoofdlijnen dat cybersecurity een continu proces is dat geborgd dient te worden binnen de bedrijfsvoering van organisaties en ook periodiek dient te worden geëvalueerd: welke dreigingen zijn er, welke belangen zijn relevant, tot welke risico's leidt dat en welke maatregelen moeten er genomen worden om te komen tot een passend niveau van weerbaarheid. Een DDoS-aanval is een scenario dat daarin kan worden meegenomen.

Vraag 4.
Kunt u een stand van zaken geven over het lopende proces om de ziekenhuissector als vitale sector te identificeren zoals aangegeven in het commissiedebat Online veiligheid en cybersecurity en zoals aangegeven in het debat over de Wet elektronische gegevensuitwisseling in de zorg?

Antwoord op vraag 4.
De minister van Volksgezondheid, Welzijn en Sport zal u uiterlijk voor de zomer per Kamerbrief informeren over de stand van zaken van het aanwijzen van de zorgsector als vitale sector. In deze brief wordt u ook geïnformeerd over de implementatie van de herziene richtlijn voor Netwerk- en Informatiebeveiliging (NIB2) en de richtlijn Veerkracht van Kritieke Entiteiten (CER) in het zorgveld.

Vraag 5.
Bestaat er een 'scrubbing center' voor de zorg en de nu al aangewezen vitale infrastructuren/sectoren, waarin dataverkeer wordt opgeschoond en geanalyseerd, en kwaadaardig dataverkeer zoals DDoS wordt verwijderd? Zo nee, wat vindt u van een dergelijke 'veiligheidsklep' voor deze infrastructuren/sectoren?

Antwoord op vraag 5.
Er zijn leveranciers waar deze maatregel ('scrubbing straat') in diverse vormen als dienst kan worden afgenomen. Diverse Nederlandse ziekenhuizen maken hier ook gebruik van. Er bestaat echter geen wasstraat specifiek voor de zorg en de nu al aangewezen vitale infrastructuur/sectoren. Behalve een wasstraat ('scrubbing straat') zijn er nog andere maatregelen die genomen kunnen worden op het niveau van applicatie/diensten, netwerk en servers. Organisaties besluiten individueel welke maatregelen voor hen nodig zijn om DDoS-aanvallen af te weren. Of een wasstraat een noodzakelijke maatregel is, dient iedere organisatie voor zichzelf af te wegen op basis van het risicoprofiel en de overige maatregelen die er al zijn genomen. Ook is het goed mogelijk dat internetproviders reeds scrubbing diensten hebben opgenomen in hun dienstverlening, waarover de organisatie zelf afspraken kan maken over hoe en wanneer dergelijke technologie wordt geactiveerd.

Vraag 6.
Het ministerie van Volksgezondheid, Welzijn en Sport wil de zorg bewust maken van cyberveiligheid door onder andere de diensten van expertisecentrum Z-Cert uit te breiden naar de gehele zorgsector, waarom zijn diensten van Z-Cert nu alleen van toepassing op ziekenhuizen en de geestelijke gezondheidszorg (GGZ) en niet bijvoorbeeld op de Geestelijke Gezondheidsdiensten (GGD'en)? Welke termijn heeft u voor ogen om de diensten voor de gehele zorgsector beschikbaar te maken? In hoeverre gaat de inwerkingtreding van de NIS2 deze situatie veranderen? 2)

Vraag 7.
Bent u bereid actief te communiceren dat zorginstellingen zich aan kunnen sluiten bij Z-Cert en hoe wordt gestimuleerd dat straks de gehele zorgsector zich aansluit, aangezien in de beantwoording van eerdere schriftelijke vragen is aangegeven dat aangesloten zorginstellingen bij ICT-incidenten kunnen rekenen op de hulp van Z-Cert? 3)

Antwoord op vraag 6 en 7
Zoals eerder aan uw Kamer gecommuniceerd[1] kiezen het ministerie van VWS en Z-CERT ervoor om de verschillende sub-sectoren in het zorgveld aan te sluiten volgens een risicogebaseerde aansluitstrategie. Concreet betekent dit dat de sub-sectoren waarin de risico's op cyberincidenten en de bijbehorende gevolgen het

[1] Kamerstuknummer 27529-268

grootst zijn als eerste worden aangesloten bij Z-CERT. Op dit moment zijn bijna 300 instellingen uit verschillende sub-sectoren aangesloten bij Z-CERT. Ook de GGD'en zijn via de koepelorganisatie aangesloten. Het ministerie van VWS blijft zich inzetten om de dienstverlening van Z-CERT zo breed mogelijk beschikbaar te stellen binnen de gehele zorgsector. Daarbij wordt rekening gehouden met het absorptievermogen van Z-CERT. Voor de zomer zal de minister van VWS de Kamer informeren over de implementatie van de nieuwe Europese Netwerk en Informatiebeveiligingsrichtlijn (NIB2) en zal hij ingaan op wat dit voor de zorgsector betekent.

Vraag 8.
Hoe staat het met de toezegging dat Nederland zich inzet om de zwaarste cybercriminelen op Europese sanctielijsten te krijgen? Deelt u de mening dat de cybercriminelen van Killnet hier ook op thuishoren? Zo nee, waarom niet? Zo ja, wat gaat u doen om dit te bereiken?

Antwoord op vraag 8.
Onze eerste prioriteit lag bij het mitigeren van deze aanvallen en de getroffen systemen weer online te krijgen. Daarna kan er een onderzoek worden verricht naar de mogelijke dader(s) en kan bezien worden of sancties of strafrechtelijke vervolging tot de mogelijkheden behoren. Nederland zal hierbij zo mogelijk optrekken met de EU en afzonderlijke lidstaten, omdat een reactie sterker is als deze in coalitie-verband wordt vormgegeven.

Als internationaal recht en in VN-verband overeengekomen normen geschonden worden door cyberaanvallen, kunnen diplomatieke maatregelen in coalitieverband worden genomen. In EU-verband hebben we hiertoe de Cyber Diplomacy Toolbox, die mede door Nederland tot stand is gekomen. Op dit moment wordt de Toolbox herzien, hier nemen we een actieve rol in. Het EU Cyber Sanctie Regime is onderdeel van deze Toolbox. Welke respons opportuun is, zal afhankelijk zijn van de ernst en impact van het incident. Voor inzet van het sanctiemiddel is bovendien unanimiteit vereist in de EU-besluitvorming.

1) NOS, 30 januari 2023, 'Pro-Russische DDoS-aanvallers vallen Nederlandse ziekenhuizen aan' (https://nos.nl/artikel/2461833-pro-russische-ddos-aanvallers-hebben-het-gemunt-op-nederlandse-ziekenhuizen).

2) Kamerstuk 36200-XVI, nr. 125.

3) Aanhangsel van de Handelingen II, vergaderjaar 2021–2022, nr. 3969.

Toelichting:

Deze vragen dienen ter aanvulling op eerdere vragen terzake van het lid Hijink (SP), ingezonden 2 februari 2023 (vraagnummer 2023Z01695).