Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Omgaan met DDoS-aanvallen van hacktivistische groeperingen

Publicatiedatum: 1 februari 2023

Toegestane verspreiding van TLP:CLEAR
(Traffic Light Protocol)

Deze dreigingsanalyse bevat het label TLP:CLEAR en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp). Deze dreigingsanalyse is te gebruiken binnen uw organisatie, te delen met collega's of externe partijen zoals klanten op basis van *need-to-know* zodat zij zich kunnen beschermen of verdere schade kan worden voorkomen. Het is echter niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Handelingsperspectief

Dit handelingsperspectief biedt advies om te voorkomen dat onlinedienstverlening onbereikbaar wordt door een DDoS-aanval. Dit advies is in het bijzonder relevant voor organisaties in vitale sectoren en de Rijksoverheid voor wie het van kritiek belang is om online (publiekelijk) bereikbaar te zijn.

Mogelijke beveiligingsmaatregelen

Een DDoS-aanval op een onlinedienst kan niet voorkomen worden, maar wel afgeslagen. Voor adequate detectie van en respons op een DDoS-aanval is het van belang om basismaatregelen voor cybersecurity te nemen [🔒]. De volgende maatregelen zijn in het bijzonder relevant:

- **Loginformatie** helpt bij het detecteren van aanvallen en het afhandelen van incidenten. Aan de hand van logging kan worden bepaald wat gewoonlijk en acceptabel gebruik van een onlinedienst is. Om verdacht en oneigenlijk gebruik te detecteren kunnen notificaties worden ingesteld.
- Door het **verkleinen van uw aanvalsoppervlak** zorgt u ervoor dat uw netwerk online niet meer publiekelijk bereikbaar is dan nodig. U kunt uw aanvalsoppervlak onder andere verkleinen door bijvoorbeeld ongebruikte services en poorten uit te schakelen. Zo voorkomt u dat er op andere wijze met uw servers gecommuniceerd kan worden dan bedoeld.
- Door **netwerksegmentatie** voorkomt u dat een DDoS-aanval niet alle componenten van uw netwerk treft.
- Ook het **up-to-date houden van de software van uw apparatuur** is belangrijk. Applicaties kunnen kwetsbaarheden bevatten die gebruikt kunnen worden in een DDoS-aanval. Let er daarom op dat de applicaties die u gebruikt voorzien zijn van de laatste beveiligingsupdates.
- Als uw eigen netwerkomgeving niet in staat is om grote DDoS-aanvallen af te weren, kunt u gebruik maken van een **Content Distribution Network (CDN)**. Hierdoor worden aanvallen omgeleid en wordt een overbelasting van uw netwerkomgeving voorkomen.

Verdiepende informatie

Op de website van het NCSC [🔒] vindt u informatie over (technische) maatregelen tegen DDoS-aanvallen en over de Anti-DDoS-Coalitie. Informatie over de Nationale Wasstraat tegen DDoS-aanvallen (NaWas) vindt u op de website van de Nationale Beheersorganisatie Internet Providers (NBIP).

- **Factsheet Continuïteit van online diensten** [🔒]
- **Factsheet Technische maatregelen voor continuïteit voor online diensten** [🔒]
- **Anti-DDoS-Coalitie** [🔒]
- **Nationale Wasstraat** [🔒]

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

februari 2023

TLP:CLEAR