

Aangifte (D)DoS

“Mijn website/server was ineens onbereikbaar!”

(D)DoS, wat is dat?

Helaas bent u slachtoffer geworden van een (D)DoS-aanval, voluit een (Distributed) Denial of Service-aanval: Er is bij u een (voltooide) poging gedaan om uw website of server onbereikbaar te maken. Het kan zijn dat dit met één computer (een DoS-aanval) is gedaan, maar dit kan ook met meerdere computers (een DDoS-aanval) gedaan zijn. Bij een DDoS-aanval gebeurt dit vaak via een “botnet”, een netwerk van gehackte computers dat centraal wordt aangestuurd. In dat geval bezochten de computers massaal, tegelijk uw website of server, waardoor deze overbelast raakte en crashte.

Gegevens aangifte

U maakt een afspraak voor het doen van aangifte. Voordat u de afspraak heeft, is het belangrijk dat u alle benodigde gegevens al bij de hand heeft. Vul hieronder uw gegevens in.

U dient dit document op een *computer* in te vullen. Om het document in te vullen klikt u boven in beeld op “BEELD” en vervolgens op “Document bewerken”.

Omdat de aard van een (D)DoS-aanval best technisch is, adviseren wij u om dit formulier in te vullen samen met een mogelijke specialist van een IT afdeling/ ingehuurd bedrijf die onderzoek bij u heeft gedaan.

Gegevens aangever

- Voornaam
- Achternaam
- Geboortedatum
- Adres
- Postcode
- E-mailadres
- Telefoonnummer
- Burgerservicenummer
- Welk identiteitsbewijs neemt u mee naar de aangifte? Dit kan een paspoort, identiteitskaart, rijbewijs of Nederlands vreemdelingendocument zijn.

- Documentnummer identiteitsbewijs

Vragen aangifte

Wilt u ter voorbereiding van de aangifte alvast antwoord geven op onderstaande vragen? De antwoorden vult u in onder de vraagstelling achter 'A:'.

Gegevens benadeelde

- Naam bedrijf
- Adres
- Vestigingsplaats
- KVK-nummer
- E-mailadres
- Telefoonnummer

Gegevens IT-partij benadeelde

- Naam bedrijf (indien externe partij)
- Adres (indien externe partij)
- Vestigingsplaats (indien externe partij)
- KVK-nummer (indien externe partij)
- Naam contactpersoon
- E-mailadres
- Telefoonnummer

Algemene vragen

V: Op welke dag/datum/tijd heeft het misdrijf plaatsgevonden? Binnen welke periode heeft dit plaatsgevonden?

A:

V: Kunt u in chronologische volgorde vertellen wat er is gebeurd?

A:

Wanneer een IT-afdeling of een ingehuurd bedrijf voor u onderzoek heeft gedaan naar alle feitelijke gegevens zoals rekeningnummers, telefoonnummers, IP-adressen, logbestanden en e-mailadressen etc., voeg deze bij uw aangifte.

Gegevens (D)DoS aanval

V: Kan de omvang van de (D)DoS-aanval worden omschreven; Hoeveel verzoeken zijn er tijdens de (D)DoS-aanval verstuurd en/of hoeveel bandbreedte is er gebruikt in een bepaalde periode?

A:

V: Is een patroon te herkennen in de aanvallen (bijvoorbeeld hetzelfde tijdstip, of zelfde contactwijze, zelfde technische benadering, etc.)? Mocht er een patroon zijn, wat is de relevantie rond dit tijdstip? Denk bijvoorbeeld aan een school die altijd op vrijdag na 13 uur een (D)DoS-aanval krijgt omdat een leerling dan niet naar school wil.

A:

V: Is er ooit eerder (langer geleden) een vergelijkbare aanval uitgevoerd? Zo ja, wanneer was dat?

A:

V: Hoe zit de aangevallen infrastructuur in elkaar? Bijvoorbeeld netwerkconfiguratie, applicaties?

A:

V: Welke beschermende maatregelen zijn er getroffen?

A:

V: Welke maatregelen zijn er getroffen om de aanval af te wenden?

A:

V: Omschrijf de aangevallen infrastructuur. Gebruik hiervoor de IP-adressen of domeinnamen.

A:

V: Wat is het zwakke punt in de infrastructuur?

A:

Communicatie met een eventuele crimineel

V: Is/zijn de aanval(len) opgeëist? Zo ja, door wie?

A:

V: Is er een reden gegeven voor de aanval(len)?

A:

V: Welk medium is gebruikt om de aanval(len) op te eisen (bijvoorbeeld e-mail, sociale media, klantenservice of helpdesk etc.)?

A:

V: Is dit vastgelegd? Zo ja, voeg dit bij.

A:

V: Is er contact opgenomen met de crimineel? Zo ja, hoe heeft dat contact plaatsgevonden? Met welke gegevens (accountnaam, etc.)?

A:

V: Is er op dit moment nog contact met de crimineel?

A:

Neemt u zo veel mogelijk correspondentie mee om bij de aangifte op te nemen. Neemt u ook de technische details mee, zoals de e-mailheaders & logging van de webserver rondom alle contactmomenten. Op de website internetsporen.nl kunt u lezen hoe u de e-mailheaders, belangrijk voor het opsporingsonderzoek, kunt veiligstellen.

V: Is er open bronnenonderzoek gedaan om te kijken of de aanval opgeëist is?

A:

V: Indien de aanval niet is opgeëist: is er aanleiding om te denken dat de aanval door een bepaald persoon of een bepaalde organisatie is uitgevoerd, zo ja, door wie?

A:

V: Wat is volgens u het belang van deze persoon om de aanval uit te voeren?

A:

V: Is er gedreigd met een (grotere) aanval (met andere woorden: is er sprake van afpersing/afdreiging)? Zo ja, is het dreigement uitgevoerd?

A:

V: Werd er een geldbedrag geëist? Zo ja, welk bedrag werd geëist en in welke valuta (bijvoorbeeld Bitcoin)?

A:

V: Is er een tegenrekening (bijvoorbeeld Bitcoin adres) bekend waarnaar betaald moest worden?

A:

V: Is er betaald? Zo ja, hoe heeft de overdracht plaatsgevonden?

A:

Vul in per cryptotransactie:

Datum en tijdstip:

Aantal en valuta:

Van wallet:

Naar wallet:

Transactie hash:

Vul in per banktransactie:

Datum en tijdstip:

Bedrag en valuta:

Van bankrekeningnummer:

Tenaamgestelde:

Naar bankrekeningnummer:

Tenaamgestelde:

Omschrijving:

V: Wie heeft de onderhandelingen verricht (bedrijf zelf of externe partij)? En was de politie betrokken bij het incident?

A:

V: Is er een verslag gemaakt van de onderhandelingen? Zo ja, voeg dit verslag toe.

A:

V: Indien er op een andere wijze betaald moest worden, op welke wijze was dit en wat zijn hier de nadere betalingsdetails van? Denkt u er hierbij ook aan om de volledige omschrijving die op de bankafschriften terecht zijn gekomen te benoemen.

A:

V: Werden er andere eisen gesteld? Zo ja, wat werd er geëist?

A:

V: Is er aan de eis(en) voldaan?

A:

V: Is er op dit moment nog contact met de eiser(s)?

A:

Schade

Kunt u de schadebedragen specificeren (zie hiervoor de onderstaande vragen)

V: In het geval van afpersing: is er betaald, en zo ja, hoeveel?

A:

V: In het geval van uitval van dienstverlening: wat zijn de gederfde inkomsten en/of wat is de overige schade?
In het geval van omzetverlies, is alleen de winst, die u over de gemiste omzet had kunnen realiseren op te voeren als schadebedrag.

A:

V: Is er onderzoek verricht waarvoor kosten gemaakt zijn?

In het geval van extra inzet van bijvoorbeeld een systeembeheerder/IT-bedrijf, zijn de extra uren die aan dit voorval besteed worden een schadepost.

A:

V: Was er sprake van mediatie/bemiddeling?

A:

V: Zijn er bemiddelingskosten gemaakt?

A:

V: Zijn er kosten bekend van bijvoorbeeld NAWAS/CloudFlare?

A:

V: Hoe lang is de website/shop onbereikbaar geweest?

A:

V: Wat is uw verwachting van de gederfde inkomsten?

A:

V: Was dit tijdens een jaarlijkse piekperiode, bijvoorbeeld een feestdag?

Hierbij is het bijvoorbeeld mogelijk dat potentiële klanten naar een andere site of webshop zijn gegaan zijn en niet later alsnog bij u een aankoop hadden kunnen doen.

A:

Indien er naar aanleiding van uw aangifte een verdachte wordt aangehouden, is het belangrijk dat u uw geleden schade inzichtelijk kunt maken. Hoe korter u dit na het misdrijf kunt doen, hoe eenvoudiger dit doorgaans voor uzelf is en hoe succesvoller een eventuele schadeclaim ten aanzien van de verdachte zal zijn.

Technische informatie

Indien er incidentrapporten met technische informatie beschikbaar zijn met betrekking tot de aanval(len) (bijvoorbeeld van een mitigatie provider of ISP), deze graag bij de aangifte voegen en het origineel goed bewaren.

V: Welk soort aanval is dit geweest? Specificeer het type en/of de 'layer' waarop de aanval is gedaan.

A:

V: Indien het om een Layer7 (Application Layer) aanval gaat, is er een unieke cookie of andere ID meegestuurd?

A:

Indien er netwerkverkeer, bijvoorbeeld pcap-data of NetFlow-data, van de aanval(len) beschikbaar is, deze graag goed bewaren ten behoeve van een eventueel strafrechtelijk onderzoek. **We ontvangen graag de originele pcap-data of NetFlow-data bestanden.**

V: Is er bekend uit welk netwerk de aanval afkomstig is, bijvoorbeeld een hostingbedrijf uit het buitenland? De upstream provider kan dit mogelijk indicatief aangeven.

A:

V: Zijn er logbestanden (access logs) beschikbaar van langere tijd rond (voor/tijdens/na) de aanval?

Vaak doet een aanvaller vooronderzoek en wil een aanvaller controleren of de website nog bereikbaar is, dus of de aanval werkt

A:

V: Heeft u nog andere relevante informatie voor het onderzoek beschikbaar?

A:

Technische details van de aanval(len)

Alleen in te vullen bij het ontbreken van een technische rapportage van een IT-afdeling of onderzoek van een onafhankelijk bedrijf.

Aanval 1

V: Startdatum en tijd van de aanval (inclusief de tijdzone)

A:

V: Einddatum en tijd van de aanval (inclusief de tijdzone)

A:

V: Omvang van de datapakketten

A:

V: Hoogst aantal datapakketten per seconde

A:

V: Bandbreedte van de aanval

A:

V: Type aanvalsverkeer

A:

V: TCP- of UDP-flags

A:

V: Bron IP-adres(sen)

A:

V: Bron poortnummer(s)

A:

V: Aangevallen IP-adres(sen)

A:

V: Aangevallen poortnummer(s)

A:

V: Aangevallen service(s)

A:

V: Periode van onbeschikbaarheid van de service(s)

A:

V: Geleden schade bij deze aanval in euro's (leg uit)

A:

Als u meer aanvallen heeft gehad, kopieert u dan de bovenstaande gegevens om in te vullen.

Slachtofferhulp

V: Heeft u behoefte aan slachtofferhulp of nazorg? (zie informatie op <https://www.politie.nl/informatie/ik-ben-slachtoffer-wat-nu.html>)

Deze vraag graag met **ja** of **nee** beantwoorden. A:

Bijlagen

Belangrijke feitelijke informatie dient u ook letterlijk te benoemen bij Algemene vragen. Voeg alle relevante bijlages bij de aangifte. Denk hierbij aan:

- Onderzoeksrapport IT-specialist
- Technische details, zoals de e-mailheaders en logbestanden van de webserver rondom alle contactmomenten
- Transactieoverzichten
- Pcap-data en/of NetFlow-data

Wat kunt u doen tegen (D)DoS-aanvallen?

Een (D)DoS-aanval uitvoeren wordt steeds gemakkelijker en goedkoper; hierdoor lopen steeds meer bedrijven, organisaties en particulieren kans slachtoffer te worden.

U kunt technische en organisatorische maatregelen treffen om uw organisatie tegen verschillende vormen van (D)DoS-aanvallen te beschermen. Bijvoorbeeld door een overzicht te maken van uw complete ICT-infrastructuur. En door technische maatregelen voor onderdelen binnen eigen beheer te treffen, en afspraken te maken met de leverancier aan wie u beheer heeft uitbesteed. Zet ook een respons- en communicatiestrategie op. Voor meer informatie zie <https://www.digitaltrustcenter.nl/informatie-advies/ddos-aanval>

Voor meer informatie verwijzen we u naar onze internetpagina over [\(D\)DoS](#).