GIDS

De complete gids voor DDoS-bescherming

Typen aanvallen, kosten, beschermingsmodellen, selectiecriteria, NIS2 en trends. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

DDoS-aanvallen in Nederland stijgen explosief. De impact op bedrijfscontinuiteit is enorm -- en de meeste MKB-bedrijven zijn niet voorbereid.

+75%
Groei DDoS-aanvallen in 2025 bovenop de 137% stijging in 2024
ChannelConnect [1]

EUR 5.700
Kosten per minuut downtime door een DDoS-aanval
Security Magazine [2]

5+ uur
DigiD platgelegd in januari 2025 -- miljoenen Nederlanders getroffen
DutchNews.nl [3]

70%+
Kans op vervolgaanvallen na een eerste DDoS -- gemiddeld 2,8 keer
ChannelConnect [1]

EUR 10M
Maximale NIS2-boete bij onvoldoende beschikbaarheidsmaatregelen
Digitale Overheid [4]

EUR 95K
Gemiddelde schade per DDoS-aanval voor een klein bedrijf
Dutch IT Channel [5]

2,5M
.nl-domeinen beschermd door NaWas -- 43% van alle Nederlandse domeinen
SIDN/NBIP [6]

+231%
Stijging carpet-bombing aanvallen -- verkeer verspreid over brede IP-reeksen
StormWall [7]

1. Wat is een DDoS-aanval?

Een DDoS-aanval (Distributed Denial of Service) overspoelt je systemen met verkeer vanuit duizenden tot miljoenen apparaten tegelijk. Het doel: jouw website, webshop of applicatie onbereikbaar maken voor klanten en medewerkers.

HOE WERKT HET?

Aanvallers gebruiken botnets -- netwerken van gehackte computers, servers en IoT-apparaten -- om tegelijkertijd enorme hoeveelheden verkeer naar je systemen te sturen. [8] Je server kan het verkeer niet meer verwerken en wordt onbereikbaar. Voor je klanten lijkt het alsof je website er simpelweg niet is.

DRIE TYPEN DDOS-AANVALLEN

TYPE	LAAG	WERKING	VOORBEELD
Volumetrisch	L3/L4	Overspoelt je bandbreedte met enorme hoeveelheden data	UDP flood, DNS amplification
Protocol	L3/L4	Misbruikt zwakheden in netwerkprotocollen	SYN flood, Smurf attack
Applicatie	L7	Richt zich op specifieke applicaties -- lijkt op normaal verkeer	HTTP flood, Slowloris

> **Let op:** Applicatielaag-aanvallen (L7) zijn het moeilijkst te detecteren omdat ze eruitzien als normaal websiteverkeer. Ze vereisen minder bandbreedte maar veroorzaken disproportioneel veel schade. [9]

IMPACT OP MKB

Als MKB-ondernemer denk je misschien dat DDoS-aanvallen alleen grote bedrijven treffen. De realiteit is anders: 23% van de Nederlandse middelgrote bedrijven is al slachtoffer geweest. [10] Moderne aanvallen zijn geautomatiseerd via DDoS-as-a-Service platforms die vanaf EUR 50 beschikbaar zijn. Elk bedrijf met een online aanwezigheid is een potentieel doelwit.

> **COLLATERAL DAMAGE**
>
> Ook als jij niet het directe doelwit bent, kun je geraakt worden. Bij carpet-bombing aanvallen wordt verkeer verspreid over brede IP-reeksen. Zit jouw server in hetzelfde netwerk als het doelwit? Dan ga je mee onderuit.

2. Waarom is het belangrijk?

DDoS-aanvallen in Nederland zijn in twee jaar tijd verdrievoudigd. De vraag is niet of je wordt aangevallen, maar wanneer.

NEDERLANDSE CIJFERS 2024--2025

PERIODE	AANVALLEN (NAWAS)	TREND
2024	1.377 (Q2-Q4)	+137% groei t.o.v. 2023 [11]
Q2 2025	2.292	5,5x meer dan Q1 2025 -- enorme piek [12]
Q3 2025	1.406	Nog steeds 2x Q3 2024 [13]
2025 totaal	--	+75% bovenop 2024, 3 aanvallen >1 Tbps [1]

Nederland staat in de top-10 van meest getroffen landen wereldwijd, samen met de VS, China en het VK. [14]

CASE STUDIES

DigiD -- januari 2025

Meer dan vijf uur platgelegd door een grootschalige DDoS-aanval. Miljoenen Nederlanders konden niet inloggen bij de Belastingdienst, gemeenten, SVB en zorgverzekeraars. Een aanval op een digitaal knooppunt raakt het hele land. [3]

NAVO-top Den Haag -- juni 2025

Pro-Russische groep NoName057(16) voerde gerichte DDoS-aanvallen uit rondom de NAVO-top. DigiD, BSN, Digiport en MijnOverheid hadden beperkte beschikbaarheid. Het NCSC classificeerde dit als hybride oorlogsvoering. [15]

UMCG -- 2023

De Russische hackersgroep Killnet viel meerdere Europese ziekenhuizen aan, waaronder het UMCG. Websites crashten, wat de bereikbaarheid van zorginformatie in gevaar bracht. [16]

DE VERVOLGAANVAL

Na een eerste DDoS-aanval is de kans op vervolgaanvallen meer dan 70%. Gemiddeld volgen er 2,8 extra aanvallen -- 80% meer dan een jaar eerder. [1] Wie pas na de eerste klap bescherming regelt, is structureel te laat.

DE FINANCIELE IMPACT

60% van kleine bedrijven gaat failliet binnen 6 maanden na een ernstige cyberaanval. [17] Voor DDoS-aanvallen specifiek:

- **EUR 5.700 per minuut** downtime [2]
- **EUR 95.000** gemiddelde schade voor een klein bedrijf per aanval [5]
- **EUR 40.000** gemiddelde schade voor MKB per aanval [10]
- **75--80% snellere oplossing** met professionele bescherming (MTTR-reductie) [18]

REKENVOORBEELD

Een MKB-webshop met EUR 2 miljoen omzet: 5 uur DDoS = EUR 11.000--96.000 schade. Professionele bescherming kost EUR 2.400--3.000 per jaar. Dat is een ROI van 4--40x bij een enkele aanval. [5][2]

3. Hoe werkt DDoS-bescherming?

DDoS-bescherming werkt door aanvalsverkeer te scheiden van legitiem verkeer voordat het je systemen bereikt. Er zijn verschillende modellen, elk met eigen voor- en nadelen.

BESCHERMINGSMODELLEN

MODEL	WERKING	ACTIVATIETIJD	GESCHIKT VOOR
Always-on	Verkeer loopt continu door een scrubbing-service	0 seconden	Bedrijfskritische websites en webshops
On-demand	Verkeer wordt omgeleid bij detectie van een aanval (BGP redirect)	30 sec -- minuten	Lagere risicoprofielen, kostenbewust MKB
Hybride	Basis always-on met opschaling naar on-demand bij grote aanvallen	Basis: 0 sec, opschaling: 30+ sec	Bedrijven met wisselend risicoprofiel

HET CLEAN PIPE MODEL

Bij het clean pipe model wordt al je internetverkeer via een extern scrubbing center geleid. Daar wordt aanvalsverkeer gefilterd en alleen "schoon" verkeer doorgestuurd naar jouw servers. Vergelijk het met een autowasstraat: vuil verkeer gaat erin, schoon verkeer komt eruit. [19]

> **Kostenindicatie:** Een clean pipe service kost doorgaans 20--100% van je connectiviteitskosten, afhankelijk van de SLA en kwaliteit. [19]

CDN-BASED BESCHERMING

Bij CDN-based bescherming fungeert een Content Delivery Network als reverse proxy. Alle HTTP/HTTPS-verkeer loopt via het CDN-netwerk, dat aanvallen absorbeert met zijn wereldwijde capaciteit. Dit model is altijd actief en combineert DDoS-bescherming met snellere laadtijden.

Beperking: CDN-based bescherming werkt alleen voor HTTP/HTTPS-verkeer. Andere protocollen (mail, VPN, custom applicaties) vereisen aanvullende bescherming.

GELAAGDE AANPAK

Professionele DDoS-bescherming werkt op meerdere lagen tegelijk:

LAAG	BESCHERMING TEGEN	TECHNIEKEN
Netwerk (L3/L4)	Volumetrische en protocol-aanvallen	Rate limiting, scrubbing, BGP blackholing
Applicatie (L7)	HTTP floods, slowloris, API abuse	WAF, gedragsanalyse, challenge pages
DNS	DNS amplification, NXDOMAIN flood	Anycast DNS, DNS firewalling

VEELGEMAAKTE FOUT

Alleen L3/L4-bescherming inzetten en L7 vergeten. Applicatielaag-aanvallen lijken op normaal verkeer en passeren volumetrische filters ongehinderd. [9]

NAWAS: HET NEDERLANDSE COLLECTIEVE MODEL

Nederland heeft een uniek collectief beschermingsmodel: de Nationale anti-DDoS Wasstraat (NaWas), beheerd door de non-profit NBIP. Bijna 200 deelnemers in 10 Europese landen zijn aangesloten. NaWas beschermt 2,5 miljoen .nl-domeinen -- 43% van alle Nederlandse domeinen. [6]

NaWas werkt via BGP-sessies met deelnemers. Bij een aanval wordt het aangevallen IP-prefix omgeleid naar NaWas-hardware, waar meerdere scrubbing-apparaten het verkeer in serie filteren. Schoon verkeer gaat via een apart VLAN terug naar de deelnemer. Activatietijd: circa 30 seconden. [20]

Het model is primair beschikbaar voor ISP's, hostingproviders en digitale infrastructuur providers. MKB-bedrijven profiteren indirect als hun hostingprovider is aangesloten bij NaWas.

4. Wat kost het?

DDoS-bescherming varieert van gratis basisoplossingen tot enterprise-diensten. Voor MKB liggen de kosten tussen EUR 0 en EUR 250 per maand.

PRIJSTABEL MKB

SEGMENT	OPLOSSING	KOSTEN (INDICATIEF)
Startend MKB	Gratis CDN-tier met basis L3/L4 bescherming	EUR 0/maand
Klein MKB	CDN met uitgebreide L3/L4 + basis WAF	EUR 20--25/maand
MKB	CDN + WAF + geavanceerde DDoS-bescherming	EUR 200--250/maand
MKB (cloud)	Cloud-native DDoS IP Protection	EUR 199/maand per publiek IP
MKB (hosting)	DDoS-bescherming via hostingprovider	Vanaf ~EUR 5/maand (bij hosting)

ALWAYS-ON VS ON-DEMAND KOSTEN

MODEL	KOSTEN	VOORDELEN	NADELEN
Always-on	Hoger (vast maandbedrag)	Directe mitigatie, geen activatietijd	Duurder bij weinig aanvallen
On-demand	Lager (betaal bij gebruik)	Goedkoper bij laag risico	Activatietijd van minuten tot uren
Hybride	Midden	Basis always-on + opschaling bij aanval	Complexere configuratie
CDN-based	Vaak inbegrepen	Gecombineerd met CDN-voordelen	Alleen HTTP/HTTPS verkeer

> **NaWas als collectief model:** De NaWas werkt met een flat-fee per /24 prefix en is als non-profit significant goedkoper dan commerciele alternatieven. MKB-bedrijven profiteren hier indirect van als hun hostingprovider is aangesloten. Vraag je hoster of zij NaWas-bescherming bieden. [20]

ROI-BEREKENING

Een Forrester-studie berekende 223% ROI op DDoS-bescherming, met een terugverdientijd van minder dan 1 jaar. [18] De NaWas alleen al heeft EUR 425 miljoen aan potentieel omzetverlies voorkomen voor aangesloten organisaties. [6]

VUISTREGEL

Elke 1% investering in DDoS-bescherming voorkomt circa 3% verlies. Wordt een aanval binnen 24 uur gedetecteerd, dan worden de kosten bijna gehalveerd vergeleken met latere detectie. [18][21]

5. Waar moet je op letten?

Niet elke DDoS-bescherming is gelijk. Hieronder de selectiecriteria die er toe doen -- zonder aanbiedernamen, zodat je objectief kunt vergelijken.

SELECTIECRITERIA

CRITERIUM	WAAROM BELANGRIJK	MINIMUM VOOR MKB
Netwerkcapaciteit	Hoe groter de capaciteit, hoe meer aanvalsverkeer geabsorbeerd kan worden	>1 Tbps mitigatiecapaciteit
L7-bescherming	Applicatielaag-aanvallen zijn het snelst groeiende type	WAF + gedragsanalyse inbegrepen
24/7 SOC	Aanvallen komen op elk moment -- handmatige respons is te traag	Geautomatiseerde detectie + menselijke escalatie
AI-detectie	Onderscheidt aanvalsverkeer van pieken in legitiem verkeer	Machine learning-gebaseerde detectie
Kostenprotectie	Voorkomt dat je bij een grote aanval extra betaalt voor bandbreedte	Geen meerkostenclauses bij aanvallen
SLA	Garantie op beschikbaarheid en mitigatietijden	99,9% uptime, mitigatie <10 seconden

RED FLAGS

VERMIJD AANBIEDERS DIE

Alleen L3/L4-bescherming bieden zonder L7 | Geen SLA-garantie geven op mitigatietijd | Extra kosten in rekening brengen tijdens een aanval | Geen transparantie bieden over hun netwerkcapaciteit | Geen incident-rapportages leveren na een aanval | Activatietijden van meer dan 5 minuten hebben voor always-on diensten

10 VRAGEN AAN JE AANBIEDER

STEL DEZE VRAGEN VOOR JE TEKENT

1. Wat is jullie totale mitigatiecapaciteit in Tbps?
2. Bieden jullie zowel L3/L4 als L7-bescherming?
3. Wat is de gegarandeerde mitigatietijd in jullie SLA?
4. Zijn er meerkosten tijdens een actieve aanval?
5. Hoe werkt de detectie -- regelgebaseerd of AI/ML?
6. Hebben jullie een 24/7 SOC met menselijke analisten?
7. Krijg ik incident-rapportages na elke aanval?
8. Hoe snel kan ik opschalen bij een aanval die jullie capaciteit nadert?
9. Beschermen jullie ook tegen multi-vector aanvallen (volumetrisch + L7 + DNS tegelijk)?
10. Wat is de opzegtermijn en wat gebeurt er bij contracteinde met mijn configuratie?

6. Veelgemaakte fouten

De meeste MKB-bedrijven maken dezelfde fouten bij DDoS-bescherming. Herken je er een? Dan is het tijd om actie te ondernemen.

1. "Wij zijn geen doelwit"

De meest voorkomende fout. Aanvallen zijn geautomatiseerd via DDoS-as-a-Service platforms die voor minder dan EUR 50 beschikbaar zijn. [8] 23% van de Nederlandse middelgrote bedrijven is al getroffen. [10] Daarnaast tref je als MKB vaak collateral damage bij carpet-bombing: jouw server deelt een netwerk met het eigenlijke doelwit en gaat mee onderuit.

2. Alleen vertrouwen op je ISP

Standaard ISP-connectiviteit biedt zelden meer dan basis volumetrische filtering. L7-aanvallen -- het snelst groeiende type -- passeren deze filters ongehinderd. [9] Een gelaagde aanpak met specifieke DDoS-bescherming is nodig bovenop wat je ISP levert.

3. Geen incident response plan

Wie belt wie bij een aanval? Wanneer schaal je op? Hoe communiceer je naar klanten? Tijdens een actieve aanval is het te laat om dit uit te zoeken. Leg procedures vast, houd contactgegevens van je beschermingsprovider paraat, en oefen het plan minimaal jaarlijks. [22]

4. Geen schaalbaarheid ingebouwd

DDoS-aanvallen groeien in omvang. De grootste aanval ooit (31,4 Tbps) was in Q4 2025. [23] Als je bescherming niet mee kan schalen, ben je bij de volgende grote aanval alsnog onbeschermd. Kies een oplossing die automatisch opschaalt of snel handmatig kan worden uitgebreid.

5. Bescherming niet up-to-date houden

Aanvalstechnieken veranderen continu. Carpet-bombing steeg 231% in 2025. [7] AI-gedreven botnets passen hun strategie real-time aan. Bescherming die vorig jaar werkte, is niet per definitie voldoende voor dit jaar. Evalueer je bescherming minimaal halfjaarlijks.

6. Pas actie ondernemen na de eerste aanval

Na een eerste DDoS-aanval is de kans op vervolgaanvallen meer dan 70%, met gemiddeld 2,8 extra aanvallen. [1] Wie reactief bescherming regelt, krijgt te maken met hogere kosten (spoed-implementatie), langere activatietijden (BGP-configuratie duurt dagen) en een onbeschermd venster tot de volgende klap.

7. NIS2 negeren

De Cyberbeveiligingswet (NIS2) verplicht "passende maatregelen" voor continuiteit van diensten. [4] Geen DDoS-bescherming terwijl je onder NIS2 valt, kan leiden tot boetes tot EUR 10 miljoen of 2% van je omzet. Bovendien: als je door een DDoS-aanval wordt geraakt en niet aan je meldplicht voldoet, krijg je een dubbele klap.

7. Compliance: NIS2

De Cyberbeveiligingswet (de Nederlandse implementatie van NIS2) maakt beschikbaarheidsmaatregelen verplicht. DDoS-bescherming valt hier direct onder.

ZORGPLICHT -- ARTIKEL 21

NIS2 verplicht organisaties om "passende en evenredige technische, operationele en organisatorische maatregelen" te nemen om de continuiteit van diensten te waarborgen. [4] DDoS is een evident risico voor beschikbaarheid. Een risicoanalyse die DDoS niet adresseert, is onvolledig.

MELDPLICHT -- 24 UUR

Significante incidenten die de beschikbaarheid van je diensten verstoren, moeten binnen 24 uur worden gemeld. [24] Een DDoS-aanval die je systemen meer dan enkele uren platlegt, valt hier vrijwel zeker onder.

BOETES

CATEGORIE	MAXIMALE BOETE
Essentiele entiteiten	EUR 10 miljoen of 2% van de jaaromzet
Belangrijke entiteiten	EUR 7 miljoen of 1,4% van de jaaromzet

DE DUBBELE KLAP

> **SCENARIO**
> Je wordt getroffen door een DDoS-aanval. Je hebt geen adequate bescherming en geen incident response plan. De schade: directe omzetderving + reputatieschade + NIS2-boete wegens onvoldoende maatregelen + boete wegens te late melding. Vier kostenposten in plaats van een.

WIE VALT ERONDER?

Essentiele sectoren: energie, transport, bankwezen, gezondheidszorg, drinkwater, digitale infrastructuur, ICT-dienstverlening.

Belangrijke sectoren: post/koeriersdiensten, afvalverwerking, levensmiddelen, chemie, digitale aanbieders, onderzoek.

Het wetsvoorstel is op 4 juni 2025 ingediend bij de Tweede Kamer. Verwachte inwerkingtreding: Q2 2026. [4]

NIS2 EN DDOS

NIS2 noemt DDoS niet expliciet als verplichte maatregel. Maar de beschikbaarheidsverplichting en de verplichte risicoanalyse maken het in de praktijk onvermijdelijk. Een auditor die ziet dat je geen DDoS-bescherming hebt terwijl je diensten online beschikbaar zijn, zal dat als tekortkoming aanmerken.

8. Verschil met verwante oplossingen

DDoS-bescherming wordt vaak verward met andere beveiligingsoplossingen. Ze vullen elkaar aan, maar zijn niet uitwisselbaar.

OPLOSSING	PRIMAIRE FUNCTIE	BESCHERMT TEGEN DDOS?	RELATIE
DDoS-bescherming	Filtert aanvalsverkeer op netwerk- en applicatieniveau	Ja -- kernfunctie	--
WAF (Web Application Firewall)	Beschermt webapplicaties tegen exploits (SQL injection, XSS)	Deels -- filtert L7 aanvallen die op web-exploits lijken	Aanvullend op DDoS-bescherming voor L7
CDN (Content Delivery Network)	Versnelt content delivery via caching op edge-locaties	Deels -- absorbeert volumetrisch verkeer door verspreiding	Vaak gecombineerd met DDoS-bescherming
Firewall (traditioneel)	Filtert verkeer op basis van regels (IP, poort, protocol)	Minimaal -- geen capaciteit voor volumetrische aanvallen	Eerste verdedigingslinie, onvoldoende als enige maatregel

> **Beste aanpak:** Combineer DDoS-bescherming (L3/L4 + L7) met een WAF voor applicatiebeveiliging en een CDN voor prestatie-optimalisatie. Een traditionele firewall is nuttig als lokale eerste filter, maar biedt geen DDoS-bescherming bij serieuze aanvallen.

9. Trends 2025--2026

DDoS-aanvallen worden groter, slimmer en geautomatiseerder. Dit zijn de trends die je beschermingsstrategie beinvloeden.

CARPET-BOMBING: +231%

Bij carpet-bombing wordt aanvalsverkeer niet op een enkel IP gericht, maar verspreid over brede IP-reeksen. Daardoor blijft de aanval per IP onder detectiedrempels, maar is het cumulatieve effect verwoestend. Deze techniek steeg met 231% in 2025. [7] Traditionele per-IP detectie mist deze aanvallen -- je hebt netwerk-brede analyse nodig.

AI-GEDREVEN DDOS

Botnets gebruiken AI-tools (waaronder WormGPT en FraudGPT) om aanvallen dynamisch aan te passen. [25] Ze analyseren in real-time welke mitigatiemaatregelen actief zijn en passen hun aanvalsvectoren daarop aan. Dit maakt statische regelsets steeds minder effectief.

IOT-BOTNETS

Het Aisiru-botnet beheert naar schatting 1--4 miljoen IoT-apparaten en kan aanvallen tot 22,2 Tbps genereren. [23] Slecht beveiligde camera's, routers en smart home-apparaten worden massaal ingezet. Met het groeiende aantal IoT-apparaten neemt ook de potentiele aanvalscapaciteit toe.

VERWACHTING 2026

PROGNOSE

- **58 miljoen DDoS-aanvallen** verwacht in 2026 -- 3x meer dan 2025 [7]
- **Piekvolumes >3 Tbps** worden regelmatig verwacht
- **Multi-vector aanvallen** (L3/L4 + L7 + DNS tegelijk) worden de norm
- **DDoS-as-a-Service** maakt aanvallen toegankelijk voor iedereen met EUR 50

WAT BETEKENT DIT VOOR JOU?

Statische bescherming volstaat niet meer. Je hebt bescherming nodig die:

- Multi-vector aanvallen detecteert en mitigeert
- AI/ML gebruikt voor detectie -- niet alleen regelsets
- Automatisch opschaalt bij aanvallen boven je normale capaciteit
- Netwerk-brede analyse biedt (niet alleen per-IP)

- Minimaal halfjaarlijks wordt geevalueerd op actuele dreigingen

10. Aan de slag

Je weet nu wat DDoS-bescherming inhoudt, wat het kost en waarom het nodig is. De volgende stap: de juiste oplossing vinden voor jouw situatie.

1. **Breng je risicoprofiel in kaart**
   Wat is de impact als je website of applicatie 1 uur onbereikbaar is? 4 uur? 24 uur? Bereken je omzetderving per uur downtime en bepaal je maximale acceptabele downtime.

2. **Check je huidige bescherming**
   Vraag je hostingprovider of ISP welke DDoS-bescherming er nu actief is. Is je hoster aangesloten bij NaWas? Heb je al een WAF? Welke lagen zijn gedekt (L3/L4, L7, DNS)?

3. **Bepaal je beschermingsmodel**
   Always-on voor bedrijfskritische systemen, on-demand voor lagere risicoprofielen, hybride als je wilt groeien. Gebruik de selectiecriteria uit hoofdstuk 5 om aanbieders te vergelijken.

4. **Maak een incident response plan**
   Leg vast wie wat doet bij een aanval, hoe je escaleert, hoe je communiceert naar klanten en hoe je voldoet aan je NIS2-meldplicht (als van toepassing).

5. **Vergelijk en kies**
   Vraag offertes op bij minimaal 3 aanbieders. Gebruik de 10 vragen uit hoofdstuk 5 als leidraad. Let specifiek op kostenprotectie, L7-dekking en SLA-garanties.

> **Hulp nodig bij het vergelijken?** Op ibgids.nl/word-gematcht vul je je wensen in en ontvang je binnen 48 uur vrijblijvende offertes van geselecteerde DDoS-beschermingsaanbieders. Geen verplichtingen, geen kosten.

Bronnenlijst

Alle bronnen in deze gids zijn geverifieerd op basis van publiek beschikbare Nederlandse en internationale data.

[1] **ChannelConnect** -- DDoS-aanvallen namen in 2025 met 75% toe.
https://www.channelconnect.nl/security-en-privacy/ddos-aanvallen-namen-in-2025-met-75-toe/

[2] **Security Magazine** -- DDoS downtime costs $6,130/min.
https://www.securitymagazine.com/articles/100123

[3] **DutchNews.nl** -- Government login service DigiD frozen in large-scale cyberattack.
https://www.dutchnews.nl/2025/01/government-login-service-digid-frozen-in-large-scale-cyberattack/

[4] **Digitale Overheid** -- Cyberbeveiligingswet (NIS2).
https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[5] **Dutch IT Channel** -- DDoS-aanval leidt gemiddeld tot EUR 95.000 schade voor klein bedrijf.
https://www.dutchitchannel.nl/news/139762/ddos-aanval-leidt-gemiddeld-tot-euro-schade-voor-klein-bedrijf

[6] **SIDN/NBIP** -- DDoS-bescherming voorkomt grote verliezen voor Nederlands bedrijfsleven.
https://www.sidn.nl/en/news-and-blogs/ddos-protection-prevents-major-losses-for-dutch-business-community

[7] **StormWall** -- DDoS Attack Statistics 2025.
https://stormwall.network/resources/blog/ddos-attack-statistics-2025

[8] **Digital Trust Center** -- DDoS-aanval: wat kun je eraan doen?
https://www.digitaltrustcenter.nl/informatie-advies/ddos-aanval

[9] **NCSC** -- De onzichtbaarheid van applicatielaag DDoS-aanvallen.
https://www.ncsc.nl/actueel/weblog/weblog/2020/de-onzichtbaarheid-van-applicatielaag-ddos-aanvallen

[10] **Kaspersky** -- Bijna een vierde van Nederlandse middelgrote bedrijven slachtoffer van DDoS-aanval.
https://www.kaspersky.nl/about/press-releases/bijna-een-vierde-van-nederlandse-middelgrote-bedrijven-slachtoffer-van-ddos-aanval

[11] **NBIP** -- 2024 gekenmerkt door gerichte, complexere DDoS-aanvallen.
https://www.nbip.nl/en/actueel/2024-characterised-by-targeted-increasingly-complex-ddos-attacks/

[12] **NBIP** -- DDoS attacks in Q2 2025.
https://www.nbip.nl/en/actueel/ddos-attacks-in-q2-2025/

[13] **NBIP** -- DDoS-aanvallen in Q3 2025.
https://www.nbip.nl/actueel/ddos-aanvallen-in-q3-2025/

[14] **Executive People** -- Nederland in top van meest getroffen landen door DDoS-aanvallen.
https://executive-people.nl/582094/nederland-in-top-van-meest-getroffen-landen-door-ddos-aanvallen.html

[15] **Rijksoverheid** -- DDoS-aanvallen op Nederlandse organisaties rondom NAVO-top.
https://www.rijksoverheid.nl/actueel/nieuws/2025/06/23/ddos-aanvallen-op-nederlandse-organisaties-rondom-navo-top

[16] **Bitdefender** -- Killnet attacks European hospitals including UMCG in the Netherlands.
https://www.bitdefender.com/en-us/blog/hotforsecurity/killnet-attacks-european-hospitals-including-umcg-in-the-netherlands

[17] **Laurus Verzekeringen** -- 60% van kleine bedrijven failliet na cyberaanval.
https://www.laurusverzekeringen.nl/cyberverzekering/

[18] **NETSCOUT** -- Confirmed: NETSCOUT Arbor DDoS Protection Solution Has 223% ROI.
https://www.netscout.com/blog/confirmed-netscout-arbor-ddos-protection-solution-has-223-roi

[19] **Nexusguard** -- The Cost of DDoS Security.
https://www.nexusguard.com/white-paper/the-cost-of-ddos-security

[20] **NBIP** -- NaWas: Nationale anti-DDoS Wasstraat.
https://www.nbip.nl/diensten/nawas/

[21] **KPN Zakelijk** -- Een DDoS attack: wat is het en wat zijn de gevolgen?
https://www.kpn.com/zakelijk/blog/een-ddos-attack-wat-is-het-en-wat-zijn-de-gevolgen.htm

[22] **NCSC** -- Lopende DDoS-aanvallen op Nederlandse organisaties (april 2025).
https://www.ncsc.nl/actueel/nieuws/2025/04/30/lopende-ddos-aanvallen-op-nederlandse-organisaties

[23] **Cloudflare** -- DDoS Threat Report Q4 2025.
https://blog.cloudflare.com/ddos-threat-report-2025-q4/

[24] **NCSC** -- Bereid je voor op de Cyberbeveiligingswet.
https://www.ncsc.nl/cyberbeveiligingswet-nis2/bereid-je-voor

[25] **Nokia** -- DDoS in 2025: The Year Automation Took the Wheel.
https://www.nokia.com/blog/ddos-in-2025-the-year-automation-took-the-wheel/