HACKHELPDESK

Eerste hulp bij cybercrime voor ondernemers

HACKHELPDESK.NL

DDOS-AANVAL

Wat is een DDos-aanval?

Een DDos-aanval (voluit: Distributed Denial of Service) is een aanval waarbij een site wordt platgelegd.

Hoe gebeurt het?

Een cybercrimineel stuurt zoveel verkeer af op een website of dienst, dat deze onbeschikbaar wordt gemaakt voor de rest van de gebruikers.

Met wat kan je een DDos-aanval het beste vergelijken?

Je kunt een DDos-aanval het beste vergelijken met een grote groep mensen die voor de ingang van de winkel staat en de toegang blokkeert. Doordat de groep daar staat kun je de winkel niet inkomen. Er is namelijk geen ruimte om door de ingang heen te komen.

Wat is het gevolg?

Het gevolg van een DDos-aanval is dat de website of dienst niet meer bereikbaar is voor degenen die erbij willen. Heeft je bank dus last van een DDos-aanval, dan kan jij niet meer internetbankieren. Het is erg vervelend, maar niet gevaarlijk.

Wat is de oplossing?

Een dergelijke aanval is niet snel opgelost, omdat het verkeer vaak van allerlei verschillende plekken komen. Hier wordt een zogenaamd botnetwerk voor gebruikt. Dit is een collectie van computers die door anderen worden aangestuurd. Vaak gaat het om heel veel machines die verbinding proberen te maken. Dat blokkeer je dus niet zomaar.

REPRESSIE

Wat je vooral wel moet doen.

Stap 1

Ligt je website eruit? Check eerst of er geen storing bekend is via www.allestoringen.nl

Stap 2

Vermoeden dat je slachtoffer bent geworden van een DDos-aanval? Neem contact op met je website hoster en bespreek de situatie. Het is vaak een kwestie van tijd voor de aanval stopt en de website weer bereikbaar is.

Stap 3

Wordt er gedreigd met een DDos-aanval om je af te persen? Lees op de site de tips over afpersing en chantage.

HACKHELPDESK

Eerste hulp bij cybercrime voor ondernemers

HACKHELPDESK.NL

PREVENTIE

Tip 1

Analyseer de risico's van je website. Maak een prioriteitenoverzicht van je online diensten en applicaties en leg vast welke ICT-infrastructuur deze diensten ondersteunt. Alleen als je weet welke risico's je loopt, kun je de juiste maatregelen nemen om deze te beperken.

Tip 2

Vraag welke maatregelen je provider neemt. In je serviceovereenkomst staat wat je provider doet om de impact van een DDos-aanval te beperken. Als je provider niets doen, moet je zelf actie ondernemen.

Tip 3

Maak een noodplan. Bedank nu al wat er moet gebeuren als je website er tijdelijk uit ligt door een DDos-aanval. Hoe sneller je dan in actie komt, hoe beter je de schade weet te beperken.

Tip 4

Neem preventieve maatregelen, zoals bijvoorbeeld het installeren van Cloudfare.

Tip 5

Kijk op site van de anti DDos coalitie op nomoreddos.org.