19 november 2018, 08:30 (CET)

DDoS-bescherming behoedt Nederlandse bedrijven voor substantiële schade

DDoS-aanvallen zouden ondernemingen zonder bescherming ruim een miljard euro kunnen kosten

Zonder effectieve verdediging hadden DDoS-aanvallen het Nederlandse bedrijfsleven en de Nederlandse overheid vorig jaar mogelijk meer dan een miljard euro aan gederfde inkomsten gekost. Dat blijkt uit onderzoek naar de economische impact van DDoS-aanvallen in Nederland van de stichting Nederlandse Beheersorganisatie Internet Providers (NBIP) en SIDN (Stichting Internet Domeinregistratie Nederland).

Maandag 19 november presenteren de NBIP en SIDN het rapport 'The impact of DDoS attacks on Dutch enterprises'. Voor dit onderzoek is data van de NaWas (Nationale Wasstraat), een initiatief van NBIP, gecombineerd met data van SIDN over de organisaties achter de getroffen .nl-domeinnamen, waarvan SIDN de beheerder is.

Op basis hiervan schatten beide organisaties dat de bij NaWas aangesloten ondernemingen 425 miljoen euro aan inkomsten zouden zijn misgelopen wanneer bescherming niet aanwezig was geweest. Omdat de NaWas 43% van de .nl domeinen beschermt (2,5 miljoen domeinen), en de data van SIDN zich beperkt tot .nl-domeinnamen (64% van alle domeinnamen in Nederland) vermoeden beide instanties dat de potentiële schade in werkelijkheid veel hoger zou uitvallen. Ook ontbreekt de data nog van een aantal grote organisaties die hun eigen DDoS-oplossing aanbieden.

Sectoren

Per sector zijn de verschillen groot. Er is ook een verschil in de manier van aanvallen: bewust of als nevenschade (*collateral damage*). De potentiële schade van een bewust doelwit is het grootst in de overheidssector: bijna 60 miljoen euro. De *Home and Garden* is de sector die het meeste te lijden heeft van potentiële nevenschade (35 miljoen euro).

De nevenschade komt door aanvallen op domeinen die bij een *shared host* staan. De kans dat een domein daardoor geraakt wordt door een DDoS-aanval is 35 keer hoger dan bij een domein dat een VPS (virtual private server) of *dedicated host* heeft.

Awareness

Bedrijven moeten er dus rekening mee houden dat de effecten van DDoS-aanvallen kunnen verschillen voor verschillende soorten hosting. Hosting kan steeds sneller en goedkoper, maar het is niet zonder risico om alleen naar de laagste prijs te kijken. “Aan de andere kant ligt er ook een verantwoordelijkheid voor de hosters zelf: zij dienen, in het belang van hun klanten, hen te wijzen op dit risico”, stelt Octavia de Weerdt, algemeen directeur stichting NBIP. “We hopen dat dit onderzoek bijdraagt aan de awareness van dit probleem bij beide kanten.”

Michiel Steltman, directeur van Stichting Digitale Infrastructuur Nederland (DINL) zegt daarom ook in het rapport: "De meeste bedrijven hebben tegenwoordig online activiteiten die cloudinfrastructuur of hosting vereisen. De prijs is vaak het leidende criterium voor het selecteren van zulke diensten. Maar nu DDoS-aanvallen steeds vaker voorkomen en de wet vereist dat persoonlijke gegevens worden beschermd, moeten beveiliging en het vermogen aanvallen te beperken een veel hogere prioriteit hebben."

Economische gevolgen

De economische impact is een schatting op basis van misgelopen inkomsten, wanneer er geen bescherming aanwezig was. Daarbij keken NBIP en SIDN naar omzetgegevens van de getroffen bedrijven en de duur van de aanvallen.

“Het onderzoek heeft daarmee een indicatief karakter en pretendeert daarmee zeker geen exacte uitspraak te kunnen doen. Het Centraal Planbureau concludeerde in oktober al dat de exacte schade die DDoS aanricht moeilijk te kwantificeren is. Zo is het lastig te beoordelen of het gedurende een dag niet beschikbaar zijn van een website leidt tot uitstel of afstel van een zakelijke transactie”, aldus Michiel Henneke, marketingmanager SIDN. Ook betekent het gebruik van data aangeleverd door een anti-DDoS platform (in dit geval de NaWas) dat de schade vaak niet daadwerkelijk is opgetreden - er was immers bescherming.

Met het gezamenlijke onderzoek hopen NBIP en SIDN daarom een startpunt voor verder onderzoek te bieden.

“In Nederland is er bijna geen onderzoek gedaan naar de financiële kanten van een DDoS-aanval. Het is ook een lastig onderwerp, want hoe meet je precies hoe ontwrichtend iets is voor de maatschappij? Samen met SIDN hopen we hiertoe een eerste gedegen aanzet te hebben geleverd”, zegt de Weerdt. “We roepen daarom overheden, instellingen en partijen in de markt op om meer onderzoek te doen naar de economische gevolgen van DDoS-aanvallen.”

Het volledige rapport is te downloaden op nbip.nl/impact

- - - EINDE PERSBERICHT - - -

Over NBIP en de NaWas

De NaWas (‘Nationale Wasstraat’) biedt full service on-demand bescherming tegen DDoS-aanvallen. De NaWas is ontwikkeld en gebouwd met de modernste anti-DDoS apparatuur en is centraal gelegen in Nederland. In geval van een aanval wordt het netwerkverkeer door de machines van de NaWas geleid. De NaWas herkent en reinigt het verkeer van kwaadaardige pakketten. Vervolgens stuurt de NaWas het schone verkeer via een aparte VLAN door naar de klant.

De NaWas is een initiatief van de Stichting Nationale Beheersorganisatie Internet Providers (NBIP). Deze stichting zonder winstoogmerk is jaren geleden opgericht door ISP's om te voldoen aan de wettelijke eisen op het gebied van interceptie zoals gesteld in de Telecommunicatiewet. Het levert nu diensten aan meer dan 100 ISP's en VoIP-providers in en buiten Nederland. Meer informatie over de NBIP vind je op *www.nbip.nl*.

Over SIDN en SIDN Labs

SIDN beheert het .nl-domein. Dat houdt natuurlijk in dat we alle 5,8 miljoen .nl-domeinnaamregistraties beheren en die veilig beschikbaar maken via het Domain Name System (DNS) . Maar we doen ook andere dingen. Zo delen we onze kennis en ontwikkelen we nieuwe diensten. En we ondersteunen initiatieven om het internet beter en veiliger te maken. We werken eraan om ervoor te zorgen dat je vertrouwen kunt hebben in je digitale wereld. We leveren hoogwaardige diensten gekoppeld aan innovatieve, veilige domeinen en digitale identiteiten.

SIDN Labs is het researchteam van SIDN. Ons doel is het verder verhogen van de veiligheid en stabiliteit van end-to-end internetcommunicatie door middel van grootschalige metingen en het prototypen en evalueren van nieuwe technologieën en systemen. Onderwerpen waar we onderzoek naar doen zijn DDoS-resilience, misbruik van domeinnamen, IoT-veiligheid, collaborative security en de evolutie van de kern van het internet. We werken vaak samen met onderzoeksinstituten, waaronder de Universiteit Twente, de Technische Universiteit Delft, de University of Southern California en NLnet Labs.

Noot voor de redactie

Voor vragen, neem contact op met:
Octavia de Weerdt - algemeen directeur NBIP
octavia@nbip.nl
0318 48 93 50

wereld snel veranderen. Neem contact met ons op en laat je inspireren.

Splend!

Splendnewsroom