DIT KAN EEN DDOS-AANVAL MET JE DOEN

Risico's en oplossingen

TELE2

DIT KAN EEN DDOS-AANVAL MET JE DOEN

Risico's en oplossingen

Distributed Denial of Service-aanvallen (DDoS), cyberaanvallen die een website of webapplicatie platleggen door deze te bestoken met aanvragen voor informatie, zorgen voor ernstige schade aan uw organisatie. Nog maar tien jaar geleden was DDoS het domein van vaardige online pestkoppen die zich wilden laten gelden. Tegenwoordig kunnen grootschalige DDoS-aanvallen eenvoudig worden ingekocht en worden ze uit persoonlijke of commerciële motieven ingezet.
Deze aanvallen komen daardoor steeds vaker voor en zijn in staat om ook zeer robuuste netwerken onbereikbaar te maken. Omdat de schade van een DDoS-aanval in de tonnen kan lopen is het cruciaal om de organisatie tegen dit soort vandalisme te beschermen. In deze whitepaper leest u hoe een DDoS-aanval werkt, hoe groot het probleem is en wat ertegen valt te doen.

Aanwezigheid online vormt voor steeds meer organisaties een cruciaal onderdeel van de business. Websites en webapplicaties zijn primaire bronnen van omzet, of zijn een niet te missen schakel binnen het volledige dienstenpakket. Dat betekent dat bij een verstoring van dit onderdeel de kosten meteen torenhoog zijn. Op relatief eenvoudige manieren kan een organisatie zich indekken tegen 'gewone' storingen en calamiteiten. Noodstroomgeneratoren kunnen bijvoorbeeld soelaas bieden bij een stroomstoring, en een redundante uitvoering kan falende ICT ondervangen. Maar storingen veroorzaakt door kwaadwilligen zijn een stuk moeilijker te voorkomen. Vooral DDoS-aanvallen vormen een grote en potentieel kostbare bedreiging waartegen een organisatie zich in zijn eentje moeilijk kan wapenen.

Bij een DDoS-aanval wordt een systeem bestookt met grootschalig internetverkeer. De aanvallers genereren deze aanvragen door een groot aantal computers te kapen via malware. Zonder dat de eigenaren het weten, worden hun computers van een afstand bestuurd. Deze zogenaamde 'botnets' kunnen soms uit miljoenen PC's bestaan. Het gegenereerde verkeer is zo groot dat de internetverbinding van de klant dit onmogelijk kan verwerken. Hierdoor loopt deze volledig vol en kan het doelsysteem niet meer bereikt worden. Het gevolg is dat gebruikers en klanten niet meer bij de dienstverlening kunnen, wat precies het doel is van de aanvallers.

Geen organisatie veilig

Veel bedrijven kunnen daarover meepraten. In het voorjaar van 2015 werd bijvoorbeeld een scholengemeenschap in Almere getroffen door een serie DDoS-aanvallen uitgevoerd door twee leerlingen. Maar de school bevindt zich in goed gezelschap, want ook de overheid en internationale bedrijven worden regelmatig aangevallen. Zo strandden 1.400 passagiers op het vliegveld van Warschau toen hackers systemen van de Poolse nationale luchtvaartmaatschappij LOT platlegden. Zoals de CEO van de luchtvaartmaatschappij aangaf: LOT maakt gebruik van de nieuwste systemen, dus een dergelijke aanval kan iedereen overkomen. Vooral omdat technische kennis niet langer noodzakelijk is. Verschillende louche websites bieden 'DDoS op bestelling' aan, waarbij iemand voor een bedrag een aanval kan laten uitvoeren. Hoe meer wordt betaald, des te langer en geniepiger de aanval. En een organisatie wordt al snel gekozen als doelwit (Zie kader: wie is een makkelijk doelwit voor een DDoS-aanval?)

Wie is makkelijk doelwit voor een DDoS-aanval?

Hacktivisten en cybervandalen vinden altijd wel een excuus om een bepaalde organisatie aan te vallen. Bij sommige organisaties is het echter makkelijker om een aanleiding of reden te vinden. Daarnaast zullen criminelen sneller een organisatie aanvallen als deze hierdoor voelbare schade oploopt. Hier zijn zes vragen die managers zichzelf kunnen stellen om vast te stellen hoe groot het risico is dat iemand de organisatie op de korrel neemt:

- Zou mijn organisatie doelwit kunnen zijn om politieke doeleinden? Is het een (semi-) publieke overheidsinstelling?
- Zou mijn organisatie doelwit kunnen zijn om religieuze doeleinden?
- Zou mijn organisatie doelwit kunnen zijn om ideologische doeleinden?
- Vormt online retail een belangrijk verkoopkanaal?
- Vormen websites of webapplicaties een integraal onderdeel van de dienstverlening?
- Zijn de internetaansluitingen en/of systemen reeds doelwit van aanvallen geweest?

Verschillende internationale onderzoeken laten zien dat meer dan 40 procent van de bedrijven wereldwijd met een DDoS-aanval te maken heeft gehad. Alleen in het eerste kwartaal van 2015 zijn volgens beveiligingsspecialist Kaspersky wereldwijd meer dan 23.000 dergelijke aanvallen wereldwijd gemeld. Volgens het Centraal Planbureau staat Nederland hoog op de ranglijst van landen waar organisaties worden getroffen door deze aanvallen.

De aanvallen worden ook steeds heviger. Er zijn gevallen gemeld dat een DDoS-aanval 6 dagen achtereen aanhield, terwijl sommige netwerken gedurende een hele maand herhaaldelijk te kampen hebben met pogingen tot cybervandalisme.

De vormen van een DDoS-aanval: Volume en Sophisticated

Een DDoS-aanval kan op vele verschillende manieren worden uitgevoerd. Het doel is echter altijd hetzelfde: het laten crashen van het systeem. Het verschil tussen de methodes zit hem in de detecteerbaarheid en hoe eenvoudig een dergelijke aanval is te voorkomen.

Volume-aanval

Ruwweg zijn DDoS-aanvallen in twee categorieën te verdelen, waarbij per categorie andere lagen van het ICT-systeem worden aangevallen. De meest voorkomende en eenvoudige vorm is de Volume-aanval. Hierbij wordt gebruikgemaakt van de meest eenvoudige methodes om zo snel mogelijk een opstopping op de internetverbinding(en), het netwerk of systemen van de klant. Aanvallers doen met een Volume-aanval weinig moeite om de aanval te maskeren en vertrouwen zodoende op de brute kracht van hun botnet. Het zijn vooral digitale vandalen en hacktivisten die van deze aanvallen gebruik maken. Volume-aanvallen komen dan ook veruit het meeste voor. Per dag worden wereldwijd duizenden van dit soort aanvallen uitgevoerd. Sommige organisaties, zoals overheid en universiteiten, melden zelfs meerdere aanvallen per uur.

Sophisticated DDos-aanvallen

Geniepiger zijn de Sophisticated (geraffineerde) DDoS-aanvallen. Hierbij worden zwakheden in applicaties zelf uitgebuit om het systeem neer te halen. Meestal genereren deze aanvallen veel minder verkeer, maar doen ze dat precies op punten die bottlenecks vormen. Ze zijn moeilijker uit te voeren, maar ook veel lastiger te detecteren. Het verkeer wordt zoveel mogelijk gecamoufleerd en doet zich voor als ‘legitiem’ verkeer. Deze aanvallen worden dan ook steeds populairder onder cybercriminelen, die hiermee organisaties dwarszitten.
Dikwijls eisen ze daarbij losgeld: ‘betaal, of wij gooien het systeem plat.’ Maar een crimineel kan DDoS ook inzetten als afleidingsmanoeuvre. Terwijl de specialisten van een bedrijf proberen de dienst weer online te krijgen, stort de hacker zich op de systemen waar ze minder scherp op letten. Dit soort aanvallen komt steeds vaker voor. Arbor Networks, een specialist op het gebied van DDoS-preventie, heeft na uitgebreid onderzoek vastgesteld dat in 2005 nog bij 90% van de aanvallen Volume-aanvallen waren terwijl dit in 2014 gedaald is naar 65%.

De kosten en consequenties van een DDoS-aanval

Welke vorm een DDoS-aanval ook heeft, hij kan op meerdere fronten grote gevolgen hebben voor de organisatie. De kosten zijn daarbij dikwijls hoger dan van tevoren geschat, en worden steeds hoger. Steeds meer aangevallen bedrijven lijden directe financiële schade. Volgens verschillende onderzoeken kan een enkele aanval hierdoor een middelgroot bedrijf 50 duizend euro kosten, tot bijna 4 ton voor grote bedrijven. Sony heeft na een aanval in 2011 zelfs 170 miljoen dollar moeten uitgeven nadat het Playstation Network was platgelegd.

Enkele grote mogelijke schadeposten zijn:

Business continuity - De meest directe schade is dat de dienstverlening niet werkt terwijl de aanval gaande is. In die zin lijkt deze schade op die van stroomuitval. Eventuele omzet op dat moment gaat verloren. Bovendien is het niet altijd evident hoe de draad moet worden opgepakt. Hoe worden de verloren gegevens teruggehaald? Hoe kunnen klanten worden geactiveerd om terug te keren? De naweeën van een DDoS-aanval kunnen zo nog lang aanhouden.
Juridische kosten - Maar de uiteindelijke kosten liggen bij een DDoS-aanval veel hoger dan alleen gemiste omzet. Klanten kunnen met claims komen als ze zelf directe schade ondervinden. En ook de advocaatkosten kunnen enorm in de papieren lopen, vooral als gevoelige gegevens verloren gaan.

Extra beveiliging - Omdat het cruciaal is om te voorkomen dat een dergelijk incident zich opnieuw voordoet, nemen veel bedrijven na een aanval consultants in de arm, die ook nog eens extra in rekening brengen voor het feit dat eventuele adviezen met spoed moeten worden afgegeven. Tevens wordt de infrastructuur aangepast en robuuster gemaakt, wat ook een grote uitgave kan zijn.
Reputatieschade - Geslaagde DDoS-aanvallen halen regelmatig het nieuws, hoe groot een organisatie ook is, van middelbare school tot grote multinational. Reputatieschade is moeilijk in geld uit te drukken, maar kan een bedrijf lang achtervolgen, vooral als het om een dienst gaat die voor klanten onmisbaar zijn. Het terugwinnen van vertrouwen vergt tijd en investeringen.

Wat valt er tegen te doen?

Veel organisaties hopen DDoS-aanvallen te voorkomen door zoveel mogelijk bandbreedte in te kopen. Meer bandbreedte is immers moeilijker te overrompelen. Het probleem is dat cybervandalen in deze wapenwedloop in het voordeel zijn. Het lukt ze al om meer dan honderden Gigabits per seconde aan verkeer te generen, genoeg om zelfs de grootste netwerken plat te krijgen. Uiteindelijk heeft iedere organisatie een beperkt budget voor breedband, terwijl de aanvallers hun botnets constant kunnen uitbreiden.

Dat neemt niet weg dat het verstandig is extra bandbreedte beschikbaar te houden. Als een aanval begint, kan de extra bandbreedte cruciale tijdwinst opleveren om te kunnen reageren. Het is daarbij belangrijk om een goed inzicht te hebben in het soort verkeer dat het systeem normaal gesproken trekt. Zo kunnen afwijkingen van normaal verkeer snel ontdekt worden en kan vlot op een aanval worden geacteerd. Dit is slechts een oplossing voor de zeer korte termijn, doordat het verkeer tijdens een aanval exponentieel toeneemt. Hierdoor loopt de internetverbinding alsnog vol. Voor de meeste organisaties is het dan ook niet te doen om effectieve beveiliging tegen dit soort cyberaanvallen in eigen beheer te houden.

Hoe pakt een specialist het aan?

Er worden speciale diensten aangeboden die specifiek bescherming bieden tegen DDoS-aanvallen. Niet alleen hebben deze dienstverleners meer mogelijkheden om het verkeer te verwerken, ze hebben vaak ook betere filtermogelijkheden. Daarnaast heeft het als voordeel dat aanvallen zo vroeg mogelijk in de keten worden onderschept.

Dat is de reden dat steeds meer organisaties de verbinding tot hun netwerk en applicaties door de provider laten beschermen. Het zwakste punt is immers de internetverbinding. Wanneer deze volloopt, kan men het netwerk en bescherming op netwerkniveau überhaupt niet bereiken. In het netwerk van de provider kunnen daarentegen verschillende beschermingsprofielen worden aangemaakt die specifieke onderdelen zoals de webserver of mailserver afschermen door ongewenst verkeer te filteren.

Omdat ze op het netwerk van de provider werken, beschikken specialisten ook over meer capaciteit dan op de eigen bedrijfsnetwerken van de klanten. Ze analyseren de binnekomende data en blokkeren en schonen het verkeer terwijl legitieme aanvragen worden doorgelaten. Daarbij worden verschillende mogelijke knelpunten van het netwerk afzonderlijk in de gaten gehouden. Normaal verkeer wordt meteen aan het netwerk van de klant doorgegeven. DDoS-verkeer daarentegen wordt naar een zogenaamde wasstraat geleid waar dit verkeer wordt geschoond en vervolgens alsnog afgeleverd bij de klant. Deze manier van DDoS-neutralisatie werkt voor aanvallen tegen de infrastructuur en wordt door de dienstverlener aangeboden zonder dat de gebruiker hier iets van merkt. Een aanval kan binnen een minuut worden gedetecteerd, en binnen een paar minuten omgeleid worden naar de wasstraat. De ICT van de klant hoeft daarvoor niet speciaal uitgebreid te worden.

Op deze manier kan tegen de overgrote meerderheid van aanvallen beschermd worden. De primaire doelstelling, business continuity, kan zo worden gewaarborgd. Bij meer geraffineerde aanvallen op de applicaties komt wat meer kijken. Omdat het applicatielandschap per organisatie enorm verschilt, moet de oplossing worden toegesneden op de bestaande situatie. Een goede oplossing hiervoor is het plaatsen van speciaal uitgeruste IT-apparatuur in de omgeving van de klant. De applicaties van de klant krijgen zo een eigen, op maat gesneden 'bodyguard', die de klant beschermt tegen Sophisticated aanvallen.

Om de klant optimaal te beschermen tegen DDoS-aanvallen moeten deze twee oplossingen volledig samenwerken en door van elkaar te leren steeds slimmere aanvallen kunnen afwenden. Na een aanval, afgeslagen of niet, is het werk namelijk nog niet gedaan. Ook criminelen zitten niet stil en zijn constant bezig hun methodes verder aan te scherpen. Daarom is het van belang een gedegen analyse te maken van de aanval zelf en waar mogelijk de filters verder te optimaliseren. Het standaardverkeer moet zo goed mogelijk worden geprofileerd, zodat bij afwijkingen die kunnen duiden op een DDoS snel kan worden ingegrepen. Uiteindelijk is reactiesnelheid alles, want indruk maken is meestal een belangrijk onderdeel van hun doelstelling.

Conclusie

DDoS-aanvallen vormen een steeds grotere dreiging voor de business van organisaties. Het relatieve gemak van een dergelijke aanval maakt dat de drempel zeer laag ligt, terwijl technische kennis door de opkomst van 'DDoS op bestelling' niet eens meer nodig is. Tegelijkertijd worden DDoS-aanvallen ook geavanceerder, en kunnen zij steeds grotere netwerken sneller en langer uitschakelen. Hoewel de overgrote meerderheid van aanvallen nog steeds op brute kracht wordt uitgevoerd, worden steeds vaker specifieke applicaties bestookt.

Gezien de directe en indirecte schade die DDoS-aanvallen kunnen aanrichten, door het wegvallen van de business continuity, de indirecte kosten die een DDoS veroorzaakt en de reputatieschade, is een goede afweer essentieel. Het is daarbij niet langer voldoende om domweg meer bandbreedte in te kopen, want de aanvallers zijn bij deze wapenwedloop in het voordeel. Een effectieve DDoS-verdediging bestaat uit filtertechnologie die zo vroeg mogelijk in de netwerkketen is geplaatst, namelijk in het netwerk van de provider, gecombineerd met gespecialiseerde apparatuur op klantlocatie voor meer sophisticated aanvallen.

Gedegen analyse zorgt na een aanval voor betere bescherming in de toekomst. Niet onbelangrijk, omdat criminelen hun methodes steeds verder verfijnen. Dit zorgt niet alleen voor bescherming tijdens een aanval, maar verkleint ook de kans dat een organisatie door cybervandalen als doelwit wordt gekozen. Voorkomen is nog altijd beter dan genezen, zeker als het erom gaat uw organisatie bereikbaar te houden!

Deze whitepaper wordt u aangeboden door Tele2

Tele2 is opgericht in 1996 en heeft roots in Zweden. Het bedrijf heeft op dit moment 14 miljoen klanten in 9 landen. Tele2 is uitgegroeid tot de tweede speler op het gebied van vaste telefonie en datadiensten en verbindt heel zakelijk Nederland: van een pinautomaat op de hoek tot de telefoon van onze premier. Het zit in ons DNA om monopolies en ouderwetse business modellen uit te dagen en om de bestaande regels te veranderen, zodat we de voordelen daarvan kunnen delen met onze klanten. Vele gemeenten, provincies, ministeries, banken, scholen en ziekenhuizen, maar ook uw bakker op de hoek, de vuilnisophaalservice en nationale omroepen vertrouwen dagelijks op de diensten of netwerken van Tele2.

In Nederland beschikt Tele2 over een eigen landelijk dekkend glasvezelnetwerk en een state-of-art mobiel 4G netwerk, de funderingen van onze vaste en mobiele spraak- en datadiensten in de zakelijke markt. De afgelopen jaren hebben we ons portfolio verder gecomplementeerd met zakelijk mobiel 4G, oplossingen voor de integratie van vaste en mobiele telefonie, Unified Communications en Machine-to-Machine. Anno 2016 maken 1,1 miljoen klanten in Nederland gebruik van onze dienstverlening.

Inspelen op de vraag van de klant is een van onze sterkste punten. Wij vinden dat telecommunicatie onnodig ingewikkeld en duur is geworden en geloven dat dit anders kan. Dat communicatieoplossingen gemakkelijk, eenvoudig en schaalbaar moeten zijn in te passen in iedere organisatie, zonder concessies te doen aan kwaliteit. Wij gaan altijd verder voor onze klanten. Met onze dienstverlening bieden we hen een wereld aan communicatie- en samenwerkingsmogelijkheden. Slimmer en voor minder.

Voor meer informatie kijk op onze website of neem direct contact met ons op via het formulier of door te bellen met 0800 - 1242.