Beschrijving webinar: “Jullie kunnen allemaal de DDos krijgen!”

“Op 1 oktober 2020 vond van 13:00 tot 14:00 uur het Webinar “Jullie kunnen allemaal de DDoS krijgen” plaats. Dit webinar werd gepresenteerd door Theo van Diepen, CISO bij Logius. Hij had ook een tafelgast die zich voorstelde als ‘hacker in spé’ en een masker droeg. Beiden zijn in een tekeningetje van een beeldscherm met twee poppetjes afgebeeld.

Wat is een DDos aanval?

Allereerst werd ingegaan op “Wat is een DDos aanval?” Dat is een aanval om een systeem of dienst ongeschikt te maken. “Dit houdt mij als CISO van de straat” gaf Theo aan. “Dit wil je voorkomen!”. De afkorting DDoS staat voor ‘Distribtued Denial of Service’. Uitgelegd werd dat vooral de toevoeging ‘Distributed’ ervoor zorgt dat dit complex is.

Historie

Via een tekeningetje van een poppetje achter een ouderwetse computer wordt het verhaal verteld dat de eerste geslaagde DDOS-aanval plaatsvond door de 13 jarige David Dennis in 1974. Hij zorgde ervoor dat de terminals van zijn universiteit overbelast raakten. Vervolgens staat in een getekend tabelletje met 3 kolommen het verloop van de DDoS-aanvallen door de jaren heen. Waarbij eind jaren 2000 je zag dat de georganiseerde misdaad DDoS-aanvallen steeds meer is gaan gebruiken. In de volgende kolom staat het jaartal 2016. Toen vond de tot nu toe grootste DDoS-aanval plaats, beter bekend als Mirai-botnet. Dit legde half Amerika plat. In de laatste kolom staat het jaartal 2018. En is een tekeningetje van een kat en muis opgenomen. Om aan te geven dat er nu steeds vaker protectie is tegen DDoS-aanvallen, maar de aanval via een kat en muis spel nog steeds wordt uitgevoerd.

Waarom worden DDos aanvallen uitgevoerd?

Vervolgens wordt ingegaan op de vraag: “Waarom worden er DDoS aanvallen uitgevoerd?” Dit is kort samengevat met een paar tekeningen die de redenen visualiseren:

- Een getekend uitroepteken met armen en boze blikken: symboliseert dat de aanvaller aandacht wil trekken.
- Een poppetje met een bordje met daarop het woord “protest” symboliseert dat de aanvaller ergens tegen wil protesteren.
- Een tekeningetje waarbij een poppetje met een schoolrugzak hard wegrent bij een school waar een bord “gesloten” voor hangt: symboliseert dat de aanvaller soms iets wil ‘ontregelen’. Via een spreekwolkje bij het wegrennende poppetje met de schoolrugzak wordt het in het webinar aangehaalde voorbeeld weergegeven: de leerling had die dag zijn proefwerk niet geleerd en besloot de systemen van de school aan te vallen.
- Vervolgens een tekening van een laptop met een doodshoofd erin: DDoS wordt ook gebruikt door de aanvaller om te bedreigen.
- En een tekening ernaast van een laptop met kettingen rond het beeldscherm en in het midden een hangslot: niet meer te gebruiken, op slot gezet door de hacker. Waarmee wordt gesymboliseerd dat het ook gebruikt wordt om af te persen. Via een spreekwolkje uit deze laptop wordt het voorbeeld vanuit het webinar verteld dat de aanvaller geld wil verdienen

door rond de kerst de websites van de concurrenten plat te leggen, zodat alle bestellingen bij jou worden geplaats.
- Tot slot staat er een tekeningetje van een “game controller” met voetjes. In het webinar is namelijk verteld dat ook gamers DDoS inzetten. Zij hebben dan tot doel om de tegenstander te verslaan, puur om het spel te winnen dus.

Hoe werkt het?

De volgende sectie van de tekening gaat in op “hoe werkt het?”. Daarbij is aangegeven dat vroeger het vooral een aanval was waarbij de hacker ‘het publiek’ nodig had. Tegenwoordig vindt het plaats via zogeheten ‘botnets’: hier is een tekeningetje ingevoegd waarop je ziet dat een hacker achter zijn laptop zit en een zogeheten Commanding Control Center gebruikt om andere computers te hacken (afgebeeld met pc-schermen met een ‘bug’ erop) die vervolgens als ‘botnets’ dienen om een site of server aan te vallen. Ook bestaat er tegenwoordig de optie om een aanval via een website simpelweg te kopen. Je hebt dus tegenwoordig geen enkele kennis nodig om een DDoS-aanval uit te voeren. Er staat een tekening van een winkelkarretje met een lange afstandsraket erin waaruit een spreekwolkje komt met de tekst “Even Googlen op “Booter” of “IP-stresser”.

Theorie

Daarna wordt ingegaan op een stukje theorie. Allereerst: hoe werkt internet eigenlijk. Waarop een plaatje is getekend van een aantal lagen. Met onderin een kabel. En bovenin “Webservices” zoals Facebook. Die verschillende lagen zijn een soort ‘lasagne’ (er is een smiley met een tongetje ernaast afgebeeld die dit via een spreekwolkje roept). Tussen die lagen vindt communicatie plaats. Dit is ook afgebeeld met een tekeningetje van een megafoon. En eronder staat dat die communicatie plaatsvindt o.b.v. protocollen. En daarnaast een spreekwolkje die aangeeft dat internet één groot netwerk is.

Begrippen

In het webinar werden vervolgens enkele begrippen uitgelegd. Het “Transmission Control Protocol”, beter bekend als de “Three way handshake”. Er is een tekeningetje gemaakt van 2 knuffelende olifantengezichten. Er komt een verzoek (stap 1, ‘SYN’ genoemd). Dat gaat van olifant 1 naar olifant 2. Olifant 2 accepteert het verzoek (stap 2, ‘SYN’-‘ACK’ genoemd) en stuurt data terug naar olifant 1. Olifant 1 accepteert dat vervolgens (stap 3, ‘ACK’) en de knuffel kan beginnen! Het volgende begrip wat wordt uitgelegd is het “User Datagram Protocol”. Ook om te communiceren. Hierbij zijn 2 giraffen getekend. Daarbij geeft de ene giraf een verzoek aan de andere giraf. En de andere giraf geeft op basis daarvan data terug. Daar stopt het echter. Bij de tweede giraf staat vervolgens een denkwolkje getekend met daarin de tekst “Geen idee of het aankomt!” En het derde en laatste begrip dat is afgebeeld is een tekening van twee maskers (op de voorgrond met een grimas en op de achtergrond, half verscholen erachter een droevig gezicht). Zij symboliseren het begrip “spoofing” wat wordt vertaald naar het “vervalsen van je identiteit”.

In de praktijk

Na de voorgaande uitleg over hoe het internet werkt en de drie begrippen staat uitgewerkt via twee pijlen hoe een DDoS-aanval werkt. De linker pijl naar beneden beschrijf een “Syn Flood Attack”. Daarbij is er een hacker die een SYN-verzoek stuurt naar de server van DigID. Ondertussen zorgt hij ervoor dat hij via spoofing zijn identiteit vervalst, afgebeeld met meerdere beeldschermen die eronder staan getekend met daarop een “bug”. Digid stuurt via een Firewall (afgebeeld met een

vlammetje en een muurtje erachter) een ‘SYN-ACK’-melding terug naar de ‘gespoofde monitoren’. Die herkennen dit bericht echter niet en zullen dus geen ‘ACK’ terugsturen. En daarmee raakt de firewall overbelast (afgebeeld met een driehoekig verkeersbord met een uitroepteken erin) en dat zorgt ervoor dat de website van Digid onbereikbaar wordt. Er staat ook nog een vraag getekend vanuit het begrip ‘Spoofing’. Deze vraag is in het webinar door een kijker gesteld en luidt: Hoe werk dat spoofing? Het antwoord is dat “in de header van je pakketje je je bronadres aanpast. En daar is gewoon een tooltje voor beschikbaar”. Dit alles is afgebeeld met een spreekwolkje.

Amplification Attack

Naast deze vorm van aanval is er een rechter pijl naar beneden die de “Amplification Attack” beschrijft. Daarbij zien we een hacker achter een pc die een ‘klein verzoek’ (dunne pijl) verstuurt naar de server van DigiD. DigiD stuurt daarop een groot antwoord (dikke pijl) terug. De hacker gaat nu echter wederom ‘spoofen’ en creëert een heleboel pc-schermen die hij allemaal zich laat voordoen alsof ze DigiD zijn. En dus wordt vanuit die computers een klein verzoek naar DigiD verstuurd. De server van DigiD zal hierop grote antwoorden terugsturen, in dit geval naar zichzelf. En zo zal de server overbelast raken. Afgebeeld met een plaatje van een server waar rookwolkjes uitkomt vanwege de dikke pijlen die via een boomerang-effect terugkomen.
Onder deze twee varianten staat een kort kader met een aanduiding NIEUW: in het webinar is namelijk gemeld dat een nieuwe trend is dat DDoS aanvallen nu ook via Applicaties plaatsvinden i.p.v. via netwerken. En dus: be aware!

Wat is het probleem?

Het op één-na-laatste onderwerp op de plaat gaat over ‘wat is het probleem nu eigenlijk’?
Daarbij wordt eerst geduid dat internet een open en transparante infrastructuur is. Waarbij nooit bedacht is dat wij het zouden gebruiken zoals we dat nu doen. Tegenwoordig willen we juist niet dat alles zo open en transparant is. Dat is afgebeeld met een poppetje met een paarse deken in zijn hand met een spreekwolkje waarin staat “Ik heb hier een lappendeken voor onze gevoelige info”.
Ernaast staat een plaatje waarin we meegenomen worden in de geschiedenis en ontwikkeling van het internet. In de jaren ’90 moesten we nog inbellen. Afgebeeld met een poppetje dat via een oude bakkeliet-telefoon aan het bellen is met internet. Het internet was toen traag. Onze ‘way of life’ is inmiddels sterk door internet beïnvloed. Het is nu razendsnel. En we zijn ontzettend afhankelijk geworden van een goed werkend internet. Afgebeeld door een poppetje wat vooruitgeduwd wordt door een pratende smartphone die zegt “Nu ga je dát doen!”. En die afhankelijkheid zorgt ervoor dat we kwetsbaar zijn! Ernaast is een tekeningetje gemaakt van een bootje in een sluis. De sluis heeft een gezichtje en twee armpjes en vraagt via een spreekwolkje: “Bestuurders, willen jullie mij écht met internet verbinden?”

Hoe kun je het voorkomen?

Het laatste onderdeel op de plaat is “Wat kan je doen om het te voorkomen”. Ernaast staat meteen een spreekwolkje dat zegt “Er zullen altijd kwetsbaarheden blijven”.
Vervolgens wordt de vraag beantwoord via twee kolommen. De eerste kolom kent een kop “Online” waarbij staat dat je daar 3 dingen kunt doen. Het 1e is “Creëer een content delivery network”. Dit is afgebeeld met een grote wolk waaraan de server hangt. In die wolk zie je allemaal poppetjes en locaties. En daartussen lopen groene stippellijnen, die de ‘content’ vertegenwoordigen. De content blijft van jou, maar een andere partij (de poppetjes en de locaties) distribueren die content. Door de ‘grootte’ die je hiermee creëert, wordt dit moeilijker aan te vallen. Het 2e wat je kan doen heet een ‘Anti DDos-Appliance” dit is afgebeeld met een wasmachine met gezichtje en armen en beentjes die een enorme hoeveelheid pijltjes op zich af ziet komen. Ernaast staat een spreekwolkje met de tekst

“Ik “was” op basis van algoritmen”. En ernaast zie je een pijltje naar de server waarboven de tekst staat “schoon verkeer”. Het 3e wat je kan doen lijkt op de 2e variant, maar heet “Scrubbing Provider” en bevat niet 1 wasmachine, maar een hele wasstraat (in dit geval 3 wasmachines naast elkaar getekend). Hieronder staat dat hiermee een grote bandbreedte wordt gecreëerd en er staat een tekstwolkje bij dat je hiermee een amplification attack aan kan. Wederom staat er na de wasmachines een aantal pijlen naar de server met schoon verkeerd met de kreet ‘ISP’ erbij. Tot slot staat onder deze 3 varianten: “Combineer deze 3, maar voer eerst een goede risico- en kosten/baten-analyse uit: stem de maatregelen af op de eigen dienstverlening!”.

Offline maatregelen

Na deze eerste kolom “online” staat er rechts naast een kolom “offline”. Offline kan je de volgende dingen doen. Het 1e is het werken met een besloten infrastructuur. Afgebeeld door het woord besloten in een huisje te tekenen en een internetbolletje te tekenen en dat door te kruizen. Het 2e wat je offline kunt doen is samenwerken. Afgebeeld door elke letter van het woord SAMEN als een soort poppetje te tekenen die gearmd staan. De S laat via een spreekwolkje weten dat je ook met je provider moet samenwerken. Eronder staat in een opvallende banner waarom je moet samenwerken: een DDos kan ons namelijk allemaal overkomen. Dus deel je kennis en ervaring. In het webinar is in dat kader specifiek de Anti-DDoS Coalitie genoemd en daarbij expliciet ook het Clearing House. Hier afgebeeld als een database met gezichtje, armen en beentjes die via een spreekwoordje uitlegt: “Ik bevat alle karakteristieken van recente aanvallen”. Het 3e wat je offline kunt doen is oefenen, oefenen, oefenen. Er staat een lampenbolletje met armen en beentjes die via een spreekwolkje de volgende suggestie doet: ‘Crisis situatie? Hack je eigen systeem! Neem maatregelen voor toekomstige aanvallen’. Eronder staat een afbeelding waar we links een poppetje zien met bokshandschoenen aan die via een spreekwolkje zegt: “Kom maar op”. Rechts ervan zien we een vrouw achter de laptop , waaruit lange afstandsraketjes richting de bokser worden geschoten. Ze heeft geen masker meer op en een hartje boven haar hoofd. Ernaast staat te lezen: “Ethical hacker is your new best friend forever!”.”