NTT Security

Whitepaper

Distribuerad överbelastningsattack (Distributed Denial of Service - DDoS)

Hur mycket kostar en DDoS-attack er verksamhet?

Distribuerade överbelastnings-attacker, eller Distributed Denial of Service – DDoS, har i olika former existerat i årtionden – ändå orsakar de fortfarande stora rubriker. De första högprofilerade exemplen av distribuerade överbelastningsattacker mot globala företag såsom Amazon, Buy.com och eBay rapporterades i februari år 2000. Många oroade sig över att deras tjänster skulle gå ner och befarade en dramatisk påverkan på försäljning och vinst, men snart var allt glömt och man gick vidare. Det handlade ju ändå bara om internetbaserade företag.

Nu, mer än tio år senare, förlitar vi oss alla på internet för våra affärer och ser tillgängligheten som någonting självklart. Samtidigt toppar DDoS-attacker år 2014 listan över säkerhetsbekymmer, enligt företagen i Arbor Networks nionde årliga Worldwide Infrastructure Security Report. Varför är DDoS plötsligt så högt rankat bland säkerhetsexperternas alla olika huvudbryn? Kanske beror det på den tydliga eskalering i antalet attacker på datorhallar och mobila nätverk, eller så är det kanske den ökande frekvensen av incidenter - enligt Arbors rapport har antalet attacker ökat med 50 procent och antalet incidenter med 100 procent. Men större medvetenhet betyder inte att distribuerade överbelastningsattacker ges tillräcklig fokus och investeringar, trots den högst påtagliga effekt attackerna har på organisationer runt om i världen. Vår Global Threat Intelligence Report[1] visar att DDoS-attacker stod för 31 procent av all incidenthantering år 2013. Fakta visar att kostnaden av överbelastningsattacker inte enbart ska ses i begrepp som potentiellt inkomstbortfall och otillgängliga system, vilket för vissa organisationer kan räknas i tiotusentals kronor per sekund – utan också i stigande kostnader för omedelbara åtgärder och återställande av system.

Vår erfarenhet är att de allra flesta organisationer inte lyckas inse de möjliga effekterna av en DDoS-attack, vilket är anledningen till att många fortfarande inte budgeterar för och implementerar förebyggande åtgärder, eller planerar för hur man bäst lindrar skadorna och sköter incidenthanteringen. När man står under attack är inte tiden den rätta för att äska pengar, investera i lösningar och få godkännande för att implementera kontroller, inte samtidigt som man desperat försöker förstå vad det är för hot man står inför och försöker att återställa systemen. Resultatet blir sannolikt både dyrare och mindre effektivt.

Hur har DDoS-attackerna utvecklats och vad betyder det för existerande informationssäkerhetsarkitektur?

Överbelastningsattacker syftar generellt till att störa eller totalt blockera en organisations webbtjänster. Resultatet innebär till exempel att kunder, anställda och samarbetspartner inte längre kan nå verksamhetskritiska webbapplikationer, alla nätbaserade transaktioner stoppas, organisationens personal och andra tillgångar försvinner i ett mörker. De bakomliggande orsakerna till sådana attacker varierar från brottsligt uppsåt till skadligt ofog utfört av någon som vill skada den drabbade organisationens anseende och goodwill. Och fokuset har breddats. Ursprungligen riktades DDoS-attackerna mot e-handel, onlinespel och finansplattformar, men de har nu alla verksamheter med internetnärvaro som mål.

För att säkerställa att investeringar i DDoS-skydd och åtgärder utvecklas innan hoten förverkligas måste organisationer:

1. Känna till hur DDoS-attacker har utvecklats och vilken påverkan de kan ha på existerande informationssäkerhetsarkitektur
2. Förstå alternativen för hur man får ut mesta möjliga värde av förebyggande
3. Implementera rätt incidenthanteringsmodell för er verksamhet

1. NTT Group Security Global Threat Intelligence Report. Besök www.nttgroupsecurity.com för mer information

Jämte traditionella motiv bakom DDoS-attacker, så som hacktivism, utpressning och andra IT-relaterade brott, finns nu andra risker som till exempel den fördel en konkurrent får om deras sajt är uppe medan er ligger nere. Om er bransch är specifikt utsatt för DDoS-attacker och ni klarar er ifrån incidenter så har ni en betydande fördel i att skydda både verksamheten som ert goda rykte. Ett exempel på detta var då flera olika banker i USA år 2012 samtidigt drabbades hårt av överbelastningsattacker. De banker som hade bra skydd lyckades inte bara ostört fortsätta med sin verksamhet utan lockade även till sig en ström av kunder från konkurrenter som inte klarat sig så bra. Användarnas förväntningar på ständig tillgänglighet innebär att minsta lilla nedtid betyder förlorade kunder.

Så vad är DDoS?

DDoS ses vanligen som en överbelastningsattack som konsumerar alla resurser som ert nätverk, era brandväggar och webbservrar klarar av. En mer lömsk sida av DDoS blir dock allt vanligare, då kriminella grupper använder överbelastningsattacker som en avledningsmanöver: informationssäkerhetsresurserna distraheras samtidigt som man genom så kallade APT-attacker (Advanced Persistent Threat) siktar in sig på att stjäla information och intellektuella tillgångar. Men oavsett vilket syftet är skadar förlorad webbtillgänglighet det förtroende ni har hos investerare, kunder och anställda.

För att effektivt kunna hantera DDoS måste ni se när det händer, och sanningen är att det inte alls är uppenbart för en nätverks- eller systemadministratör att se när organisationens infrastruktur står under attack. När de nås av en första varning om att nätverket tyngs ner av någonting, är ofta den första slutsatsen att det är ett tekniskt problem eller tillfällig men naturlig hög belastning. DDoS-attacker har normalt en uppbyggnadsfas, och det kan vara först när attacken intensifieras och verkligen börjar att på allvar påverka tillgängligheten som den identifieras.

Hur kategoriserar vi de här attackerna?

Volumetriska attacker

Dessa attacker kan ofta spåras tillbaka till botnät eller sårbara nätverk. De karaktäriseras av hög bandbredd och geografisk spridning. Volymetriska attacker resulterar ofta i indirekta skador, då enheter som routrar, brandväggar och lastbalanserare, blir överbelastade och nätverket som utsätts blir oåtkomligt.

- **TCP SYN Flood:** En angripare gör anslutningsbegäran riktad mot offrets server med paket som består av onåbara källadresser. Det resulterar i att offret förbrukar alla nätverksresurser.
- **UDP Flood:** UDP är billigt och enkelt att skapa.
- **ICMP Flood:** Enkelt och billigt att skapa. De här attackerna är inte så vanliga då nätverksoperatörer vidtar åtgärder för att begränsa eller blockera dem.
- **Reflection-Attack:** Dessa attacker har blivit populärare då det verkliga ursprunget till en attack är svårt att hitta (de kräver inte ett botnät) och de kan enkelt förstärkas.

Applikationslageratttacker

Applikationslagerattacker är välskrivna och har en specifik tjänst hos värden som mål. Dessa attacker kan vara svåra att upptäcka då de initialt förefaller vara legitima anslutningar, men ofta fyllda med skräptrafik. De är även populära tack vare det stora antal verktyg som finns tillgängliga, som till exempel:

- **HTTP-GET-Attack:** HTTP-GET-attacker är utformade för att förbruka webbserverresurser och ser ut som legitim trafik
- **HTTP-POST-Attack:** Dessa attacker opererar på ett liknande sätt med den skillnaden att de skickar i stället för att begära data
- **SSL-Attack:** Allt fler tjänster flyttas till SSL-kryptering vilket gör att attacker mot SSL ökar över hela världen

Åskådlighet och kontroll av applikationslagertrafik är nyckelelement när man skapar ett DDoS-försvar i flera lager. Nätverkslagerlösningar som utvecklats till att bekämpa volymetriska attacker ser inte applikationslagerattacker, då de saknar en fördjupad insikt i applikationsprotokoll och förmåga att avbryta och ta kontroll över applikationssessioner och sanera dem.

Följder av DDoS-attacker på existerande infrastruktur och kontroller

DDoS-skydd är inte en obetydlig investering, så det är värt att låta det ta lite tid att fatta rätt beslut för er verksamhet. I vissa avseenden kräver DDoS-skydd en förändring i er organisations inställning till hur en onlinetjänst driftsätts och levereras. Det finns ett antal gropar att falla i och hanteringen av en DDoS-lösning är någonting som tveklöst tar tid att förankra i vilken infrastruktur som helst. Er investering är bortkastad om ni inte också investerar i rätt processer för att få ut det mesta av lösningen. Ett stort misstag är att fokusera på DDoS-skyddets teknik, snarare än på vad du vill att det ska skydda. Där DDoS-implementeringen ofta blir fel är gällande planering och exekvering av hur man får sina tjänster och applikationer på plats bakom DDoS-lösningen.

Säkert är dock att det inte räcker att slå på DDoS-skyddet på er UTM-brandvägg (Unified Threat Manager) eller next-generation-brandvägg för att skydda er mot de flesta attackerna. Faktum är att det kräver en mycket större mängd datorkraft att ta hand om en volymetrisk attack än vad er brandvägg kan erbjuda. Så låt oss se över vilka alternativ ni har att skydda er organisation.

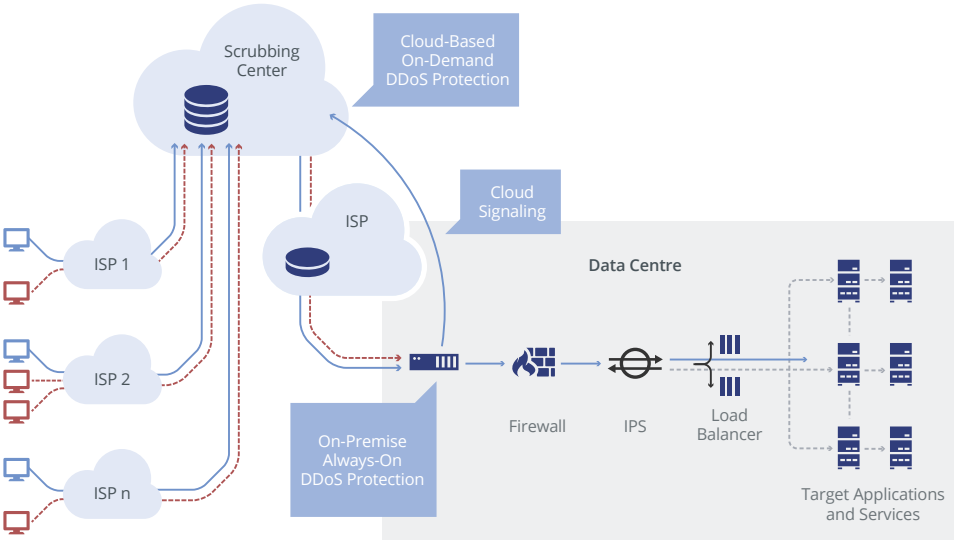
Maximera värdet av offensiva säkerhetsprocesser och teknik

Det finns ett antal olika angreppssätt för att begränsa DDoS. Åverkan av DDoS-attacker kan lindras genom att använda enheter fysiskt på plats i nätverket, molnbaserade renhållningslösningar eller en omsorgsfullt kombinerad lösning av dessa båda.

Undersökningar visar att kommersiella kunder är vanligaste målet för volymetriska attacker. Sådana attacker är som sagt, snabba, enkla och billiga att köra, och är vanligtvis över 1 Gbps i storlek. Detta innebär att när man ska välja rätt lösning måste organisationen vara kapabel att behandla stora volymer av trafik som normalt skulle överbelasta internetanslutningen.

Baserat på utvecklingen globalt av DDoS-attacker anser vi att en hybrid utgör den mest pålitliga och kostnadseffektiva lösningen, och skapar trygghet genom vetskapen att er investering gör det möjligt att hantera alla incidenter, oavsett storlek, till en förutsägbar, budgeterad kostnad.

How a hybrid Cloud and on-premise Availability Protection System works



1. *Utrustning på plats skyddar mot applikationslagerattacker och signalerar till molnet om en volymetrisk attack upptäcks*
2. *Molnbaserat skydd träder in under volymetriska attacker och rensar data för att tillåta sanerad affärstrafik att passera*

Implementera rätt incidentrespons för er verksamhet

Så vad händer när ni attackeras? För att svara på den frågan måste organisationen utvärdera sin strategi för incidenthantering. Hur man agerar och hanterar en DDoS-attack är en avgörande del i den planen.

I en idealisk värld skulle en investering i en DDoS-lösning skydda er från att aldrig någonsin drabbas av en attack. I praktiken är 100-procentig säkerhet väldigt svårt att uppnå och angripare hittar hela tiden nya sätt att störa er tjänst, drivna av ekonomiska, politiska eller kommersiella faktorer. Men vad en effektiv DDoS-lösning ger er är kapacitet att övervaka för att kunna reagera snabbt på en attack. Koppla ihop det med robust incidenthantering så kan ni neutralisera störningar och kommersiella följder av en attack.

I förberedelse för att hantera en säkerhetsincident bör organisationer:

- Tänka mer på processer och personal - utvecklad incidentrespons behöver inte nödvändigtvis betyda att man spenderar mer pengar på teknik
- Tänk igenom vad det är ni skyddar - bra incidentrespons börjar med bra riskinsikt och kännedom om era informationstillgångar
- Överväg värdet av att genomföra övningar, där ni simulerar möjliga incidenter för att öka medvetenheten och definiera roller och ansvar utöver IT-avdelningen
- Etablera vilka kunskaper ni redan har, vad ni skulle behöva om ni drabbades och vart ni ska vända er i händelse av en incident
- Förstå vad lagar och regleringar betyder för er incidenthantering och ha en tydlig procedur för att uppfylla era specifika skyldigheter

Fallstudie:
Hur vår kund maximerade en investering i DDoS-skydd

En global kund drabbades av en DDoS-attack på en tjänst som var avgörande för verksamheten. Organisationen hotades av utpressning och kontaktade NTT Security för krisrådgivning och hjälp med att begränsa vad som kunde ha blivit en katastrofal attack för företaget.

Affärsvärdet av rätt lösning för DDoS-skydd

- En DDoS-lösning sattes snabbt på plats för att minimera skadorna på den löpande verksamheten
- Därefter vägrade kunden att betala utpressarna varefter dessa försökte att tvinga ner webbplatsen, men lösningen gav avgörande skydd vilket hindrade attacken från att få allvarliga konsekvenser.
- Företaget är nu i en position där de ligger steget före möjliga attacker och hanterar risk förebyggande.

Slutsats

Verksamheter kan i dag inte kosta på sig att ha tjänster otillgängliga i dagar medan en incidenthanteringsplan formuleras och verkställs. Behovet av att få till en komplex DDoS-lösning snabbt och korrekt redan från start är en anledning till att våra kunder ofta engagerar oss tidigt i processen, så att vi kan hjälpa till att identifiera riskerna, välja rätt lösning, samt den tekniska installationen och konfigurationen.

DDoS är inte ett nytt problem, men vi ser hela tiden nya varianter av den här typen av attacker. Företag måste se på problemet med utgångspunkt i strategisk informationssäkerhet, med definierade riktlinjer, tjänstenivåer och riskvärdering, för att säkerställa att lösningen är korrekt utformad för att leverera rätt förebyggande och avhjälpande åtgärder.

Att förstå värdet på informationstillgångar: hur ett relevant DDoS-response hjälpte vår kund att uppnå rätt skyddsnivå

En av NTT Securitys kunder hade valt en DDoS-leverantör men var osäker på hur man inom den multinationella organisationen skulle få rätt nivå på skydd av individuella tillgångar och tjänster. Företaget kontaktade NTT Security för att få hjälp med att förstå och bestämma den process genom vilken de inblandade kunde överblicka och uppnå rätt skyddsnivå för varje system.

Affärsvärdet av rätt DDoS-skydd och strategi för incidenthantering

- NTT Security hjälpte kunden att formulera rätt incidenthantering med affärsmål och krav från start till slut
- Genom att förtydliga och förmedla kriteriet för "opt-in/opt-out" hjälpte systemägare att förstå sina roller och sitt ansvar och hur de bör arbeta med det centraliserade DDoS-systemet
- Kunden förbättrade sin planering och genomförande av incidenthantering, samt förenklade DDoS-lösningens omfattning för att säkerställla att rätt nivå av skydd uppnås

Om ni vill veta mer om NTT Security och våra unika tjänster för informationssäkerhet och riskhantering kan ni kontakta er kontoansvarige eller besöka **www.nttsecurity.com**, där det finns regionala kontaktuppgifter.

Om NTT Security

NTT Security stärker kundens skydd mot cyberattacker genom att bygga de mest robusta och effektiva system som ökar säkerheten och minskar riskerna. Genom att ta ansvar för hela säkerhetslivscykeln kan man bättre möta de ökande säkerhetsproblemen i en digitaliserad och nätbaserad ekonomi. Med hjälp av våra konsulter, produkter och driftstjänster, som levereras av lokala experter med tillgång till globala resurser, kan vi erbjuda en kostnadseffektiv och effektiv leverans av rådgivning och tjänster i egen infrastruktur som tjänst eller i hybrida kombinationer. NTT Security är en del av NTT Group (Nippon Telegraph & Telephone Corporation), en av världens största IT-organisationer. Läs mer på **www.nttsecurity.com**.