NTT Security

Campaign

Undvik nertid orsakat av överbelastningsattacker (ADoS/DoS/DDoS)

Fem råd till rätt skydd

Överbelastningsattacker sker hela tiden, till och med kanske utan att du märker det. Stora attacker är ovanligare, men har desto större konsekvenser. Här delar vi med oss av några råd för hur man undviker att viktiga nättjänster blir instabila eller går ner.

Stora distribuerade överbelastnings-attacker (Distributed Denial of Service - DDoS) får mycket uppmärksamhet i såväl press som sociala medier. Lite för ofta upplever vi situationer där många stora verksamheter angrips samtidigt - nätbanker, flygbolag, dagstidningar, butiker och andra centrala system har gått ner. Det uppmärksammas både av kunder och andra intressenter. Konsekvenserna blir förlorade intäkter och skadat rykte.

Stora attacker gör mycket väsen av sig, men små (de vi kallar "low and slow") inträffar sannolikt oftare än du tror. Det är inte ens säkert att du alls märker dessa mindre attacker som vållar instabilitet. Du kanske tror att det är vanliga nätverksproblem, men det kan mycket väl vara sådana "low and slow"-attacker.

Vi var uppe då alla andra var nere

Under en av norsk historias mest omtalade överbelastningsattacker, då en 17-åring angrep en rad stora verksamheter och institutioner gick stora samhällskritiska webbsidor ner. Våra uppdragsgivare, som även de var under attack, red ut stormen. En stor samhällsdebatt följde i kölvattnet och många ställde sig frågan hur viktiga instanster kan lida så stor skada så pass enkelt.

Attacken varade i 4,5 timmar. I motsats till väldigt många andra verksamheter klarade sig våra kunder igenom det hela med bara några få sekunders nertid. Hemligheten låg i våra avancerade verktyg för larm och hantering. Angreppet riktade sig direkt mot en applikation (Application Denial of Service, ADoS), och var inte en traditionell DDoS-attack, som dramatiskt reducerar bandbredden så att kunder inte når fram. Den här typen av attacker som riktas direkt mot tjänster och efterliknar kundens trafikmönster, kräver lokalt skydd och annan kompetens än vad vanliga säkerhetslösningar kan ge.

Små attacker med stora konsekvenser

Små attacker på dina system sker oftare än de stora som får mycket uppmärksamhet. Ofta kan man vara under attack utan att veta om det. Har du oförklarliga störningar, prestandaproblem och nertid i dina produktionsnätverk eller webbservrar? Det kan betyda att du är utsatt för små attacker på dina dataresurser eller verksamhetskritiska program.

Som all annan säkerhetsstrategi är det viktigt att först värdera:

> Vilka dina viktigaste uppkopplade tjänster är
> Sannolikheten för att de blir attackerade
> Vilka konsekvenserna blir

Våra kunder berättar att korta händelser av nertid, avbrott, prestandafall och andra incidenter, har minskat dramatiskt och nästan helt eliminerats efter att man börjat använda tjänster från NTT Security.

Medan traditionell säkerhetsteknik som brandväggar och antivirus är nödvändiga ses skydd mot överbelastningsattacker ofta som ett valfritt tillägg. Detta är ett synsätt som ändras när man börjar att räkna på kostnaderna under och efter en attack.

När det gäller överbelastningsattacker är det relevant att skydda de tjänster som har störst betydelse för den dagliga driften och intjäningen, särskilt sedan allt fler affärssystem fungerar som nättjänster. Riktigt skydd gör det möjligt att hantera attacker innan de blir allvarliga och påverkar er verksamhet.

Hur skyddar man sig?

Rätt skydd skräddarsys för varje enskild organisation. Ingen verksamhet är den andra lik, och det finns inte en mall som passar alla när det gäller skydd mot DoS-, ADoS- och DDoS-attacker.

Skyddet handlar om att identifiera och filtrera illasinnad trafik från systemen utan att det hindrar vanlig drift och användare med ärligt uppsåt. Bra lösningar har era verksamhetsmål som utgångspunkt, så att ni skyddar det viktigaste och låter driften fortlöpa oavsett IT-säkerhetsåtgärderna.

1. Gör en analys för att definiera en summa för direkta och indirekta kostnader av nertid. Den fungerar som underlag för att avgöra vilka delar av er infrastruktur som bör skyddas med en ADoS-, DoS-, DDoS-lösning och gör det lättare att hitta rätt skydd.
2. Hitta rätt skydd – Det bästa är att ha en lösning eller tjänst som skyddar både lokalt hos er ("on premise") och i molnet. On premise-komponenten skyddar bäst mot de mindre angreppen och överbelastning på applikationer (ADoS - Application Denial of Service). Samtidigt bör man ha skydd kopplat mot större system i molnet, som kan hindra kombinerade, volymetriska attacker, det vill säga större DDoS-attacker.
3. Utvärdera hanteringsalternativen – Kan ni sköta skyddet själva eller finns det behov av extern hjälp? De flesta har varken kompetens eller kapacitet till den kontinuerliga övervakning dygnet runt som krävs för att man ska vara säker.
4. Implementering – Den här delen kräver noggrann planering, och kan baseras på dina tidigare analyser. Teknologisystemen är komplicerade, och du vill att DDoS-skyddet endast ska stoppa oönskad trafik utan att hindra kunderna att göra sina transaktioner. Här utvärderas skyddade och oskyddade zoner, skapandeprocesser och integration av lösningen i strategin för händelsehantering.
5. Analys och övervakning – När skyddet är på plats kan du övervaka och analysera datatrafiken. Då du tidigare kanske inte visste att du var under attack ska du nu kunna identifiera oönskad trafik som skapar instabilitet i tjänsterna, och eliminera denna. Det kommer att ta bort onödig irritation och effektivitetsförluster. Målet är tjänster som aldrig går ner, angripare som ger upp, samt mer stabilitet och kontinuitet för verksamheten.

För mer information om NTT Security, ta kontakt med din kundansvarige i Sverige eller gå till **www.nttsecurity.com**