Dnr 3.1:4331/23:1

NATIONELLT CYBERSÄKERHETSCENTER

Informationsmaterial:

Överbelastningsangrepp

2023

NATIONELLT CYBERSÄKERHETSCENTER

[TLP:CLEAR]

Informationsblad

Överbelastningsangrepp

Bakgrund

Informationsbladet har tagits fram av Nationellt cybersäkerhetscenters finansforum. Materialet riktar sig till ledningsfunktioner inom finanssektorn. Syftet är att ge en övergripande bild av överbelastningsangrepp, bakomliggande orsaker och konsekvenser, samt ge råd vid hantering.

Överbelastningsangrepp

Överbelastningsangrepp (DoS) och distribuerade överbelastningsangrepp (DDoS) är cyberangrepp där angriparen försöker göra en tjänst otillgänglig. Det kan exempelvis vara en webbsida, DNS (Domain Name System), e-post eller annan externt åtkomlig tjänst som angriparen försöker hindra de avsedda användarna från att nyttja. Det finns många olika typer av överbelastningsangrepp som riktas mot olika funktioner hos servern, så som nätverkskommunikation eller applikationer som körs på servern. I vissa fall används en kombination av olika tekniker för att göra det svårare att försvara sig.

Gemensamt för angreppen är att de uppehåller servern som ska tillhandahålla den drabbade tjänsten genom att skicka trafik som utarmar serverns resurser. Distribuerade överbelastningsangrepp (DDoS) använder ett större antal datorer, så som ett botnät, för att angripa den drabbade tjänsten.

I det enklaste fallet skickar angriparen en stor mängd trafik till den drabbade servern. Ofta utnyttjar angriparen funktioner i protokoll som servern använder för att kommunicera. Ett exempel på det är SYN-flood, en typ av angrepp som utnyttjar hur kommunikation upprättas när protokollet TCP används. TCP är ett vanligt förekommande protokoll som används för att upprätthålla en förbindelse mellan en klient och en server. Servern kan hantera ett begränsat antal förbindelser samtidigt och en angripare kan utnyttja detta genom att starta ett stort antal förbindelser och sedan sluta svara. På så sätt fylls den drabbade serverns kapacitet och servern kan inte upprätta nya förbindelser med legitima användare som vill nyttja serverns tjänster. Angreppet kan jämföras med när många användare försöker använda en tjänst samtidigt, till exempel köpa biljetter till en populär konsert, och på så sätt överbelastar servern så att fler inte kan ansluta.

Angriparen kan också utnyttja funktioner i applikationslagret som inkluderar bland annat DNS och HTTP som används för att överföra webbsidor. När en användare vill nå en webbsida skickar användarens klient en förfrågan till servern som svarar. En angripare kan använda detta för att skicka ett stort antal förfrågningar till servern och på så sätt uppehålla den med att svara på angriparens förfrågningar istället för sådana som kommer från legitima användare. Angriparen kan också välja att skicka förfrågningar som är

krävande för servern att svara på, till exempel sökningar som kräver att servern går igenom mycket information för att svara.

I vissa fall kan angriparen utnyttja en sårbarhet i en programvara på servern för att göra den otillgänglig. Det är däremot inte en förutsättning för att servern ska kunna utsättas för ett överbelastningsangrepp.

Konsekvenser

Överbelastningsangrepp har sällan bestående eller destruktiv påverkan på systemen som utsätts. Ett överbelastningsangrepp innebär inte heller att angriparen kommer in i systemet och kan ta del av eller ändra på information. Vid ett överbelastningsangrepp är det endast tillgängligheten på tjänsten som påverkas.

Överbelastningsangrepp kan däremot vara störande och skapa både verksamhetskonsekvenser och oro hos legitima användare som hindras från att använda drabbade tjänster under tiden angreppet pågår. Digitaliseringen har lett till att ett större beroende av digitala tjänster i vardagen, exempelvis finns idag en förväntan på tillgång till kortbetalningar och internetbank. Överbelastningsangrepp kan också få verksamhetskonsekvenser om tillhandahållande av den digitala tjänsten är en viktig del av företagets verksamhet. Om tjänsten som utsätts är tidskritisk kan alternativa lösningar behövas för att i möjligaste mån tillgodose behovet.

Flera skäl till överbelastningsangrepp

Det kan finnas flera olika skäl till att en angripare väljer att utföra ett överbelastningsangrepp. Det kan vara politiska syften, inklusive ”hacktivism”, för att utpressa den drabbade organisationen eller som en distraktion från andra samtida angrepp. Angriparen kan välja att rikta angreppet mot en publik tjänst som är synlig för många, så som en välbesökt webbsida, för att på så sätt få mer uppmärksamhet. Eftersom överbelastningsangrepp kan användas för att dra uppmärksamhet från andra aktiviteter är det klokt att vara vaksam på eventuella samtidiga angrepp.

Råd

Det är mycket svårt att helt förhindra överbelastningsangrepp, men rätt förberedelser och säkerhetsåtgärder kan mildra konsekvenserna av eventuella framtida angrepp. Genom ett systematiskt informationssäkerhetsarbete där skyddet kontinuerligt anpassas utifrån organisationens behov och risker är det lättare att hantera när en incident inträffar. Det bör finnas en tydlig plan för vem som ska göra vad när något händer.

Råd – teknisk hantering

Det finns inte någon enskild lösning som kan skydda mot alla typer av överbelastningsangrepp. En kombination av flera tillvägagångssätt behöver implementeras, samtidigt som det är viktigt att regelbundet granska och uppdatera dessa åtgärder för att följa angreppsmetodernas utveckling.

Det finns flera tillvägagångssätt som kan användas för att vara förberedd och mildra effekterna av ett överbelastningsangrepp:

- Identifiera vilka system och tjänster som är mest kritiska innan något inträffar. Att veta vilka system och tjänster som är mest kritiska underlättar prioriteringen under pågående angrepp.

- Säkerställ att verksamheten har rutiner för hur ni ska agera om ni drabbas av ett överbelastningsangrepp och genomför övningar.

- En god dialog med verksamhetens internetleverantör (ISP) är viktig, både i det förebyggande arbetet och vid hantering av ett pågående angrepp.

- Uppdatera regelbundet. Håll all programvara och säkerhetsåtgärder uppdaterade för att undvika att de har kända sårbarheter som kan utnyttjas vid ett överbelastningsangrepp eller andra typer av angrepp.

- Följ utvecklingen. Genom att följa hur tekniker, taktiker och metoder förändras kan organisationen bättre förutse hur skyddet kan behöva anpassas.

- Ha koll på helheten. Ett överbelastningsangrepp kan ibland vara ett sätt att styra verksamhetens uppmärksamhet och resurser bort från andra typer av angrepp. Det är därför viktigt att säkerställa övervakning av händelser i hela nätverksmiljön för att upptäcka och hantera sådana försök.

- Använd skyddstjänster mot överbelastningsangrepp. Många internetleverantörererbjuder skyddstjänster som kan absorbera och filtrera den inkommande trafiken. Alternativt kan ett Content Delivery Network (CDN) användas.

- Aktivera hastighetsbegränsning. Detta innebär att sätta en gräns för antalet förfrågningar som en användare kan göra till tjänsten inom en given tidsperiod. Att aktivera hastighetsbegränsning kan hjälpa till att förhindra att servern överväldigas av mängden trafik.

- Använd trafikfiltrering. Implementera filter för att blockera trafik från kända skadliga ip-adresser eller trafik som inte uppfyller vissa kriterier (bedöm om exempelvis blockering av trafik från utlandet kan vara ett alternativ). En web application firewall (WAF) kan nyttjas för att hantera överbelastningsangrepp som riktar in sig på applikationslagret. Tillgången till loggar är viktigt för att kunna avgöra vilken typ av angrepp eller vilka system som drabbats.

- Upprätta polisanmälan och informera gärna CERT-SE. Genom att kontakta berörda myndigheter finns möjlighet att få råd och stöd i hanteringen. Det skapar också bättre förutsättningar för att både förhindra framtida angrepp och att hjälpa er och andra verksamheter som drabbas.

Råd – kommunikation

Det är önskvärt att ha en plan för hur man ska kommunicera vid en händelse på plats innan något inträffar. Oavsett om det är ett överbelastningsangrepp eller en driftstörning som leder till att en tjänst blir otillgänglig kan det väcka frågor från användarna.

För att möta intressenternas oro och informationsbehov, och för att medarbetarna ska få arbetsro att lösa situationen, finns det några saker som är bra att tänka på i den tidiga kommunikationen.

- Kommunicera tidigt. Bekräfta om ni känner till störningen.

- Se över vilka alternativa kanaler ni har om era ordinarie kommunikationsvägar är otillgängliga.

- Det kan finnas olika målgrupper med olika informationsbehov, både internt och externt. Identifiera om någon målgrupp har ett specifikt informationsbehov och i så fall när de behöver informationen.

- Sträva efter transparens, om sådant man fått bekräftat, som inte stör verksamheten, saknar sekretess och som kan ge mottagaren möjlighet att värdera problemets konsekvenser korrekt. Kommunicera om möjligt vad ni gör för att hantera incidenten. Hitta en rimlig nivå när det gäller att ge detaljer.

- Förklara vad som har hänt. Det är inte säkert att mottagarna är medvetna om vad ett överbelastningsangrepp innebär.

- Undvik att svara ”inga kommentarer”. Är det något ni inte kan svara på går det ofta att förklara varför ni inte kan svara på det istället.

- Håll er till fakta, spekulera inte och förmedla bara det ni vet. Om ni behöver förmedla information som inte är bekräftad, var tydlig med att det är obekräftade uppgifter. Om man inte har mer information att dela vid tillfället kan man svara ”Vi vet inte ännu.”, ”Vidare utredning pågår.” eller ”Vi ber att få återkomma.”.