Myndigheten för
samhällsskydd
och beredskap

Att hantera överbelastningsattacker

Att hantera överbelastningsattacker

Myndigheten för samhällsskydd och beredskap (MSB)

Layout: Advant Produktionsbyrå AB
Tryck: DanagårdLiTHO

Publ.nr: MSB709 - juni 2014

Förord

Sveriges kommuner står för en stor del av de offentliga tjänster som är viktiga för att samhället ska fungera. En säker informationshantering borgar för fungerande tjänster som åtnjuter kommuninvånarnas förtroende. Informationssäkerhet är därför en central fråga för kommunerna.

Myndigheten för samhällsskydd och beredskap (MSB) har regeringens uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet. En viktig del i detta uppdrag är att ge kommunerna ett bra stöd i både strategiska informationssäkerhetsfrågor och då det gäller att hantera dagsaktuella utmaningar.

Detta informationsblad är framtaget med bakgrund av att flera kommuner under det senaste året drabbats av överbelastningsattacker. Överbelastningsattacker är i bästa fall ett oönskat störningsmoment för verksamheten men kan i allvarliga fall orsaka stora problem för organisationen och dessutom skada förtroendet mellan kommunen och dess invånare.

Syftet är att höja kunskapsnivån kring den här typen av risker och ge råd om förebyggande åtgärder samt om hur den här typen incidenter kan hanteras. Råden är givetvis applicerbara även i andra verksamheter än kommunala.

Richard Oehme
Verksamhetschef,
Samhällets informations- och cybersäkerhet

Att hantera överbelastningsattacker

Överbelastningsattacker – Denial of Service (DoS) eller Distributed Denial of Service (DDoS) – har blivit vanligare och drabbar allt fler kommuner. Attackerna är relativt enkla att utföra och bakomliggande krafter kan vara allt från ungdomar som utan att tänka på konsekvenserna testar sin tekniska förmåga, till kriminella grupper ofta med andra bakomliggande motiv som exempelvis ekonomiska eller politiska. Det är viktigt att påpeka att en överbelastningsattack utgör dataintrång enligt 4 kap 9c § i brottsbalken och kan ge böter eller fängelse upp till två år. MSB rekommenderar därför att kommuner som utsätts för attacker gör en polisanmälan.

Överbelastningsattacker kan se olika ut, men syftar i grunden till att förhindra normal åtkomst, men även i vissa fall för att mörklägga en annan pågående attack. I regel innebär attackerna att system eller nätverksresurser blir otillgängliga på grund av att trafik med stora datamängder riktas mot organisationens it-tjänster. Vanligen blir man varse om en attack genom att åtkomst till internet känns långsamt eller inte fungerar över huvud taget, alternativt att vissa system eller den externa webbplatsen inte går att nå från egna eller externa nät.

Det finns olika sätt att genomföra överbelastningsattacker. Ett sätt är att överösa målet med så mycket trafik som möjligt och lägga beslag på all tillgänglig bandbredd. Att urskilja vilken del av trafiken som är legitim och vilken del som ingår i attacken kan vara svårt och kräver särskild utrustning eller manuell analys.

När en överbelastningsattack drabbar en kommun blir det ofta både kostsamt och kräver stora arbetsinsatser av kommunens personal. Även om kommunen inte kan skydda sig helt mot attackerna kan förebyggande åtgärder minska konsekvenserna. Att vara förberedd gör det också lättare att hantera situationen på ett kontrollerat och lugnt sätt när incidenten väl inträffar. I förberedelserna ingår att bestämma vilka aktiviteter som ska genomföras när en incident inträffar. En annan viktig del i förberedelsearbetet är att organisationen klarlagt ansvarsförhållanden, vilka verksamheter och resurser som ska prio-

riteras samt hur kommunikation ska ske internt och med externa parter som till exempel kommunens internetleverantör (Internet Service Provider, ISP).

Alla som kan komma att involveras vid en incident ska känna till sin roll och vad som förväntas av dem. Alternativa kontaktvägar och kommunikationslösningar för prioriterade verksamheter ska också finnas beskrivna eftersom en överbelastningsattack i de flesta fall leder till att exempelvis e-post och webbplatser inte fungerar. Planeringen bör också övas, inte minst för att felaktig hantering i vissa fall kan förvärra skadan och försvåra utredningen. En viktig framgångsfaktor i hantering av överbelastningsattacker är tillgången till loggar samt tillgången till trafikdumpar. Utan loggar kan det vara svårt att veta vilken typ av attack det handlar om eller vilka system som varit inblandade. Därför bör behovet av loggar i olika system klargöras som en förberedande åtgärd.

En nödvändig förutsättning, både i det förebyggande arbetet och när kommunen hanterar attacken, är att se till att de åtgärder som vidtas inte strider mot de lagar och förordningar som gäller för kommunens olika verksamheter.

Att hantera en överbelastningsattack – checklista i 4 steg

1. Förebygga – Vad gör vi innan det händer?

Det förebyggande arbetet är nyckeln till att begränsa skadorna av en överbelastningsattack. Förutom att ha god kännedom om den egna kommunens verksamhet, förutsättningar och it-lösningar är det viktigt att ha upparbetade kontakter utanför den egna organisationen för att kunna få stöd och råd vid en incident. Det gäller till exempel kontakter med internetleverantörer, CERT:ar[1], polisen, leverantörer och programvarutillverkare. När det gäller de tekniska råden så måste varje organisation verifiera om de är tillämpbara i den egna miljön.

Lämpliga förberedelser:

- Gör en riskanalys för att identifiera vilka system som är mest verksamhetskritiska. Allt går inte att hantera och ibland krävs det prioriteringar. Vilka konsekvenser skulle en attack få, förutom att den externa webben inte går att nå? Finns det andra funktioner som påverkas som en följd av det?
- Formulera reservrutiner för att hantera verksamheten under en attack.
- Ge de som är ansvariga för verksamheten en relevant uppfattning om vilka risker som finns.
- Utse en grupp som ansvarar för hanteringen av en framtida incident.
- Förbered en alternativ webbplats – vilken kan aktiveras vid en attack – som innehåller ett minimum av bilder och dokument med minimal filstorlek (vilket bör verifieras periodiskt) för att kunna upprätthålla kommunikationen.

1. Computer emergency response teams. CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga it-incidenter. Verksamheten bedrivs vid Myndigheten för samhällsskydd och beredskap (MSB).

- Öva gruppen i scenariobaserad incidenthantering.
- Kontrollera vilka system som sparar loggar, exempelvis brandväggar, intrångsdetekteringssystem (IDS) eller syslog-servrar. Om möjligt är det bra att sätta upp en nätverkssniffer och spela in trafiken som flödar på det drabbade nätsegmentet. Det kan vara till stor hjälp vid en senare analys av attacken. Se till att det finns loggar tillgängliga från system som brandväggar, routrar, DNS (Domain Name System), webbservrar och proxyservrar.
- Kontakta internetleverantören eller tjänsteleverantören och ta reda på om de kan erbjuda skydd mot eller vara behjälpliga vid en attack.
- Kontrollera att externa leverantörer har en plan vid överbelastningsattacker som de kan redovisa. Inkludera incidenthantering av överbelastningsattacker i avtal med it-partners.
- Utred behovet av dels en reservwebbplats hos en annan leverantör, dels anslutning till fler än en internetoperatör.
- Etablera en baslinje över den normala systemlasten och ha god övervakning för att kunna upptäcka en attack i ett tidigt skede.
- Använd lastbalanserare för att sprida trafiken och lasten på flera bakomliggande servrar. Vissa lastbalanserare har även DDoS skydd.
- Sprid bilder och dokument på flera webbservrar till exempel på andra nätsegment.
- Använd ett enhetligt loggformat för att skapa en tydligare bild från flera loggkällor.

2. Identifiera – Vad har hänt?

Att snabbt skaffa sig en överblick när en överbelastningsattack sker är viktigt för att kunna vidta rätt åtgärder.

Lämpliga åtgärder:

- I första hand måste attacken identifieras och om möjligt loggar analyseras för att avgöra vilken typ av attack det handlar om och vad som attackeras. Det är viktigt att spara alla typer av loggar som kan användas vid analys av incidenten.
- Dokumentera allt som är relevant. Vem som gjort vad, vilka kontakter som tagits, vilka åtgärder som vidtagits samt tidpunkter för dessa. Detta underlättar sammanställningen av en rapport. Om kommunen har tillräcklig forensisk kompetens kan man påbörja en analys av incidenten. I många fall är det dock lämpligare att söka expertis utanför den egna organisationen. Viktigt är att undvika att bevismaterial förstörs.
- Vid ett resultat som pekar på att en incident pågår bör beslut tas om begränsande åtgärder eller fortsatt analys.
- När det är konstaterat att det rör sig om en överbelastningsattack gäller det att avbryta eller begränsa konsekvenserna av attacken.
- Kontakta organisationens internetleverantör som kan hjälpa till att blockera angripande IP-adresser. Se till att ha kontaktlistor uppdaterade och kontrollera regelbundet att uppgifterna stämmer.

Följande data är intressant att samla för vidare analys:

- Loggar (från internetleverantörer, brandväggar, routrar, IDS/IPS, webbservrar, e-post, DNS, nätverksanalysator med mera).
- Insamling av data från maskin/-er som är föremål för överbelastningsattacken.
- Vilken typ av attack det är.

Vid analyser av nätverksloggar kan exempelvis följande program användas:

- Wireshark (analyserar Pcap-data).
- Argus (analyserar NetFlow- och Pcap-data).
- Nfdump (analyserar NetFlow-data).

3. Begränsa – Vad? Hur? När? Var? Vem?

Första steget vid en attack efter att incidentorganisationen skaffat sig en överblick över vad som hänt är att försöka begränsa skadan. Om det är möjligt bör man isolera den aktuella miljön. Den viktigaste kontakten vid ett allvarligt fall är organisationens internetleverantör som är den första länken till internet och hos vilken ett visst skydd och motmedel kan etableras.

Det är sällan en organisation kan avhjälpa en överbelastningsattack helt på egen hand. För att avbryta eller begränsa en attack behövs det ofta hjälp av andra organisationer såsom internetleverantörer, tjänsteleverantörer, CERT:ar och polisen. Några frågor som bör ställas i ett tidigt skede vid en incident är:

- Är det konstaterat att det rör sig om en överbelastningsattack?
- Finns det loggar från nätverk eller drabbat system?
- Vad är det för typ av attack?
- Går det att blockera trafik i någon nätverksutrustning?
- Vad har organisationen gjort för att begränsa/avbryta attacken?
- Är någon internetleverantör eller tjänsteleverantör kontaktad?
- Är någon CERT kontaktad?
- Sköts systemdriften av en utomstående leverantör?

För att få en god helhetsbild av situationen är det viktigt att så tidigt som möjligt sätta upp en nätverkssniffer och spela in trafiken för att få en uppfattning om vilken typ av attack som drabbat organisationen. Alla typer av loggar från nätverksutrustning och andra system är också av största vikt att samla in för att få en bild av incidenten.

För att begränsa eller avbryta attacken:

- Kontakta internetleverantör eller tjänsteleverantör. De kan erbjuda olika lösningar för skydd mot överbelastningsattacker.
- Konfigurera filter (ACL:er) i nätverksutrustningar. Filter kan ibland tas fram med bakgrund av analysen som gjordes i identifieringsfasen.

4. Återställning och erfarenhetsinsamling

För de it-resurser som drabbats av attacken ska ordinarie rutiner för återställning användas. Återhämtade system bör granskas ur säkerhetssynpunkt och testas innan de tas i skarp drift igen.

Erfarenheterna från incidenten bör också användas för att förebygga och minimera verkan av framtida attacker. En incidentrapport fyller syftet att samla och systematisera erfarenheterna.

En metod som brukar fungera bra vid större incidenter är att samla in synpunkter och erfarenheter från de som deltagit i incidenthanteringen, sammanställa dessa och sedan presentera dem vid ett uppföljningsmöte där samtliga deltagare har möjlighet att diskutera rapporten. Rör det sig om mindre incidenter, med ett fåtal inblandade, kan synpunkter och erfarenheter samlas in direkt på uppföljningsmötet.

Det är viktigt att inte utse någon syndabock. Se till att kommunicera ut detta till mötesdeltagarna. Syftet med uppföljningsmötet är att öka organisationens förmåga att bemöta nya incidenter.

Kommunicera vad som händer

Dokumenterade processer och övade rutiner är bra för hantering och återhämtning, men ni behöver också kommunicera med journalister, invånare och övriga intressenter. I en situation där en attack leder till att samtliga eller vissa av kommunens tjänster är otillgängliga är det viktigt att kommunicera med omvärlden. Har ni en kommunikationsplan och vet ni vad ni ska säga?

Informationen bör innehålla:

- Vad som har hänt och vad som drabbats av konsekvenser.
- Hur lång tid man räknar med att det tar att lösa.
- Vad man som kommuninvånare kan göra om det finns något alternativ.
- När man kan förvänta sig mer information och var den kan hittas.

Den interna kommunikationen är också viktig. Telefonisterna i växeln kan behöva veta vad de ska säga när klagomålen kommer.

Mer stöd och kontakt med MSB

En mer utförlig beskrivning av incidenthanteringsprocessen går att ta del av på www.cert.se.

Kontakt till CERT-SE:
Telefon: 08-678 57 99
E-post: cert@cert.se

På webbplatsen www.informationssäkerhet.se finns information och stödmaterial samlat rörande det systematiska informationssäkerhetsarbetet.

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB709 - juni 2014