Information kring N.nu:s driftavbrott 27-28 augusti 2014

Sedan N.nu skapades i slutet av 2009 har det aldrig haft ett likande stort driftavbrott. N.nu har regelbundet haft 99,9% i upptid sedan 2009 vilket har varit bättre än många andra leverantörer. Prestanda och snabb laddning har alltid varit i topp. Detta driftavbrott är något alldeles extraordinärt.

Summering

N.nu blev offer för en stor överbelastningsattack och hela N.nu gick ner ca 03:00 på natten den 28 augusti. Vi har nu satt in rutiner för attt förhindra detta igen. Hemsidorna på N.nu kom upp 14:30 svensk tid och prestanan återgick till det normala kl 16:00 svensk tid.
Ingen information har förlorats eller stulits.

Djupare teknisk förklaring

N.nu hyr servrar från företaget Glesys i Falkenberg. Under den 27 augusti hade Glesys nätverksproblem som varade mellan 06:15 till 08:17 svensk tid.

Senare under dagen, ca 20:00 svensk tid, märker vi på TodaysWeb som driver N.nu att sidor på N.nu har upp till 5-10 sekunders fördröjning. Vi undersöker och kommer fram till att det inte handlar om varken PHP eller MySQL. Vår misstanke är att Glesys fortfarande har nätverksproblem och vi skickar ett epost till dem 22:50 svensk tid och inom 20 minuter har vi ett svar från dem att de inte har problem med nätverket men misstänker att "webbservern slagit i taket på max antal samtidiga besökare".

Vi kontrollerar med Redistas som mäter global statistik för hela N.nu att det finns en spammig engelsk hemsida med över 60 000 besökare per dag, vi stänger av denna hemsida på DNS-nivå. Trafiken ligger annars på en normal nivå. Sedan går vi hem från kontoret (18:00 tid i Bolivia, 24:00 svensk tid).

Runt ca 03:00 svensk tid kraschar MySQL och alla hemsidor på N.nu går ner.

Jag blir meddelad via telefon av min kollega när jag kör bil på väg in till kontoret och jag kommer in vid ca 08:30 bolivia tid (14:30 svensk tid). Vi startar direkt om MySQL och hemsidorna kommer upp igen, dock med samma fördröjning som gårdagen. Vi uppdaterar mjukvara på servern men det löser inte problemet. Vi upptäcker när vi analyserar att servern hammras av bottar - tusentals per sekund - och enligt statistik från Glesys hade servern under den 28 augusti haft upp till 43

Gbit/s i bandbredd (över 50 000 gånger mer trafik än normalt). Eftersom det var bottar så hade dessa inte registrerats av Redistas.

Felet berodde alltså på överbelastning av Apache precis som Glesys sa från början. Vi stängde genast av all spammig trafik på DNS-nivå och höjde konfigurationsvärdena för Apache. Detta löste helt problemet med fördröjningen. Allt var klart innan kl 16:00 svensk tid.

För att det inte ska hända igen har vi

- Uppgraderat mjukvaran på servern
- Ökat gränsen för maxbelastningen
- Förbättrat våra larm så att nästa incident kan lösas även under nattetid
- Förbättrat våra rutiner för att upptäcka liknande incidenter i förväg.

Slutord

Vi beklagar verkligen det som inträfffade och förstår att många har drabbats av detta. Det är synd att de finns de som skapar överbelastningsattacker och fördärvar för andra.

Jag tackar ödmjukast för fortsatt förtroende.

Mvh

Jim Westergren
VD, TodaysWeb Ltda.