

Angrep truer krumtappene på internett

Skrevet av **Dag-Rune Z. Vollen** | Publisert 02.10.2006 kl 06:57 | [PC World Norge](#)

De viktigste serverne som styrer internett i siste instans trues av angrep som i verste fall kan ta ut hele nettet. Med på lasset følger en god del bedriftsnettverk.

Algarve (PC World Norge): Et angrep med ondsinnet kode i mars år, tok ut tre av de elleve tjenermaskinene som styrer internett i siste instans. Dette var bare et alfa-angrep, altså en test av hva som var mulig.

I følge sikkerhetsfirmaet Infoblox, som har undersøkt saken, skyldes dette feil oppsett av tjenere. De har registrert tre mindre angrep som bare har rammet noen titusen brukere i månedene etterpå. Tallene ble presentert av Richard Kagan, Vice President of Marketing i Infoblox.

Feilen er omfattende. Under de elleve toppnivåtjenerne er det rundt ni millioner tjenere. Det antas at 3,8 millioner tjenere inneholder feil i oppsettet som kan brukes til å angripe og ta ut toppnivåtjenere. Disse tjenerne er for en stor del Unix- og Linux-baserte tjenermaskiner, Windows er svært lite tilstede i denne tjenermaskintypen.

Det er tjenestemaskiner som omsetter internett-navn til maskin-nummer og som dirigerer mye av trafikken på Internett – DNS-tjenerne (Domain Name System). Hver eneste tilkoblede enhet på internett har sitt eget nummer, kalt IP-nummer (Internet Protocol). Siden vi stort sett ikke gidder å lære oss tallrekker, men heller vil ha forståelige navn, lar vi disse navnene representere et nummer på internett.

Når du legger inn www.idg.no i web-leseren din, er det en DNS-tjener hos deg eller internettleverandøren din som omsetter dette til et IP-nummer, slår opp hvor og hvordan denne tjeneren er og sender beskjeden din om å få IT-nyheter og IT-fakta levert til pcen din.

DNS-ene står i et hierarki med nasjonale domener (som .no og .se) og internasjonale domener (som .com og .org). I siste instans er det de elleve servere som kontrollerer trafikken og domenesystemet.

Nye trafik øker sårbarheten

I grunndesign er DNS-systemet en genial måte å gjøre internett stabilt. Om noen DNS-tjenere feiler, er systemet satt opp slik at sekundære og tertiære tjenere tar over og dirigerer trafikk, evt. over alternative veier. Og tidligere var dette en enkel og grei tjeneste som ofte ble utført av enkle tjenermaskiner, gjerne gamle og utragerte tjenermaskiner.

Problemet som nå har oppstått, er at nye tjenester krever mer av DNS-tjenerne enn før – for eksempel IP-telefoni eller anti-spam-programmer sender enorme mengder trafikk til «sin» DNS-tjener. Og kapasiteten for å sende trafikk øker med bruken.

DNS-tjenere som er oppsatt feil, vil imidlertid på ulike måter feile og/eller videresende meldinger om den overbelastes. Om dette gjøres i et koordinert angrep, vil man få en «tsunami» av meldinger som tar ut DNS etter DNS, og til slutt så vil denne overfloden nå toppnivå-tjenerne. Disse har tilstrekkelig kapasitet til daglig trafikk og trafikktopper, men det finnes en grense. Og uten DNS, intet internett.

Konsekvensene av at DNS-tjenere slutter å virke, er ikke bare at all internett-basert trafikk bremses og stopper opp. Mange interne nettverk er avhengig av eksterne DNSer for å fungere, f.eks. vil katalogtjenesten Active Directory fra Microsoft også kunne feile. Og de som har tatt i bruk interne IP-telefoniløsninger vil også miste denne telefonien. Antallet DNS-tjenere har økt med 20 prosent på et år, men det er ikke de nyeste DNS-tjenere som årsaken til problemet.

Løsningen i følge Infoblox er enkel, det kan gjøres helt enkle grep i standardoppsettet for DNS som reduserer eller fjerner sårbarheten. I visse tilfeller vil det være nødvendig å oppgradere både programvare og maskinvare slik at de tåler trafikkpresset fra internettbruken i dag.

Mer informasjon hos [Infoblox](#).