



Under fredag 21:a oktober drabbades flera stora Internet-tjänster i USA av problem och även Spotify och svenska regeringens sida drabbades och kunde inte nås under ett antal timmar. Men vad hände egentligen?

Enligt uppgifter i media var det en överbelastningsattack mot företaget Dyn som hanterar DNS (översättning av domännamn till IP-nummer) för flera stora kunder som orsakade problemen. Attacken bestod i ett nätverk med tusentals eller miljontals enheter (datorer, routrar, kameror m.m.) som kapats och samtidigt styrdes att skicka en mängd frågor till Dyn:s servrar. När trafiken uppgår till hundratals gigabit blir både anslutningar och servrar överlastade oavsett vilken kapacitet dessa har. Och förfrågningar för vanlig surf med mer kommer inte fram. Så även om Din mobil och Spotifys servrar fungerade fint så fanns ingen som kunde ange "vägen" mellan enheterna när Dyn var överbelastade.

För vår egen del "var det nära" att vi drabbades. Fram till 2014 använde vi DNS-hantering genom Nettica, en smidig tjänst med ett webbaserat gränssnitt där domännamn kunde hanteras och deras servrar världen över hanterade översättning av namn till IP snabbt och säkert så webb och epost nådde våra servrar. Men så köpte just Dyn upp Nettica och förändrade villkoren drastiskt. Istället för ett teknikskifte till högre pris valde vi att dra igång egna DNS-servrar och lämnade Dyn.

Denna gång innebar det att vi och våra kunder inte drogs med i Internet-problemen i fredags, men naturligtvis skulle en överbelastningsattack riktad mot oss kunna orsaka skada. Faktum är att när hackarna - eller som man misstänker i fredags - någon nationell säkerhetstjänst - verkligen vill ta ner en del av Internet, då kan de göra det. Risken att vi skall drabbas av denna typ av medvetet riktade attacker torde dock vara mindre, men då script och bot:ar löpande söker efter svagheter att utnyttja på nätet - på alla IP-nummer - gäller det att hålla våra system uppdaterade, kontrollera loggfiler och åtgärda sånt som kan åtgärdas i tid.

Läser man mera om det inträffade framgår att under de senaste månaderna har DNS-system och andra tjänster som utgör själva grunden för Internet utsatts för tester "från den mörka sidan" där de verkar försökt avgöra vilken kapacitet dessa delsystem klarar. Kanske eller snarare troligen är det test och förberedelser för antingen ett riktat eller ett fullskaligt IT-krig där man som en del i en konflikt vill kunna slå ut kommunikation och nyhetsförmedling helt. Störningen i fredags var därför *tyvärr inte den sista*.