

Varför DNSSEC?

Domännamnssystemet DNS, kan förenklat beskrivas som telefonkatalogen på Internet, där man genom att skriva ett namn som exempelvis www.2thepoint.se gör att man hittar fram till rätt dator på Internet, istället för att behöva skriva in adressatens IP-adress (man gör en nummeruppslagning). När DNS skapades var tanken att göra den centrala administrationen av Internet enkel och underlätta för att smidigt kunna ansluta nya datorer till "nätet". Man lade alltså ingen större vikt på säkerheten. Säkerhetsbristerna i DNS har öppnat upp för olika typer av hot och attacker där bl a svaren på DNS-uppslagningar kan förfalskas. Därför kan Internetanvändare manipuleras att tro att man t ex har kommit till sin bank och luras att lämna ut känslig information som lösenord, personnummer, kontonummer etc.

Även om man aktivt arbetar med säkerhetsfrågorna och att täppa till säkerhetshålen med hjälp av olika verktyg som utnyttjas vid DNS-uppslagningar, ligger själva grundproblematiken i hur DNS fungerar idag. Därför har DNSSEC, DNS Security Extensions, "uppfunnits". Med DNSSEC säkrar man upp domännamnssystemet genom att svaren på DNS-uppslagningar signeras med hjälp av kryptonycklar. Då säkerställs att svaren verkligen kommer från rätt källa och inte har ändrats under själva dataöverföringen. Det innebär att den som söker information på en webbplats med DNSSEC kan vara säker på att det är den äkta webbplatsen man besöker. Om ett DNS-svar ändras från sitt ursprungliga äkta svar och en hackare försöker framställa det manipulerade svaret som äkta, upptäcker den DNSSEC-säkrade klienten detta. DNSSEC är även ett bra komplement till andra viktiga säkerhetsfunktioner som ssl-certifikat och ddos mitigation.

DNSSEC är idag det enda heltäckande skyddet för att upptäcka förfalskade DNS-svar och minskar risken att bli utsatt för bedrägerier vid e-handel, bankaffärer, myndighets- och samhällskontakter, e-post osv, eftersom det går att fastställa att man verkligen kommunicerar med rätt adressat.