"Decentralisering ger skydd för information"

Ola Bini

Krönika **"Vi har ett ansvar att inte samla information i stora högar, risken för att informationen används på fel sätt är för stor" skriver Ola Bini.**

I min förra krönika skrev jag om hur man skapar decentraliserade system inuti en organisation med hjälp av mikrotjänster. Den här typen av arkitektur har många fördelar, men den skyddar inte mot vissa typer av attacker. Efter det senaste årets avslöjanden är det mer tydligt än någonsin att vi har ett ansvar att bygga system som inte gör det lätt att komma åt stora mängder information om många människor samtidigt.

Så hur kan man göra det? Decentralisering är en stor del av svaret, men inte den typ av decentralisering jag pratade om förra gången. I stället måste man anamma lösningar i vilka informationen inte finns på ett ställe, inuti samma organisation. Det kan göras med olika typer av peer-to-peer-lösningar. En viktig aspekt är att större delen av funktionaliteten i ett system måste finnas på många punkter i systemet. Det innebär också att man måste designa protokoll för kommunikation mellan de olika punkterna i nätverket.

Läs även: "Decentralisera systemen och bli en vinnare"

Ett stort problem i den här typen lösningar är hur man ska gå tillväga för att hitta varandra. En grundsten i peer-to-peer-arkitekturer är att olika noder kommer behöva kommunicera med varandra. Men för att göra det måste de först kunna hitta varandra. Det finns tre olika varianter på hur man kan göra det. Den första och enklaste metoden går ut på att ha centrala servrar som håller koll på var noderna finns någonstans. Exempel på det är Tors katalogservrar och Bittorrents spårningsservrar. Problemet med den här varianten är att säkerheten för systemet nu bygger på att de centrala servrarna är säkra. Det går också att förstöra systemet genom att blockera tillgång till de centrala servrarna.

Den andra varianten använder en algoritm för att hitta noder baserat på identiteter för noderna. Distributed Hash Tables är en av de vanligaste algoritmerna för det. Den tredje varianten kallas ibland "vän-till-en-vän". Tanken är att varje nod har några vännoder. När man vill hitta en nod frågar man sina vänner. Om den andra noden inte finns i ens nätverk av vänner kan man inte kommunicera med den.

Den här typ av arkitektur kan vara komplicerad att få till, men långsiktigt finns det enorma fördelar för oss alla att gå i den här riktningen. Om Facebook inte samlade all information på en och samma plats skulle det inte vara möjligt att väldigt billigt få övervakningsinformation om över en miljard människor på en och samma plats.

Vi har ett ansvar att inte samla information i stora högar. Risken för att informationen används på fel sätt är för stor.