Till Informationsanvarig hos:

Regeringskansliet

Kustbevakningen

Myndlingen för sammhällskydd och beredskap

Ärende:
Begäran om uppgifter runt upphandling av DNS-system i enlighet med offentlighetsprincipen.

DNS-är en vital komponent som möjliggör kommunikation över Internet. För att nå en myndighets webbsida eller för att kunna skicka epost till en myndighet måste först ett uppslag i DNS-systemet göras. I DNS-systemet översätts domännamnet exempel.se till en IP-address som behövs av datorn för att kommunicera.

Det visar sig att svenska regeringen och samhällsviktiga departement har byggt upp sin DNS lösning på ett sårbart sätt. Vi kan konstatera genom att skicka testtrafik att Regeringskansliet någon gång i början av maj i år flyttade DNS driften av domänen regeringen.se till en extern part. Samma flytt har tidigare (år 2010) även ha skett hos myndigheten för samhällskydd och beredskap samt hos Kustbevakningen (någon gång mellan febuari 2011 och Mars 2012). Båda dessa myndigheter lyder under Försvarsdepartementet. De domäner som har berörts hos MSB är msb.se, krisberedskap.se och säkerhetspolitik.se. Kustbevakningens huvuddomän kustbevakningen.se är berörd.

Den bakomliggande DNS tjänsten som Regeringskansliet och Försvarsdepartementet har valt är leverad av DynDNS via den svenska återförsäljaren Excedo. Utan tillgång till DNS servrarna kan alltså inte Internet kommunikation med myndigheterna ske. När vi gör testförfrågningar till DNS-systemet kan vi konstatera att Excedo verkar sakna egen DNS infrastruktur utan förlitar sig till fullo på DynDNS infrastruktur. DynDNS saknar DNS infrastruktur i Sverige (se karta http://dyn.com/dns/network-map/). De närmaste servrarna är belägna i Amsterdam i Nederländerna samt Frankfurt i Tyskland.

Det är chockerade att Regeringskansliet och Försvarsdepartementet har valt en sådan lösning. Man undrar hur tillgängligheten till dessa system garanteras i händelse av en kris såsom en naturkatastrof eller ett krig?

DynDNS är ett amerikansk företag. DynDNS med huvudkontor i Manchester, New Hampshire lyder således under Amerikanska lagar. Tillgängligheten på Regeringskansliet och Försvarsdepartementets externt nåbara IT system är alltså beroende av främmande makt. Detta har givetvis implikationer under en eventuell konflikt, men har även konsekvenser under fredstid. Tex. så har det under 2012 pågått en debatt i USA om censurering av webbsidor skall tillåtas utan rättegång för att mer effektivt kunna släcka ner sidor som sprider

upphovsrättsskyddat material. Skulle ett sådan lagförslag klubbas igenom i USA samtidigt som Piratpartiet har framgångar i Sverige så skulle det eventuellt kunna uppstå en juridiskt intressant situation.

Samtliga ovan nämnda domännamn är signerade med säker DNS, eller så kallad DNSSEC. Detta kräver att en privat nyckel lagras hos DNS leverantören. Om någon får tillgång till nyckelarna till dessa domäner så kan förövaren förfalska signerad e-post, certifikat och annat känsligt material. Det är med andra ord väldigt viktigt att dessa nycklar säkras på ett bra sätt. Man undrar om dessa nycklar är förvarade i Sverige, eller om DynDNS har skapat och förvarar dessa nycklar i utlandet?

Det är mycket graverande att viktiga domäner som Regeringen.se och Krisinformation.se har dessa problem. Dessa domäner har väldigt höga krav på tillgänglighet så att medborgare kan kommunicera med myndigheterna även under kriser. Man kan tex. läsa på Krisberedskap.se att: "*UNDER en kris försöker vi ge en översiktlig bild av vad som har hänt. Vi länkar till krisinformation hos myndigheter, kommuner och andra aktörer. Vi informerar också om telefonnummer som allmänheten kan ringa för att få veta mer.*".

Det är svårt att förstå hur detta ska gå till under en kris om deras DNS system inte är nåbart vilket får till följden att deras webbsida inte är nåbar.

Vi skulle vilja ta del av den kravspecification som användes när den nya DNS tjänsten upphandlades hos Regeringskansliet, Kustbevakningen och Myndigheten för sammhällskydd och beredskap. Vi skulle även vilja att ansvarig tjänsteman förklarar hur tillgängligheten i dessa system säkerställs under en kris. Vänligen skicka information och samtliga allmänna handlingar till nedanstående epost addresser, alternativt använd nedanstående address.

Tack på förhand,

Stephan Lagerholm
Stephan.lagerholm@secure64.com

Torbjörn Eklöv
torbjorn.eklov@interlan.se