SÄRTRYCK UR *STRATEGISK UTBLICK 8*

Så kan vi skydda Sveriges säkerhetskänsliga it-tjänster

Anders Elfving och Anton Dahlmark, Fortifikationsverket

En väsentlig del av uppbyggnaden av den svenska totalförsvarsförmågan handlar om skydd av samhällsviktig verksamhet. Det finns därför anledning att se över myndigheternas samlade behov av fysiskt skyddade datacenter för säkerhetskänslig it-verksamhet. Höga krav på exempelvis fysiskt skydd mot vapenverkan och tillgänglighet för it-miljöns försörjningssystem leder dock till ökade kostnader och längre produktionstid. Ombyggnation av befintliga anläggningar måste även vägas mot att bygga nytt. Det förändrade omvärldsläget och insikten kring sårbarheten hos vårt digitaliserade samhälle gör att en nationell satsning inom området är en för samhället och totalförsvaret betydande men nödvändig investering.

Digitaliseringens framfart för med sig sårbarheter

Det har knappast undgått någon hur digitaliseringen av vår vardag har förenklat våra liv och förändrat vårt beteende. De stora mängderna data som genereras processas ofta i molntjänster och lagras över tid i serverhallar. Man tar i regel för givet att dessa tjänster fungerar utan avbrott dygnet runt. Debatten om vår ökade sårbarhet genom den digitala revolutionen pågår med ökad insikt om hur stora konsekvenserna blir vid eventuella störningar, som attacker eller elavbrott.

Medan it-säkerhet numera står högt på agendan hos svenska myndigheter har även det fysiska skyddet av statliga it-tjänster pekats ut som ett mycket viktigt område att se över för att stärka totalförsvaret. 2017 fick Post- och telestyrelsen i uppdrag av regeringen att utarbeta ett förslag till en nationell förvaltningsmodell för skyddade it-utrymmen, vilket i branschen kallas för datacenter. Det är långt ifrån all data som kräver ett förstärkt fysiskt skydd, men delar av den är säkerhetskänslig och behöver skyddas mot både intrång och militära angrepp.

Datacenter i befintliga eller nya anläggningar?

Ett skyddat it-utrymme kan ligga i en skyddad anläggning i berg eller i en säker byggnad ovan mark. En anläggning i berg har de fysiska barriärer som skyddar mot effekterna av vapen men även skydd av datacentrets funktioner och försörjningssystem, ett så kallat fortifikatoriskt skydd. En säker byggnad ovan mark utformas med säkerhetshöjande åtgärder för att förhindra eller försvåra skadeverkan på dess funktioner men har inte samma fortifikatoriska skydd som en berganläggning. Den period vi har bakom oss med ett stabilt omvärldsläge och besparingar inom försvaret har lett till att skyddade objekt som till exempel bergrum har frigjorts. Därför har myndigheter på senare år ställt frågan om dessa skulle kunna användas för skyddade it-utrymmen eller om det är mer lämpligt att bygga nya anläggningar.

En vanlig uppfattning är att etablering av skyddade it-utrymmen i bergrum är enkla att genomföra. Argumenten brukar handla om:

- att det finns ett stort antal tomma bergrum som efter smärre ombyggnader och till låg kostnad borde kunna användas som it-utrymmen
- att bergrum per automatik innebär ett skydd mot alla förekommande effekter och nivåer av vapenverkan
- att ett bergrum, med bibehållet fortifikatoriskt skydd, enkelt kan anpassas för it-utrymmen på tio megawatt (MW) effekt eller mer, vilket motsvarar elproduktionen från ungefär sex vindkraftverk eller effektåtgången för över 4000 villor

FOI Memo 6751
Projekt Nr I181103
Godkänd av Mike Winnerstig

Augusti 2019

- att bergrum finns inom ett avstånd av 15 till 20 km från nuvarande verksamhets geografiska placering
- att etablering i bergrum går snabbt att genomföra.

Förutom ovan nämnda förväntningar finns också ofta en önskan om höga tillgänglighetsnivåer, det vill säga hur stor del av tiden som något är i drift och levererar avsedd förmåga. Redundanta system ger generellt högre tillgänglighet, men det medför ofta högre kostnader än förväntat.

Verkligheten är emellertid en annan. Det finns få tillgängliga bergrum som är lämpliga för it-utrymmen och de som finns ligger sällan nära städer. Ofta krävs ett stort saneringsbehov och omfattande investeringar innan anläggningen kan tas i bruk. Det är en stor utmaning att med bibehållet fortifikatoriskt skydd skapa en lösning för den nödvändiga kylningen av it-miljön. Trots att berget till stor del är urgrävt, tar anpassningsarbeten längre tid än man räknar med. Anskaffningstiden vid ombyggnad av en tomställd berganläggning är dock väsentligt kortare än vid nyproduktion.

Fördelen med att bygga nytt är att anpassning till it-utrymmen görs redan från början. När det gäller samordning av fysiskt skydd, byggkostnader och kostnader för driftverksamhet finns ekonomiska fördelar med att samlokalisera så att flera samhällsaktörer delar på samma fysiskt skyddade anläggning. Det finns dock även negativa konsekvenser vid samlokalisering. Om det innebär att endast ett fåtal anläggningar etableras riskerar de att ur en angripares perspektiv ses som mer högvärdiga mål jämfört med ett stort antal utspridda angreppsmål. Konsekvenserna vid ett angrepp mot ett högvärdigt mål riskerar därför att blir större.

Strömförsörjning utan avbrott

En annan aspekt att ta hänsyn till är behovet av robust energiförsörjning. Lagring och hantering av data av väsentlig samhällsbetydelse måste ske utan avbrott i strömförsörjningen. Samtidigt är it-tjänster energiintensiva och behöver en effektiv infrastruktur för kylning. Utan kylning överhettas it-utrustning, ofta så snabbt som inom loppet av minuter, med följden att anläggningens funktioner slås ut. De stora mängderna energi som behöver forslas bort från ett it-utrymme gör att vattenkylning anses vara klart mest effektivt jämfört med luftkylning eller bergkyla. När det gäller datacenter som kräver hög energiförbrukning och är inrymda i bergrum är fysisk placering intill stora vattenreservoarer eller vattendrag därför lämpligt, vilket naturligtvis begränsar antalet möjliga platser för etablering.

Just nu ställer samhället om till fossilfri energianvändning. Samtidigt slår Svenska kraftnät fast att behovet av reservkraft ökar. Driftsäker och tillförlitlig reservkraft är helt nödvändig inom en rad samhällssektorer som är viktiga för att upprätthålla ett fungerande totalförsvar, till exempel landsting, kommuner och frivilligorganisationer. Nuvarande reservkraftförsörjning består i de flesta fall av dieselelverk som har flera begränsningar som (i) stor miljöpåverkan, (ii) svårigheter med distributionen av bränsle i en krissituation (iii) importberoende från andra länder, (iv) hög värmesignatur vid förbränning, vilket gör en anläggning lättare att upptäcka, och (v) buller.
Sammantaget finns det därför behov av att testa nya alternativa energilösningar för driftsäker reservkraft i samhällsviktiga objekt, som exempelvis framtida datacenter. Batteri- och bränslecellsteknologi är exempel på områden där det just nu sker stora framsteg som är intressanta ur ett robust samhällsperspektiv. För skyddade datacenter är det särskilt viktigt att framtidens reservkraft inte bara är robust – den ska även vara lätt att underhålla och billig i drift. Dessutom måste intagen för el- och kylförsörjning skyddas mot tryckvågen från bombangrepp, elmiljöhot (exempelvis elektromagnetisk puls och mikrovågor, *high power microwaves*), och andra hot vilket kan vara en utmaning då de ofta måste dimensioneras med en stor area.

Krav på tillgänglighet och säkerhet varierar

Samhällets grundläggande funktionalitet är sällan beroende av endast en aktörs förmåga att leverera en tjänst under svåra förhållanden. Elkraft, data- och telekommunikation, finansiella tjänster, transporter, drivmedelsdistribution, livsmedelsförsörjning – allt hänger ihop i olika och invecklade beroenden. Om en samhällsaktörs funktion sviktar, som när en it-tjänst slås ut, kan det få konsekvenser för alla som i sin tur är beroende av att tjänsten fungerar. Samhället skulle vinna på att ha en helhetssyn på enskilda delfunktioners skyddsvärde, valda skyddsnivåer och tillgänglighet.

Högkravställning på skydds- och tillgänglighetsnivåer är starkt kostnadsdrivande. Kostnaden för ett it-utrymme ökar snabbt med graden av tillgänglighet och kan därför leda till en mycket kostsam etablering. En rimlig utgångspunkt är att huvuddelen av den samhällsviktiga it-verksamheten har varierande krav på tillgänglighet och säkerhet och att de kan variera i fredstid såväl i kris som under krig. En djupare analys är förstås nödvändig, men ett troligt scenario är att

antalet it-tjänster med höga tillgänglighetskrav är stort i fredstid och betydligt mindre under krigstid då endast de mest väsentliga funktionerna förväntas vara i drift. I fredstid är antalet it-tjänster som kräver en säker byggnad ovan jord sannolikt betydligt större än de it-tjänster som kräver en skyddad berganläggning. En förenklad beskrivning av förhållandet kan se ut som i Tabell 1.

Tabell 1. Antaget behov av antal och krav på olika it-tjänster under olika skeden.

	Fred	Kris	Krig
Hög tillgänglighet	Högre behov	Medelstort behov	Lägre behov
Säker byggnad	Högre behov	Högre behov	Medelstort behov
Skyddad anläggning	Lägre behov	Lägre behov	Lägre behov

Enligt krisberedskapens ansvarsprincip har den enskilda aktören, såsom en myndighet, samma ansvar i krig som i fred och tar själv beslut om sitt skydds- och tillgänglighetsbehov. Frågor om vilka aktörers verksamhet som ska utgöra skyddsobjekt alternativt riksintressen, vilka fysiska hotnivåer som ska mötas och vilka tillgänglighetsnivåer varje enskild delfunktion måste uppnå borde vinna på att hanteras på en övergripande samhällsnivå. Post- och telestyrelsens förslag till en aktörsmodell avseende skyddade it-utrymmen kan vara en bra utgångpunkt. Den föreslår följande aktörer:

- **Prioriteringsfunktion**. En funktion inom staten med uppdrag att ur ett övergripande samhällsperspektiv klassificera och prioritera behov av skydd för säkerhetskänsliga verksamheters it-tjänster.
- **Utrymmesförvaltare**. En organisation som utifrån den föreslagna förvaltningsmodellen förvaltar beståndet av skyddade it-utrymmen.
- **Anläggningsägare**. En anläggningsägande och förvaltande organisation som äger och förvaltar de anläggningar där skyddade it-utrymmen placeras.
- **Nyttjare**. Aktörer som har säkerhetskänslig verksamhet och som har behov av att placera hela eller delar av sina it-miljöer i skyddade it-utrymmen.

Hur kan ett statligt datacenterkoncept se ut?

En skyddad anläggning med hög nyttoeffekt, det vill säga effekt som kommer till nytta för anläggningens funktioner, är dyr och tar lång tid att bygga. Skyddade anläggningar med hög fortifikatorisk kapacitet är dock nödvändiga ur ett totalförsvarsperspektiv. Ett möjligt sätt att balansera förhållandet mellan nytta, risk och kostnad för en skyddad anläggning vore att sänka kraven på hög nyttoeffekt. Detta skulle resultera i ett mindre komplext utförande till en lägre kostnad. Det skulle även skynda på anskaffningsprocessen. Det kan dessutom vara enklare att närma sig miljömålen samt få bättre avsättning för överskottsvärmen.

En säker byggnad bör i de flesta avseenden uppföras så likt moderna kommersiella datacenter som möjligt. För att vinna synergier i takt med en framtida utbyggnad av ett nationellt datacenterkoncept bör principer och erfarenheter återvinnas och utvecklas, men till stor del kan de repeteras till utformning och kapacitet på nya platser. En avgörande skillnad från de kommersiella referensobjekten är dock att fysiska säkerhetsaspekter kommer kosta mer eftersom det är angeläget att skydda it-utrymmet mot de hotscenarier som finns under fredstid. Det kan till exempel handla om inbrott, sabotage, angrepp med skjutvapen, personburna bomber, fordonsburna bomber och forcerande fordon.

Det är sannolikt att det stora flertalet it-tjänster som kan komma i fråga för ett statligt datacenterkoncept har höga krav på fysisk säkerhet, men inte på nivån som en skyddad berganläggning erbjuder. En säker byggnad som planeras, placeras och utformas för ändamålet kan å ena sidan troligen erbjuda en fullt tillfredsställande fysisk säkerhetsnivå för de allra flesta samhällsviktiga it-tjänster. Å andra sidan finns det en hel del it-tjänster som även måste klara krigets krav genom de fortifikatoriska förutsättningar en skyddad anläggning erbjuder.

Ytterligare ett sätt att dra nytta av en skyddad anläggning är att använda den till lagring och backup som på det hela taget är mindre energiintensivt. Energiintensiva servertjänster med högre krav på tillgänglighet kan huvudsakligen hanteras i säkra byggnader. På så sätt ges samhällsviktiga it-tjänster hög kapacitet när det gäller tillgänglighet och god säkerhet i daglig drift medan den samlade datamängden regelbundet säkerhetskopieras till en skyddad anläggning. I detta koncept kommer vid oönskade händelser visserligen säkerhetskopierad data i en skyddad anläggning å ena sidan vara otillgänglig under den tid det tar att återläsa till en annan säker

byggnad i drift, men å andra sidan ha god riktighet i bemärkelsen att data inte går förlorad och därmed är möjlig att återställa.

Skyddad anläggning och säker byggnad - en fördelaktig kombination

Dimensionerande nyttoeffekt och behovet av antalet skyddade anläggningar bör utredas djupare ur ett strategiskt perspektiv. Men som ett avslutande exempel nedan kan ett samlat nationellt effektbehov om strax över 20 MW (effektåtgång för ungefär 9000 villor) uppnås genom en fördelning på 15 stycken byggnader samt skyddade anläggningar (nyetablering respektive ombyggda bergrum) fördelade i hela landet:

En konceptuell etablering av ett regionalt datacenterkluster skulle kunna fördelas som:

- två säkra byggnader om två MW effekt vardera (nyetablering)
- en skyddad anläggning om en halv MW effekt (ombyggnad av befintlig berganläggning som inte är i drift).

Fem sådana regionala datacenterkluster fördelade över landet skulle då innebära totalt:

- tio säkra byggnader om två MW vardera (nyetablering)
- fem skyddade anläggningar om en halv MW vardera (ombyggnad av befintliga berg-anläggningar som inte är i drift).

Det är som tidigare nämnt värt att notera den relativt långa anskaffningstiden för ett datacenterkoncept. Tidskritiska parametrar som påverkar produktions-tiden för en ny säker byggnad är bland annat mark-anskaffning, miljöprövning och säkerhetsskyddad upphandling av entreprenörer.

Anskaffningstiden för en säker byggnad uppskattas vara omkring två år. En ombyggnad av ett fortifikatoriskt skyddat bergrum bedöms ligga på fyra till fem år. Uppförandet av flera regionala datacenterkluster kan utföras efter hand eller samtidigt. Det är dock rimligt att anta att behovet av den fulla kapaciteten inte inträffar i det korta perspektivet och att det därmed inte finns behov av att utföra hela konceptet parallellt. Det finns även en logik i att ta tillvara erfarenheter från initiala uppföranden innan för stora steg tas. Det är därför skäligt att anta att en total anskaffningstid kan ta cirka tio år.

Sammantaget kan ett tänkbart datacenterkoncept som beskrivs i exemplet ovan erbjuda hög tillgänglighet och redundans till en rimligare kostnad än om alla it-utrymmen består av nyproducerande fortifikatoriskt utformade berganläggingar. Även om tillgängligheten påverkas för samhällsviktiga och säkerhetskritiska it-tjänster i datacenterkonceptet, ger det en god säkerhet både när det gäller fysiska perspektiv och riktighet i bemärkelsen att data inte går förlorat även under stora påfrestningar. Den uppskattade anskaffningstiden på cirka tio år förutsätter dock att nödvändiga strategiska delar är avklarade som kravställning, finansiering och organisation. Det gör att beslutsfattare bör höja medvetenheten kring behov och utmaningar förenade med nationell samordning av skyddade it-tjänster, så att processen kan påbörjas. För Sveriges totalförsvar är det en viktig och nödvändig investering för framtiden.

För vidare läsning

Fortifikationsverket, Förstudie av skyddade it-utrymmen för offentliga aktörer inom samhällsviktig verksamhet – Delrapport, 2018, Dnr 727/2017-22.

Fortifikationsverket, Förstudie av skyddade it-utrymmen för offentliga aktörer inom samhällsviktig verksamhet – Ett statligt datacenterkoncept, 2018, Dnr 727/2017-29.

Fortifikationsverket, Handbok Skydd av byggnader, 2017, Utgåva 4.

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Telefon: +46 8 5550 3000
www.foi.se