ROS-ISÄK
Helena Andersson

helena.andersson@msbmyndigheten.se

Konsekvensutredning för föreskrift om krav på informationssäkerhet

1. Beskrivning av problemet och vad man vill uppnå

Hot och risker som kan relateras till IT och informationsbehandling i allmänhet är oförutsägbara och föränderliga. Det beror inte minst på en mycket snabb teknisk utveckling där många gånger ofullgångna tekniska lösningar snabbt vinner gehör i en organisations önskan att effektivisera och modernisera. Ett säkerhetsarbete måste därför i huvudsak vara framåtsyftande och långsiktigt även om det naturligtvis också måste innehålla åtgärder som inriktas på att hantera en inträffad incident eller allvarlig kris. Ett väl genomfört informationssäkerhetsarbete kan ses som en försäkring mot oförutsedda och oönskade händelser som kan åsamka en verksamhet eller intressent skada av mer eller mindre allvarlig karaktär.

Ledningssystem för informationssäkerhet (LIS) beskriver en process för informationssäkerhetsarbete som består av policy, regler, förslag till skyddsåtgärder och procedurer . LIS utgår ifrån att det är nödvändigt med en helhetssyn på informationssäkerhet som täcker in alla delar. Skälet till det är att man inte kan åstadkomma god säkerhet utan tydliga regler, personella resurser, tekniska skyddsåtgärder, administrativa rutiner och uppföljning som leder till förbättringsåtgärder, d.v.s. samma komponenter som krävs i vilket annat kvalitetsarbete som helst. Det finns ofta en övertro på tekniska skyddsåtgärder som är viktig att uppmärksamma.

LIS helhetssyn hindrar inte att man tar till sig dess arbetssätt successivt och i en takt som kan avpassas till verksamhetens möjligheter. LIS ger genom sin syn på värdering av informationstillgångar, bedömning av hot och risker en ändamålsenlig beslutsmodell för vilka skyddsåtgärder som bör vidtas och med vilken prioritering de bör införas. Den ger därmed en metod för bedömning av en myndighets egna behov av åtgärder. Därmed kan också ett kostnads- och intäktsresonemang vara en del av beslutsunderlaget för de

åtgärder som är lämpliga att vidta med hänsyn till de risker man önskar reducera, eliminera eller acceptera. Genom sin syn på att informationssäkerhetsarbete skall bedrivas i enlighet med en organisations identifierade behov ger LIS också stor frihet att bedöma vilken nivå av säkerhet som är relevant. Det innebär att man kan välja att ta större eller mindre risker med hänsyn till verksamhetens möjligheter.

De flesta myndigheter hanterar sina informationssäkerhetsfrågor på något sätt. Eftersom det inte finns någon ”rikslikare” är det svårt att få en bra uppfattning om kvaliteten på detta arbete. Många undersökningar som gjorts av offentliga och privata organisationers informationssäkerhet har visat på uppenbara brister. Inte minst när det gäller styrningsfrågor.

I syfte att stärka statliga myndigheters arbete med informationssäkerhet fattade Verva i november 2007 beslut om föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte, VERVAFS 2007:2, och gav samtidigt ut allmänna råd, VERVAFS 2007:2AR, till föreskriften. Genom beslutet föreskrivs att myndigheterna från och med år 2008 i sitt arbete för ett säkert elektroniskt informationsutbyte ska tillämpa ledningssystem för informationssäkerhet enligt standarden SS-ISO/IEC 27001:2006 och riktlinjer för styrning av informationssäkerhet enligt standarden SS-ISO/IEC 27002:2005.

Verva lades ned den 31 december 2008 vilket av vissa uppfattades som att även kraven på ett systematiskt informationssäkerhetsarbete enligt LIS upphörde. VERVAFS 2007:2 gäller dock fortfarande och har för närvarande Regeringskansliet som huvudman.

MSB bildades den 1 januari 2009 och erhöll både föreskriftsrätt inom informationssäkerhetsområdet och en utpekad uppgift att stödja och samordna samhällets informationssäkerhet. Föreskriftsrätten, som har sitt stöd i 34 § förordningen (2006:942) om krisberedskap och höjd beredskap, utformades bland annat i syfte att MSB skulle ersätta VERVAFS 2007:2 med egna föreskrifter. För att betona betydelsen av fortsatt fokus på informationssäkerhet samt tydliggöra MSB:s stödjande roll på informationssäkerhetsområdet är det av stor betydelse att så snart som möjligt ersätta Vervas föreskrifter med motsvarande föreskrifter från MSB. För att samtidigt säkerställa att det påbörjade och ändamålsenliga informationssäkerhetsarbetet med LIS fortgår och därmed signalera kontinuitet och långsiktighet är de av MSB föreslagna föreskrifterna i stor utsträckning likalydande med VERVSFS 2007:2.

2. Beskrivning av alternativa lösningar för det man vill uppnå och vilka effekterna blir om någon reglering inte kommer till stånd

Med hänsyn till den informationsmängd som myndigheter hanterar är det enligt MSB av stor betydelse att skapa förutsättningar för att myndigheternas informationssystem uppfyller sådana säkerhetskrav att verksamheten kan utföras på ett tillfredsställande sätt.

Idag finns föreskrifter utfärdade av Verva som reglerar statliga myndigheters arbete med informationssäkerhet och MSB har som målsättning att dessa ska ersättas med i stort sett likalydande föreskrifter från MSB.

De alternativa lösningar som finns att tillgå är att:

- Låta Vervas föreskrifter fortsätta att gälla, MSB utfärdar inte några motsvarande föreskrifter.
- Låta Vervas föreskrifter upphöra, MSB utfärdar inte några motsvarande föreskrifter.
- Låta Vervas föreskrifter upphöra, MSB utfärdar föreskrifter med samma syfte men som inte föreskriver tillämpning av LIS.

I november 2008 publicerade Verva en sammanställning och analys av myndigheters arbete inom e-förvaltning i rapporten ”69 myndigheter redovisar 915 strategiska insatser för utveckling av e-förvaltning” 2008:14. Med anledning av de nyinförda kraven på myndigheter i VERVAFS 2007:2 ägnades i ett kapitel särskild uppmärksamhet åt myndigheters arbete med informationssäkerhet och införande av ledningssystem för informationssäkerhet.

I rapporten drog Verva slutsatsen att myndigheterna behöver ytterligare stöd och påtryckningar för att fokusera och implementera ett verksamhetsintegrerat LIS. Det gäller troligtvis inte minst de 24 myndigheter som inte inrapporterade några vidtagna åtgärder inom informationssäkerhetsområdet.

Verva lades ned den 31 december 2008 och har inte längre möjlighet att trycka på eller ge stöd till myndigheterna i deras arbete med informationssäkerhet. Med hänsyn till detta är det mindre ändamålsenligt att låta Vervas föreskrifter fortsätta gälla i obestämd framtid. Informationssäkerhetsarbetet främjas av tydlighet vad gäller olika aktörers roller och MSB har fått till uppgift att stödja och samordna samhällets informationssäkerhetsarbete samt att ge ut föreskrifter på området. MSB kan bedriva ett betydligt mer ändamålsenligt arbete för att stödja samhällets informationssäkerhet när myndigheten får möjlighet att forma både föreskrifter och annat stöd till en fungerande helhet.

Vervas föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte och det allmänna råd som är kopplat till den har varit ikraft sedan den 1 januari 2008. Föreskriften ålägger statliga myndigheter att

deras informationssäkerhetsarbete ska bedrivas i former enligt etablerade svenska standarder för informationssäkerhet. Föreskriften anger också ett antal grundläggande krav som ska vara uppfyllda. Myndigheterna ska tillämpa ett ledningssystem för styrning av sitt informationssäkerhetsarbete och till detta är kopplat ett antal grundkrav. En viktig grund är att åtgärder baseras på risk- och sårbarhetsanalyser tillsammans med resultatet av arbete med incidenthantering.

Syftet med föreskriften var att i förvaltningen skapa förutsättningar för ett säkert och förtroendefullt elektroniskt informationsutbyte genom att myndigheterna bedriver sin verksamhet med den säkerhet som är nödvändig med hänsyn till den enskilda myndighetens förutsättningar.

För att få underlag till rapporten om myndigheters arbete med e-förvaltning skickade Verva ut en enkät där dessa bland annat ombads redovisa åtgärder som gjordes eller planerades med anledning av införande av LIS. Relevanta åtgärder innefattade exempelvis att upprätta en informationssäkerhetspolicy, utse ansvariga för säkerhetsarbetet eller att utföra risk- och sårbarhetsanalyser. Myndigheterna ombads också redovisa åtgärder som innebar att ta fram underlag för att kunna redovisa för myndighetsledningen hur arbetet fortskrider, att upprätta styrande dokument som berör informationssäkerheten eller att ta fram andra rutiner för myndighetens arbete med informationssäkerhet.

Ett positivt resultat av uppföljningen var att de inrapporterande myndigheterna över lag tycktes ha kommit igång väl med sitt informationssäkerhetsarbete. Vervas föreskrifter verkar på så sätt ha haft en positiv igångsättningseffekt. Några goda exempel på myndigheter som tagit ett rejält grepp om arbetet med ledningssystem för informationssäkerhet finns också. Valmyndigheten, CSN och Sveriges geologiska undersökningar (SGU) nämnde att de certifierats eller verkar för att erhålla certifiering inom informationssäkerhetsområdet.

De inrapporterade åtgärderna hade dock ett relativt starkt IT-fokus. Informationssäkerhetsarbetet innefattar ett bredare perspektiv på informationssäkerhet
än det som omfattas av IT-området. Detta snäva perspektiv kan i sin tur ha sin
grund i bristande kunskap om informationssäkerhet hos myndigheterna och/eller bero på en bristande förståelse för informationssäkerhetsarbetets nytta och relevans i utförandet av myndighetens kärnuppgifter. Informationssäkerhetsarbetet skulle därmed gynnas av ett bredare perspektiv.

Verva konstaterade i rapporten att myndigheterna inrapporterar få åtgärder eller insatser där det framgår att en längre tids fokusering på

informationssäkerhetsarbete pågått. Det saknas därmed beskrivningar som vittnar om en mer komplett och genomarbetad struktur för hantering av informationssäkerhetsfrågor. Anledningen kan delvis ligga i enkätens form som uppmuntrade till kortfattade svar. Med kännedom från andra projekt inom Verva blev dock slutsatsen snarare att många myndigheters informationssäkerhetsarbete fortfarande var i sin linda. Verva konstaterade att det på sikt var viktigt att säkerställa att myndigheterna etablerar strukturer för, och inte minst implementerar, ett verksamhetsintegrerat informationssäkerhetsarbete. Ledningens stöd och engagemang för informationssäkerhetsfrågorna lyftes fram som avgörande för myndighetens prioritering av frågorna och framgång i arbetet.

Fråga är på vilket sätt MSB ska agera när Vervas föreskrifter upphävs. Är det nödvändigt att MSB utfärdar egna motsvarande föreskrifter som planerats eller är det tillräckligt med annan typ av stöd? Som framgår ovan har Vervas föreskrifter haft en stor betydelse för myndigheternas informationssäkerhetsarbete. På samma sätt som Verva gör MSB bedömningen att när alla myndigheter tilllämpar ett ledningssystem för informationssäkerhet i enlighet med etablerade standarder ökar förutsättningarna för att åstadkomma och behålla nödvändig och ändamålsenlig informationssäkerhet i verksamheten. För att säkerställa att det påbörjade och ändamålsenliga informationssäkerhetsarbetet med LIS fortgår är det inte bara viktigt med stöd i form av vägledning, modeller och metoder. Vervas rapport ger även stöd för slutsatsen att uttryckliga krav i föreskriftsform på att införa LIS i många fall är en förutsättning för att arbetet med uppgiften påbörjas. MSB bör därför utfärda föreskrifter på området. För att signalera kontinuitet och långsiktighet är det dessutom av vikt att de föreslagna föreskrifterna så långt som möjligt är likalydande med VERVSFS 2007:2.

Vad gäller myndigheternas behov av olika typer av stöd för sitt arbete med LIS så ägnar MSB detta särskild uppmärksamhet och arbete pågår redan med att ta fram sådant stöd.

3. Uppgifter om vilka som berörs av regleringen

Föreskriften riktar sig till statliga myndigheter under regeringen, med undantag av Regeringskansliet, kommittéväsendet och Försvarsmakten.

4. Uppgifter om kostnadsmässiga och andra konsekvenser regleringen medför och en jämförelse av konsekvenserna för de övervägda regleringsalternativen

Att på något normerande sätt ange hur stor del av en verksamhets kostnader som bör läggas på säkerhet är svårt att göra. Varje organisation har på något

sätt en unik situation när det gäller verksamhet, geografisk och fysisk placering av lokaler, förhållanden till omvärlden m.m.

IT ger som den kanske viktigaste delen av produktionstekniken, åtminstone i mera administrativa organisationer som t.ex. myndigheter, i sig en relativt hög kostnad. En kostnad som ändå vanligen är acceptabel från ett effektivitets- och service-perspektiv. I denna kostnad ingår normalt kostnader för säkerhetsåtgärder. I första hand kanske tekniska skyddsåtgärder men också administrativa kostnader för kringrutiner och förvaltning av tekniken.

Som vanligt utgörs en stor del av kostnadsmassan av personella resurser. Ledningen måste ägna sig åt säkerhetsfrågor om än under begränsad tid. Något mera tid måste avsättas för personal som är särskilt utsedd att samordna och leda säkerhetsarbete mera direkt. Naturligtvis behövs även personal som handlägger behörighetsadministration, övervakar brandväggar, uppdaterar virusskydd, följer upp säkerheten, utbildning, etc.

De åtgärder som LIS anger kan sägas vara av ”best-practice”-karaktär eller ”hygien”-åtgärder som de flesta organisationer med IT-verksamhet rimligen redan borde tillämpa. Tillkommande kostnader handlar därför snarare om kostnader som redan borde ha uppstått eftersom åtgärder rimligen borde vara vidtagna. Ett bristfälligt eller dåligt styrt säkerhetsarbete genererar sannolikt avsevärt högre kostnader än vad som är nödvändigt med hänsyn till behoven.

En kostnadspost som det finns anledning att kommentera är för certifiering mot standarden. Certifiering av ett oberoende revisionsföretag kan kosta mellan 100 – 300 tkr beroende på verksamhetens storlek. Avsikten med föreskriften är dock inte att myndigheter måste certifiera sig varför man i detta resonemang kan bortse från den kostnaden.

Det är minst lika svårt att bedöma intäkter av informationssäkerhetsarbete som det är att bedöma relevanta kostnader. En vanlig modell är att bedöma minskade skadekostnader som resultat av skyddsåtgärder. Negativa effekter av incidenter av olika slag, rättsförluster, störningar i verksamheten, obehörig åtkomst, skada för tredje man etc. kan i många fall bedömas kostnadsmässigt. Det innebär också att man kan bedöma minskade kostnader och se dessa som en intäkt av planerade eller vidtagna skyddsåtgärder.

Ett väl genomfört informationssäkerhetsarbete kan innebära minskade kostnader. Det finns exempel på att organisationer efter riskanalys och skyddsnivåklassificering funnit att man tillämpat skyddsåtgärder som inte varit relevanta eller helt verkningslösa när det gäller de hot som identifierats, med möjlighet till besparingar som följd. En positiv effekt av

ett informationssäkerhetsarbete som följer former som delas av många organisationer är möjligheten till mätbarhet och därmed också jämförelser med andra liknande verksamheter. De organisationer inom offentlig och privat sektor som har erfarenhet av informationssäkerhetsarbete med LIS som grund ger inte uttryck för att säkerhetsarbetet kostar för mycket i förhållande till nyttan.

En allmänt accepterad uppfattning inom de flesta verksamhetsområden är att god styrning är en förutsättning för att nå uppställda mål. Vi talar om ekonomistyrning, kvalitetsstyrning, projektstyrning etc. Det finns inget skäl att tro att samma förhållande inte skulle gälla i fallet informationssäkerhetsarbete.

Ett informationssäkerhetsarbete enligt LIS innebär normalt inte högre kostnader än om säkerhetsarbetet sker enligt andra principer. Troligen gäller det motsatta förhållandet, lägre kostnader, eftersom arbetet sker strukturerat och systematiskt. Man får också förbättrade möjligheter att skapa ökad kontroll och nyttoeffekt genom styrning och samsyn. Detta skapar också nödvändiga förutsättningar för trovärdighet och tillit i förhållande till vår omvärld. Effekten av och omvärldens dom i händelse av en allvarlig incident mildras troligen högst väsentligt om man följt vedertagen praxis.

5. Bedömning av om regleringen överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen

Europeiska unionens råd har i sin resolution av den 28 januari 2002 om en gemensam inställning och särskilda åtgärder på området för nät- och informationssäkerhet identifierat ISO/IEC 17799, d v s LIS, som en erkänd metod för säkerhetshantering i privata och offentliga organisationer. I resolutionen uppmanar Rådet medlemsstaterna att främja goda rutiner för hantering av informationssäkerhet baserat på internationellt erkända standarder när så är lämpligt. Enligt vår uppfattning är föreskriften ett viktigt steg mot att på rekommenderat sätt främja goda rutiner för informationssäkerhetsarbete och sålunda väl i överensstämmelse med det europeiska regelverket.

6. Bedömning av om särskilda hänsyn behöver tas när det gäller tidpunkten för ikraftträdande och om det finns behov av speciella informationsinsatser

Genom att MSB:s föreskrifter syftar till att ersätta Vervas motsvarande föreskrifter och då de båda föreskriftstexterna innehållsmässigt i stort sett stämmer överens spelar den exakta tidpunkten för MSB föreskriftens ikraftträdande begränsad roll. Det är dock viktigt att Vervas föreskrift upphävs i direkt anslutning till ikraftträdandet av MSB:s föreskrift för att

både signalera kontinuitet (genom att undvika en oreglerad period) samt undvika en situation med dubbelreglering. Vad gäller informationsinsatser kommer MSB att i anslutning till ikraftträdandet använda flera kanaler för att uppmärksamma myndigheterna på de nyutkomna föreskrifterna. MSB kommer även att dela ut ett exemplar av den tillämpliga standarden till varje myndighet.

7. Miljö- och hälsokonsekvenser

Föreskriften bedöms inte innebära några direkta konsekvenser för miljö och hälsa. Däremot underlättar väl fungerande och säker informationshantering inom miljö- och hälsoområdet arbetet med dessa frågor.

8. Kontaktperson

Helena Andersson
010-240 4133
Helena.andersson@msbmyndigheten.se