Vid korrespondens åberopa
FOI beteckning

Datum
2015-09-14

Nr
FOI-2015-887

Justitiedepartementet
103 33 Stockholm

Er referens
Linda Ericson
Ju2015/2659/SSK

Vår handläggare
Magnus Sparf

Remissvar avseende betänkandet SOU 2015:23 Informations- och cybersäkerhet i Sverige - Strategi och åtgärder för säker information i staten

Sammanfattning

FOI bejakar betänkandets förslag kring en nationell styrmodell för informationssäkerhet. Myndigheter har idag olika interna regelverk för klassificering och hantering av information. Detta är i sig en säkerhetsrisk vid utbyte och delning av sekretessklassad information mellan myndigheter.

FOI menar således att det för rikets säkerhet är viktigt med gemensamma principer och gemensamt regelverk för klassificering av information samt gemensamma hanteringsregler och krav på säkerhetsfunktioner på de informationssystem som ska hantera informationen i syfte att underlätta för statliga myndigheter att utbyta skyddsvärd information.

FOI vill lyfta upp att den föreslagna strategin inte omhändertar behovet av forskning, utveckling och kompetensförsörjning i ett område som är kunskapsintensivt och under ständig utveckling. FOI menar att detta bör utredas vidare.

Inledning

FOI ställer sig överlag positivt till betänkandet och att områdets betydelse lyfts eftersom informationssäkerhet får anses vara en allt viktigare fråga för samhället som helhet. Området utvecklas fort och är som forskningsområde fortfarande i sin linda.

FOI menar att *avsnittet Behov av en strategi för staten (s. 15-16)* skulle behövts förtydligas. Skrivningen kan tolkas som att det inte är någon mening med att arbeta med strategier för kompetensförsörjning eller arbeta med forskning och utveckling innan de mest angelägna bristerna i statsförvaltningen har åtgärdats. Betänkandet har således gjort en avgränsning och gett förslag på en strategi som inte omhändertar behov av forskning, utveckling och kompetensförsörjning i ett område som är kunskapsintensivt och under ständig utveckling. För de statliga myndigheterna krävs kompetent personal och aktuell kunskap för att hantera komplexiteten, dynamiken och hotbilden inom området. Forskning och utveckling behövs för att möta den ständiga utveckling som sker inom it-området.

FOI
Totalförsvarets forskningsinstitut

Postadress	Besöksadress	Telefon	Fax	registrator@foi.se
FOI 164 90 STOCKHOLM	Gullfossgatan 6, Kista Leveransadress Gullfossgatan 12, Kista	08-5550 3000	08-5550 3100	Orgnr: 202100-5182 www.foi.se

FOI

Datum
2015-09-14

Nr
FOI-2015-887

FOIs uppfattning är att det arbete som pågår ska fortsätta samt att arbete med andra strategier bör kunna igångsättas parallellt samtidigt som de mest angelägna bristerna i statsförvaltningen åtgärdas. FOI menar att synergier till *SOU 2015:25 En ny säkerhetsskyddslag* är påtaglig och att den sammanvägda konsekvensen inklusive myndigheters tillsyns- och ansvarsförhållanden bör utredas vidare.

FOI har sedan lång tid stor kompetens inom informationssäkerhetsområdet och har uppdrag från såväl civila som militära myndigheter gällande forskning, expertstöd och kompetenshöjande åtgärder inom området.

FOI ser samordningsmöjligheter avseende de statliga myndigheternas behov av forskning och utveckling inom området. Flera av de myndigheter som har särskilda uppgifter har ett gemensamt behov av metod- och kunskapsutveckling inom ett antal delområden. Exempel på sådana områden är it-forensik, analys av skadlig kod, riskanalys, samt sårbarhetsanalys. Under avsnittet *Förebyggande och bekämpande av it-relaterad brottslighet stärks (s.19)* finns det till exempel inget om hur den metodmässiga och tekniska förmågan, inom exempelvis it-forensik, ska stärkas. En tänkbar lösning på detta är att ett kompetenscentrum etableras. Inom it-forensik skulle detta till exempel kunna bestå av Nationellt Forensiskt Centrum och FOI som i samverkan stödjer andra myndigheter med expertstöd.

FOI anser att det bör utredas hur de operativa myndigheternas, med särskilda uppgifter inom informationssäkerhet, gemensamma behov av forskning, metod- och teknikutveckling ska omhändertas på ett för staten ändamålsenligt och kostnadseffektivt sätt.

FOI lämnar i särskild bilaga ytterligare förtydliganden och synpunkter på betänkandet.

Detta remissvar har beslutats av undertecknad stf generaldirektör Anna-Lena Österborg efter föredragning av forskningsledare Magnus Sparf. I den slutliga beredningen har jurist Thomas Wallander deltagit.

Anna-Lena Österborg
Stf generaldirektör

Magnus Sparf

Bilaga: Förtydliganden och synpunkter

FOI

Datum
2015-09-14

Nr
FOI-2015-887
Bilaga

Förtydliganden och synpunkter

Förtydligandena och synpunkterna följer den ordning som framgår av betänkandet

Författningsförslag (s.27-33)

Avsnittet *Myndighetens informationssäkerhetsarbete (s. 28-29)* ger intryck av att vara inriktat på information som hanteras av administrativa system.

FOI ser ett behov av att även de krav som bör ställas på andra typer av system, såsom inbyggda system och industriella informations- och styrsystem, fastighetsautomation och larmsystem, tydliggörs. Vidare bör i detta sammanhang även systemens funktioner beaktas.

I *7 § (s. 29)* anges att "*Myndigheten ska kartlägga sina informationsprocesser och klassificera sin information ...*"

FOI anser att det bör övervägas att byta informationsprocesser till verksamhetsprocesser, dvs. ta ett helhetsgrepp om verksamheten med dess ingående information och analysera vad som kan gå snett i verksamheten när information eller it-tjänster går ner eller infiltreras.

I avsnittet *Myndighetens informationssäkerhetsarbete (s. 29)* är det oklart vad som avses med säkra it-produkter.

FOI anser att det finns få produkter som är säkra i bemärkelsen att inget kan gå fel med dem och säkerhet kan sällan garanteras med enbart tekniska lösningar. Stycket bör omformuleras så att det inte förefaller vara så att så kallade säkra it-produkter skulle kunna lösa säkerhetsutmaningar. Istället bör det tydligt framgå att endast de it-produkter som tillsammans med nödvändiga rutiner och processer uppfyller ställda informationssäkerhetskrav ska användas. Detta bör också gälla alla system och inte endast de som hanterar "*information där bristande informationssäkerhet kan medföra en betydande försämring av myndighetens förmåga att bedriva sin verksamhet*".

Begreppet *säkra it-produkter* används på några ställen i hela betänkandet och i förslaget till ny förordning. FOI anser att en omformulering till it-produkter som uppfyller tillämpliga säkerhetskrav eller liknande bör övervägas. Endast i *Bilaga 4 (s. 306)* fyller termen säkra it-produkter sin funktion. Där framgår det också att detta är närmast en utopi när det kommer till generella it-produkter. Erfarenhet visar att sårbarheter är sannolika i implementation av generella it-produkter som saknar tydliga och snäva begräsningar i sitt användningsområde.

FOI vill framhålla att i avsnittet *Upphandling och utveckling av it-system och it-produkter (s. 31)* finns det risk att tolkningen blir att informationsklassificering och riskanalys bara ska ske med avseende på sekretess/konfidentialitet och att det missas avseende riktighet, tillgänglighet och spårbarhet. I tidigare utredningar har riktighet, tillgänglighet och spårbarhet delvis glömts bort eller hamnat i skuggan av sekretess. I *SOU 2015:25 En ny säkerhetsskyddslag avsnitt 16.1 (s. 344)* beskrivs distinktionen på ett utmärkt sätt och bör samordnas med skrivningar i förslaget till förordning.

FOI

Datum
2015-09-14

Nr
FOI-2015-887
Bilaga

FOI anser att avsnittet *It-incidentrapportering 17 § (s. 32)* är otydlig med var gränsen går för vad man ska rapportera. Med skrivningen "*rapportera it-incidenter som allvarligt kan påverka säkerheten...*" undantas till exempel incidenter som redan inträffat och orsakat skada eftersom dessa inte längre kan påverka säkerheten. Det går även att resonera så att de angreppsförsök som upptäckts och hanterats de facto inte kunde påverka säkerheten. Historiska incidenter är av värde vid analyser av trender och liknande. Dessutom är även hejdade angrepp av alla typer potentiellt värde att rapportera. Man kan mycket väl tänka sig att samma skadliga kod kan användas mot flera myndigheter men att framgången för angriparen och konsekvenser blir olika för respektive myndighet. Ett misslyckat och upptäckt försök till intrång i en inte skyddsvärd del av en myndighets informationssystem kan således vara relevant att rapportera eftersom samma angrepp kan leda till allvarliga konsekvenser om det görs mot en annan myndighet. Först då information om både misslyckade och lyckade it-incidenter kan aggregeras av i detta fall MSB kan mönster ses och varningar och förslag på åtgärder kan ges som då kan ge myndigheter som inte upptäckt något en möjlighet att upptäcka den skadliga koden.

Informationssäkerhet och cybersäkerhet (avsnitt 2.4.3)

I avsnittet ges tveksamma definitioner av informationssäkerhet. För tillgänglighet räcker det inte att informationen finns den måste också vara möjlig att komma åt. I *SOU 2015:25 En ny säkerhetsskyddslag avsnitt 16.1 (s. 345)* definieras informationssäkerhet på ett utmärkt sätt och skrivningarna bör samordnas.

Strategins innehåll (avsnitt 9.1.4)

Ur *avsnitt 9.1.4 Strategins innehåll* och i samband med *strategins första mål* samt i förslag till förordning 5 § går det att läsa texten som att man vill att de statliga myndigheterna ska införa egna ledningssystem för informationssäkerhet.

Här finns det redan en stor kunskap och erfarenhet bland statliga myndigheter som bör tas tillvara innan man på bredd tar sig an att driva på och införa ett ledningssystem för informationssäkerhet. Lämpligen bör denna erfarenhet utredas vidare som ett stöd för ett bredare införande i statsförvaltningen.

Kravställning vid upphandling (avsnitt 9.3.1)

I *avsnitt 9.3.1 Kravställning vid upphandling (s. 236)* framgår "*MSB... anger minimikrav i vanligt förekommande it-produkter.*" vilket bör förtydligas.

Menar man inte egentligen krav på vilka säkerhetsfunktioner som ska finnas i ett system, inte vilka specifika produkter (leverantörsknutna) som ska finnas eller hur de ska se ut?

En omformulering till "MSB… anger minimikrav avseende säkerhet i vanligt förekommande it-system…" eller liknande bör övervägas. Det är dock svårt att se vad detta innebär förutom redan etablerad kunskap såsom användning av anti-virus, krypterade hårddiskar på bärbara datorer med mera om man inte går längre mot riktigt nedlåsta system där användbarheten påverkas. Förslaget verkar vila på ett antagande om att det finns krav som särskiljer statligt använda it-produkter från produkter som används till liknande saker inom kommuner och företag med mera. Det framgår dock inte vad detta antagande baseras på eller vad dessa särskilda krav är.

FOI

Datum
2015-09-14

Nr
FOI-2015-887
Bilaga

I det fortsatta arbetet bör det tas hänsyn till att Försvarsmakten redan har utvecklat standardiserade krav på it-system som skall hantera olika typer av information – de så kallade ”Krav på säkerhetsfunktioner”.

I *avsnitt 9.3.1 Kravställning vid upphandling (s. 237) It-standarder och krav på certifiering* nämns även "nationellt godkända system".

Uttrycket behöver förtydligas då det i resterande del av texten får det att låta som om Sverige tar fram egna nationella system som inte bygger på COTS. Det låter kostsamt. Dessutom verkar det som om man vill att leverantörerna ska utforma speciella produkter åt Sverige, vilket också låter kostsamt.

Av samma avsnitt framgår en övertro på certifiering som sätt att lösa statens behov av it-system. Det finns flera kritiska rapporter om certifiering som ansats som bör tas hänsyn till i det fortsatta arbetet enligt betänkandet, till exempel artikeln Certification and Evaluation: A Security Economics Perspective, 2009, Anderson, R. and Fuloria, S:

> ”The Common criteria have not worked particularly well, whether in their original role of certifying secure computer systems for government purchasers or in their new role of providing some assurance for products on which third parties have to rely”

I *avsnitt 9.3.1 Kravställning vid upphandling (s. 240) Koncentration av leverantörer* går att tolka som att koncentrering av drifttjänster är negativt vilket är lite motsats till tidigare skrivningar om att standardisering är positivt som således också bör vara negativt.

För att undvika att vi använder samma produkter och leverantörer inom olika myndigheter ska det enligt betänkandet rapporteras till MSB vilka it-lösningar som valts i ramavtal. Problembeskrivningen i avsnittet tar dock sin utgångspunkt i *driftstjänster* och föreslår sedan att *it-lösningar* ska rapporteras där det förra (drifttjänster) är mer avgränsat än det senare (it-lösningar) och det bör utredas vidare vad som menas med it-lösningar och då eventuellt på det utreda vidare vad nyttan relativt kostnaden och risken är att alla myndigheter ska rapportera deras val av it-lösningar till ett och samma ställe.

Statliga nätverk (avsnitt 9.4.1)

I *avsnitt 9.4.1 Statliga nätverk* finns en skarp formulering som verkar uttala sig om säkerheten på ett mycket negativt sätt: "*Merparten av myndigheternas informationshantering sker i dag via publika system. Stora delar av den information som hanteras, såväl i form av datatrafik som tal, är skyddsvärd. Den publika infrastrukturen som används omfattas inte av något kontrollerat eller dimensionerat säkerhetsskydd.*"

Det är inte tydligt vilken empiri som ligger till grund för påståendena att säkerheten i publika system inte kan erbjuda ett dimensionerat säkerhetsskydd och att en stor del av den information som hanteras i dessa system är skyddsvärd. Idag och framtiden bedöms dessutom myndigheter behöva kommunicera med publika aktörer över publika system och om det finns grund i påstående bör det förtydligas eller utredas vidare.