LÄKEMEDELSVERKET
MEDICAL PRODUCTS AGENCY

Yttrande

Robert Reineck
Säkerhetsansvarig
Telefon: 018-17 42 93

Datum: 2015-09-09 Dnr: Dnr 3.4-2015-040639

registrator@regeringskansliet.se

Yttrande över remissen om Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten (Dnr 3.4-2015-040639)

Sammanfattning

Läkemedelsverket är generellt positivt till förslagen och ambitionen att förbättra informationssäkerheten i Sverige, till nytta för samhället.

En tydligare kravställning på myndigheter och ett tydligare ansvar i myndighetens ledning för kontroll och uppföljning av informationssäkerhet är välkommet.

Författningsarbetet inom områdena säkerhetsskydd, krisberedskap och informationssäkerhet skulle vinna på en större samordning då områdena går i varandra och till stora delar använder samma termer och begrepp.

Att utredningens omfattning begränsats och inte inbegriper landsting, kommun och privata aktörer kan medföra att effekten av förslagna åtgärder i vissa fall uteblir då beroendena mellan dessa aktörer och myndigheter är omfattande med avseende på informationshantering och informationssäkerhet. Ett exempel på avsaknad av samordning på detta område är att utredningen "Nästa fas i e-hälsoarbetet" SOU 2015:32 föreslår en central roll för e-Hälsomyndigheten avseende rådgivning och stöd inom informationssäkerhet vilket inte framgår av utredningen Informations- och cybersäkerhet i Sverige.

Vi efterlyser även en tydligare reglering av hur Regeringskansliet ska arbeta samordnat med informationssäkerhet, detta inte minst utifrån Riksrevisionens konstateranden i Informationssäkerheten i den civila statsförvaltningen (RiR 2014:23).

Övriga synpunkter

Utredningen bedömer att förslagen inte kommer medföra några ökade kostnader för myndigheterna vilket kan ifrågasättas då det trots allt handlar om en ambitionshöjning och ett ytterligare tryck på efterlevnad av gällande författning.

Att inte svensk standard för ledningssystem för informationssäkerhet lyfts fram tydligare är olyckligt då det i sig är en grund för en gemensam styrmodell, kravställning och nivå på informationssäkerheten

Angående förslaget om IT-incidentrapportering så ställer sig Läkemedelsverket positivit till principen. Dock behöver alternativa benämningar övervägas eller så måste det bli betydligt mer konkret vad som avses. Betydelsen av termen IT-incident varierar mycket mellan organisationer.

Det är inte definierat vad som avses med säkra IT-produkter. Att i föreskriften och med hänvisning till *betydande försämring* och *samhällsviktig verksamhet* kräva att dessa ska användas begränsar myndighetens egna valmöjligheter och ger ett alltför stort utrymme för tolkningar.

Att etablera en tillsynsmyndighet för informationssäkerhet är positivit. Dock bör MSB:s uppdrag och mandat tydligt definieras för att minimera risken för att intressekonflikter uppstår. Även Myndighetsrådets syfte och uppgifter är otydliga då de utgör en blandning av strategiskt och operativt stöd.

Arbetet med informationssäkerhet på en myndighet är starkt beroende av myndighetens struktur för intern styrning och kontroll. Utredningen saknar ett resonemang kring detta och om hur arbetet med informationssäkerhet relaterar till Ekonomistyrningsverkets uppdrag.

För att en ambitionshöjning ska kunna genomföras krävs ett utökat praktiskt stöd och samordning av modeller, metoder och lösningar inom offentlig sektor. Detta behov finns redan idag men kommer att öka ytterligare med utredningens förslag. Därför behöver ansvaret för detta ytterligare lyftas fram och kompletteras med nödvändiga resurser. Arbetet behöver även balanseras med avseende på vad som ska uttryckas som verkställighetsföreskrifter och vad som kan utgöra allmänna råd. Detta då modeller och metoder i nuläget varierar mellan myndigheterna beroende på olika förutsättningar samt att det krävs samordning och tid för att etablera ett gemensamt synsätt.

Enligt författningsförslaget 7 § anges att arbetet med informationssäkerhet ska föregås av en kartläggning av informationsprocesser. Detta borde formuleras som ett bör-krav och benämnas ”verksamhetsprocesser” eller ännu hellre hänvisa till arbetssätt enligt SS-ISO/IEC 27001:2014.

Att, som utredningen föreslår, ta fram gemensamma underlag och kravställningar för upphandling ser vi som mycket positivt då det annars kan vara resurskrävande för den enskilda myndigheten samtidigt som leverantörerna riskerar mötas av divergerande krav från olika myndigheter.

Enligt standarden SS-ISO/IEC 27001:2014 handlar informationssäkerhet om att bevara informationens konfidentialitet, riktighet och tillgänglighet. Spårbarhet bör ses som en konsekvens av krav på konfidentialitet, riktighet och tillgänglighet, men kan lyftas fram som ett viktigt perspektiv. Ytterligare exempel på begrepp som behöver förtydligas är, som tidigare nämnts, IT-incident.

Vi föreslår att begreppsanvändningen görs mer konsekvent och harmoniseras med svensk standard för att öka tydligheten.

Chefsjurist Joakim Brandberg har beslutat i detta ärende efter föredragning av säkerhetsansvarig Robert Reineck. I den slutliga handläggningen har också följande

personer deltagit: projektledare Ewa Palfelt, IT-säkerhetsarkitekt Magnus Josefsson, verksstrateg Lena Viklund samt gruppchef Linda Melkersson.

På Läkemedelsverkets vägnar

Joakim Brandberg

Robert Reineck